AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Western District of Texas - Waco Division on the following

☐ Trademarks or ☒ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:22-cv-01094	October 21, 2022	Western District of Texas - Waco Division

PLAINTIFF	DEFENDANT
Taasera Licensing LLC	CrowdStrike, Inc. and CrowdStrike Holdings, Inc.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	7,673,137	3/2/2010	Taasera Licensing LLC
2	8,327,441	12/4/2012	Taasera Licensing LLC
3	8,850,517	9/30/2014	Taasera Licensing LLC
4	8,955,038	2/10/2015	Taasera Licensing LLC
5	8,990,948	3/24/2015	Taasera Licensing LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 9,092,616	7/28/2015	Taasera Licensing LLC
2 9,608,997	3/28/2017	Taasera Licensing LLC
3 9,923,918	3/20/2018	Taasera Licensing LLC
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

AO 120 (Rev. 08/10)

TO:	Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00427	10/31/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	MUSARUBRA US LLC, D/B/A TRELLIX

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	7,673,137	3/2/2010	Taasera Licensing LLC
2	8,327,441	12/4/2012	Taasera Licensing LLC
3	8,850,517	9/30/2014	Taasera Licensing LLC
4	8,955,038	2/10/2015	Taasera Licensing LLC
5	8,990,948	3/24/2015	Taasera Licensing LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

IPR2023-01466
CrowdStrike EX1002 Page 2

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00427	10/31/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	MUSARUBRA US LLC, D/B/A TRELLIX

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	9,071,518	6/30/2015	Taasera Licensing LLC
2	9,092,616	7/28/2015	Taasera Licensing LLC
3	9,608,997	3/28/2017	Taasera Licensing LLC
4	9,923,918	3/20/2018	Taasera Licensing LLC
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

IPR2023-01466
CrowdStrike EX1002 Page 3

AO 120 (Rev. 08/10)

TO:	Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00415	10/21/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	FORTINET INC.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	8,327,441	12/4/2012	Taasera Licensing LLC
2	8,819,419	8/26/2014	Taasera Licensing LLC
3	8,955,038	2/10/2015	Taasera Licensing LLC
4	8,990,948	3/24/2015	Taasera Licensing LLC
5	9,092,616	7/28/2015	Taasera Licensing LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

IPR2023-01466
CrowdStrike EX1002 Page 4

AO 120 (Rev. 08/10)

TO:	Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00415	10/21/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	FORTINET INC.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	9,118,634	8/25/2015	Taasera Licensing LLC
2	9,608,997	3/28/2017	Taasera Licensing LLC
3	9,628,453	4/18/2017	Taasera Licensing LLC
4	9,860,251	1/2/2018	Taasera Licensing LLC
5	9,923,918	3/20/2018	Taasera Licensing LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

IPR2023-01466
CrowdStrike EX1002 Page 5

AMENDED

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00063	7/5/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	CHECK POINT SOFTWARE TECHNOLOGIES LTD.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	6,842,796	1/11/2005	Taasera Licensing LLC
2	8,327,441	12/4/2012	Taasera Licensing LLC
3	8,955,038	2/10/2015	Taasera Licensing LLC
4	8,990,948	3/24/2015	Taasera Licensing LLC
5	9,092,616	7/28/2015	Taasera Licensing LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

AMENDED

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00063	7/5/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	CHECK POINT SOFTWARE TECHNOLOGIES LTD.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	9,608,997	3/28/2017	Taasera Licensing LLC
2	9,923,918	3/20/2018	Taasera Licensing LLC
3	9,071,518	6/30/2015	Taasera Licensing LLC
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading		
	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1			
2			
3			
4			
5			

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

IPR2023-01466
CrowdStrike EX1002 Page 7

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00063	2/25/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	CHECK POINT SOFTWARE TECHNOLOGIES LTD.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	6,842,796	1/11/2005	Taasera Licensing LLC
2	8,327,441	12/4/2012	Taasera Licensing LLC
3	8,955,038	2/10/2015	Taasera Licensing LLC
4	8,990,948	3/24/2015	Taasera Licensing LLC
5	9,092,616	7/28/2015	Taasera Licensing LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00063	2/25/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	CHECK POINT SOFTWARE TECHNOLOGIES LTD.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	9,608,997	3/28/2017	Taasera Licensing LLC
2	9,923,918	3/20/2018	Taasera Licensing LLC
3			
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

IPR2023-01466
CrowdStrike EX1002 Page 9

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 **Director of the U.S. Patent and Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00062	2/25/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	PALO ALTO NETWORKS, INC.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	6,842,796	1/11/2005	Taasera Licensing LLC
2	7,673,137	3/2/2010	Taasera Licensing LLC
3	8,127,356	2/28/2012	Taasera Licensing LLC
4	8,327,441	12/4/2012	Taasera Licensing LLC
5	8,850,517	9/30/2014	Taasera Licensing LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

IPR2023-01466
CrowdStrike EX1002 Page 10

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 **Director of the U.S. Patent and Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00062	2/25/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	PALO ALTO NETWORKS, INC.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	8,955,038	2/10/2015	Taasera Licensing LLC
2	8,990,948	3/24/2015	Taasera Licensing LLC
3	9,092,616	7/28/2015	Taasera Licensing LLC
4	9,923,918	3/20/2018	Taasera Licensing LLC
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

IPR2023-01466
CrowdStrike EX1002 Page 11

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00063	2/25/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	CHECK POINT SOFTWARE TECHNOLOGIES LTD.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	6,842,796	1/11/2005	Taasera Licensing LLC
2	8,327,441	12/4/2012	Taasera Licensing LLC
3	8,955,038	2/10/2015	Taasera Licensing LLC
4	8,990,948	3/24/2015	Taasera Licensing LLC
5	9,092,616	7/28/2015	Taasera Licensing LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

IPR2023-01466
CrowdStrike EX1002 Page 12

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00063	2/25/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	CHECK POINT SOFTWARE TECHNOLOGIES LTD.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	9,608,997	3/28/2017	Taasera Licensing LLC
2	9,923,918	3/20/2018	Taasera Licensing LLC
3			
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

IPR2023-01466
CrowdStrike EX1002 Page 13

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00063	2/25/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	CHECK POINT SOFTWARE TECHNOLOGIES LTD.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	6,842,796	1/11/2005	Taasera Licensing LLC
2	8,327,441	12/4/2012	Taasera Licensing LLC
3	8,955,038	2/10/2015	Taasera Licensing LLC
4	8,990,948	3/24/2015	Taasera Licensing LLC
5	9,092,616	7/28/2015	Taasera Licensing LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading		
	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1			
2			
3			
4			
5			

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

IPR2023-01466
CrowdStrike EX1002 Page 14

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00063	2/25/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	CHECK POINT SOFTWARE TECHNOLOGIES LTD.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	9,608,997	3/28/2017	Taasera Licensing LLC
2	9,923,918	3/20/2018	Taasera Licensing LLC
3			
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

IPR2023-01466
CrowdStrike EX1002 Page 15

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00062	2/25/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	PALO ALTO NETWORKS, INC.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	6,842,796	1/11/2005	Taasera Licensing LLC
2	7,673,137	3/2/2010	Taasera Licensing LLC
3	8,127,356	2/28/2012	Taasera Licensing LLC
4	8,327,441	12/4/2012	Taasera Licensing LLC
5	8,850,517	9/30/2014	Taasera Licensing LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

IPR2023-01466
CrowdStrike EX1002 Page 16

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00062	2/25/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	PALO ALTO NETWORKS, INC.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	8,955,038	2/10/2015	Taasera Licensing LLC
2	8,990,948	3/24/2015	Taasera Licensing LLC
3	9,092,616	7/28/2015	Taasera Licensing LLC
4	9,923,918	3/20/2018	Taasera Licensing LLC
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

IPR2023-01466
CrowdStrike EX1002 Page 17

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:21-cv-00441	11/30/2021	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	TREND MICRO INCORPORATED

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	6,842,796	1/11/2005	Taasera Licensing LLC
2	7,673,137	3/2/2010	Taasera Licensing LLC
3	8,327,441	12/4/2012	Taasera Licensing LLC
4	8,850,517	9/30/2014	Taasera Licensing LLC
5	8,955,038	2/10/2015	Taasera Licensing LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

IPR2023-01466
CrowdStrike EX1002 Page 18

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:21-cv-00441	11/30/2021	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	TREND MICRO INCORPORATED

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	8,990,948	3/24/2015	Taasera Licensing LLC
2	9,092,616	7/28/2015	Taasera Licensing LLC
3	9,608,997	3/28/2017	Taasera Licensing LLC
4	9,923,918	3/20/2018	Taasera Licensing LLC
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

PETITION TO ACCEPT UNINTENTIONALLY DELAYED PAYMENT OF MAINTENANCE FEE IN AN EXPIRED PATENT (37 CFR 1.378(b))

Patent Number	Issue Date	Application Number	Filing Date	Docket Number (if applicable)
9092616	28-Jul-2015	13559766	27-Jul-2012	

CAUTION: Maintenance fee (and surcharge, if any) payment must correctly identify: (1) the patent number and (2) the application number of the actual U.S. application leading to issuance of that patent to ensure the fee(s) is/are associated with the correct patent. 37 CFR 1.366(c) and (d).

Applicants claims the following fee status:

- (◉) Small Entity
- (◯) Micro Entity
- (◯) Regular Undiscounted

Applicants selects the following :

(◉) 3 1/2	(◯) 7 1/2	(◯) 11 1/2

PETITION FEE
The petition fee required by 37 CFR 1.17(m) (Fee Code 1558/2558) must be paid as a condition of accepting unintentionally delayed payment of the maintenance fee.

MAINTENANCE FEE (37 CFR 1.20(e)-(g))
The appropriate maintenance fee must be submitted with this petition.

STATEMENT
THE UNDERSIGNED CERTIFIES THAT THE DELAY IN PAYMENT OF THE MAINTENANCE FEE TO THIS PATENT WAS UNINTENTIONAL

PETITIONER(S) REQUEST THAT THE DELAYED PAYMENT OF THE MAINTENANCE FEE BE ACCEPTED AND THE PATENT REINSTATED

THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES

37 CFR 1.378(c) states: "Any petition under this section must be signed in compliance with 37 CFR 1.33(b) ."

I certify, in accordance with 37 CFR 1.4(d)(4) that I am

- (◯) An attorney or agent registered to practice before the Patent and Trademark Office who has been given power of attorney in this application.
- (◉) An attorney or agent registered to practice before the Patent and Trademark Office
- (◯) A sole patentee
- (◯) A joint patentee; I certify that I am authorized to sign this submission on behalf of all the other patentees as evidenced by the power of attorney in the application
- (◯) A joint patentee; all of whom are signing this e-petition
- (◯) The assignee of record of the entire interest that qualifies as an authorized party under 37 CFR 1.33(b)

Patent Practitioner			
A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature			
Signature	/Daniel Buri/		
Name	Daniel Buri	Registration Number	61245

Electronic Patent Application Fee Transmittal

Application Number:	13559766
Filing Date:	27-Jul-2012
Title of Invention:	SYSTEMS AND METHODS FOR THREAT IDENTIFICATION AND REMEDIATION
First Named Inventor/Applicant Name:	Srinivas KUMAR
Filer:	Daniel Buri
Attorney Docket Number:	0079152-000016

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
MAINTENANCE FEE DUE AT 3.5 YEARS	2551	1	1000	1000
PET. DELAY PYMT MAINTAIN PATENT IN FORCE	2558	1	1050	1050
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**2050**

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

In re Patent No. 9092616
Issue Date: July 28,2015
Application No. 13559766
Filed: July 27,2012
Attorney Docket No. 0079152-000016

:
:DECISION GRANTING PETITION
:UNDER 37 CFR 1.378(b)
:

This is a decision on the electronic petition, filed November 13,2020 ,under 37 CFR 1.378(b) to accept the unintentionally delayed payment of the 3.5 year maintenance fee for the above-identified patent.

The petition is **GRANTED**.

The maintenance fee is accepted, and the above-identified patent reinstated as of November 13,2020 . This decision also constitutes notice that the fee has been accepted. An electronic copy of the petition and this decision has been created as an entry in the Image File Wrapper. Nevertheless, petitioner should print and retain an independent copy.

Telephone inquiries related to this electronic decision should be directed to the Electronic Business Center at 1-866-217-9197.

Electronic Acknowledgement Receipt	
EFS ID:	41123620
Application Number:	13559766
Patent Number:	9092616
Confirmation Number:	9330
Petition Issued Date:	November 13,2020
Title of Invention:	SYSTEMS AND METHODS FOR THREAT IDENTIFICATION AND REMEDIATION
First Named Inventor/Applicant Name:	Srinivas KUMAR
Customer Number:	21839
Filer:	Daniel Buri
Filer Authorized By:	
Attorney Docket Number:	0079152-000016
Receipt Date:	13-NOV-2020
Filing Date:	27-JUL-2012
Time Stamp:	18:16:31
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$2050
RAM confirmation Number	E2020ACI16473600
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Petition automatically granted by EFS	petition-request.pdf	32626 d34b05391feafc71ff70a95f6ca75ec13ef879fe	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	31579 3f4508b3860178aab14571427fc86471348c5199	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	64205		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/559,766	07/28/2015	9092616	0079152-000016	9330

21839 7590 07/08/2015

BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 182 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Srinivas KUMAR, Cupertino, CA;
Dennis Pollutro, Clymer, NY;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

21839 7590 05/22/2015
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/559,766	07/27/2012	Srinivas KUMAR	0079152-000016	9330

TITLE OF INVENTION: SYSTEMS AND METHODS FOR THREAT IDENTIFICATION AND REMEDIATION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	08/24/2015

EXAMINER	ART UNIT	CLASS-SUBCLASS
SAVENKOV, VADIM	2431	726-025000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 BUCHANAN INGERSOLL & ROONEY PC
2
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: TAASERA, INC.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): ERIE, PENNSYLVANIA

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
- ☒ Issue Fee
- ☐ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ☐ A check is enclosed.
- ☒ Payment by credit card.
- ☒ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number 02-4800 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ☐ Applicant certifying micro entity status. See 37 CFR 1.29 — NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ☐ Applicant asserting small entity status. See 37 CFR 1.27 — NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ☐ Applicant changing to regular undiscounted fee status. — NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date June 18, 2015

Typed or printed name Charles F. Wieland III Registration No. 33,096

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

IPR2023-01466
CrowdStrike EX1002 Page 28

Electronic Patent Application Fee Transmittal

Application Number:	13559766
Filing Date:	27-Jul-2012
Title of Invention:	SYSTEMS AND METHODS FOR THREAT IDENTIFICATION AND REMEDIATION
First Named Inventor/Applicant Name:	Srinivas KUMAR
Filer:	Patrick C. Keane/Wallace Clegg
Attorney Docket Number:	0079152-000016

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl Issue Fee	2501	1	480	480

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**480**

Electronic Acknowledgement Receipt	
EFS ID:	22677449
Application Number:	13559766
International Application Number:	
Confirmation Number:	9330
Title of Invention:	SYSTEMS AND METHODS FOR THREAT IDENTIFICATION AND REMEDIATION
First Named Inventor/Applicant Name:	Srinivas KUMAR
Customer Number:	21839
Filer:	Patrick C. Keane/Wallace Clegg
Filer Authorized By:	Patrick C. Keane
Attorney Docket Number:	0079152-000016
Receipt Date:	18-JUN-2015
Filing Date:	27-JUL-2012
Time Stamp:	18:06:50
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$480
RAM confirmation Number	5195
Deposit Account	024800
Authorized User	WIELAND, CHARLES F.
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	2015-06-18_Fees_Transmittal_Filed.pdf	69290 c11eb2a95955cda8c326b40582709b10f9a5221f	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30666 1b52bd6e101b2cf2f1fe654fde7d44722853e4ed	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	99956		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

21839 7590 05/22/2015
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER
SAVENKOV, VADIM

ART UNIT	PAPER NUMBER
2431	

DATE MAILED: 05/22/2015

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/559,766	07/27/2012	Srinivas KUMAR	0079152-000016	9330

TITLE OF INVENTION: SYSTEMS AND METHODS FOR THREAT IDENTIFICATION AND REMEDIATION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	08/24/2015

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

IPR2023-01466
CrowdStrike EX1002 Page 33

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

21839 7590 05/22/2015
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/559,766	07/27/2012	Srinivas KUMAR	0079152-000016	9330

TITLE OF INVENTION: SYSTEMS AND METHODS FOR THREAT IDENTIFICATION AND REMEDIATION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	08/24/2015

EXAMINER	ART UNIT	CLASS-SUBCLASS
SAVENKOV, VADIM	2431	726-025000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:
- ❑ Issue Fee
- ❑ Publication Fee (No small entity discount permitted)
- ❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ❑ A check is enclosed.
- ❑ Payment by credit card. Form PTO-2038 is attached.
- ❑ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ❑ Applicant certifying micro entity status. See 37 CFR 1.29 — NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ❑ Applicant asserting small entity status. See 37 CFR 1.27 — NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ❑ Applicant changing to regular undiscounted fee status. — NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

IPR2023-01466
CrowdStrike EX1002 Page 34

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/559,766	07/27/2012	Srinivas KUMAR	0079152-000016	9330

21839 7590 05/22/2015

BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
SAVENKOV, VADIM	

ART UNIT	PAPER NUMBER
2431	

DATE MAILED: 05/22/2015

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

IPR2023-01466
CrowdStrike EX1002 Page 35

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 13/559,766	Applicant(s) KUMAR ET AL.	
	Examiner VADIM SAVENKOV	Art Unit 2431	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *communication dated 4/14/2014*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1 and 3-21*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 4/14/2014; 7/22/2014
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☐ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/CORDELIA ZECHER/
Supervisory Patent Examiner, Art Unit 2431

IPR2023-01466
CrowdStrike EX1002 Page 37

DETAILED ACTION

The present application is being examined under the pre-AIA first to invent provisions.

Information Disclosure Statement

The 4/14/2014 and 7/22/2014 IDSs have been considered by the examiner.

Response to Arguments

Regarding the rejection of claim 20 under 35 USC 112 (1st paragraph):

Applicant's arguments, see pages 12-13 of Applicant's arguments, filed 4/14/2014, with respect to rejection of claim 20 under 35 USC 112 (1st paragraph) have been fully considered and are persuasive. The rejection of claim 20 under 35 USC 112 (1st paragraph) has been withdrawn.

Regarding the rejection of claims 1-20 under 35 USC 103(a):

Applicant's arguments, see pages 13-17 of Applicant's arguments, filed 4/14/2014, with respect to the rejection of claims 1-20 under 35 USC 103(a) have been fully considered and are persuasive. The rejection of claims 1-20 under 35 USC 103(a) has been withdrawn.

Allowable Subject Matter

1. Claims 1 and 3-21 are allowed.

2. The following is an examiner's statement of reasons for allowance: Applicant's reply makes evident the reasons for allowance, satisfying the "record as a whole" proviso of the rule 37 CFR 1.104(e). Specifically, applicant's arguments filed on 4/14/2014 are persuasive, as such the reasons for allowance are in all probability evident from the record and no statement is deemed necessary (see MPEP 1302.14).

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to VADIM SAVENKOV whose telephone number is (571)270-5751. The examiner can normally be reached on Monday - Friday 10:00 AM - 6:30 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, CORDELIA P. ZECHER can be reached on (571) 272-7771. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/V. S./
Examiner, Art Unit 2431

/CORDELIA ZECHER/
Supervisory Patent Examiner, Art Unit 2431

Notice of References Cited	Application/Control No. 13/559,766	Applicant(s)/Patent Under Reexamination KUMAR ET AL.	
	Examiner VADIM SAVENKOV	Art Unit 2431	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2012/0311715	12-2012	TAL et al.	726/25
*	B	US-2010/0175134	07-2010	Ali-Ahmad et al.	726/24
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	17	(US-20090328222-$ or US-20080229422-$ or US-20050044418-$ or US-20120110174-$ or US-20130042317-$ or US-20120137375-$ or US-20120102458-$ or US-20070192863-$ or US-20120260342-$ or US-20120072968-$ or US-20100251000-$ or US-20080244748-$).did. or (US-8214497-$ or US-8272061-$ or US-6742128-$ or US-7735140-$).did. or (US-20090138939-$).did.	US-PGPUB; USPAT; DERWENT	OR	ON	2015/05/15 01:22
L2	44	("20050033987" | "20050132031" | "20050132202" | "20050138384" | "20050204404" | "20050221766" | "20050283660" | "20060005009" | "20060200680" | "20070005992" | "20070185856" | "20080015808" | "20080083039" | "20080141027" | "20080235372" | "20080289028" | "20090172814" | "20090178138" | "20090187988" | "20090204806" | "20090204964" | "20100281273" | "20110035577" | "20110154500" | "20110173643" | "20110179477" | "20110185423" | "20120084850" | "20120131334" | "20120284282" | "6091835" | "6507904" | "6760441" | "6990579" | "6996710" | "7013481" | "7194759" | "7587607" | "7797544" | "7882221" | "7979696" | "7984304" | "8108536" | "8429454").PN.	US-PGPUB; USPAT	OR	ON	2015/05/15 01:48
L3	2	("20110145711" | "5604862").PN.	US-PGPUB; USPAT	OR	ON	2015/05/15 01:48
L4	43	attest$6 WITH (endpoint or end-point)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 02:22
L5	10191	(assess$3 or assessment or evaluat$3 or atest$6 or attest$6) WITH (endpoint or end-point)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 02:33
L6	331	(assess$3 or assessment or evaluat$3 or atest$6 or attest$6) WITH (endpoint or end-point) SAME (run-time or	US-PGPUB; USPAT; USOCR;	OR	ON	2015/05/15 02:34

IPR2023-01466
CrowdStrike EX1002 Page 42

		runtime or execution or executing or running)	FPRS; EPO; JPO; DERWENT; IBM_TDB			
L7	333	(assess$3 or assessment or evaluat$3 or atest$6 or attest$6) WITH (endpoint or end-point) SAME (run-time or runtime or execution or executing or running or run adj time)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 02:34
L8	50	(assess$3 or assessment or evaluat$3 or atest$6 or attest$6) WITH (endpoint or end-point) SAME (run-time or runtime or execution or executing or running or run adj time) SAME2 (integrity or trust or fidelity or risk or riskiness or danger$5 or hazard$5)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 02:35
L9	65	("20020138756" | "20020199203" | "20030074580" | "20030105978" | "20030135611" | "20030172292" | "20040005886" | "20040088565" | "20040107360" | "20040123162" | "20040167984" | "20040193907" | "20040221174" | "20050015622" | "20050033596" | "20050044418" | "20050060537" | "20050086511" | "20050132225" | "20050138408" | "20050144475" | "20050154885" | "20050166065" | "20050172142" | "20050188065" | "20050223221" | "20050246767" | "20070124803" | "20070143827" | "20070143851" | "20110099255" | "20130007245" | "5666411" | "5673322" | "5732074" | "5987611" | "6012100" | "6061650" | "6081508" | "6151628" | "6185609" | "6253327" | "6298445" | "6377982" | "6453035" | "6493349" | "6539482" | "6643782" | "6654891" | "6694437" | "6732270" | "6748543" | "6751729" | "6760444" | "6766453" | "6778498" | "6785823" | "6850943" | "6874139" | "7058821" | "7185192" | "7243148" | "7673323" | "7805752" | "8104077").PN. OR ("8955038").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2015/05/15 02:46
L10	30	(assess$3 or assessment or evaluat$3 or atest$6 or attest$6) WITH (endpoint or end-point) SAME (run-time or runtime or execution or executing or running or run adj time) SAME2 ((integrity or trust or fidelity or risk or riskiness or danger$5 or hazard$5) AND server)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 02:48
L11	19	(US-20090328222-$ or US-20080229422-$ or US-20050044418-$ or US-20120110174-$ or US-20130042317-$ or US-20120137375-$ or US-20120102458-$ or US-20070192863-$ or US-20120260342-$ or US-20120072968-$ or US-20100251000-$ or US-20080244748-$	US-PGPUB; USPAT; DERWENT	OR	ON	2015/05/15 02:51

IPR2023-01466
CrowdStrike EX1002 Page 43

		or US-20100175134-$ or US-20070143851-$).did. or (US-8214497-$ or US-8272061-$ or US-6742128-$ or US-7735140-$).did. or (US-20090138939-$).did.				
L12	98689	H04L63/$.CPC.	US-PGPUB; USPAT; DERWENT	OR	ON	2015/05/15 02:55
L13	209591	H04L63/$.CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 02:55
L14	34117	H04L63/14$.CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 02:55
L15	45697	G06F21/5$.CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 02:56
L16	46	2 3	US-PGPUB; USPAT; DERWENT	OR	ON	2015/05/15 02:56
L17	157	16 8 9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 02:57
L18	40	17 AND 14	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 02:57
L19	71	17 AND 15	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 02:57
L20	21	18 AND 19	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 02:57

IPR2023-01466
CrowdStrike EX1002 Page 44

L21	92	17 AND (assess$3 or assessment or evaluat$3 or atest$6 or attest$6) near7 (endpoint or end-point or server or client or terminal or slave or remote)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 03:01
L22	32	21 AND 14	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 03:01
L23	54	21 AND 15	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 03:01
L24	7	("20050182937" | "20060174115" | "20070030539" | "20080064383" | "20080072311").PN. OR ("2010/0175134" | "2012/0233700" | "8281396" | "8925093").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2015/05/15 03:03
L25	3	(US-20080072311-$ or US-20080064383-$ or US-20070030539-$).did.	US-PGPUB	OR	ON	2015/05/15 03:05
L26	19	(endpoint or end-point) WITH (run-time or runtime or execution or executing or running or run adj time) near4 (report or context or assessment) WITH (send$3 or transmit$4 or transfer$4 or broadcast$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 04:25
L27	1064	(application or app or program or applet) WITH (run-time or runtime or execution or executing or running or run adj time) near7 (report or context or assessment) WITH (send$3 or transmit$4 or transfer$4 or broadcast$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 04:32
L28	641	(application or app or program or applet) near5 (report$3 or context or assessment) near4 (run-time or runtime or execution or executing or running or run adj time) WITH (send$3 or transmit$4 or transfer$4 or broadcast$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 04:32
L29	476	(application or app or program or applet) near3 (run-time or runtime or execution or executing or running or run adj time) WITH (report or context or assessment) near3 (send$3 or transmit$4 or transfer$4 or broadcast$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 04:33
L30	12	29 AND 14	US-PGPUB; USPAT; USOCR; FPRS;	OR	ON	2015/05/15 04:33

IPR2023-01466
CrowdStrike EX1002 Page 45

			EPO; JPO; DERWENT; IBM_TDB			
L31	20	29 AND 15	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 04:33
L32	11	30 AND 31	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 04:33
L33	10	(30 31) NOT 32	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 04:34
L34	96	agent WITH (run-time or runtime or execution or executing or running or run adj time) near8 (report or context or assessment) near3 (send$3 or transmit$4 or transfer$4 or broadcast$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 04:37
L36	20	34 AND 14	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 04:38
L37	20	34 AND 15	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 04:38
L38	18	36 AND 37	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 04:38
L39	4	(36 37) NOT 38	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 04:39
L40	238	agent WITH (app or application or program or OS or operating adj	US-PGPUB; USPAT;	OR	ON	2015/05/15 04:40

IPR2023-01466
CrowdStrike EX1002 Page 46

		system) near3 (run-time or runtime or execution or executing or running or run adj time) near8 (report or context or assessment)	USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
L41	57	40 AND (14 15)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 04:40
L42	660	(agent or applet or plugin or plug-in) WITH (app or application or program or OS or operating adj system) near3 (run-time or runtime or execution or executing or running or run adj time) WITH (report$3 or assessment or send$3 or transmit$4 or transfer$4 or broadcast$3) near8 (server or service)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 04:44
L43	82	42 AND (14 15)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 04:46
L44	86	(agent or applet or plugin or plug-in) WITH (app or application or program or OS or operating adj system) near3 (run-time or runtime) SAME (report$3 or assessment or send$3 or transmit$4 or transfer$4 or broadcast$3) near5 (server or service)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 05:10
L45	86	(agent or applet or plugin or plug-in) WITH (app or application or program or OS or operating adj system) near3 (run-time or runtime or run adj time) SAME (report$3 or assessment or send$3 or transmit$4 or transfer$4 or broadcast$3) near5 (server or service)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 05:10
L46	14	45 AND (14 15)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 05:11
L47	11	45 AND 726/22-25.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 05:11
L48	15	46 47	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	2015/05/15 05:11

IPR2023-01466
CrowdStrike EX1002 Page 47

			IBM_TDB			
L49	10	(agent or applet or plugin or plug-in) WITH (app or application or program or OS or operating adj system) near3 (run-time or runtime or run adj time) SAME (report$3 or assessment or send$3 or transmit$4 or transfer$4 or broadcast$3) near5 (server or service) SAME3 (integrity or trust or fidelity or risk or riskiness or danger$5 or hazard$5)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/05/15 05:16
S1	17	(KUMAR near2 SRINIVAS).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:13
S2	18	(POLLUTRO near2 DENNIS).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:13
S3	33	S1 OR S2	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:14
S4	3	(TAASERA).as.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:14
S5	3	(TAASERA$10).as.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:15
S6	34	S1 OR S2 OR S4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:15
S7	11	S6 AND (attest$6 or risk or fidelity or reputation or vouch$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:15
S8	3	S6 AND (attest$6 or risk or fidelity or	US-PGPUB;	OR	ON	2013/07/02

IPR2023-01466
CrowdStrike EX1002 Page 48

		reputation or vouch$3).clm.	USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			17:15
S9	0	S6 AND openflow.clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:19
S10	0	S6 AND orchestrat$4.clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:20
S11	1	S6 AND integrity.clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:21
S12	2002	726/25.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:23
S13	1095	S12 AND (reputation or attest$6 or integrity or fidelity or risk or trust) AND (assess$4 or scan$4 or evaluat$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:27
S14	818	S12 AND ((reputation or attest$6 or integrity or fidelity or risk or trust) AND (assess$4 or scan$4 or evaluat$4)) WITH (network or device or system or endpoint or computer)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:28
S15	125	S12 AND ((reputation or attest$6 or integrity or fidelity or risk or trust) AND (assess$4 or scan$4 or evaluat$4)) WITH (network or device or system or endpoint or computer) SAME3 (correlat$6 or co-relat$6)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:29
S16	24	S12 AND (endpoint or end-point) near2 (assess$4 or scan$4 or evaluat$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	2013/07/02 17:31

IPR2023-01466
CrowdStrike EX1002 Page 49

			IBM_TDB			
S17	0	S12 AND (temporal adj event)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:31
S18	8	S15 AND S16	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:32
S19	20	("20050289072" | "20070143474" | "20070174406" | "20090094584" | "20090138939" | "20090144818" | "20090241170" | "20090276204" | "20090328186" | "20120216244").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:35
S20	22	("20050289072" | "20070143474" | "20070174406" | "20090094584" | "20090133110" | "20090138939" | "20090144818" | "20090241170" | "20090276204" | "20090328186" | "20120216244").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:35
S21	2	S20 NOT S19	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:35
S22	0	S12 AND openflow	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:38
S23	8	("20040230835" | "20050102534" | "20050257267" | "20060136986" | "20060156408" | "20070150957" | "6530024" | "7178166").PN. OR ("8136164").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2013/07/02 17:39
S24	1	"20080276317"	US-PGPUB; USPAT; USOCR	OR	ON	2013/07/02 17:44
S25	2	"20050044418"	US-PGPUB; USPAT; USOCR	OR	ON	2013/07/02 17:45
S26	582	S12 AND (security or integrity or risk or fidelity) near2 (assessment or report or scan or profile)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	2013/07/02 17:49

IPR2023-01466
CrowdStrike EX1002 Page 50

			IBM_TDB			
S27	383	S12 AND (security or integrity or risk or fidelity) adj (assessment or report or scan or profile)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:49
S28	20	S12 AND (security or integrity or risk or malware or spyware or pestware or virus or rootkit or trojan or worm or hazard$4 or danger$4 or infect$4) adj (vector or trajectory or possibilities or "attack path" or "scenario graph" or "attack graph")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:53
S29	217	S12 AND (security or integrity or risk or malware or spyware or pestware or virus or rootkit or trojan or worm or hazard$4 or danger$4 or infect$4) with (vector or trajectory or possibilities or "attack path" or "scenario graph" or "attack graph")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:53
S30	73	S12 AND (((security or integrity or risk or malware or spyware or pestware or virus or rootkit or trojan or worm or hazard$4 or danger$4 or infect$4) adj (vector or trajectory or possibilities)) or ("attack path" or "scenario graph" or "attack graph"))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:54
S31	103	S12 AND (((security or integrity or risk or malware or spyware or pestware or virus or rootkit or trojan or worm or hazard$4 or danger$4 or infect$4) adj (vector or trajectory or possibilities or condition)) or ("attack path" or "scenario graph" or "attack graph"))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:55
S32	2	"8214497".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:56
S33	509	("20010037311" | "20010049793" | "20020004902" | "20020013692" | "20020016910" | "20020023089" | "20020023140" | "20020026591" | "20020032871" | "20020035683" | "20020042876" | "20020046041" | "20020049853" | "20020051575" | "20020059454" | "20020062368" | "20020078382" | "20020087882" | "20020095492" | "20020112013" | "20020112185" | "20020116627" | "20020120853" | "20020133365" | "20020138416" | "20020138755" | "20020138759" | "20020138762" | "20020143963" | "20020147734" | "20020152399" | "20020165971" | "20020169954" | "20020172367" | "20020178227" | "20020178383" | "20020178410" | "20020188864" |	US-PGPUB; USPAT; USOCR	OR	ON	2013/07/02 17:56

IPR2023-01466
CrowdStrike EX1002 Page 51

		"20020194469" | "20020199095" |						
		"20030005326" | "20030005331" |						
		"20030009554" | "20030009693" |						
		"20030009696" | "20030009699" |						
		"20030014664" | "20030023692" |						
		"20030023695" | "20030023736" |						
		"20030023873" | "20030023874" |						
		"20030023875" | "20030028803" |						
		"20030033516" | "20030033542" |						
		"20030041264" | "20030046253" |						
		"20030051026" | "20030051163" |						
		"20030051168" | "20030055931" |						
		"20030061506" | "20030065943" |						
		"20030084280" | "20030084320" |						
		"20030084323" | "20030084347" |						
		"20030088792" | "20030093667" |						
		"20030093695" | "20030093696" |						
		"20030095555" | "20030097439" |						
		"20030097564" | "20030105976" |						
		"20030110392" | "20030110396" |						
		"20030115485" | "20030115486" |						
		"20030123665" | "20030126464" |						
		"20030126472" | "20030135749" |						
		"20030140137" | "20030140250" |						
		"20030145212" | "20030145225" |						
		"20030145226" | "20030149887" |						
		"20030149888" | "20030152096" |						
		"20030154393").PN. OR						
		("20030154399" | "20030154402" |						
		"20030158905" | "20030159069" |						
		"20030159070" | "20030167308" |						
		"20030167402" | "20030172166" |						
		"20030172167" | "20030172289" |						
		"20030172291" | "20030172292" |						
		"20030172294" | "20030172301" |						
		"20030172302" | "20030182421" |						
		"20030187936" | "20030187996" |						
		"20030204596" | "20030204719" |						
		"20030212791" | "20030233328" |						
		"20040015554" | "20040025044" |						
		"20040054886" | "20040058673" |						
		"20040059811" | "20040088570" |						
		"20040111519" | "20040111531" |						
		"20040122926" | "20040139160" |						
		"20040139334" | "20040167968" |						
		"20040177120" | "20040203589" |						
		"20040205135" | "20040221062" |						
		"20040236884" | "20040249895" |						
		"20040267893" | "20050021738" |						
		"20050021997" | "20050052998" |						
		"20050060643" | "20050065810" |						
		"20050086300" | "20050091319" |						
		"20050091320" | "20050102366" |						
		"20050141427" | "20050149383" |						
		"20050159998" | "20050160148" |						
		"20050192958" | "20050198159" |						
		"20050204001" | "20050216564" |						
		"20050256866" | "20050262209" |						
		"20050262210" | "20050262556" |						
		"20060009994" | "20060015942" |						
		"20060023940" | "20060031314" |						
		"20060031483" | "20060036693" |						
		"20060036727" | "20060041508" |						
		"20060042483" | "20060059238" |						

IPR2023-01466
CrowdStrike EX1002 Page 52

		"20060095404" | "20060095586" |						
		"20060123083" | "20060129810" |						
		"20060149821" | "20060155553" |						
		"20060168024" | "20060174337" |						
		"20060179113" | "20060191002" |						
		"20060212925" | "20060212930" |						
		"20060212931" | "20060225136" |						
		"20060230039" | "20060230134" |						
		"20060251068" | "20060253447" |						
		"20060253458" | "20060253582" |						
		"20060253584").PN. OR						
		("20060277259" | "20070019235" |						
		"20070124803" | "20070130350" |						
		"20070130351" | "20070199070" |						
		"20070214151" | "20080005223" |						
		"20080077517" | "20080091765" |						
		"20080104180" | "20080123823" |						
		"20080159632" | "20080175266" |						
		"20080178259" | "20080178288" |						
		"20090003204" | "20090113016" |						
		"20090122699" | "20090125980" |						
		"20090254499" | "20090254572" |						
		"4289930" | "4384325" | "4386416" |						
		"4532588" | "4713780" | "4754428" |						
		"4837798" | "4853961" | "4864573" |						
		"4951196" | "4975950" | "4979210" |						
		"5008814" | "5020059" | "5051886" |						
		"5054096" | "5105184" | "5119465" |						
		"5144557" | "5144659" | "5144660" |						
		"5167011" | "5210824" | "5210825" |						
		"5235642" | "5239466" | "5247661" |						
		"5276869" | "5278901" | "5283887" |						
		"5293250" | "5313521" | "5319776" |						
		"5355472" | "5367621" | "5377354" |						
		"5379340" | "5379374" | "5404231" |						
		"5406557" | "5414833" | "5416842" |						
		"5418908" | "5424724" | "5479411" |						
		"5481312" | "5483466" | "5485409" |						
		"5495610" | "5509074" | "5511122" |						
		"5513126" | "5513323" | "5530852" |						
		"5535276" | "5541993" | "5544320" |						
		"5550984" | "5550994" | "5557742" |						
		"5572643" | "5577209" | "5602918" |						
		"5606668" | "5608819" | "5608874" |						
		"5619648" | "5621889" | "5632011" |						
		"5638487" | "5644404" | "5657461" |						
		"5673322" | "5675507" | "5675733" |						
		"5677955" | "5694616" | "5696822" |						
		"5706442" | "5708780" | "5708826" |						
		"5710883" | "5727156" | "5740231" |						
		"5742759" | "5742769" | "5745574" |						
		"5751956" | "5758343" | "5764906" |						
		"5768528" | "5771348" | "5778372" |						
		"5781857" | "5781901").PN. OR						
		("5790789" | "5790790" | "5790793" |						
		"5793763" | "5793972" | "5796942" |						
		"5796948" | "5801700" | "5805719" |						
		"5812398" | "5812776" | "5822526" |						
		"5822527" | "5826013" | "5826014" |						
		"5826022" | "5826029" | "5835087" |						
		"5845084" | "5850442" | "5855020" |						
		"5860068" | "5862325" | "5864852" |						
		"5878230" | "5884033" | "5892825" |						
		"5893114" | "5896499" | "5898836" |						

IPR2023-01466
CrowdStrike EX1002 Page 53

		"5903723" | "5911776" | "5923846" | "5930479" | "5933478" | "5933498" | "5937164" | "5940591" | "5948062" | "5958005" | "5963915" | "5978799" | "5987609" | "5991881" | "5999932" | "6003027" | "6006329" | "6012144" | "6014651" | "6023723" | "6029256" | "6035423" | "6052709" | "6058381" | "6058482" | "6061448" | "6061722" | "6072942" | "6088804" | "6092114" | "6092194" | "6094277" | "6094731" | "6104500" | "6108688" | "6108691" | "6108786" | "6118856" | "6118886" | "6119137" | "6119142" | "6119230" | "6119236" | "6122661" | "6141695" | "6141778" | "6145083" | "6151675" | "6161130" | "6165314" | "6185689" | "6192360" | "6192407" | "6199102" | "6202157" | "6219714" | "6223213" | "6249575" | "6249807" | "6260043" | "6269447" | "6269456" | "6272532" | "6275942" | "6279113" | "6279133" | "6282565" | "6285991" | "6289214" | "6298445" | "6301668" | "6304898" | "6304973" | "6311207" | "6317829" | "6320948" | "6321267" | "6324569" | "6324647" | "6324656" | "6330589" | "6347374" | "6353886" | "6363489" | "6370648" | "6373950" | "6385655" | "6393465" | "6393568" | "6405318" | "6434624" | "6442588" | "6442686" | "6453345" | "6460141").PN. OR ("6470086" | "6487599" | "6487666" | "6502191" | "6516411" | "6519703" | "6539430" | "6546416" | "6546493" | "6550012" | "6574737" | "6578025" | "6609196" | "6650890" | "6654787" | "6675153" | "6681331" | "6687687" | "6697950" | "6701440" | "6704874" | "6711127" | "6711687" | "6725377" | "6732101" | "6732157" | "6735703" | "6738462" | "6742124" | "6742128" | "6754705" | "6757830" | "6760309" | "6768991" | "6769016" | "6772196" | "6775657" | "6792546" | "6880156" | "6892178" | "6892179" | "6892237" | "6895385" | "6907430" | "6910135" | "6928556" | "6941348" | "6941467" | "6968461" | "6981143" | "7051077" | "7089428" | "7092992" | "7117358" | "7143213" | "7152105" | "7155243" | "7164678" | "7254712" | "7272149" | "7272853" | "7349332" | "7376731" | "7385924" | "7460476" | "7461339" | "7496634" | "7522516" | "7543056" | "7545748" | "7610344" | "7617160" | "7620986" | "7644127" | "7730316" | "7739253" | "7870203" | "7899866" | "7937480" | "8079087").PN. OR ("8214497").URPN.				
S34	11	("20040111632" | "20040128543" | "20050193430" | "20070220606" | "6324656" | "6546493" | "6952779" | "6968377" | "7016499" | "7058821" |	US-PGPUB; USPAT; USOCR	OR	ON	2013/07/02 17:58

IPR2023-01466
CrowdStrike EX1002 Page 54

		"7359962").PN. OR ("8272061").URPN.				
S35	2	"6742128".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:58
S36	77	("5568471" | "6279113" | "6324647" | "6442144").PN. OR ("6742128").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2013/07/02 18:00
S37	10	"20030172294" "7899866"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 18:03
S38	1	(US-20090328222-$).did.	US-PGPUB	OR	ON	2013/07/03 16:25
S39	1	S38 AND host with central	US-PGPUB	OR	ON	2013/07/03 16:25
S40	78	lookout.as.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/10 18:32
S41	596	openflow or open-flow	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/10 19:23
S42	9	S41 AND "726".clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/10 19:23
S43	2	2011/0307951	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/10 19:33
S44	291	S41 AND (security or integrity or risk or malware or spyware or pestware or virus or rootkit or trojan or worm or hazard$4 or danger$4 or infect$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/10 19:36
S45	11	S41 AND (security or integrity or risk or malware or spyware or pestware or virus or rootkit or trojan or worm or	US-PGPUB; USPAT; USOCR;	OR	ON	2013/07/10 19:37

IPR2023-01466
CrowdStrike EX1002 Page 55

		hazard$4 or danger$4 or infect$4).clm.	FPRS; EPO; JPO; DERWENT; IBM_TDB			
S46	4	S41 AND (security or integrity or risk or malware or spyware or pestware or virus or rootkit or trojan or worm or hazard$4 or danger$4 or infect$4).ab.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/10 19:37
S47	14	S45 OR S46	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/10 19:37
S48	977	information adj flow adj control	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 11:55
S49	1	S48 AND (openflow or open-flow)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 11:55
S50	78	S48 AND "726".clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 11:57
S51	241	"binary analysis"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 16:47
S52	8502	"static analysis" or "dynamic analysis" or "taint analysis"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 16:50
S53	52	S51 AND S52	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 16:50
S54	3	"binary analysis" with ("static analysis"	US-PGPUB;	OR	ON	2013/07/11

IPR2023-01466
CrowdStrike EX1002 Page 56

		or "dynamic analysis" or "taint analysis")	USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			16:51
S55	542	("binary analysis" or "static analysis" or "dynamic analysis" or "taint analysis") AND "726".clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 16:52
S56	224	("binary analysis" or "static analysis" or "dynamic analysis" or "taint analysis") with image	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 16:52
S57	3	("binary analysis" or "static analysis" or "dynamic analysis" or "taint analysis") with image AND endpoint	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 16:53
S58	392	("binary analysis" or "static analysis" or "dynamic analysis" or "taint analysis") AND endpoint	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 16:53
S59	956	("binary analysis" or "static analysis" or "dynamic analysis" or "taint analysis") SAME (endpoint or end-point or end adj point or node or server or router or host or switch or firewall)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 16:54
S60	28	("binary analysis" or "static analysis" or "dynamic analysis" or "taint analysis") SAME (endpoint or end-point or end adj point)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 16:54
S61	13	"6002869".pn. "20100058475".pn. "20110231828".pn. "20120084754".pn. "20120151592".pn. "20120233599".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 16:58
S62	105	(("binary analysis" or "static analysis" or "dynamic analysis" or "taint analysis") AND (network$3 or IDS or intru$6 adj detect$3 or firewall)).ab.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	2013/07/11 17:00

IPR2023-01466
CrowdStrike EX1002 Page 57

			IBM_TDB			
S63	94	(("binary analysis" or "static analysis" or "dynamic analysis" or "taint analysis") AND (network$3 or IDS or intru$6 adj detect$3 or firewall)).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 17:01
S64	2	S62 AND S63	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 17:01
S65	51	(("binary analysis" or "static analysis" or "taint analysis") AND (network$3 or IDS or intru$6 adj detect$3 or firewall)).ab.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 17:04
S66	199	(("binary analysis" or "static analysis" or "taint analysis" or analy$6 near3 (source adj code or compiled or interpreted or byte)) AND (network$3 or IDS or intru$6 adj detect$3 or firewall)).ab.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 17:05
S67	14	S66 AND ("713" or "726" or "709").clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 17:05
S68	58	("20020004827" | "20030028257" | "20030061568" | "20030098887" | "20030115305" | "20030226131" | "20040030771" | "20040040016" | "20040111499" | "20040117624" | "20040153536" | "20040179142" | "20040205737" | "20040210654" | "20040230681" | "20050004942" | "20050015624" | "20050108387" | "20050114479" | "20050149872" | "20050174484" | "20050182969" | "20050262225" | "20060004680" | "20060195564" | "20070180432" | "4617643" | "4686623" | "4972264" | "6219706" | "6243862" | "6282546" | "6301668" | "6324656" | "6405318" | "6421719" | "6477651" | "6487666" | "6502112" | "6523172" | "6597666" | "6601059" | "6615257" | "6636972" | "6775657" | "6839850" | "6920458" | "6950865" | "6968377" | "7032014" | "7113989" | "7216298" | "7284009" | "7287069" | "7376719" | "7376969" | "7418733" | "7457884").PN. OR ("7735140").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2013/07/11 17:08
S69	11	("20020032766" | "20020075809" |	US-PGPUB;	OR	ON	2013/07/11

IPR2023-01466
CrowdStrike EX1002 Page 58

		"20060209794" | "20070011317" | "20070192863" | "20070201359" | "20080016115" | "5774668" | "6449650" | "7290283").PN. OR ("7792959").URPN.	USPAT; USOCR			17:12
S70	0	S68 AND S69	US-PGPUB; USPAT; USOCR	OR	ON	2013/07/11 17:12
S71	5	S66 AND "717".clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 17:13
S72	69	S68 OR S69	US-PGPUB; USPAT; USOCR	OR	ON	2013/07/11 17:36
S73	6	S72 AND ("binary analysis" or "static analysis" or "dynamic analysis" or "taint analysis")	US-PGPUB; USPAT; USOCR	OR	ON	2013/07/11 17:36
S74	319	("binary analysis" or "static analysis" or "dynamic analysis" or "taint analysis") with (".iso" or image or compiled or byte)	US-PGPUB; USPAT; USOCR	OR	ON	2013/07/11 17:44
S75	287	("binary analysis" or "static analysis" or "dynamic analysis" or "taint analysis") near15 (".iso" or image or compiled or byte)	US-PGPUB; USPAT; USOCR	OR	ON	2013/07/11 17:44
S76	69	("binary analysis" or "static analysis" or "dynamic analysis" or "taint analysis") near15 (".iso" or image or compiled or byte) AND ((network or endpoint or end-point) with (secur$4 or safe$3) or ids or intru$6 adj detect$4)	US-PGPUB; USPAT; USOCR	OR	ON	2013/07/11 17:46
S77	69	("binary analysis" or "static analysis" or "dynamic analysis" or "taint analysis") near15 (".iso" or image or compiled or byte) AND ((network or endpoint or end-point) with (secur$4 or safe$3) or "ids" or intru$6 adj detect$4)	US-PGPUB; USPAT; USOCR	OR	ON	2013/07/11 17:47
S78	27	("binary analysis" or "static analysis" or "dynamic analysis" or "taint analysis") near15 (".iso" or image or compiled or byte) AND ((network or endpoint or end-point) with (secur$4 or safe$3) or intru$6 adj detect$4)	US-PGPUB; USPAT; USOCR	OR	ON	2013/07/11 17:47
S79	9672	726/22,24-25.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 17:38
S80	2467	H04L63/1433.CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	2014/01/08 17:39

IPR2023-01466
CrowdStrike EX1002 Page 59

			IBM_TDB			
S81	2	"20130298244".PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 17:40
S82	827	G06F21/50.CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 17:42
S83	3474	G06F21/51.CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 17:42
S84	2658	G06F21/52.CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 17:42
S85	2002	G06F21/566.CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 17:43
S86	10652	S80 S82 S83 S84 S85	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 17:44
S87	7648	((reputation or attest$6 or integrity or fidelity or risk or trust) SAME (assess$4 or scan$4 or evaluat$4)) WITH (application or app or program or executable)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 18:34
S88	311	S87 AND S86	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 18:36
S89	486	S87 AND S79	US-PGPUB; USPAT; USOCR; FPRS;	OR	ON	2014/01/08 18:36

IPR2023-01466
CrowdStrike EX1002 Page 60

			EPO; JPO; DERWENT; IBM_TDB			
S90	163	S88 and S89	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 18:36
S91	183	((endpoint or end-point) near2 (assess$4 or scan$4 or evaluat$4) SAME (assess$4 or scan$4 or evaluat$4)) WITH (application or app or program or executable)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 18:37
S92	95	S87 AND (endpoint or end-point) near2 (assess$4 or scan$4 or evaluat$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 18:37
S93	30	S92 AND S79	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 18:37
S94	11	S92 AND S86	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 18:37
S95	25	S93 NOT S94	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 18:43
S96	140	((endpoint or end-point) near2 (assess$4 or scan$4 or evaluat$4) SAME (assess$4 or scan$4 or evaluat$4)) near6 (application or app or program or executable)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 18:46
S97	140	((endpoint or end-point) near2 (assess$4 or scan$4 or evaluat$4) AND (assess$4 or scan$4 or evaluat$4)) near6 (application or app or program or executable)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 18:46
S98	14	S97 AND (S79 or S86)	US-PGPUB; USPAT;	OR	ON	2014/01/08 18:46

IPR2023-01466
CrowdStrike EX1002 Page 61

			USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S99	27	("20060015942" | "20080276317" | "20110072506" | "20110162073" | "20110276468" | "20120011590" | "7174566" | "7370359" | "8010469" | "8214497").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/09 16:23
S100	7685	(end-point or endpoint or end adj point) near6 (security or assess$5 or trust or integrity or risk or fidelity)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/09 18:33
S101	253	(end-point or endpoint or end adj point) near15 (security or trust or integrity or risk or fidelity) near10 (assessment or profile or apparaisal or audit or rating or score)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/09 18:39
S102	2468	H04L63/1433.CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/09 18:40
S103	828	G06F21/50.CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/09 18:40
S104	3474	G06F21/51.CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/09 18:40
S105	2658	G06F21/52.CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/09 18:40
S106	2002	G06F21/566.CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/09 18:40

IPR2023-01466
CrowdStrike EX1002 Page 62

S107	10654	S102 S103 S104 S105 S106	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/09 18:40
S108	9682	726/22,24-25.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/09 18:41
S109	40	S101 AND S108	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/09 18:41
S110	20	S101 AND S107	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/09 18:41
S111	81	S101 AND (third adj party or third-party)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/09 18:42
S112	24	S111 AND (S107 or S108)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/09 18:43
S113	17	(US-20090328222-$ or US-20080229422-$ or US-20050044418-$ or US-20120110174-$ or US-20130042317-$ or US-20120137375-$ or US-20120102458-$ or US-20070192863-$ or US-20120260342-$ or US-20120072968-$ or US-20100251000-$ or US-20080244748-$).did. or (US-8214497-$ or US-8272061-$ or US-6742128-$ or US-7735140-$).did. or (US-20090138939-$).did.	US-PGPUB; USPAT; DERWENT	OR	ON	2014/01/09 20:28
S114	7	S113 AND (third adj party or third-party)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/09 20:28

IPR2023-01466
CrowdStrike EX1002 Page 63

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L50	12	((agent or applet or plugin or plug-in) SAME (app or application or program or OS or operating adj system) SAME (run-time or runtime or run adj time or executing or execution) SAME (report$3 or assessment or send$3 or transmit$4 or transfer$4 or broadcast$3) SAME (server) SAME (integrity or trust or fidelity or risk or riskiness or danger$5 or hazard$5)).clm.	US-PGPUB; UPAD	OR	ON	2015/05/15 05:35
L52	8528	H04L63/14$.CPC.	US-PGPUB; UPAD	OR	ON	2015/05/15 05:37
L53	10985	G06F21/5$.CPC.	US-PGPUB; UPAD	OR	ON	2015/05/15 05:37
L54	2	50 AND 52	US-PGPUB; UPAD	OR	ON	2015/05/15 05:37
L55	6	50 AND 53	US-PGPUB; UPAD	OR	ON	2015/05/15 05:37
L56	20	((agent or applet or plugin or plug-in) SAME (app or application or program or OS or operating adj system) SAME (run-time or runtime or run adj time or executing or execution) SAME (server) SAME (integrity or trust or fidelity or risk or riskiness or danger$5 or hazard$5)).clm.	US-PGPUB; UPAD	OR	ON	2015/05/15 05:39
L57	4	56 AND 52	US-PGPUB; UPAD	OR	ON	2015/05/15 05:40
L58	12	56 AND 53	US-PGPUB; UPAD	OR	ON	2015/05/15 05:40
L59	3	(50 56) AND 726/22-25.ccls.	US-PGPUB; UPAD	OR	ON	2015/05/15 05:42
L60	2	((endpoint or end-point or end adj point) SAME (app or application or program or OS or operating adj system) SAME (run-time or runtime or run adj time or executing or execution) SAME (report$3 or assessment or send$3 or transmit$4 or transfer$4 or broadcast$3) SAME (server) SAME (integrity or trust or fidelity or risk or riskiness or danger$5 or hazard$5)).clm.	US-PGPUB; UPAD	OR	ON	2015/05/15 05:43

5/15/2015 5:43:20 AM
C:\Users\vsavenkov\Documents\EAST\Workspaces\13559766.wsp

IPR2023-01466
CrowdStrike EX1002 Page 64

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13559766	KUMAR ET AL.
	Examiner	Art Unit
	VADIM SAVENKOV	2431

CPC- SEARCHED		
Symbol	Date	Examiner
H04L63/14-1491	5/15/2015	VS
G06F21/50-568	5/15/2015	VS

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	25	7/12/2013	VS
726	22,24	1/10/2014	VS

SEARCH NOTES		
Search Notes	Date	Examiner
See attached EAST search history of all the relevant databases.	7/12/2013	VS
Double Patenting search: Inventor/Assignee in PALM/EAST	7/12/2013	VS
Consulted with SPE Nathan Flynn regarding OPENFLOW claim language.	7/12/2013	VS
Class search of 726/22-25; Word search within and outside of said class/subclasses.	7/12/2013	VS
Forward and Backward citation searching relevant prior art.	7/12/2013	VS
Google and IEEE search for relevant prior art; search history not included.	7/12/2013	VS
See updated EAST search history which is attached.	1/10/2014	VS
CPC searching performed.	1/10/2014	VS
Class/subclass, CPC, text, forward/backward citation searching, various combinations, etc.	1/10/2014	VS
Updated general Google/IEEE search; search history not included.	1/10/2014	VS
See updated EAST search history which is attached.	5/15/2015	VS
Updated general Google/IEEE search; search history not included.	5/15/2015	VS
Class/subclass, CPC, text, forward/backward citation searching, various combinations, etc.	5/15/2015	VS
Interference searching.	5/15/2015	VS

/V.S./ Examiner.Art Unit 2431	

INTERFERENCE SEARCH			
US Class/ CPC Symbol	**US Subclass / CPC Group**	**Date**	**Examiner**
726	22-25	5/15/2015	VS
H04L63	14-1491	5/15/2015	VS
G06F21	50-568	5/15/2015	VS

/V.S./ Examiner.Art Unit 2431	

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13559766	KUMAR ET AL.
	Examiner	**Art Unit**
	VADIM SAVENKOV	2431

CPC							
Symbol						**Type**	**Version**
G06F	/	21	/	52		F	2013-01-01
H04L	/	63	/	1408		I	2013-01-01
G06F	/	21	/	51		I	2013-01-01
G06F	/	21	/	564		I	2013-01-01
H04L	/	63	/	145		A	2013-01-01
	/		/				
	/		/				
	/		/				
	/		/				
	/		/				
	/		/				
	/		/				
	/		/				
	/		/				
	/		/				

CPC Combination Sets							
Symbol					**Type**	**Set**	**Ranking**	**Version**
	/		/					
	/		/					

/VADIM SAVENKOV/ Examiner.Art Unit 2431	05/15/2015	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	20	
/DEDE ZECHER/ Supervisory Patent Examiner.Art Unit 2431	05/15/2015	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13559766	KUMAR ET AL.
	Examiner	**Art Unit**
	VADIM SAVENKOV	2431

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION									
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED				
726	25	G	0	6	F	11 / 00 (2006.0)	G	0	6	F	11 / 00 (2006.0)
CROSS REFERENCE(S)		G	0	6	F	12 / 14 (2006.0)	G	0	6	F	12 / 14 (2006.0)
		G	0	6	F	12 / 16 (2006.0)	G	0	6	F	12 / 16 (2006.0)
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)	G	0	8	B	23 / 00 (2006.0)	G	0	8	B	23 / 00 (2006.0)

/VADIM SAVENKOV/ Examiner.Art Unit 2431 (Assistant Examiner)	05/15/2015 (Date)	**Total Claims Allowed:** 20
/DEDE ZECHER/ Supervisory Patent Examiner.Art Unit 2431 (Primary Examiner)	05/15/2015 (Date)	O.G. Print Claim(s): 1 O.G. Print Figure: 1

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13559766	KUMAR ET AL.
	Examiner	**Art Unit**
	VADIM SAVENKOV	2431

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	17	17												
	2	18	18												
2	3	19	19												
3	4	20	20												
4	5	7	21												
5	6														
6	7														
8	8														
9	9														
10	10														
11	11														
12	12														
13	13														
14	14														
15	15														
16	16														

/VADIM SAVENKOV/ Examiner.Art Unit 2431	05/15/2015	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	20	
/DEDE ZECHER/ Supervisory Patent Examiner.Art Unit 2431	05/15/2015	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	13559766
Filing Date	2012-07-27
First Named Inventor	Kumar, Srinivas
Art Unit	2431
Examiner Name	Vadim SAVENKOV
Attorney Docket Number	0079152-000016

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5604862		1997-02-18	Midgely et al.	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20110145711		2011-06-16	Njemanze et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.S./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13559766
	Filing Date	2012-07-27
	First Named Inventor	Kumar, Srinivas
	Art Unit	2431
	Examiner Name	Vadim SAVENKOV
	Attorney Docket Number	0079152-000016

	1	July 17, 2014 Office Action issued in U.S. Patent Application No. 13/559,707.	☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Vadim Savenkov/	Date Considered	05/15/2015

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.S./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13559766
	Filing Date	2012-07-27
	First Named Inventor	Kumar, Srinivas
	Art Unit	2431
	Examiner Name	Vadim SAVENKOV
	Attorney Docket Number	0079152-000016

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

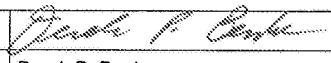
☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature		Date (YYYY-MM-DD)	2014-07-22
Name/Print	Derek P. Benke	Registration Number	56944

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.S./

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	)	**MAIL STOP**
Kumar, Srinivas et al.	)	Group Art Unit: 2431
Application No.: 13/559,766	)	Examiner: SAVENKOV, Vadim
Filed: July 27, 2012	)	Confirmation No.: 9330
For: Systems and Methods for Threat Identification and Remediation	)	

INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Madam:

In accordance with the duty of disclosure as set forth in 37 C.F.R. § 1.56, the accompanying information is being submitted in accordance with 37 C.F.R. §§ 1.97 and 1.98.

Pursuant to 37 C.F.R. § 1.98, a copy of each of the documents cited is enclosed. However, copies of the listed U.S. patents and U.S. patent application publications are not enclosed since it is no longer required.

The information is submitted before the mailing of a first Office Action after the filing of a Request for Continued Examination under 37 C.F.R. § 1.114. Continued examination is requested and the fee required under 37 C.F.R. § 1.17(e) accompanies the present submission.

To assist the Examiner, the documents are listed on the attached form PTO-1449. It is respectfully requested that an Examiner initialed copy of this form be returned to the undersigned.

The Director is hereby authorized to charge any appropriate fees under 37 C.F.R. §§ 1.16, 1.17 and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 02-4800.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: April 14, 2014

By: _____
Derek P. Benke
Registration No. 56,944

Customer No. 21839
703 836 6620

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.S./

Substitute for PTO/SB/08a&b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO				**Complete if Known**	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Application Number*	**13/559,766**
				Filing Date	**July 27, 2012**
				First Named Inventor	**Kumar, Srinivas**
				Art Unit	**2431**
(Use as many sheets as necessary)				*Examiner Name*	**SAVENKOV, Vadim**
Sheet	1	of	3	*Attorney Docket Number*	**0079152-000016**

U.S. PATENT DOCUMENTS

Examiner Initials'	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-6,091,835	7/18/2000	Smithies et al.	
		US-6,507,904 B1	1/14/2003	Ellison et al.	
		US-6,760,441 B1	7/6/2004	Ellison et al.	
		US-6,990,579 B1	1/24/2006	Herbert et al.	
		US-6,996,710 B1	2/7/2006	Ellison et al.	
		US-7,013,481 B1	3/14/2006	Ellison et al.	
		US-7,194,759 B1	3/20/2007	Chess et al.	
		US-7,587,607 B2	9/8/2009	Brickell et al.	
		US-7,797,544 B2	9/14/2010	Dillaway et al.	
		US-7,882,221 B2	2/1/2011	Sailer et al.	
		US-7,979,696 B2	7/12/2011	Kim et al.	
		US-7,984,304 B1	7/19/2011	Waldspurger et al.	
		US-8,108,536 B1	1/31/2012	Hernacki et al.	
		US-8,429,454 B2	4/23/2013	Yuan et al.	
		US-2005/0033987 A1	2/10/2005	Yan et al.	
		US-2005/0132202 A1	6/16/2005	Dillaway et al.	
		US-2005/0132031 A1	6/16/2005	Sailer et al.	
		US-2005/0138384 A1	6/23/2005	Brickell et al.	
		US-2005/0204404 A1	9/15/2005	Hrabik et al.	
		US-2005/0221766 A1	10/6/2005	Brizek et al.	
		US-2005/0283660 A1	12/22/2005	McKeen et al.	
		US-2006/0005009 A1	1/5/2006	Ball et al.	
		US-2006/0200680 A1	9/7/2006	Ellison et al.	
		US-2007/0005992 A1	1/4/2007	Schluessler et al.	
		US-2007/0185856 A1	8/9/2007	Mittal et al.	
		US-2008/0015808 A1	1/17/2008	Wilson et al.	
		US-2008/0083039 A1	4/3/2008	Choi et al.	
		US-2008/0141027 A1	6/12/2008	Kim et al.	
		US-2008/0235372 A1	9/25/2008	Sailer et al.	
		US-2008/0289028 A1	11/20/2008	Jansen et al.	
		US-2009/0172814 A1	7/2/2009	Khosravi et al.	
		US-2009/0178138 A1	7/9/2009	Weiss et al.	
		US-2009/0187988 A1	7/23/2009	Hulten et al.	
		US-2009/0204806 A1	8/13/2009	Kanemura et al.	
		US-2009/0204964 A1	8/13/2009	Foley et al.	
		US-2010/0281273 A1	11/4/2010	Lee et al.	
		US-2011/0035577 A1	2/10/2011	Lin et al.	
		US-2011/0154500 A1	6/23/2011	Sahita et al.	

Examiner Signature	/Vadim Savenkov/	Date Considered	05/15/2015

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.S./

Substitute for PTO/SB/08a&b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO				*Complete if Known*	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Application Number*	**13/559,766**
				Filing Date	**July 27, 2012**
				First Named Inventor	**Kumar, Srinivas**
				Art Unit	**2431**
(Use as many sheets as necessary)				*Examiner Name*	**SAVENKOV, Vadim**
Sheet	2	of	3	*Attorney Docket Number*	**0079152-000016**

U.S. PATENT DOCUMENTS

Examiner Initials'	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-2011/0173643 A1	7/14/2011	Nicolson et al.	
		US-2011/0179477	7/21/2011	Starnes et al.	
		US-2011/0185423 A1	7/28/2011	Sallam	
		US-2012/0084850 A1	4/5/2012	Novak et al.	
		US-2012/0131334 A1	5/24/2012	Haikney et al.	
		US-2012/0284282 A9	11/8/2012	Ghosh et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials'	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		December 5, 2013 Office Action issued in U.S. Application No. 13/559,665.	
		December 10, 2013 Office Action issued in U.S. Application No. 13/559,732.	
		October 23, 2013 Office Action issued in U.S. Application No. 13/559,692.	
		June 20, 2013 Office Action issued in U.S. Application No. 13/559,732.	
		July 18, 2013 Office Action issued in U.S. Application No. 13/559,766.	
		Event Tracker ver 7.0 Enterprise Users Guide. "Event Tracker ver 7.0 Enterprise User's; Guide. Prism Microsystems, 28 July 2010. Web. 29 Nov. 2013 <http://www.eventtracker.com/wp-content/uploads/EventTracker-v7.0-Enterprise-User-Guide.pdf>.	
		Statement of FIPS 140-2 Compliance. "Statement of FIPS 140-2 Compliance. Prism Microsystems, 6 Oct. 2010. Web 29 Nov. 2010. ,http://www.eventtracker.com/wp-content/uploads/2013/01/EventTracker_v7.0_FIPS_Compliance.pdf>.	
		Trend Micro, Inc.. "OfficeScan 10 Administrator/s Guide." docs.trendmicro.com/all/ent/officescan/v10.0/en-us/osce_10.0_ag.pdf. N.p. 20 Apr. 2009. Web. 27 Nov. 2013 http://docs.trendmicro.com/all/ent/officescan/v10.0/en-us/osce_10.0_ag.pdf.	
		August 27, 2012 International Search Report issued in PCT/US2012/025551.	

Examiner Signature	/Vadim Savenkov/	Date Considered	05/15/2015

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6]Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.S./

Substitute for PTO/SB/08a&b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Application Number*	**13/559,766**
				Filing Date	**July 27, 2012**
				First Named Inventor	**Kumar, Srinivas**
				Art Unit	**2431**
(Use as many sheets as necessary)				*Examiner Name*	**SAVENKOV, Vadim**
Sheet	3	of	3	*Attorney Docket Number*	**0079152-000016**

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		August 27, 2012 Written Opinion issued in PCT/US2012/025551.	
		August 21, 2013 International Preliminary Report on Patentability issued in PCT/US2012/025551.	

Examiner Signature	/Vadim Savenkov/	Date Considered	05/15/2015

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.S./

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13559766	KUMAR ET AL.
	Examiner	**Art Unit**
	VADIM SAVENKOV	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	07/12/2013	01/10/2014	05/15/2015						
1	1	✓	✓	=						
	2	✓	✓	-						
2	3	✓	✓	=						
3	4	✓	✓	=						
4	5	✓	✓	=						
5	6	✓	✓	=						
6	7	✓	✓	=						
8	8	✓	✓	=						
9	9	✓	✓	=						
10	10	✓	✓	=						
11	11	✓	✓	=						
12	12	✓	✓	=						
13	13	✓	✓	=						
14	14	✓	✓	=						
15	15	✓	✓	=						
16	16	✓	✓	=						
17	17	✓	✓	=						
18	18	✓	✓	=						
19	19	✓	✓	=						
20	20	✓	✓	=						
7	21			=						

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	13559766
	Filing Date	2012-07-27
	First Named Inventor	Kumar, Srinivas
	Art Unit	2431
	Examiner Name	Vadim SAVENKOV
	Attorney Docket Number	0079152-000016

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5604862		1997-02-18	Midgely et al.	
If you wish to add additional U.S. Patent citation information please click the Add button.						

U.S.PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20110145711		2011-06-16	Njemanze et al.	
If you wish to add additional U.S. Published Application citation information please click the Add button.						

FOREIGN PATENT DOCUMENTS								
Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐
If you wish to add additional Foreign Patent Document citation information please click the Add button								

NON-PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13559766
	Filing Date	2012-07-27
	First Named Inventor	Kumar, Srinivas
	Art Unit	2431
	Examiner Name	Vadim SAVENKOV
	Attorney Docket Number	0079152-000016

	1	July 17, 2014 Office Action issued in U.S. Patent Application No. 13/559,707.	☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13559766
	Filing Date	2012-07-27
	First Named Inventor	Kumar, Srinivas
	Art Unit	2431
	Examiner Name	Vadim SAVENKOV
	Attorney Docket Number	0079152-000016

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

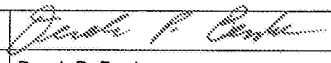
☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature		Date (YYYY-MM-DD)	2014-07-22
Name/Print	Derek P. Benke	Registration Number	56944

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Electronic Acknowledgement Receipt	
EFS ID:	19643937
Application Number:	13559766
International Application Number:	
Confirmation Number:	9330
Title of Invention:	SYSTEMS AND METHODS FOR THREAT IDENTIFICATION AND REMEDIATION
First Named Inventor/Applicant Name:	Srinivas KUMAR
Customer Number:	21839
Filer:	Derek P. Benke/Shaunna Lloyd
Filer Authorized By:	Derek P. Benke
Attorney Docket Number:	0079152-000016
Receipt Date:	22-JUL-2014
Filing Date:	27-JUL-2012
Time Stamp:	12:08:05
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS.pdf	754792 54603dd31fed664f504b0fa54e79fa5ae80e4569	no	3

Warnings:
Information:

This is not an USPTO supplied IDS fillable form					
2	Non Patent Literature	7_17_14_OA_0079152_015.pdf	4143014 88dde573f1de5bf5f7900b766b874f28838f15a1	no	35
Warnings:					
Information:					
			Total Files Size (in bytes):	4897806	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/30 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Request For Continued Examination (RCE) Transmittal

Address to:
Mail Stop RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Application Number	13/559,766
Filing Date	July 27, 2012
First Named Inventor	Kumar, Srinivas
Art Unit	2431
Examiner Name	SAVENKOV, Vadim
Attorney Docket Number	0079152-000016

This is a Request for Continued Examination (RCE) under 37 C.F.R. § 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. See Instruction Sheet for RCEs (not to be submitted to the USPTO) on page 2.

1. Submission required under 37 C.F.R. 1.114 Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).
   - a. ☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.
     - i ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
     - ii ☐ Other _____
   - b. ☒ Enclosed
     - i ☒ Amendment/Reply
     - ii ☐ Affidavit(s)/Declaration(s)
     - iii. ☒ Information Disclosure Statement (IDS)
     - iv. ☐ Other _____

2. Miscellaneous
   - a. ☐ Suspension of action on the above-identified application is requested under 37 C.F.R. 1.103(c) for a period of _____ months. (Period of suspension shall not exceed 3 months; Fee under 37 C.F.R. 1.17(i) required)
   - b. ☐ Other _____

3. Fees The RCE fee under 37 C.F.R. 1.17 (e) is required by 37 C.F.R. 1.114 when RCE is filed.
   - a. ☒ The Director is hereby authorized to charge the following fees, any underpayment of fees, or credit any overpayments, to Deposit Account No. **02-4800**.
     - i ☒ RCE fee required under 37 C.F.R. 1.17 (e)
     - ii ☐ Extension of time fee (37 C.F.R. 1.136 and 1.17)
     - iii ☐ Other _____
   - b. ☐ Check in the amount of $ _____ enclosed
   - c. ☒ Payment by credit card

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Signature	Derek P. Benke	Date	April 14, 2014
Name (Print/Type)	Derek P. Benke	Registration No.	56,944

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop RCE, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450 or facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.

Signature			
Name (Print/Type)		Date	April 14, 2014

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Patent Application Fee Transmittal	
Application Number:	13559766
Filing Date:	27-Jul-2012
Title of Invention:	SYSTEMS AND METHODS FOR THREAT IDENTIFICATION AND REMEDIATION
First Named Inventor/Applicant Name:	Srinivas KUMAR
Filer:	Derek P. Benke/Shaunna Lloyd
Attorney Docket Number:	0079152-000016
Filed as Small Entity	

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Request for Continued Examination	2801	1	600	600
		Total in USD ($)		**600**

Electronic Acknowledgement Receipt	
EFS ID:	18755914
Application Number:	13559766
International Application Number:	
Confirmation Number:	9330
Title of Invention:	SYSTEMS AND METHODS FOR THREAT IDENTIFICATION AND REMEDIATION
First Named Inventor/Applicant Name:	Srinivas KUMAR
Customer Number:	21839
Filer:	Derek P. Benke/Shaunna Lloyd
Filer Authorized By:	Derek P. Benke
Attorney Docket Number:	0079152-000016
Receipt Date:	14-APR-2014
Filing Date:	27-JUL-2012
Time Stamp:	15:59:08
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$600
RAM confirmation Number	2527
Deposit Account	024800
Authorized User	BENKE, DEREK
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		Amendment.pdf	691110 37821e0dd1180899e2f72365672953e25afcc2aa	yes	17
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Amendment/Req. Reconsideration-After Non-Final Reject		1	1	
	Claims		2	10	
	Applicant Arguments/Remarks Made in an Amendment		11	17	
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	IDS.pdf	673402 79ddcfab40e519c4e27a0ce1c2e7ee97ba9bad1f	no	4
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Non Patent Literature	12_5_13OA665.pdf	1454882 9f7877d3233662e3e5e3a306c266e82f0966f335	no	15
Warnings:					
Information:					
4	Non Patent Literature	12_10_13OA732.pdf	2490430 bea7e19e8c3671444469941c0cac392606c5ec42	no	29
Warnings:					
Information:					
5	Non Patent Literature	10_23_13OA692.pdf	1338829 cedaa723010a9efac2173f0f01653fbc416542f1	no	12
Warnings:					
Information:					
6	Non Patent Literature	6_20_13_OA_732.pdf	2276634 9cbc709e7470bb4dbac824f317a4d5dc223f4266	no	26

Warnings:					
Information:					
7	Non Patent Literature	7_18_13_OA_766.pdf	2838180 1f28ac49b7750893e9243d39bcd43f2f715f3bb2	no	31
Warnings:					
Information:					
8	Non Patent Literature	Event_Tracker_1pdf.pdf	15121555 2b263e6ca5aae1321f202eaf9a9bfcb7e42ca64d	no	200
Warnings:					
Information:					
9	Non Patent Literature	Event_Tracker_2pdf.pdf	15131181 139a5cd2abdf5cb715d796e8eb50696a9dac8a61	no	200
Warnings:					
Information:					
10	Non Patent Literature	Event_Tracker_3pdf.pdf	14129908 c2c37d0acf28e230d21fdeaff30909a26685ceb7	no	182
Warnings:					
Information:					
11	Non Patent Literature	Statement_ofFIPS.pdf	170829 0a6af5c16bd4c62a024849cac344342a8f859f41	no	1
Warnings:					
Information:					
12	Non Patent Literature	Trend_Micro.pdf	214710 516a6d79091df760128acd3972c8ca889da254ce	no	2
Warnings:					
Information:					
13	Non Patent Literature	ISR_551.pdf	339765 36bc512d2a9423c62b4edbfd1535554b27144fe5	no	3
Warnings:					
Information:					
14	Non Patent Literature	ISR_WO_551.pdf	1157331 ad87345d847c3f47aa48b38808fc24beab578c28	no	9
Warnings:					
Information:					
15	Non Patent Literature	IPRP_551.pdf	561947 50817d453d6a21f86f047a4e7e4065931fb17ece	no	5

Warnings:					
Information:					
16	Request for Continued Examination (RCE)	RCE.pdf	62918 4d72f0ace99ec396c4d6dc0f048cf68f2a444f2f	no	1
Warnings:					
This is not a USPTO supplied RCE SB30 form.					
Information:					
17	Fee Worksheet (SB06)	fee-info.pdf	30350 0e6a4c867ee33a60a415ba9c1c0631bb28794bee	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	58683961	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	**MAIL STOP RCE**
Kumar, Srinivas	Group Art Unit: 2431
Application No.: 13/559,766	Examiner: SAVENKOV, Vadim
Filed: July 27, 2012	Confirmation No.: 9330
For: Systems and Methods for Threat Identification and Remediation	

AMENDMENT UNDER 37 C.F.R. § 1.114

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Madam:

In response to the Office Action dated January 17, 2014, please amend the above-identified patent application as follows.

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) A method of providing an attestation service for providing runtime operational integrity of a system using a computing platform comprising a network trust agent, an endpoint trust agent, and a trust orchestration server, the method comprising:

sending, by the endpoint trust agent on a monitored device, a dynamic context including endpoint events and actions of the monitored device and applications executing on the monitored device at runtime;

receiving, at the trust orchestration server, [[a]] the dynamic context including the endpoint events of [[a]] the monitored device and the applications executing on the monitored device at runtime ~~thereon~~;

analyzing, by the trust orchestration server, the received endpoint events;

receiving, by the trust orchestration server, third party network endpoint assessments;

generating, by the trust orchestration server, temporal events based at least in part on analyzing the third party network endpoint assessments;

correlating, by the trust orchestration server, the received endpoint events and the generated temporal events; and

generating, by the trust orchestration server, an integrity profile for the system.

2. (Cancelled).

3. (Previously Presented) The method of claim 1, wherein the third party network endpoint assessments are received from an endpoint assessment service.

4. (Previously Presented) The method of claim 3, further comprising:

receiving, by the trust orchestration server, integrity measurement and verification reports from the endpoint assessment service.

5. (Previously Presented) The method of claim 1, wherein the third party network endpoint assessments are received from one or more collaboration services.

6. (Previously Presented) The method of claim 5, further comprising:

receiving, by the trust orchestration server, integrity measurement and verification reports from the one or more collaboration services.

7. (Previously Presented) The method of claim 1, wherein

the endpoint events of the monitored device are received by a system event correlator of the trust orchestration server from endpoint trust agents, and

the temporal events are generated by a trust broker of the trust orchestration server and are received by the system event correlator from the trust broker.

8. (Currently Amended) A method of providing flow level remediation to isolate infected or compromised systems and platforms from a computing network fabric using a network trust agent, an endpoint trust agent, and a trust orchestrator, the method comprising:

generating, by the endpoint trust agent on an endpoint device, runtime system integrity alerts regarding execution anomalies and risks based on rulesets and a calculus of risk hypothesized by runtime actions and activities of monitored applications executing on [[an]] the endpoint device;

sending, by the endpoint trust agent, runtime system integrity warnings as endpoint events of the endpoint device to the trust orchestrator;

generating, by the trust orchestrator, a system integrity profile for the endpoint device based on analysis of the received endpoint events;

processing and correlating, by the trust orchestrator, one or more of:

a system integrity profile generated based on a calculus of risk,

a plurality of temporal events generated based on a normalization and collation of elements in endpoint assessment reports received from a plurality of collaboration services, and

a system infection profile received from a network analyzer;

sending, by the trust orchestrator to the network trust agent, system warnings based on endpoint execution state assessments; and

sending, by the network trust agent, messages or directives to computer network protocol security frameworks and/or controllers to apply flow controls based on the received execution state as a threat posture of a connection endpoint.

9. (Original) The method of claim 8, wherein the integrity warnings comprise warnings regarding data events and content events; and wherein the endpoint events comprise data events and content events.

10. (Original) The method of claim 8, wherein the remediation of an infected system is achieved without adversely reducing the total operating capacity or availability of the computing platform through on-demand instantiation and scaling of workloads.

11. (Previously Presented) The method of claim 10, further comprising forwarding a notification conveying by a service accessed by a user from a mobile computing device an infected or compromised state of a mobile computing application on the mobile computing device associated with the user, wherein the notification is one or more of:

an asynchronous push notification to an account associated with the user;

a short messaging service (SMS) text alert message forwarded to a phone number associated with the mobile computing device;

an email alert message forwarded to an email address associated with the user; and

a warning message displayed by a service on a display of the mobile computing device during initiation of a transaction with a service from the mobile computing device.

12. (Currently Amended) The method of claim 11, wherein one or more services accessed by [[a]] the mobile computing device are configured to be denied or restricted as a remediation action by a service provider.

13. (Previously Presented) The method of claim 12, wherein the remediation action is based on the geo-location of the device, user and associated service accessed by the user.

14. (Previously Presented) The method of claim 1, further comprising:

generating, by a trust supervisor, one or more tiered remediation actions based on real time warning associated with the operational runtime integrity of applications executing on an infected system;

receiving, at a remediation controller of the trust orchestrator, the tiered remediation actions; and

sending, by the trust orchestrator, to the network trust agent, one or more system warnings pertaining to a network device associated with the one or more tiered remediation actions.

15. (Currently Amended) The method of claim 14, further comprising:

generating and sending, by the network trust agent, directives to formulate commands for [[an]] a computer network protocol controller;

sending, by the computer network protocol controller, rules to a computer network protocol enabled network element or switch of the network fabric to divert or block traffic flow to/from the network device; and

enforcing, by the computer network protocol enabled network element or switch, received access restrictions or controls for the network device.

16. (Previously Presented) The method of claim 15, further comprising:

monitoring and sending, by the trust supervisor, reputation score updates for the network device to the remediation controller;

sending, by the trust orchestrator, system security posture status updates for the network device to the network trust agent; and

generating and sending, by the network trust agent, to the computer network protocol security framework, directives to formulate commands for the computer network protocol controller to restore normal flows to/from the network device.

17. (Previously Presented) The method of claim 8, further comprising:

determining, by the network analyzer, threat behaviors based on network activity correlation and malware detection based on a threat life cycle model; and

dispatching, by the trust orchestrator, the image files and attributes of an application for binary analysis, wherein the image files comprise compiled, intermediate, or interpreted code or scripts;

receiving a result of the binary analysis result identifying malicious activity as a set of threats identified based on the analysis; and

caching, by the trust broker, the results of the analysis indexed by a unique identifier for the image; and

generating and returning an image profile to the endpoint trust agent comprising assertions of malicious capabilities of the image to be monitored at runtime for subsequent generation of endpoint events by the endpoint trust agent.

18. (Original) The method of claim 17, wherein the binary analysis is performed by one or more third party malware analyzers, and wherein the dispatch mechanism uses trigger filter expressions that specify a set of criteria that warrant initiation of image analysis such as frequency and volume of requests for analysis associated with the application image across deployed endpoint trust agents.

19. (Original) The method of claim 18, wherein the third party malware analyzers are configured to perform static and dynamic analysis of application images based on policies specified by the trust broker.

20. (Previously Presented) A system for providing runtime operational integrity by determining execution anomalies and a threat posture of applications executing on computing platforms including mobile devices and client-server systems, the system comprising:

(i) an endpoint trust agent including:

a process monitor configured to observe the runtime execution context of applications executing on the computer platforms and transient operating states,

a socket monitor configured to observe runtime network activities of the applications for transient states, and

a resource utilization module monitor configured to observe the types and extent of system and platform resources consumed by the applications that may provide evidence of infected systems; and

an application integrity module configured to assess runtime operational integrity of a monitored application instance running on an instrumented device based on a ruleset to deem local actions and activities of the application to be at risk;

wherein native machine instrumentation for the computing platform is configured to (a) represent event subscriptions, callbacks, notification mechanisms provided by an operating system (OS) on the computing platforms, and (b) generate raw events;

(ii) extended trust instrumentation;

(iii) a runtime monitor configured to:

subscribe to and receive near real time asynchronous notifications of runtime operation invocations by applications executing on the computer platforms from the extended trust instrumentation, and

generate and send dynamic expressions or rules as application activity filters linked to runtime operation invocations of running instances of the applications;

(iv) a system event correlator configured to correlate system events of the computing platforms to determine a calculus of risk;

(v) a trust orchestrator configured to orchestrate actionable intelligence based on the calculus of risk by integrating security intelligence about the computing platforms and the applications; and

(vi) an endpoint trust sensor configured to measure runtime operational integrity of the computing platforms by evaluating risk based on actions of an application executing on, or a user of, the computing platforms and receiving the raw events from the native machine instrumentation.

21. (New) The method of claim 1, further comprising:

performing, by a malware analyzer, detection of code obfuscation and evasion techniques in reverse engineered code of the applications, the code obfuscation and evasion techniques including at least one of: multiple packing, anti-debug, anti-trace, anti-memory, and anti-emulation.

REMARKS

Favorable reconsideration of this application as presently amended, and in light of the following discussion, is respectfully requested.

Claims 1 and 3-21 are pending in this application, Claim 2 having been cancelled without prejudice or disclaimer; Claims 1, 8, 12, and 15 having been presently amended; and Claim 21 having been added. Support for amended Claims 1, 8, 12, and 15, and new Claim 21 can be found in the original claims, drawings, and specification as filed.[1] No new matter has been added.

In the outstanding Office Action, Claim 20 was rejected under 35 U.S.C. § 112, first paragraph; Claims 1-7 and 14-16 were rejected under 35 U.S.C. § 103(a) as unpatentable over Helman et al. (U.S. Patent Publication No. 2009/0328222; hereinafter "Helman") in view of Neystadt et al. (U.S. Patent Publication No. 2008/0244748; hereinafter "Neystadt") and Wootton et al. (U.S. Patent Publication No. 2012/0110174; hereinafter "Wootton"); Claims 8-13 were rejected under 35 U.S.C. § 103(a) as unpatentable over Helman in view of Alperovitch et al. (U.S. Patent No. 8,214,497; hereinafter "Alperovitch") and Wootton; Claim 17 was rejected under 35 U.S.C. § 103(a) as unpatentable over Helman in view of Alperovitch et al. (U.S. Patent No. 8,214,497; hereinafter "Alperovitch"), Wootton, "Static Analysis of Executables for Collaborative Malware Detection on Android" (hereinafter "Schmidt"), and Wysopal et al. (U.S. Patent Publication No. 2012/0072968; hereinafter "Wysopal"); Claims 18 and 19 were rejected under 35 U.S.C. § 103(a) as unpatentable over Helman in view of Alperovitch, Wootton,

[1] See, e.g., original Claim 2; and paragraphs [0032] and [0121] of the specification.

Schmidt, Wysopal, and Neystadt; and Claim 20 was rejected under 35 U.S.C. § 103(a) as unpatentable over Helman in view of "Windows Management Instrumentation: Create WMI Providers to Notify Applications of System Events" (hereinafter "MSDN") and Wootton.

Applicants acknowledge with appreciation the courtesy of Examiner Savenkov in granting an interview in this case with Applicants' representative on April 2, 2014, during which time the issues in the outstanding Office Action were discussed as substantially summarized hereinafter and also on the Interview Summary Sheet. No agreement was reached during the interview pending a formal response to the outstanding Office Action.

In regard to the rejection of Claim 20 under 35 U.S.C. § 112, first paragraph, page 6 of outstanding Office Action asserts that the claimed "transient operating states and transient states are believed to not be defined in Applicant's specification." Applicants respectfully disagree. As explained during the interview, these terms are described at, for example, paragraphs [0040], [0065], [0068], [0078], and [0083] of the specification. Specifically, paragraph [0040] of the specification describes that behavior deviations from a baseline healthy operational state to a vulnerable or compromised state may be detected. As this portion of the specification describes detecting behavior deviations form a healthy operational state to a vulnerable or healthy state, support is given for the feature of observing transient (i.e. changing) states/operating states, as recited in Claim 20. Paragraph [0068] of the specification describes that "temporal events 409 can be expressed as assertions about operational parameters (e.g.,

vulnerabilities, compliance, patch level, etc.) based on enterprise policies established for a baseline configuration. The trust broker 407 serves as a moderator that aggregates endpoint operational state measurements for situation awareness and threat identification by the trust orchestrator 430." As this paragraph of the specification describes that the trust broker 407 aggregates (and hence obtains) endpoint operational state measurements for threat identification, Applicants respectfully submit that adequate support is given for the feature of observing transient (i.e. changing) states/operating states, as recited in Claim 20.

Accordingly, Applicants respectfully request that the rejection of Claim 20 under 35 U.S.C. § 112, first paragraph, be withdrawn.

In response to the rejections under 35 U.S.C. § 103(a), Applicants have amended Claim 1 to include, *inter alia*, features of former Claim 2. Applicants respectfully submit that amended Claim 1 recites novel features not taught or rendered obvious by the applied references.

By way of background, independent Claim 1 is directed to a method of providing an attestation service for providing runtime operational integrity of a system using a computing platform comprising a network trust agent, and endpoint trust agent, and a trust orchestration server, the method including:

> ***sending, by the endpoint trust agent on a monitored device, a dynamic context including endpoint events and actions of the monitored device and applications executing on the monitored device at runtime;***
>
> ***receiving, at the trust orchestration server, the dynamic context including the endpoint events of the***

monitored device and the applications executing on the monitored device at runtime;

analyzing, by the trust orchestration server, the received endpoint events;

receiving, by the trust orchestration server, third party network endpoint assessments;

generating, by the trust orchestration server, temporal events based at least in part on analyzing the third party network endpoint assessments;

correlating, by the trust orchestration server, the received endpoint events and the generated temporal events; and

generating, by the trust orchestration server, an integrity profile for the system.

Independent Claims 8 and 20, although varying in claim scope and/or statutory class, recite similar features as Claim 1. Thus, the arguments presented below with respect to Claim 1 are also applicable to independent Claims 8 and 20.

Turning now to the applied references, page 10 of the outstanding Office Action acknowledges that Helman and Neystadt do "not disclose...applications executing thereon." In an attempt to cure the above-noted deficiencies of Helman and Neystadt, the outstanding Office Action cites paragraphs [0040], [0049], and [0052] of Wootton.

However, as explained during the interview, Applicants respectfully submit that Wootton fails to teach or suggest "sending, by the endpoint trust agent on a monitored device, a dynamic context including ***endpoint events and actions of the monitored device and applications executing on the monitored device at runtime***; receiving, at the trust orchestration server, the dynamic context including the endpoint events of

the monitored device and the applications executing on the monitored device at runtime," as recited in Claim 1.

Wootton is directed to storing application programs for mobile communications devices in a data store. The applications may be collected from any number of different sources, such as through an application programming interface (API), from web crawling, from users, or combinations of these. The applications are analyzed and the analysis results reported.[2] Thus, Wootton describes API analysis, not the analysis of actions of an application executing on a monitored device at runtime, as in Applicants' amended Claim 1.

Paragraph [0040] of Wootton states:

> In an embodiment, application data also includes behavioral data. Behavioral data includes information about how an application interacts with or uses a mobile communication device's resources, such as memory usage, battery usage, network usage, storage usage, CPU usages, API usage, errors and crashes, network services connected to (e.g., remote host address and port), and runtime library linkage. Behavioral data also includes information about how an application, file or data object, when it is run, utilizes the functionalities of the mobile communication device's operating system, such as notifications and messaging between processes or installed applications.

Hence, the above paragraph of Wootton describes that the application data includes behavioral data, and the behavioral data includes information about how an application interacts with or uses a mobile communication device's resources, such as memory usage, battery usage, network usage, storage usage, CPU usages, API usage, errors and crashes, network services connected to (e.g., remote host address and port),

[2] See the Abstract of Wootton.

and runtime library linkage. However, the above paragraph does not describe that an endpoint trust agent (that is on the monitored device) sends a dynamic context including endpoint events and actions of the monitored device and applications running on the monitored device at runtime, and that a trust orchestration server receives the sent dynamic contest including the endpoint events and the actions of the monitored device and applications running on the monitored device at runtime. Wootton describes the use of a whitelist, a blacklist, and static/dynamic analysis to evaluate data.[3] However, in Wootton, there is no live correlation of application actions on a device, instead behavioral data is collected from an emulator running the application and it is heuristics based.[4]

Thus, Applicants respectfully submit that independent Claims 1, 8, and 20 (and all claims depending thereon) patentably distinguish over Helman, Neystadt, and Wootton.

Similarly, the Alperovitch, Schmidt, MSDN, and Wysopal references cited in the rejections of Claims 8-13 and 17-20 likewise fail to cure the deficiencies of Helman, Neystadt and Wootton.

Accordingly, Applicants respectfully request that the rejections under 35 U.S.C. § 103(a) be withdrawn.

Consequently, in view of the present amendment, and in light of the above discussion, the pending claims as presented herewith are believed to be in condition for

[3] See paragraph [0146] of Wootton.
[4] See paragraphs [0132] and [0234] of Wootton.

formal allowance, and an early and favorable action to that effect is respectfully requested.

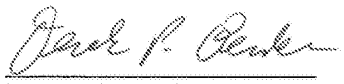
If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

If additional fees are required for any reason, please charge Deposit Account No. 02-4800 the necessary amount.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: April 14, 2014

By: 
Derek P. Benke
Registration No. 56,944

Customer No. 21839
703-836-6620

Patent
Attorney Docket No. 0079152-000016

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	**MAIL STOP**
Kumar, Srinivas et al.	Group Art Unit: 2431
Application No.: 13/559,766	Examiner: SAVENKOV, Vadim
Filed: July 27, 2012	Confirmation No.: 9330
For: Systems and Methods for Threat Identification and Remediation	

INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Madam:

In accordance with the duty of disclosure as set forth in 37 C.F.R. § 1.56, the accompanying information is being submitted in accordance with 37 C.F.R. §§ 1.97 and 1.98.

Pursuant to 37 C.F.R. § 1.98, a copy of each of the documents cited is enclosed. However, copies of the listed U.S. patents and U.S. patent application publications are not enclosed since it is no longer required.

The information is submitted before the mailing of a first Office Action after the filing of a Request for Continued Examination under 37 C.F.R. § 1.114. Continued examination is requested and the fee required under 37 C.F.R. § 1.17(e) accompanies the present submission.

To assist the Examiner, the documents are listed on the attached form PTO-1449. It is respectfully requested that an Examiner initialed copy of this form be returned to the undersigned.

The Director is hereby authorized to charge any appropriate fees under 37 C.F.R. §§ 1.16, 1.17 and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 02-4800.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: April 14, 2014

By: _____
Derek P. Benke
Registration No. 56,944

Customer No. 21839
703 836 6620

Substitute for PTO/SB/08a&b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO				*Complete if Known*	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Application Number*	**13/559,766**
				Filing Date	**July 27, 2012**
				First Named Inventor	**Kumar, Srinivas**
				Art Unit	**2431**
(Use as many sheets as necessary)				*Examiner Name*	**SAVENKOV, Vadim**
Sheet	1	of	3	*Attorney Docket Number*	**0079152-000016**

U.S. PATENT DOCUMENTS

Examiner Initials'	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-6,091,835	7/18/2000	Smithies et al.	
		US-6,507,904 B1	1/14/2003	Ellison et al.	
		US-6,760,441 B1	7/6/2004	Ellison et al.	
		US-6,990,579 B1	1/24/2006	Herbert et al.	
		US-6,996,710 B1	2/7/2006	Ellison et al.	
		US-7,013,481 B1	3/14/2006	Ellison et al.	
		US-7,194,759 B1	3/20/2007	Chess et al.	
		US-7,587,607 B2	9/8/2009	Brickell et al.	
		US-7,797,544 B2	9/14/2010	Dillaway et al.	
		US-7,882,221 B2	2/1/2011	Sailer et al.	
		US-7,979,696 B2	7/12/2011	Kim et al.	
		US-7,984,304 B1	7/19/2011	Waldspurger et al.	
		US-8,108,536 B1	1/31/2012	Hernacki et al.	
		US-8,429,454 B2	4/23/2013	Yuan et al.	
		US-2005/0033987 A1	2/10/2005	Yan et al.	
		US-2005/0132202 A1	6/16/2005	Dillaway et al.	
		US-2005/0132031 A1	6/16/2005	Sailer et al.	
		US-2005/0138384 A1	6/23/2005	Brickell et al.	
		US-2005/0204404 A1	9/15/2005	Hrabik et al.	
		US-2005/0221766 A1	10/6/2005	Brizek et al.	
		US-2005/0283660 A1	12/22/2005	McKeen et al.	
		US-2006/0005009 A1	1/5/2006	Ball et al.	
		US-2006/0200680 A1	9/7/2006	Ellison et al.	
		US-2007/0005992 A1	1/4/2007	Schluessler et al.	
		US-2007/0185856 A1	8/9/2007	Mittal et al.	
		US-2008/0015808 A1	1/17/2008	Wilson et al.	
		US-2008/0083039 A1	4/3/2008	Choi et al.	
		US-2008/0141027 A1	6/12/2008	Kim et al.	
		US-2008/0235372 A1	9/25/2008	Sailer et al.	
		US-2008/0289028 A1	11/20/2008	Jansen et al.	
		US-2009/0172814 A1	7/2/2009	Khosravi et al.	
		US-2009/0178138 A1	7/9/2009	Weiss et al.	
		US-2009/0187988 A1	7/23/2009	Hulten et al.	
		US-2009/0204806 A1	8/13/2009	Kanemura et al.	
		US-2009/0204964 A1	8/13/2009	Foley et al.	
		US-2010/0281273 A1	11/4/2010	Lee et al.	
		US-2011/0035577 A1	2/10/2011	Lin et al.	
		US-2011/0154500 A1	6/23/2011	Sahita et al.	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Substitute for PTO/SB/08a&b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO				*Complete if Known*	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Application Number*	**13/559,766**
				Filing Date	**July 27, 2012**
				First Named Inventor	**Kumar, Srinivas**
				Art Unit	**2431**
(Use as many sheets as necessary)				*Examiner Name*	**SAVENKOV, Vadim**
Sheet	2	of	3	*Attorney Docket Number*	**0079152-000016**

U.S. PATENT DOCUMENTS					
Examiner Initials'	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-2011/0173643 A1	7/14/2011	Nicolson et al.	
		US-2011/0179477	7/21/2011	Starnes et al.	
		US-2011/0185423 A1	7/28/2011	Sallam	
		US-2012/0084850 A1	4/5/2012	Novak et al.	
		US-2012/0131334 A1	5/24/2012	Haikney et al.	
		US-2012/0284282 A9	11/8/2012	Ghosh et al.	

FOREIGN PATENT DOCUMENTS						
Examiner Initials'	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code [5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		December 5, 2013 Office Action issued in U.S. Application No. 13/559,665.	
		December 10, 2013 Office Action issued in U.S. Application No. 13/559,732.	
		October 23, 2013 Office Action issued in U.S. Application No. 13/559,692.	
		June 20, 2013 Office Action issued in U.S. Application No. 13/559,732.	
		July 18, 2013 Office Action issued in U.S. Application No. 13/559,766.	
		Event Tracker ver 7.0 Enterprise Users Guide. "Event Tracker ver 7.0 Enterprise User's; Guide. Prism Microsystems, 28 July 2010. Web. 29 Nov. 2013 <http://www.eventtracker.com/wp-content/uploads/EventTracker-v7.0-Enterprise-User-Guide.pdf>.	
		Statement of FIPS 140-2 Compliance. "Statement of FIPS 140-2 Compliance. Prism Microsystems, 6 Oct. 2010. Web 29 Nov. 2010. ,http://www.eventtracker.com/wp-content/uploads/2013/01/EventTracker_v7.0_FIPS_Compliance.pdf>.	
		Trend Micro, Inc.. "OfficeScan 10 Administrator/s Guide." docs.trendmicro.com/all/ent/officescan/v10.0/en-us/osce_10.0_ag.pdf. N.p. 20 Apr. 2009. Web. 27 Nov. 2013 http://docs.trendmicro.com/all/ent/officescan/v10.0/en-us/osce_10.0_ag.pdf.	
		August 27, 2012 International Search Report issued in PCT/US2012/025551.	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Substitute for PTO/SB/08a&b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO				***Complete if Known***	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Application Number*	**13/559,766**
				Filing Date	**July 27, 2012**
				First Named Inventor	**Kumar, Srinivas**
				Art Unit	**2431**
(Use as many sheets as necessary)				*Examiner Name*	**SAVENKOV, Vadim**
Sheet	3	of	3	*Attorney Docket Number*	**0079152-000016**

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		August 27, 2012 Written Opinion issued in PCT/US2012/025551.	
		August 21, 2013 International Preliminary Report on Patentability issued in PCT/US2012/025551.	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	FOR FURTHER ACTION	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
0079152-0003		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2012/025551	**17 FEBRUARY 2012 (17.02.2012)**	17 FEBRUARY 2011 (17.02.2011)

Applicant

TAASERA, INC. et al

This International search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of **3** sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language**, the international search was carried out on the basis of :
      ☒ the international application in the language in which it was filed
      ☐ a translation of the international application into _____ , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).
   c. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.
2. ☐ **Certain claims were found unsearchable** (See Box No. II)
3. ☐ **Unity of invention is lacking** (See Box No. III)
4. With regard to the **title,**
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:
5. With regard to the **abstract,**
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.
6. With regard to the drawings,
   a. the figure of the **drawings** to be published with the abstract is Figure No. **1**
      ☒ as suggested by the applicant.
      ☐ as selected by this Authority, because the applicant failed to suggest a figure.
      ☐ as selected by this Authority, because this figure better characterizes the invention.
   b. ☐ none of the figure is to be published with the abstract.

IPR2023-01466
CrowdStrike EX1002 Page 111

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2012/025551

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/22(2006.01)i, G06F 9/44(2006.01)i, H04L 9/32(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 21/22; G06F 15/16; G06F 15/173; G06F 9/44; G06F 17/60

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords: application, attestation, runtime, execute, server, remote, security, digital, sign, authentication

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2007-0143474 A1 (MAO XIN SHENG et al.) 21 June 2007 See paragraphs [0024] - [0054]; figures 3-5.	1-26
A	US 2005-0289072 A1 (VINAY SABHARWAL) 29 December 2005 See paragraphs [0110] - [0214]; figures 1,3.	1-26
A	US 2009-0094584 A1 (DHEAP VIJAY et al.) 09 April 2009 See paragraphs [0017] - [0036]; figure 1-2.	1-26
A	US 2007-0174406 A1 (CAMERON CRAIG MORRIS et.al) 26 July 2007 See paragraphs [0033] - [0041], [0055] - [0067]; figures 2,4.	1-26

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 JULY 2012 (30.07.2012)	**27 AUGUST 2012 (27.08.2012)**

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

Shin Sang Gil

Telephone No. 82-42-481-8480

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2012/025551

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007-0143474 A1	21.06.2007	None	
US 2005-0289072 A1	29.12.2005	None	
US 2009-0094584 A1	09.04.2009	None	
US 2007-0174406 A1	26.07.2007	EP 1818850 A1 US 7574479 B2	15.08.2007 11.08.2009

IPR2023-01466
CrowdStrike EX1002 Page 113

PCT/US2012/025551

URGENT

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:

WIELAND CHARLES F., III

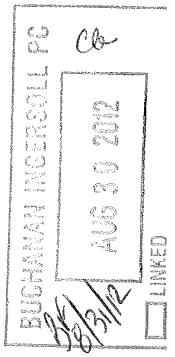
BUCHANAN INGERSOLL & ROONEY PC P. O. BOX 1404
ALEXANDRIA VA 22313-1404 USA

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

	Date of mailing *(day/month/year)* 27 AUGUST 2012 (27.08.2012)
Applicant's or agent's file reference 0079152-0003	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. **PCT/US2012/025551**	International filing date *(day/month/year)* **17 FEBRUARY 2012 (17.02.2012)**
Applicant **TAASERA, INC. et al**	



1. ☒ The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:

   The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Facsimile No.: +41 22 338 82 70

   For more detailed instructions, see *PCT Applicant's Guide*, International Phase, paragraphs 9.004 . 9.011.

2. ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. ☐ **With regard to any protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with any request to forward the texts of both the protest and the decision thereon to the designated Offices.

   ☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.

Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before the completion of the technical preparations for international publication (Rules 90bis.1 and 90bis.3).

Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.
In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19months.

For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the PCT Applicant's Guide, National Chapters.

Name and mailing address of the ISA/KR Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea	Authorized officer COMMISSIONER
Facsimile No. 82-42-472-7140	Telephone No. 82-42-481-8754

Form PCT/ISA/220 (July 2010)

* Attention

Copies of the documents cited in the international search report can be searched in the following Korean Intellectual Property Office English website for three months from the date of mailing of the international search report.

http://www.kipo.go.kr/en/ => PCT Services => PCT Services

ID : PCT international application number
PW : **9BZF99MH**

Inquiries related to PCT International Search Report or Written Opinion prepared by KIPO as an International Searching Authority can be answered not only by KIPO but also through IPKC (Intellectual Property Korea Center), located in Vienna, VA, which functions as a PCT Help Desk for PCT applicants.

Homepage: http://www.ipkcenter.com
Email: ipkc@ipkcenter.com
Phone: +1 703 388 1066
Fax: +1 703 388 1084

Notes to Form PCT/ISA/220 (July 2010)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	FOR FURTHER ACTION	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
0079152-0003		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2012/025551	**17 FEBRUARY 2012 (17.02.2012)**	17 FEBRUARY 2011 (17.02.2011)
Applicant		
TAASERA, INC. et al		

This International search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 3 sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language**, the international search was carried out on the basis of:
      ☒ the international application in the language in which it was filed
      ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).
   c. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.
2. ☐ **Certain claims were found unsearchable** (See Box No. II)
3. ☐ **Unity of invention is lacking** (See Box No. III)
4. With regard to the **title,**
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:
5. With regard to the **abstract,**
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.
6. With regard to the drawings,
   a. the figure of the **drawings** to be published with the abstract is Figure No. 1
      ☒ as suggested by the applicant.
      ☐ as selected by this Authority, because the applicant failed to suggest a figure.
      ☐ as selected by this Authority, because this figure better characterizes the invention.
   b. ☐ none of the figure is to be published with the abstract.

IPR2023-01466
CrowdStrike EX1002 Page 116

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2012/025551

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/22(2006.01)i, G06F 9/44(2006.01)i, H04L 9/32(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 21/22; G06F 15/16; G06F 15/173; G06F 9/44; G06F 17/60

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords: application, attestation, runtime, execute, server, remote, security, digital, sign, authentication

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2007-0143474 A1 (MAO XIN SHENG et al.) 21 June 2007 See paragraphs [0024] - [0054]; figures 3-5.	1-26
A	US 2005-0289072 A1 (VINAY SABHARWAL) 29 December 2005 See paragraphs [0110] - [0214]; figures 1,3.	1-26
A	US 2009-0094584 A1 (DHEAP VIJAY et al.) 09 April 2009 See paragraphs [0017] - [0036]; figure 1-2.	1-26
A	US 2007-0174406 A1 (CAMERON CRAIG MORRIS et.al) 26 July 2007 See paragraphs [0033] - [0041], [0055] - [0067]; figures 2,4.	1-26

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 JULY 2012 (30.07.2012)	**27 AUGUST 2012 (27.08.2012)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer Shin Sang Gil Telephone No. 82-42-481-8480

Form PCT/ISA/210 (second sheet) (July 2009)

IPR2023-01466
CrowdStrike EX1002 Page 117

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2012/025551

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007-0143474 A1	21.06.2007	None	
US 2005-0289072 A1	29.12.2005	None	
US 2009-0094584 A1	09.04.2009	None	
US 2007-0174406 A1	26.07.2007	EP 1818850 A1 US 7574479 B2	15.08.2007 11.08.2009

Form PCT/ISA/210 (patent family annex) (July 2009)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
WIELAND CHARLES F., III

BUCHANAN INGERSOLL & ROONEY PC P. O. BOX
1404 ALEXANDRIA VA 22313-1404 USA

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

Date of mailing *(day/month/year)*	**27 AUGUST 2012 (27.08.2012)**
Applicant's or agent's file reference 0079152-0003	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2012/025551	**17 FEBRUARY 2012 (17.02.2012)**	17 FEBRUARY 2011 (17.02.2011)

International Patent Classification (IPC) or both national classification and IPC

G06F 21/22(2006.01)i, G06F 9/44(2006.01)i, H04L 9/32(2006.01)i

Applicant

TAASERA, INC. et al

1. This opinion contains indications relating to the following items:

- [X] Box No. I Basis of the opinion
- [ ] Box No. II Priority
- [ ] Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- [ ] Box No. IV Lack of unity of invention
- [X] Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- [ ] Box No. VI Certain documents cited
- [ ] Box No. VII Certain defects in the international application
- [ ] Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.
For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/KR	Date of completion of this opinion	Authorized officer
Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. 82-42-472-7140	30 JULY 2012 (30.07.2012)	Shin Sang Gil Telephone No.82-42-481-8480

Form PCT/ISA/237 (cover sheet) (July 2011)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/025551

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed

   ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of:

   a. a sequence listing filed or furnished
      ☐ on paper
      ☐ in electronic form

   b. time of filing or furnishing
      ☐ contained in the international application as filed.
      ☐ filed together with the international application in electronic form.
      ☐ furnished subsequently to this Authority for the purposes of search.

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additioanl copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

IPR2023-01466
CrowdStrike EX1002 Page 120

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/025551

Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

I. Statement

Novelty (N)	Claims	1-26	YES
	Claims	NONE	NO
Inventive step (IS)	Claims	1-26	YES
	Claims	NONE	NO
Industrial applicability (IA)	Claims	1-26	YES
	Claims	NONE	NO

2. Citations and explanations :

Reference is made to the following documents:

D1: US 2007-0143474 A1 (MAO XIN SHENG et al.) 21 June 2007
D2: US 2005-0289072 A1 (VINAY SABHARWAL) 29 December 2005
D3: US 2009-0094584 A1 (DHEAP VIJAY et al.) 09 April 2009
D4: US 2007-0174406 A1 (CAMERON CRAIG MORRIS et.al) 26 July 2007

1. Novelty and Inventive Step

1.1. Claims 1-12

The subject matter of claim 1 differs from these prior art documents in that the method of claim 1 includes steps of generating, by an attestation server, a report indicating security risks associated with an application based on a received runtime execution context and a received security context, as an attestation result; and sending, by the attestation server, the attestation result associated with the application. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore claim 1 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 2-12 are dependent on claim 1 and therefore meet the requirements of PCT Article 33(2) and (3).

1.2. Claims 13-16

The subject matter of claim 13 differs from these prior art documents in that the non-transitory computer readable medium of claim 13 includes step of receiving and validating, by the attestation server form a server in a client server transaction or from a first peer in a peer-to-peer transaction, the first application artifact sent by the attestation server to a client in a client server transaction or to a second peer in the peer-to-peer transaction. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore claim 13 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

(Continued on Supplemental Box)

IPR2023-01466
CrowdStrike EX1002 Page 121

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of :

Box V

Claims 14-16 are dependent on claim 13 and therefore meet the requirements of PCT Article 33(2) and (3).

1.3. Claims 17-20
The subject matter of claim 17 differs from these prior art documents in that the method of claim 17 includes steps of generating assertions based on a received security context and a received local execution context; transmitting confidence metrics in a report to an identity provider; and providing attestation of a running web application or web servlet as a digital icon for rendering by a web browser. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore claim 17 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 18-20 are dependent on claim 17 and therefore meet the requirements of PCT Article 33(2) and (3).

1.4. Claim 21-26
The subject matter of claim 21 differs from these prior art documents in that the system of claim 21 includes steps of requesting and receiving dynamic assertions form a metadata repository of an attestation service, a dynamic assertions pertaining to a local execution context an introspected security context of running application instances on instrumented target platforms; continuously displaying the dynamic assertions to a system administrator. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore claim 21 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 22-26 are dependent on claim 21 and therefore meet the requirements of PCT Article 33(2) and (3).

2. Industrial Applicability
Claims 1-26 are industrially applicable under PCT Article 33(4).

IPR2023-01466
CrowdStrike EX1002 Page 122

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY
(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44*bis*)

Applicant's or agent's file reference 0079152-0003	**FOR FURTHER ACTION**	See item 4 below
International application No. PCT/US2012/025551	International filing date *(day/month/year)* 17 February 2012 (17.02.2012)	Priority date *(day/month/year)* 17 February 2011 (17.02.2011)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant TAASERA, INC.		

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 *bis*.1(a).

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.

3. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44*bis*.3(c) and 93*bis*.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44*bis* .2).

	Date of issuance of this report 21 August 2013 (21.08.2013)
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70	Authorized officer Yukari Nakamura e-mail: pt07.pct@wipo.int

Form PCT/IB/373 (January 2004)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
WIELAND CHARLES F., III

BUCHANAN INGERSOLL & ROONEY PC P. O. BOX
1404 ALEXANDRIA VA 22313-1404 USA

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

Date of mailing *(day/month/year)*	**27 AUGUST 2012 (27.08.2012)**
Applicant's or agent's file reference 0079152-0003	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2012/025551	**17 FEBRUARY 2012 (17.02.2012)**	17 FEBRUARY 2011 (17.02.2011)

International Patent Classification (IPC) or both national classification and IPC

G06F 21/22(2006.01)i, G06F 9/44(2006.01)i, H04L 9/32(2006.01)i

Applicant

TAASERA, INC. et al

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.
For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/KR	Date of completion of this opinion	Authorized officer
Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. 82-42-472-7140	30 JULY 2012 (30.07.2012)	Shin Sang Gil Telephone No.82-42-481-8480

Form PCT/ISA/237 (cover sheet) (July 2011)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/025551

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of :

   ☒ the international application in the language in which it was filed

   ☐ a translation of the international application into _____ , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of:

   a. a sequence listing filed or furnished
      ☐ on paper
      ☐ in electronic form

   b. time of filing or furnishing
      ☐ contained in the international application as filed.
      ☐ filed together with the international application in electronic form.
      ☐ furnished subsequently to this Authority for the purposes of search.

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additioanl copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

IPR2023-01466
CrowdStrike EX1002 Page 125

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/025551

Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-26	YES
	Claims	NONE	NO
Inventive step (IS)	Claims	1-26	YES
	Claims	NONE	NO
Industrial applicability (IA)	Claims	1-26	YES
	Claims	NONE	NO

2. Citations and explanations :

Reference is made to the following documents:

D1: US 2007-0143474 A1 (MAO XIN SHENG et al.) 21 June 2007
D2: US 2005-0289072 A1 (VINAY SABHARWAL) 29 December 2005
D3: US 2009-0094584 A1 (DHEAP VIJAY et al.) 09 April 2009
D4: US 2007-0174406 A1 (CAMERON CRAIG MORRIS et.al) 26 July 2007

1. Novelty and Inventive Step

1.1. Claims 1-12

The subject matter of claim 1 differs from these prior art documents in that the method of claim 1 includes steps of generating, by an attestation server, a report indicating security risks associated with an application based on a received runtime execution context and a received security context, as an attestation result; and sending, by the attestation server, the attestation result associated with the application. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore claim 1 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 2-12 are dependent on claim 1 and therefore meet the requirements of PCT Article 33(2) and (3).

1.2. Claims 13-16

The subject matter of claim 13 differs from these prior art documents in that the non-transitory computer readable medium of claim 13 includes step of receiving and validating, by the attestation server form a server in a client server transaction or from a first peer in a peer-to-peer transaction, the first application artifact sent by the attestation server to a client in a client server transaction or to a second peer in the peer-to-peer transaction. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore claim 13 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

(Continued on Supplemental Box)

IPR2023-01466
CrowdStrike EX1002 Page 126

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of :

Box V

Claims 14-16 are dependent on claim 13 and therefore meet the requirements of PCT Article 33(2) and (3).

1.3. Claims 17-20
The subject matter of claim 17 differs from these prior art documents in that the method of claim 17 includes steps of generating assertions based on a received security context and a received local execution context; transmitting confidence metrics in a report to an identity provider; and providing attestation of a running web application or web servlet as a digital icon for rendering by a web browser. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore claim 17 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 18-20 are dependent on claim 17 and therefore meet the requirements of PCT Article 33(2) and (3).

1.4. Claim 21-26
The subject matter of claim 21 differs from these prior art documents in that the system of claim 21 includes steps of requesting and receiving dynamic assertions form a metadata repository of an attestation service, a dynamic assertions pertaining to a local execution context an introspected security context of running application instances on instrumented target platforms; continuously displaying the dynamic assertions to a system administrator. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore claim 21 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 22-26 are dependent on claim 21 and therefore meet the requirements of PCT Article 33(2) and (3).

2. Industrial Applicability
Claims 1-26 are industrially applicable under PCT Article 33(4).

IPR2023-01466
CrowdStrike EX1002 Page 127

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/559,766	Filing Date 07/27/2012	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)		
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	04/14/2014	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0	X $40 =	0
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $210 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	0

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/PARTHENIA D. MERRILL/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/559,766	07/27/2012	Srinivas KUMAR	0079152-000016	9330

21839 7590 04/07/2014
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
SAVENKOV, VADIM	
ART UNIT	**PAPER NUMBER**
2431	

NOTIFICATION DATE	DELIVERY MODE
04/07/2014	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPDOC1@BIPC.com

Applicant-Initiated Interview Summary	Application No.	Applicant(s)	
	13/559,766	KUMAR ET AL.	
	Examiner	Art Unit	
	VADIM SAVENKOV	2431	

All participants (applicant, applicant's representative, PTO personnel):

(1) *VADIM SAVENKOV*.

(2) *CORDELIA ZECHER*.

(3) *DEREK P. BERKE*.

(4) *SRINIVAS KUMAR*.

Date of Interview: *02 April 2014*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☐ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☒103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1, 8, 20*.

Identification of prior art discussed: *Helman, Wootton*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Examiners, Applicant, and Applicant's representative discussed proposed amendments and potential differences between the prior art of record and said amendments. No agreement was reached. Further discussed was the 112 1st rejection of claim 20, with respect to "transient states" language. Examiners stated that the above mentioned 112 1st rejection may be withdrawn upon consultation with a 112 specialist.

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/V. S./	/CORDELIA ZECHER/
Examiner, Art Unit 2431	Supervisory Patent Examiner, Art Unit 2431

IPR2023-01466
CrowdStrike EX1002 Page 130

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	**MAIL STOP AMENDMENT**
Kumar, Srinivas	Group Art Unit: 2431
Application No.: 13/559,766	Examiner: SAVENKOV, Vadim
Filed: July 27, 2012	Confirmation No.: 9330
For: Systems and Methods for Threat Identification and Remediation	

ASSERTION UNDER 37 C.F.R. § 1.27(c) OF ENTITLEMENT TO CLAIM SMALL ENTITY STATUS

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Madam:

Applicant is entitled to claim status as a small entity. The undersigned is a party authorized to sign under 37 C.F.R. § 1.33(b).

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: March 19, 2014

By: _____
Derek P. Benke
Registration No. 56944

Customer No. 21839
703 836 6620

Electronic Acknowledgement Receipt	
EFS ID:	18518997
Application Number:	13559766
International Application Number:	
Confirmation Number:	9330
Title of Invention:	SYSTEMS AND METHODS FOR THREAT IDENTIFICATION AND REMEDIATION
First Named Inventor/Applicant Name:	Srinivas KUMAR
Customer Number:	21839
Filer:	Derek P. Benke/Shaunna Lloyd
Filer Authorized By:	Derek P. Benke
Attorney Docket Number:	0079152-000016
Receipt Date:	19-MAR-2014
Filing Date:	27-JUL-2012
Time Stamp:	11:16:16
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Assertion of entitlement to small entity status	SMALLENTITY.pdf	282498 c2dc1e3b0cf76f7ee211f90bfe0341af7b49978f	no	1

Warnings:
Information:

Total Files Size (in bytes):	282498

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/559,766	07/27/2012	Srinivas KUMAR	0079152-000016	9330

21839 7590 01/17/2014

BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
SAVENKOV, VADIM	
ART UNIT	**PAPER NUMBER**
2431	

NOTIFICATION DATE	DELIVERY MODE
01/17/2014	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPDOC1@BIPC.com

Office Action Summary	Application No. 13/559,766	Applicant(s) KUMAR ET AL.	
	Examiner VADIM SAVENKOV	Art Unit 2431	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10/1/2013*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-20* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-20* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *7/27/2012* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date *9/19/2013*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

This Office action is in response to the communication which was filed on 10/1/2013.

Claims 1-20 stand rejected.

Information Disclosure Statement

The IDS filed 9/19/2013 has been considered by the examiner.

Priority

On page 16 of Applicant Arguments/Remarks Made in an Amendment, it is stated that Instant application's foreign priority was acknowledged. However, as in the previous Office action, acknowledgement is made of Applicant's claim to provisional Application No. 61/641007, filed 5/1/2012.

Response to Amendment

Regarding the use of trademarks in Applicant's Specification:

Applicant has amended the specification such that the term OpenFlow is replaced with OpenFlow™ and is accompanied by generic terminology. Accordingly, the previously held objection to the specification regarding the use of trademarks is withdrawn.

Regarding minor informalities in Applicant's Specification:

Applicant has amended the specification at paragraphs [0019], [0080], [0116], and [0140] to correct minor typographical errors. Accordingly, the objection to the specification regarding minor informalities is withdrawn.

Regarding the rejection of claims 1-7 under 35 USC 112:

Applicant has amended independent claim 1 to recite that steps central to the respective method claim are performed by a specific device. Claims 2-7 depend upon claim 1. Furthermore, claim 7 has been amended to clarify issues which were previously identified. Accordingly, the previously held rejection of claims 1-7 under 35 USC 112 is withdrawn.

Regarding the rejection of claims 8, 15, and 16 under 35 USC 112:

Applicant has amended claims 8, 15, and 16 to recite generic terminology in place of the term OpenFlow™. Accordingly, the previously held rejection of claims 8, 15, and 16 under 35 USC 112 is withdrawn.

Regarding the rejection of claim 20 under 35 USC 112:

Applicant has amended claim 20 such that proper indentation and recitation identifiers are provided. Accordingly, the previously held rejection of claim 20 under 35 USC 112 is withdrawn.

Response to Arguments

Regarding the objection to claim 8:

Applicant's arguments, see "***Claim Objections***", filed 10/1/2013, with respect to the previously held objection to claim 8 have been fully considered and are persuasive. The objection to claim 8 has been withdrawn.

Regarding the response to Examiner's Comment:

Applicant's statement regarding the dependency of claims 14-16 is noted.

Regarding the rejection of claim 1 and its dependent claims under 35 USC 102:

Applicant's arguments, see "*Independent Claim 1 and Its Dependent Claims Are Allowable Over Helman*", filed 10/1/2013, with respect to the rejection(s) of claim(s) claims 1 and its dependent claims under 35 USC 102(b) have been fully considered and are persuasive with respect to the endpoint events of a monitored device and applications executing thereon. Furthermore, newly added claimed subject matter necessitated different application of prior art. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of **Neystadt** and **Wootton**.

Regarding the rejection of claims 14-16, as noted on pages 25-26 of Arguments/Remarks Made in an Amendment:

Applicant argues that claims 14-16 are allowable by virtue of their dependency on claim 1. However, since claim 1 is held rejected, claims 14-16 are likewise held rejected.

Regarding the rejection of claim 8 and its dependent claims under 35 USC 103(a):

Applicant's arguments, see "*Independent Claim 8 and Its Dependent Claims are Allowable Over Helman and Alperovitch*", filed 10/1/2013, with respect to the rejection(s) of claim(s) 8-10 under 35 USC 103(a) have been fully considered and are persuasive for similar reasons as those expressed with respect to claim 1 above. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of **Wootton**.

Regarding claims the rejection of 11-13 and 17-19 under 35 USC 103(a):

Applicant argues that claims 11-13 and 17-19 are allowable by virtue of their dependency on claim 8. However, since claim 8 is held rejected, claims 11-13 and 17-19 are likewise held rejected.

Regarding the rejection of claim 20 under 35 USC 103(a):

Applicant's arguments, see "*Independent Claim 20 is Allowable Over Helman and MSDN*", filed 10/1/2013, with respect to the rejection(s) of claim(s) 20 under 35 USC 103(a) have been fully considered and are persuasive for similar reasons as those expressed with respect to claim 1 above. Therefore, the rejection has been withdrawn.

However, upon further consideration, a new ground(s) of rejection is made in view of **Wootton**.

Claim Rejections - 35 USC § 112

1. The following is a quotation of the first paragraph of 35 U.S.C. 112(a):

> (a) IN GENERAL.—The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor or joint inventor of carrying out the invention.

The following is a quotation of the first paragraph of pre-AIA 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor of carrying out his invention.

2. Claim 20 is rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor or a joint inventor, or for pre-AIA the inventor(s), at the time the application was filed, had possession of the claimed invention. Claim 20 recites "*a process monitor configured to observe the runtime execution context of applications executing on the computer platforms and* ***transient operating states***" and "*a socket monitor to observe runtime network activities of the applications for* ***transient states***". Said ***transient operating states*** and ***transient states*** are believed to not be defined in Applicant's specification. Although

paragraph [0040] in Applicant's specification does address behavior deviations from a baseline healthy operational state to a vulnerable or compromised state, it is not implicit that there exists a transient operating state. For instance, this paragraph may simply imply that there is a state change from a first healthy operational state to a second vulnerable or compromised state.

Claim Rejections - 35 USC § 103

3. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-7 and 14-16 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over **Helman (US 2009/0328222 A1)** in view of **Neystadt (US 2008/0244748 A1)**; further in view of **Wootton (US 2012/0110174 A1)**.

Regarding claim 1, Helman discloses: ***A method of providing an attestation service for providing runtime operational integrity of a system using a computing platform comprising a network trust agent, an endpoint trust agent, and a trust orchestration server*** (refer to **FIG. 1** and **2** of **Helman** regarding system implementation)***, the method comprising:***

receiving, at the trust orchestration server, a dynamic context including endpoint events <u>of a monitored device</u>;

- Refer to at least **[0060]** and **FIG. 3** of **Helman** regarding the contents which are sent as part of a Security Assessment. As such, the whole of contents expressed in **FIG. 3** may be interpreted as a form of claimed dynamic context. Furthermore, Data such as Failed Login **305** may be interpreted as a form of claimed endpoint event. Finally, the Host Security Endpoint **135 (FIG.1 of Helman)** may be interpreted as a form of claimed trust orchestration server.

analyzing, by the trust orchestration server, the received endpoint events;

- Refer to at least **[0098]** of **Helman** regarding subscribing endpoints applying their specific security expertise through the application of their own correlation rules. Furthermore, it is extremely old and well known in the art to analyze incoming security data, as indicated by **[0047]**-**[0048]** of **Helman**.

receiving<u>, by the trust orchestration server,</u> network endpoint assessments;

- Refer to at least **FIG. 3** of **Helman** regarding content which is received by a subscribing endpoint such as the Host Security Endpoint. Furthermore, refer to Assessment **316** which may be interpreted as a form of claimed endpoint assessment.

generating<u>, by the trust orchestration server,</u> temporal events based at least in part on analyzing the network endpoint assessments;

- Refer to at least **[0007]** and **[0101]** of **Helman** regarding the Host Security Endpoint receiving a Security Assessment interpreted previously as a form of

claimed dynamic context, said dynamic context including both endpoint events and endpoint assessments, wherein the Host Security Endpoint generates one or more additional Security Assessments in turn; said generation encompassing use of data which is local to the Host Security Endpoint. These new assessments are interpreted as a form of claimed temporal events.

correlating, by the trust orchestration server, the received endpoint events and the generated temporal events;

- Refer to at least **[0035]** and **[0098]** of **Helman** regarding combination or correlation of evidence from Security Assessments received from a variety of different sources, and across object types. As in **[0007]** and **[0101]** of **Helman**, these sources and object types may include the Host Security Endpoint.

and generating, by the trust orchestration server, an integrity profile for the system.

- Refer to **FIG. 8A**, **FIG. 11-12**, and **[0110]** of **Helman** regarding actualization of security assessment information for a system which is monitored, wherein the Host Security Endpoint is involved in said actualization.
- Also Refer to **[0037]** of **Helman** regarding a comprehensive centralized view of system context.

Helman does not disclose ***and applications executing thereon; third party network endpoint assessments;*** However, Neystadt in the same field of endeavor discloses: ***third party network endpoint assessments;***

- Refer to at least **FIG. 3** and **[0034]**, **[0038]**, **[0042]**, and **[0058]** of **Neystadt** regarding processing security data by an SE with SAE function (relevant to the Host Security Endpoint of **Helman**) from a variety of sources (**301-304** in **FIG 3** of **Neystadt**, which are interpreted as a form of claimed third party, since they are neither the originating endpoint nor the receiving endpoint) for the purpose of generating security assessments 170.

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to combine the teachings of Helman with the teachings of Neystadt such that the Host Security Endpoint gathers data from third party security endpoints for the purpose of creating a security assessment as in **[0110]** of **Helman**. These teachings are combinable because they both relate to security assessments of security endpoints, and because the teachings of Helman comprise cross-object mapping. One of ordinary skill in the art would have been motivated to combine these teachings for the purpose of increasing the accuracy of published security assessments.

Helman in view of Neystadt does not disclose: ***and applications executing thereon.*** However, Wootton in the same field of endeavor discloses: ***and applications executing thereon;***

- Refer to at least **FIG. 2-7** of **Wootton**, wherein a client mobile device detects a change in a specific data object (**[0049]** of **Wootton**), and sends application data for said data object to a server for evaluation (**[0052]** of **Wootton**), wherein application data may include behavioral data of the data object (**[0040]** of **Wootton**).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to combine the teachings of Helman in view of Neystadt with the teachings of Wootton such that application data such as behavioral data may be transmitted as part of a security assessment. These teachings are combinable because they relate substantially to monitoring a client device on behalf of a server. One of ordinary skill in the art would have been motivated to make this combination for the purpose of more informative security assessments.

Regarding claim 2, Helman-Neystadt-Wootton discloses: ***The method of claim 1, wherein the dynamic context is sent by the endpoint trust agent.***

- Refer to **[0051]-[0056]** of **Helman** regarding exemplary endpoints which are used for generation of a security assessment, said exemplary endpoints comprising hardware and/or software. Furthermore, refer to **FIG. 5** and **[0085]-[0096]** of **Helman**). Software executing on these endpoints may be interpreted as endpoint trust agent(s).

Regarding claim 3, Helman-Neystadt-Wootton discloses: ***The method of claim 1, wherein the third party network endpoint assessments are received from an endpoint assessment service.***

- Refer to **[0051]-[0056]** of **Helman** regarding exemplary endpoints which are used for generation of a security assessment, said exemplary endpoints comprising hardware and/or software. Furthermore, refer to **FIG. 5** and **[0085]-[0096]** of

Helman). Software executing on these endpoints may be interpreted as endpoint assessment service(s).

- Refer to **301**, **302**, **303**, **304** in **FIG. 3**; refer to at least **[0040]** of **Neystadt** with regard to these products being SEs.

Refer to the combination of the teachings of Helman-Neystadt-Wootton in claim 1 above.

Regarding claim 4, Helman-Neystadt-Wootton discloses: ***The method of claim 3, further comprising:***

receiving, by the trust orchestration server, integrity measurement and verification reports from the endpoint assessment service.

- Refer to **[0070]**-**[0078]** of **Helman** regarding exemplary contents of a security assessment. Health information assessments are interpreted as a form of claimed integrity measurement and verification reports.
- Refer to security data **162** in at least **FIG. 3** of **Neystadt**.

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to combine the teachings Helman-Neystadt-Wootton such that security data may be transmitted in the form of a security assessment. These teachings are combinable for substantially the same reasons which were expressed in the rejection of claim 1 above. One of ordinary skill in the art would have been motivated to make this combination for the purpose of standardizing security data transmission in line with the security assessments of both Helman and Neystadt.

Regarding claim 5, Helman-Neystadt-Wootton discloses: ***The method of claim 1, wherein the third party network endpoint assessments are received from one or more collaboration services.***

- Refer to **[0050]** of **Helman** regarding potential additional different types of security products/endpoints that may be utilized by the ESAS system of Helman.

Regarding claim 6, Helman-Neystadt-Wootton discloses: ***The method of claim 5, further comprising:***
receiving, by the trust orchestration server, integrity measurement and verification reports from the one or more collaboration services.

- Refer to **[0050]** of **Helman** regarding potential additional different types of security products/endpoints that may be utilized by the ESAS system of Helman. More specifically, refer to the operational health monitoring and configuration management products and the variety of security evaluation products mentioned.

Regarding claim 7, Helman-Neystadt-Wootton discloses: ***The method of claim 1, wherein the endpoint events of the monitored device are received by a system event correlator of the trust orchestration server from endpoint trust agents,***

- Refer to Security Assessment and Response Engine **240** in **FIG. 2** of **Neystadt**; to **[0038]** of **Neystadt** regarding operation of said engine.

and the temporal events are generated by a trust broker of the trust orchestration server and are received by the system event correlator from the trust broker

- Furthermore, the SARE **240** in **FIG. 2** of **Neystadt** may also serve as a form of the claimed trust broker because it is responsible for generation of assessments as well as for receiving security data (refer to **[0038]** of **Neystadt**).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to combine the teachings of Helman-Neystadt-Wootton such that SARE functionality is present in the Host Security Endpoint of Helman. These teachings are combinable for substantially the same reasons as were expressed in the rejection of claim 1 above. One of ordinary skill in the art would have been motivated to make this combination because the SE with SAE function is substantially similar to the Host Security Endpoint of Helman.

Regarding claim 14, Helman-Neystadt-Wootton discloses: ***The method of claim 1, further comprising:***

generating, by a trust supervisor, one or more tiered remediation actions based on real time warning associated with the operational runtime integrity of applications executing on an infected system;

- Refer to at least **FIG. 11-12** and **[0124]** of **Helman** regarding response policies which vary according to the severity and/or fidelity of security assessments which are published.

receiving, at a remediation controller of the trust orchestrator, the tiered remediation actions;

- The response policies of **Helman** are inherently received by its endpoints since the purpose of said policies is to dictate how said endpoints individually (or together) response to security threats (for instance, see **[0005]** of **Helman**).
- Also refer to **[0036]** of **Neystadt** regarding policies which are received by the SEs.

sending, by the trust orchestrator, to the network trust agent, one or more system warnings pertaining to a network device associated with the one or more tiered remediation actions.

- Refer to **[0060]** of **Neystadt** regarding a security assessment triggering responses in several places. Refer to **[0050]** of Neystadt regarding exemplary such responses.

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to combine the teachings of Helman-Neystadt-Wootton such that the response policies of Helman may be triggered by security assessments. These teachings are combinable for substantially the same reasons as were expressed in the rejection of claim 1 above. One of ordinary skill in the art would have been motivated to make this combination because use of security assessments in triggering responses would reduce need for tailored individual communication to each SE.

Regarding claim 15, Helman-Neystadt-Wootton discloses: ***The method of claim 14, further comprising:***

generating and sending, by the network trust agent, directives to formulate commands for an computer network protocol controller;

- Refer to response policies in **FIG. 11-12** of **Helman** such as "Block All," "Block All IM," "Shut down network port," and "Block IM attachments."

sending, by the computer network protocol controller, rules to computer network protocol enabled network element or switch of the network fabric to divert or block traffic flow to/from the network device; enforcing, by the computer network protocol enabled network element or switch, received access restrictions or controls for the network device.

- Refer to security endpoints enacting said response policies in **FIG. 6-8** and **10** of **Helman**. For instance, the LOB security endpoint in **FIG. 6** temporarily suspends IM traffic while the NAP security endpoint revokes IPSEC certificate and implements port shutdown; **FIG. 7-8** and **10** comprise similar such actions.

Regarding claim 16, Helman-Neystadt-Wootton discloses: ***The method of claim 15, further comprising:***

monitoring and sending, by the trust supervisor, reputation score updates for the network device to the remediation controller;

sending, by the trust orchestrator, system security posture status updates for the network device to the network trust agent; and

generating and sending, by the network trust agent, to the computer network protocol security framework, directives to formulate commands for the computer network protocol controller to restore normal flows to/from the network device.

- Refer to FIG. 17 and to at least [0146]-[0153] of Helman regarding cancellation of security assessments and relevant response policy actions after a manual update is performed.

5. Claims 8-13 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over **Helman (US 2009/0328222 A1)** in view of **Alperovitch (8,214,497 B2)**; further in view of **Wootton (US 2012/0110174 A1)**.

Regarding claim 8, Helman discloses: ***A method of providing flow level remediation to isolate infected or compromised systems and platforms from a computing network fabric using a network trust agent, an endpoint trust agent, and a trust orchestrator, the method comprising:***
generating, by the endpoint trust agent, runtime system integrity alerts regarding execution anomalies and risks based on rulesets and a calculus of risk;

- Refer to at least DATA in **FIG. 3** and **[0060]** of **Helman** regarding generation of alerts based on the current or near-current runtime state of a monitored system. Inherently, this information is generated based on a predetermined ruleset for identifying potential security hazards. Refer to **Table 1** residing between [0063]

and [0064] of **Helman** with respect to both execution anomalies and risks. Finally, refer to **[0096]** of Helman regarding a calculus of risk.

sending, by the endpoint trust agent, runtime system integrity warnings as endpoint events <u>of the endpoint device</u> to the trust orchestrator;

- Security Assessments generated by endpoints are published to the ESAS system at large **([0057]; Helman)**, whereupon they are received by the subscribing Host Security Endpoint **([0051], [0098]; Helman)**. Said Host Security Endpoint may be interpreted as a form of claimed trust orchestrator.

generating, by the trust orchestrator, a system integrity profile for the endpoint <u>device</u> based on analysis of the received endpoint events;

- Refer to at least **[0098]** and **[0101]** of **Helman**, wherein the Host Security Endpoint evaluates the received Security Assessment further in view of its local data and ESAS data about the target endpoint. The new security assessments are interpreted as a form of claimed system integrity profile for the endpoint.

processing and correlating, by the trust orchestrator, one or more of:

a system integrity profile generated based on a calculus of risk,

- The Host Security Endpoint processes and correlates received Security Assessments **([0035], [0098]; Helman)**, which are generated based at least partly on a calculus of risk (as was discussed above, see **[0096]** of **Helman**).

a plurality of temporal events generated based on a normalization and collation of elements in endpoint assessment reports received from a plurality of collaboration services, and

a system infection profile received from a network analyzer;

sending, by the trust orchestrator to the network trust agent, system warnings based on endpoint execution state assessments;

- Refer to **[0037]** of **Helman** regarding an ESAS central server, which is interpreted as a form of the claimed network trust agent. Once the Host Security Endpoint publishes its new Security Assessments **([0102]; Helman)**, they are received by the subscribing ESAS central server **([0037]; Helman)**. The ESAS central server provides a comprehensive view of the history and current status of the enterprise as a whole and of each endpoint.

Helman does not disclose: ***sending, by the network trust agent, messages or directives to computer network protocol security frameworks and/or controllers to apply flow controls based on the received execution state as a threat posture of a connection endpoint.*** However, Alperovitch in the same field of endeavor discloses: ***sending, by the network trust agent, messages or directives to computer network protocol security frameworks and/or controllers to apply flow controls based on the received execution state as a threat posture of a connection endpoint.***

- Refer to **FIG. 10** and **Col. 13-14**, **Lines 51-67** and **1-56** of **Alperovitch**, which regard operation of a reputation based load balancer. A reputation engine of a network security system provides the load balancer with a reputation vector indicating the reputation of an entity. The load balancer directs data transfers based on the reputation vector.

- "***a threat posture of a connection endpoint***" has been interpreted as its reputation, wherein the reputation is based at least in part on the riskiness of association with said endpoint.

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to combine the teachings of Helman's ESAS system with the teachings of Alperovitch regarding load balancing based on received security/risk assessment analogues. These teachings are combinable because they both regard endpoint-agent based network security. One of ordinary skill in the art would have been motivated to combine these teachings for the purpose of more efficiently utilizing security resources.

Helman in view of Alperovitch does not disclose: ***hypothesized by runtime actions and activities of monitored applications executing on an endpoint device.*** However, Wootton in the same field of endeavor discloses: ***hypothesized by runtime actions and activities of monitored applications executing on an endpoint device;***

- Refer to at least **FIG. 2-7** of **Wootton**, wherein a client mobile device detects a change in a specific data object (**[0049]** of **Wootton**), and sends application data for said data object to a server for evaluation (**[0052]** of **Wootton**), wherein application data may include behavioral data of the data object (**[0040]** of **Wootton**). The server sends back an assessment of the data object (for instance, **311** in **FIG. 3** of **Wootton**).
- Refer to at least **[0041]** of **Wootton** regarding assessments.

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to combine the teachings of Helman in view of Alperovitch with the teachings of Wootton such that application data such as behavioral data may be transmitted as part of a security assessment. These teachings are combinable because they relate substantially to monitoring a client device on behalf of a server. One of ordinary skill in the art would have been motivated to make this combination for the purpose of more informative security assessments.

Regarding claim 9, Helman-Alperovitch-Wootton discloses: ***The method of claim 8, wherein the integrity warnings comprise warnings regarding data events and content events; and wherein the endpoint events comprise data events and content events.***

- Refer to **FIG. 3** and at least **[0060]** of **Helman** regarding the context of a Security Assessment. Furthermore, refer to **Table 1** on page 5 of **Helman**.

Regarding claim 10, Helman-Alperovitch-Wootton discloses: ***The method of claim 8, wherein the remediation of an infected system is achieved without adversely reducing the total operating capacity or availability of the computing platform through on-demand instantiation and scaling of workloads.***

- Refer to **Col. 11**, **Lines 7-56** in **Alperovitch** regarding load balancing analysis and remediation of potentially hazardous items based on the reputation of entities associated with said items.

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to combine the teachings of Helman's ESAS system with the teachings of Alperovitch regarding load balancing analysis and remediation of potentially hazardous items. These teachings are combinable for primary the same reasons as expressed in claim 8 above. One of ordinary skill in the art would have been motivated to combine these teachings for the purpose of increasing system efficiency.

Regarding claim 11, Helman-Alperovitch-Wootton discloses: ***The method of claim 10, further comprising forwarding a notification conveying by a service accessed by a user from a mobile computing device*** (Helman does not mention a mobile computing device but it is extremely old and well known in the art that a mobile computing device corresponds to a general computing device) ***an infected or compromised state of a mobile computing device associated with the user*** (refer to the triggering events in **FIG. 6-8**, **10**, **17**, and **19** of **Helman**)***, wherein the notification is one or more of:***

an asynchronous push notification to an account associated with the user;

an email alert message forwarded to an email address associated with the user;

a warning message displayed by a service on a display of the mobile computing device during initiation of a transaction with a service from the mobile computing device.

a short messaging service (SMS) text alert message forwarded to a phone number associated with the mobile computing device;

- If server 151 determines the data object to be undesirable based on universal undesirability characteristics or characteristics for the user, the server transmits a notification… The notification may take a variety of forms, such as an email, SMS message, or user interface dialog displayed on a web page, on a PC, or on a mobile communication device **([0210]; Wootton)**.

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to combine the teachings of Helman-Alperovitch's ESAS system with load balancing with the teachings of Wootton regarding the specificities of a security notification associated with a user. These teachings are combinable because they both regard informing a user of a security issue associated with a computing device. One of ordinary skill in the art would have been motivated to combine these teachings to allow for alternative ways to inform a user of potential security issues.

Regarding claim 12, Helman-Alperovitch-Wootton discloses: ***The method of claim 11, wherein one or more services accessed by a mobile device are configured to be denied or restricted as a remediation action by a service provider.***

- In block 207, mobile communication device 101 receives the notification, and in block 209, the mobile communication device 101 takes action based upon the notification. As will be discussed in more detail below, such actions may include deactivating one or more features or applications on the mobile communication device 101 **([0047]; Wootton)**.

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to combine the teachings of Helman-Alperovitch's ESAS system with load balancing with the teachings of Wootton regarding deactivating features of a mobile device in response to a security issue. These teachings are combinable for substantially the same reasons as expressed in claim 11 above. One of ordinary skill in the art would have been motivated to combine these teachings to reduce the avenues of attack or infection for a potentially hazardous entity.

Regarding claim 13, Helman-Alperovitch-Wootton discloses: ***The method of claim 12, wherein the remediation action is based on the geo-location <u>of the device, user, and associated service accessed by the user</u>.***

- Refer to at least FIG. 11A-C of Alperovitch, as well as their corresponding descriptions in **Col. 14-16**, **Lines 57-19**, regarding geo-location based operational scenarios.

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to combine the teachings of Helman, Alperovitch, and Wootton such that geolocational data is used in determining remediation actions. These teachings are combinable for substantially the same reasons as expressed in claim 11 above. One of ordinary skill in the art would have been motivated to combine these teachings to provide for additional analysis mechanisms and therefore increase security.

6. Claims 17 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over **Helman-Alperovitch-Wootton** as applied to claims 8-13 above, and further in view of "**Static Analysis of Executables for Collaborative Malware Detection on Android**," hereinafter **Schmidt**; further in view of **Wysopal (US 2012/0072968 A1)**.

Regarding claim 17, Helman-Alperovitch-Wootton discloses: ***The method of claim 8, further comprising:***

determining, by the network analyzer, threat behaviors based on network activity correlation and malware detection based on a threat life cycle model;

- Refer to at least **[0035]** and the **Abstract** of **Helman** regarding the capabilities of ESAS-enabled endpoints to determine anomalies based on malware detection and network activity correlation. Refer also to **[0034]** of **Helman** regarding a time-to-live.

Helman-Alperovitch-Wootton does not disclose: ***dispatching, by the trust orchestrator, the image files and attributes of an application for binary analysis, wherein the image files comprise compiled, intermediate, or interpreted code or scripts;***

receiving a result of the binary analysis result identifying malicious activity as a set of threats identified based on the analysis; and caching, by the trust broker, the results of the analysis indexed by a unique identifier for the image; and generating and returning an image profile to the endpoint trust agent comprising

assertions of malicious capabilities of the image to be monitored at runtime for subsequent generation of endpoint events by the endpoint trust agent.

However, Schmidt in the same field of endeavor discloses: ***dispatching, by the trust orchestrator, the image files and attributes of an application for binary analysis, wherein the image files comprise compiled, intermediate, or interpreted code or scripts;***

- Refer to "**B. Creating a Training Set With Readelf**" in **Schmidt** regarding image files and attributes of an application, wherein the image files comprise compiled, intermediate, or interpreted code or scripts. Furthermore, refer to "**IV. CLASSIFY EXECUTABLES BY STATIC ANALYSIS**" in **Schmidt** regarding the specificities of testing said image files and attributes. Finally, refer to at least **Fig. 3** and its corresponding description in **Schmidt** regarding dispatch of said image files and attributes.

receiving a result of the binary analysis result identifying malicious activity as a set of threats identified based on the analysis;

- Refer to the following in the description of **Fig. 3** in **Schmidt**: "V-The initiating node is informed about the results."

Helman-Alperovitch-Wootton in view of Schmidt does not specifically disclose: ***caching, by the trust broker, the results of the analysis indexed by a unique identifier for the image; and***

However, Wysopal in the same field of endeavor discloses:

caching, by the trust broker, the results of the analysis indexed by a unique identifier for the image;

- Refer to at least **[0017]** of **Wysopal** regarding a set of analysis-derived security data which may be associated with the image file using a secure identifier.

Furthermore, while Helman-Alperovitch-Wootton alone does not disclose: ***generating and returning an image profile to the endpoint trust agent comprising assertions of malicious capabilities of the image to be monitored at runtime for subsequent generation of endpoint events by the endpoint trust agent,*** Helman-Alperovitch-Wootton in view of Schmidt and Wysopal discloses this preceding limitation for the following reasons: Helman states that his ESAS-enabled endpoints are liable to enhance the quality of their detection of potential security threats via combination or correlation of published Security Assessments with their local rules **([0035]; Helman)**. Since a combination of the aforementioned prior art would use the publish and subscribe system of Security Assessments disclosed in Helman, then the image file analysis of Helman-Alperovitch-Wootton in view of Schmidt and Wysopal would naturally be published as a Security Assessment following its determination.

As to the distinction between binary and static analysis, refer to **[0013]** of **US 2012/0102458** regarding their interchangeability with regard to obviousness.

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention combine the teachings of Helman-Alperovitch-Wootton with the teachings of Schmidt and the teachings of Wysopal as expressed above. These teachings are combinable because Schmidt concerns distributed malware detection on

devices within a network; as well, the teachings of Wysopal are applicable to the image file and attribute analysis of Schmidt because both concern a form static analysis in use for malware detection. One of ordinary skill in the art would have been motivated to combine the teachings of Helman-Alperovitch-Wootton with the teachings of Schmidt and the teachings of Wysopal for the purpose of extending the network security ESAS system of Helman to use static analysis methods, whose benefits are expressed in the disclosures of both Schmidt and Wyspoal.

7. Claims 18-19 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Helman-Alperovitch-Wootton-Schmidt-Wysopal as applied to claim 17 above, and further in view of **Neystadt (US 2008/0244748 A1)**.

Regarding claim 18, Helman-Alperovitch-Wootton-Schmidt-Wysopal discloses: ***The method of claim 17,***
wherein the dispatch mechanism uses trigger filter expressions that specify a set of criteria that warrant initiation of image analysis such as frequency and volume of requests for analysis associated with the application image across deployed endpoint trust agents.

- The claimed dispatch mechanism which is described above is a form of previously mentioned rulesets inherent to the endpoint security software of Helman.

Helman-Alperovitch-Wootton-Schmidt-Wysopal does not disclose: ***wherein the binary analysis is performed by one or more third party malware analyzers.*** However, Neystadt in the same field of endeavor discloses: ***wherein the binary analysis*** [binary analysis is disclosed by the previous prior art combination; Neystadt is relied upon for its third party analysis] ***is performed by one or more third party malware analyzers;***

- Refer to at least **FIG. 3** and **[0034]**, **[0038]**, **[0042]**, and **[0058]** of **Neystadt** regarding processing security data by an SE with SAE function (relevant to the Host Security Endpoint of **Helman**) from a variety of sources (**301-304** in **FIG 3** of **Neystadt**, which are interpreted as a form of claimed third party, since they are neither the originating endpoint nor the receiving endpoint) for the purpose of generating security assessments 170.

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to combine the teachings of Helman-Alperovitch-Wootton-Schmidt-Wysopal with the teachings of Neystadt such that the Host Security Endpoint gathers data from third party security endpoints for the purpose of creating a security assessment as in **[0110]** of **Helman**. These teachings are combinable because they both relate to security assessments of security endpoints, and because the teachings of Helman comprise cross-object mapping. One of ordinary skill in the art would have been motivated to combine these teachings for the purpose of increasing the accuracy of published security assessments.

Regarding claim 19, it is substantially the same as claim 18 above, but with regard to static and dynamic analysis. Since both static and dynamic analysis are disclosed in the teachings of Helman-Alperovitch-Schmidt-Wysopal in view of Neystadt, claim 19 is rejected for substantially the same reasons as expressed in rejecting claim 18 above.

8. Claim 20 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over **Helman (US 2009/0328222 A1)** in view of "**Windows Management Instrumentation: Create WMI Providers to Notify Applications of System Events**," hereinafter **msdn**; further in view of **Wootton (US 2012/0110174 A1)**.

Regarding claim 20, Helman discloses: ***A system for providing runtime operational integrity by determining execution anomalies and a threat posture of applications executing on computing platforms including mobile devices and client-server systems, the system comprising:***

(i) an endpoint trust agent [Refer to software executing on hardware in FIG. 1 of Helman] ***including:***

a process monitor configured to observe applications, a socket monitor configured to observe runtime network activities of the applications for transient states,

- Refer to at least **Table 1** residing between [0063] and [0064] in **Helman** regarding the multiple types of assessment categories, which inherently imply monitoring of application execution contexts and network activities.

a resource utilization module monitor configured to observe system and platform resources consumed by the applications that may provide evidence of infected systems;

- It is extremely old and well known in the art for anti-malware/IDS/etc. systems to monitor application resource usage. For instance, refer to chapter 2, "Monitoring your system's performance" of "Norton Antivirus Product Manual".

an application integrity module configured to assess operational integrity of based on a ruleset to deem local actions and activities of the application to be at risk;

- Refer to at least **Table 1** residing between [0063] and [0064] in **Helman** regarding the multiple types of assessment categories, namely those referring to detecting that a portion of a system or network is compromised. Inherently, there must be a ruleset to assess a system or network thusly.

a system event correlator configured to correlate system events of the computing platforms to determine a calculus of risk;

- Refer to at least **[0035]** of **Helman** regarding the capability of ESAS-enabled endpoints to combine or correlate evidence from Security Assessments in order to significantly enhance the quality of its detection of potential security incidents, wherein detection is associated with publishing a Security Assessment comprising fidelity and severity ratings **(FIG. 3 and [0060]; Helman)**.

a trust orchestrator configured to orchestrate actionable intelligence based on the calculus of risk by integrating security intelligence about the computing platforms and the applications;

- Refer to **[0098]** and **[0101]** of **Helman** regarding a Host Security Endpoint which receives published Security Assessments and applies its specific security expertise through application of its own correlation rules and locally-available data to trigger an appropriate action.

an endpoint trust sensor configured to measure runtime operational integrity of the computing platforms by evaluating risk based on actions of an application executing on, or a user of, the computing platforms and receiving the raw events from the native machine instrumentation.

- Refer to at least **Table 1** residing between [0063] and [0064] in **Helman** regarding the multiple types of assessment categories, which inherently implies a sensor module which monitors a system for compromise during runtime.

Helman does not specifically disclose: ***wherein native machine instrumentation for the computing platform is configured to (a) represent event subscriptions, call backs, notification mechanisms provided by an operating system (OS) on the computing platforms, and (b) generate raw events; (ii) extended trust instrumentation; (iii) a runtime monitor configured to: subscribe to and receive near real time asynchronous notifications of runtime operation invocations by applications executing on the computer platforms from the extended trust instrumentation, and generate and send dynamic expressions or rules as***

application activity filters linked to runtime operation invocations of running instances of the applications;

However, msdn in the same field of endeavor discloses: ***wherein native machine instrumentation for the computing platform is configured to (a) represent event subscriptions, call backs, notification mechanisms provided by an operating system (OS) on the computing platforms,***

- In **[0077]** of their **Specification**, Applicant states: "In embodiments, the native machine instrumentation 511 can represent any event subscription, callback, notification mechanism provided by the supported operating system (OS) on the device 560 (e.g., MICROSOFTTM WINDOWS® Machine Instrumentation (WMI)."

(b) generate raw events;

- Refer to the **first paragraph** of "**Building an Event Provider**" in **msdn** regarding a WMI event provider that generates events.

(ii) extended trust instrumentation;

- In **[0269]** of their **Specification**, Applicant states: "The extended trust instrumentation 2501 may be layered extensions to native machine instrumentation 610, such as, for example, the WINDOWS® Management Instrumentation (WMI) on MICROSOFTTM WINDOWS® platforms."

(iii) a runtime monitor configured to: subscribe to and receive near real time asynchronous notifications of from the extended trust instrumentation,

- Refer to the **first paragraph** in the **Conclusion** of **msdn** regarding event filters and permanent subscribers which are inherent to WMI.

generate and send dynamic expressions or rules as application activity filters linked to running instances of the applications;

- Refer to the **first paragraph** in the **Conclusion** of **msdn** regarding event filters and permanent subscribers which are inherent to WMI.

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to combine the teachings of Helman's ESAS system with the teachings of msdn regarding the inherencies of WMI. These teachings are combinable for substantially similar reasons as expressed regarding exemplary software in **[0050]** of **Helman**. One of ordinary skill in the art would have been motivated to combine these teachings because of WMI's flexibility and manageability **(second paragraph in the Summary of msdn)**.

Helman in view of msdn does not disclose: ***the runtime execution context of applications executing on the computer platforms and transient operating states; the types and extent of system and platform resources consumed by the applications; operational integrity of a monitored application instance running on an instrumented device based on a ruleset to deem local actions and activities of the application to be at risk; runtime operation invocations by applications executing on the computer platforms; runtime operation invocations of.*** However, Wootton in the same field of endeavor discloses: ***the runtime execution context of applications executing on the computer platforms and transient operating states;***

the types and extent of* system and platform resources consumed by the applications; operational *integrity* of *a monitored application instance running on an instrumented device* based on a ruleset *to deem local actions and activities of the application to be at risk; runtime operation invocations by applications executing on the computer platforms; runtime operation invocations of.

- Refer to at least **[0039]-[0040]** of **Wootton** regarding exemplary types of application data which are monitored and sent for assessment. Furthermore, refer to **[0049]** of **Wootton** regarding exemplary changes in a specific data object which may be detected. As well, refer to **[0066]** of **Wootton** for further exemplary types of application data.

Therefore it would have been obvious to combine the teachings of Helman in view of msdn with the teachings of Wootton such that application data of a specific data object is monitored. These teachings are combinable because they relate substantially to monitoring a client device on behalf of a server. One of ordinary skill in the art would have been motivated to make this combination for the purpose of more informative security assessments.

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to VADIM SAVENKOV whose telephone number is (571)270-5751. The examiner can normally be reached on Monday - Friday 10:00 AM - 6:30 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, ZECHER P. CORDELIA can be reached on (571) 272-7771. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/V. S./
Examiner, Art Unit 2431

/CHRISTOPHER REVAK/
Primary Examiner, Art Unit 2431

Notice of References Cited	Application/Control No. 13/559,766	Applicant(s)/Patent Under Reexamination KUMAR ET AL.	
	Examiner VADIM SAVENKOV	Art Unit 2431	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2008/0244748	10-2008	Neystadt et al.	726/25
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13559766	KUMAR ET AL.
	Examiner	Art Unit
	VADIM SAVENKOV	2431

CPC- SEARCHED		
Symbol	Date	Examiner
H04L63/1433	1/10/2014	VS
G06F21/50,51,52,566	1/10/2014	VS

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	25	7/12/2013	VS
726	22,24	1/10/2014	VS

SEARCH NOTES		
Search Notes	Date	Examiner
See attached EAST search history of all the relevant databases.	7/12/2013	VS
Double Patenting search: Inventor/Assignee in PALM/EAST	7/12/2013	VS
Consulted with SPE Nathan Flynn regarding OPENFLOW claim language.	7/12/2013	VS
Class search of 726/22-25; Word search within and outside of said class/subclasses.	7/12/2013	VS
Forward and Backward citation searching relevant prior art.	7/12/2013	VS
Google and IEEE search for relevant prior art; search history not included.	7/12/2013	VS
See updated EAST search history which is attached.	1/10/2014	VS
CPC searching performed.	1/10/2014	VS
Class/subclass, CPC, text, forward/backward citation searching, various combinations, etc.	1/10/2014	VS
Updated general Google/IEEE search; search history not included.	1/10/2014	VS

INTERFERENCE SEARCH

/V.S./ Examiner.Art Unit 2431	

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

/V.S./ Examiner.Art Unit 2431	

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 9330

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/559,766	07/27/2012	726	2431	0079152-000016

APPLICANTS

INVENTORS

Srinivas KUMAR, Cupertino, CA;
Dennis Pollutro, Clymer, NY;

**** CONTINUING DATA ***************************

This appln claims benefit of 61/641,007 05/01/2012

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****

08/08/2012

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /VADIM SAVENKOV/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		CA	29	20	3

ADDRESS

BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404
UNITED STATES

TITLE

SYSTEMS AND METHODS FOR THREAT IDENTIFICATION AND REMEDIATION

FILING FEE RECEIVED		
1250	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	13559732
Filing Date	2012-07-27
First Named Inventor	Srinivas, KUMAR
Art Unit	2492
Examiner Name	MEJIA, FELICIANO S.
Attorney Docket Number	0079152-000016

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7174566	B2	2007-02-06	YADAV	
	2	7370359	B2	2008-05-06	HRABIK et al.	
	3	8010469	B2	2011-08-30	KAPOOR et al.	
	4	8214497	B2	2012-07-03	ALPEROVITCH et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20060015942	A1	2006-01-19	JUDGE et al.	
	2	20080276317	A1	2008-11-06	CHANDOLA et al.	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.S./

Receipt date: 09/19/2013	Application Number	13559732 13559766 - GAU: 2431
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Filing Date	2012-07-27
	First Named Inventor	Srinivas, KUMAR
	Art Unit	2492
	Examiner Name	MEJIA, FELICIANO S.
	Attorney Docket Number	0079152-000016

	3	20110072506	A1	2011-03-24	LAW et al.	
	4	20110162073	A1	2011-06-30	JESCHKE et al.	
	5	20110276468	A1	2011-11-10	LEWIS et al.	
	6	20120011590	A1	2012-01-12	DONOVAN	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	20110027386	KR	A	2011-03-16	MOZENSOFT INC.		☒

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	International Search Report and Written Opinion dated August 27, 2013, issued in corresponding International Application No. PCT/US2013/039033; 16 pp	☐
	2	Office Action issued in copending U.S. Patent Application No. 13/559,732, mailed June 20, 2013; 32 pp	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.S./

Receipt date: 09/19/2013	Application Number	13559732 13559766 - GAU: 2431
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2012-07-27
	First Named Inventor	Srinivas, KUMAR
	Art Unit	2492
	Examiner Name	MEJIA, FELICIANO S.
	Attorney Docket Number	0079152-000016

EXAMINER SIGNATURE			
Examiner Signature	/Vadim Savenkov/	Date Considered	01/09/2014

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.S./

Receipt date: 09/19/2013	Application Number	13559732	13559766 - GAU: 2431
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Filing Date	2012-07-27	
	First Named Inventor	Srinivas, KUMAR	
	Art Unit	2492	
	Examiner Name	MEJIA, FELICIANO S.	
	Attorney Docket Number	0079152-000016	

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☒ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Jennifer A. Wilson/	Date (YYYY-MM-DD)	2013-09-19
Name/Print	Jennifer A. Wilson	Registration Number	62,604

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.S./

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.S./

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	17	(KUMAR near2 SRINIVAS).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:13
S2	18	(POLLUTRO near2 DENNIS).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:13
S3	33	S1 OR S2	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:14
S4	3	(TAASERA).as.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:14
S5	3	(TAASERA$10).as.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:15
S6	34	S1 OR S2 OR S4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:15
S7	11	S6 AND (attest$6 or risk or fidelity or reputation or vouch$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:15
S8	3	S6 AND (attest$6 or risk or fidelity or	US-PGPUB;	OR	ON	2013/07/02

IPR2023-01466
CrowdStrike EX1002 Page 182

		reputation or vouch$3).clm.	USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			17:15
S9	0	S6 AND openflow.clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:19
S10	0	S6 AND orchestrat$4.clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:20
S11	1	S6 AND integrity.clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:21
S12	2002	726/25.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:23
S13	1095	S12 AND (reputation or attest$6 or integrity or fidelity or risk or trust) AND (assess$4 or scan$4 or evaluat$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:27
S14	818	S12 AND ((reputation or attest$6 or integrity or fidelity or risk or trust) AND (assess$4 or scan$4 or evaluat$4)) WITH (network or device or system or endpoint or computer)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:28
S15	125	S12 AND ((reputation or attest$6 or integrity or fidelity or risk or trust) AND (assess$4 or scan$4 or evaluat$4)) WITH (network or device or system or endpoint or computer) SAME3 (correlat$6 or co-relat$6)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:29
S16	24	S12 AND (endpoint or end-point) near2 (assess$4 or scan$4 or evaluat$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	2013/07/02 17:31

IPR2023-01466
CrowdStrike EX1002 Page 183

			IBM_TDB			
S17	0	S12 AND (temporal adj event)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:31
S18	8	S15 AND S16	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:32
S19	20	("20050289072" | "20070143474" | "20070174406" | "20090094584" | "20090138939" | "20090144818" | "20090241170" | "20090276204" | "20090328186" | "20120216244").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:35
S20	22	("20050289072" | "20070143474" | "20070174406" | "20090094584" | "20090133110" | "20090138939" | "20090144818" | "20090241170" | "20090276204" | "20090328186" | "20120216244").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:35
S21	2	S20 NOT S19	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:35
S22	0	S12 AND openflow	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:38
S23	8	("20040230835" | "20050102534" | "20050257267" | "20060136986" | "20060156408" | "20070150957" | "6530024" | "7178166").PN. OR ("8136164").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2013/07/02 17:39
S24	1	"20080276317"	US-PGPUB; USPAT; USOCR	OR	ON	2013/07/02 17:44
S25	2	"20050044418"	US-PGPUB; USPAT; USOCR	OR	ON	2013/07/02 17:45
S26	582	S12 AND (security or integrity or risk or fidelity) near2 (assessment or report or scan or profile)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	2013/07/02 17:49

IPR2023-01466
CrowdStrike EX1002 Page 184

			IBM_TDB			
S27	383	S12 AND (security or integrity or risk or fidelity) adj (assessment or report or scan or profile)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:49
S28	20	S12 AND (security or integrity or risk or malware or spyware or pestware or virus or rootkit or trojan or worm or hazard$4 or danger$4 or infect$4) adj (vector or trajectory or possibilities or "attack path" or "scenario graph" or "attack graph")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:53
S29	217	S12 AND (security or integrity or risk or malware or spyware or pestware or virus or rootkit or trojan or worm or hazard$4 or danger$4 or infect$4) with (vector or trajectory or possibilities or "attack path" or "scenario graph" or "attack graph")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:53
S30	73	S12 AND (((security or integrity or risk or malware or spyware or pestware or virus or rootkit or trojan or worm or hazard$4 or danger$4 or infect$4) adj (vector or trajectory or possibilities)) or ("attack path" or "scenario graph" or "attack graph"))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:54
S31	103	S12 AND (((security or integrity or risk or malware or spyware or pestware or virus or rootkit or trojan or worm or hazard$4 or danger$4 or infect$4) adj (vector or trajectory or possibilities or condition)) or ("attack path" or "scenario graph" or "attack graph"))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:55
S32	2	"8214497".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:56
S33	509	("20010037311" | "20010049793" | "20020004902" | "20020013692" | "20020016910" | "20020023089" | "20020023140" | "20020026591" | "20020032871" | "20020035683" | "20020042876" | "20020046041" | "20020049853" | "20020051575" | "20020059454" | "20020062368" | "20020078382" | "20020087882" | "20020095492" | "20020112013" | "20020112185" | "20020116627" | "20020120853" | "20020133365" | "20020138416" | "20020138755" | "20020138759" | "20020138762" | "20020143963" | "20020147734" | "20020152399" | "20020165971" | "20020169954" | "20020172367" | "20020178227" | "20020178383" | "20020178410" | "20020188864"	US-PGPUB; USPAT; USOCR	OR	ON	2013/07/02 17:56

IPR2023-01466
CrowdStrike EX1002 Page 185

		"20020194469"	"20020199095"					
		"20030005326"	"20030005331"					
		"20030009554"	"20030009693"					
		"20030009696"	"20030009699"					
		"20030014664"	"20030023692"					
		"20030023695"	"20030023736"					
		"20030023873"	"20030023874"					
		"20030023875"	"20030028803"					
		"20030033516"	"20030033542"					
		"20030041264"	"20030046253"					
		"20030051026"	"20030051163"					
		"20030051168"	"20030055931"					
		"20030061506"	"20030065943"					
		"20030084280"	"20030084320"					
		"20030084323"	"20030084347"					
		"20030088792"	"20030093667"					
		"20030093695"	"20030093696"					
		"20030095555"	"20030097439"					
		"20030097564"	"20030105976"					
		"20030110392"	"20030110396"					
		"20030115485"	"20030115486"					
		"20030123665"	"20030126464"					
		"20030126472"	"20030135749"					
		"20030140137"	"20030140250"					
		"20030145212"	"20030145225"					
		"20030145226"	"20030149887"					
		"20030149888"	"20030152096"					
		"20030154393").PN. OR ("20030154399"						
		"20030154402"	"20030158905"					
		"20030159069"	"20030159070"					
		"20030167308"	"20030167402"					
		"20030172166"	"20030172167"					
		"20030172289"	"20030172291"					
		"20030172292"	"20030172294"					
		"20030172301"	"20030172302"					
		"20030182421"	"20030187936"					
		"20030187996"	"20030204596"					
		"20030204719"	"20030212791"					
		"20030233328"	"20040015554"					
		"20040025044"	"20040054886"					
		"20040058673"	"20040059811"					
		"20040088570"	"20040111519"					
		"20040111531"	"20040122926"					
		"20040139160"	"20040139334"					
		"20040167968"	"20040177120"					
		"20040203589"	"20040205135"					
		"20040221062"	"20040236884"					
		"20040249895"	"20040267893"					
		"20050021738"	"20050021997"					
		"20050052998"	"20050060643"					
		"20050065810"	"20050086300"					
		"20050091319"	"20050091320"					
		"20050102366"	"20050141427"					
		"20050149383"	"20050159998"					
		"20050160148"	"20050192958"					
		"20050198159"	"20050204001"					
		"20050216564"	"20050256866"					
		"20050262209"	"20050262210"					
		"20050262556"	"20060009994"					
		"20060015942"	"20060023940"					
		"20060031314"	"20060031483"					
		"20060036693"	"20060036727"					
		"20060041508"	"20060042483"					
		"20060059238"	"20060095404"					

IPR2023-01466
CrowdStrike EX1002 Page 186

		"20060095586" | "20060123083" | "20060129810" | "20060149821" | "20060155553" | "20060168024" | "20060174337" | "20060179113" | "20060191002" | "20060212925" | "20060212930" | "20060212931" | "20060225136" | "20060230039" | "20060230134" | "20060251068" | "20060253447" | "20060253458" | "20060253582" | "20060253584").PN. OR ("20060277259" | "20070019235" | "20070124803" | "20070130350" | "20070130351" | "20070199070" | "20070214151" | "20080005223" | "20080077517" | "20080091765" | "20080104180" | "20080123823" | "20080159632" | "20080175266" | "20080178259" | "20080178288" | "20090003204" | "20090113016" | "20090122699" | "20090125980" | "20090254499" | "20090254572" | "4289930" | "4384325" | "4386416" | "4532588" | "4713780" | "4754428" | "4837798" | "4853961" | "4864573" | "4951196" | "4975950" | "4979210" | "5008814" | "5020059" | "5051886" | "5054096" | "5105184" | "5119465" | "5144557" | "5144659" | "5144660" | "5167011" | "5210824" | "5210825" | "5235642" | "5239466" | "5247661" | "5276869" | "5278901" | "5283887" | "5293250" | "5313521" | "5319776" | "5355472" | "5367621" | "5377354" | "5379340" | "5379374" | "5404231" | "5406557" | "5414833" | "5416842" | "5418908" | "5424724" | "5479411" | "5481312" | "5483466" | "5485409" | "5495610" | "5509074" | "5511122" | "5513126" | "5513323" | "5530852" | "5535276" | "5541993" | "5544320" | "5550984" | "5550994" | "5557742" | "5572643" | "5577209" | "5602918" | "5606668" | "5608819" | "5608874" | "5619648" | "5621889" | "5632011" | "5638487" | "5644404" | "5657461" | "5673322" | "5675507" | "5675733" | "5677955" | "5694616" | "5696822" | "5706442" | "5708780" | "5708826" | "5710883" | "5727156" | "5740231" | "5742759" | "5742769" | "5745574" | "5751956" | "5758343" | "5764906" | "5768528" | "5771348" | "5778372" | "5781857" | "5781901").PN. OR ("5790789" | "5790790" | "5790793" | "5793763" | "5793972" | "5796942" | "5796948" | "5801700" | "5805719" | "5812398" | "5812776" | "5822526" | "5822527" | "5826013" | "5826014" | "5826022" | "5826029" | "5835087" | "5845084" | "5850442" | "5855020" | "5860068" | "5862325" | "5864852" | "5878230" | "5884033" | "5892825" | "5893114" | "5896499" | "5898836" | "5903723" | "5911776" | "5923846" |				

IPR2023-01466
CrowdStrike EX1002 Page 187

		"5930479" | "5933478" | "5933498" | "5937164" | "5940591" | "5948062" | "5958005" | "5963915" | "5978799" | "5987609" | "5991881" | "5999932" | "6003027" | "6006329" | "6012144" | "6014651" | "6023723" | "6029256" | "6035423" | "6052709" | "6058381" | "6058482" | "6061448" | "6061722" | "6072942" | "6088804" | "6092114" | "6092194" | "6094277" | "6094731" | "6104500" | "6108688" | "6108691" | "6108786" | "6118856" | "6118886" | "6119137" | "6119142" | "6119230" | "6119236" | "6122661" | "6141695" | "6141778" | "6145083" | "6151675" | "6161130" | "6165314" | "6185689" | "6192360" | "6192407" | "6199102" | "6202157" | "6219714" | "6223213" | "6249575" | "6249807" | "6260043" | "6269447" | "6269456" | "6272532" | "6275942" | "6279113" | "6279133" | "6282565" | "6285991" | "6289214" | "6298445" | "6301668" | "6304898" | "6304973" | "6311207" | "6317829" | "6320948" | "6321267" | "6324569" | "6324647" | "6324656" | "6330589" | "6347374" | "6353886" | "6363489" | "6370648" | "6373950" | "6385655" | "6393465" | "6393568" | "6405318" | "6434624" | "6442588" | "6442686" | "6453345" | "6460141").PN. OR ("6470086" | "6487599" | "6487666" | "6502191" | "6516411" | "6519703" | "6539430" | "6546416" | "6546493" | "6550012" | "6574737" | "6578025" | "6609196" | "6650890" | "6654787" | "6675153" | "6681331" | "6687687" | "6697950" | "6701440" | "6704874" | "6711127" | "6711687" | "6725377" | "6732101" | "6732157" | "6735703" | "6738462" | "6742124" | "6742128" | "6754705" | "6757830" | "6760309" | "6768991" | "6769016" | "6772196" | "6775657" | "6792546" | "6880156" | "6892178" | "6892179" | "6892237" | "6895385" | "6907430" | "6910135" | "6928556" | "6941348" | "6941467" | "6968461" | "6981143" | "7051077" | "7089428" | "7092992" | "7117358" | "7143213" | "7152105" | "7155243" | "7164678" | "7254712" | "7272149" | "7272853" | "7349332" | "7376731" | "7385924" | "7460476" | "7461339" | "7496634" | "7522516" | "7543056" | "7545748" | "7610344" | "7617160" | "7620986" | "7644127" | "7730316" | "7739253" | "7870203" | "7899866" | "7937480" | "8079087").PN. OR ("8214497").URPN.				
S34	11	("20040111632" | "20040128543" | "20050193430" | "20070220606" | "6324656" | "6546493" | "6952779" | "6968377" | "7016499" | "7058821" | "7359962").PN. OR ("8272061").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2013/07/02 17:58

IPR2023-01466
CrowdStrike EX1002 Page 188

S35	2	"6742128".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 17:58
S36	77	("5568471" | "6279113" | "6324647" | "6442144").PN. OR ("6742128").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2013/07/02 18:00
S37	10	"20030172294" "7899866"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/02 18:03
S38	1	(US-20090328222-$).did.	US-PGPUB	OR	ON	2013/07/03 16:25
S39	1	S38 AND host with central	US-PGPUB	OR	ON	2013/07/03 16:25
S40	78	lookout.as.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/10 18:32
S41	596	openflow or open-flow	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/10 19:23
S42	9	S41 AND "726".clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/10 19:23
S43	2	2011/0307951	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/10 19:33
S44	291	S41 AND (security or integrity or risk or malware or spyware or pestware or virus or rootkit or trojan or worm or hazard$4 or danger$4 or infect$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/10 19:36
S45	11	S41 AND (security or integrity or risk or malware or spyware or pestware or virus or rootkit or trojan or worm or hazard$4 or danger$4 or infect$4).clm.	US-PGPUB; USPAT; USOCR; FPRS;	OR	ON	2013/07/10 19:37

IPR2023-01466
CrowdStrike EX1002 Page 189

			EPO; JPO; DERWENT; IBM_TDB			
S46	4	S41 AND (security or integrity or risk or malware or spyware or pestware or virus or rootkit or trojan or worm or hazard$4 or danger$4 or infect$4).ab.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/10 19:37
S47	14	S45 OR S46	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/10 19:37
S48	977	information adj flow adj control	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 11:55
S49	1	S48 AND (openflow or open-flow)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 11:55
S50	78	S48 AND "726".clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 11:57
S51	241	"binary analysis"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 16:47
S52	8502	"static analysis" or "dynamic analysis" or "taint analysis"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 16:50
S53	52	S51 AND S52	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 16:50
S54	3	"binary analysis" with ("static analysis" or "dynamic analysis" or "taint	US-PGPUB; USPAT;	OR	ON	2013/07/11 16:51

IPR2023-01466
CrowdStrike EX1002 Page 190

		analysis")	USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S55	542	("binary analysis" or "static analysis" or "dynamic analysis" or "taint analysis") AND "726".clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 16:52
S56	224	("binary analysis" or "static analysis" or "dynamic analysis" or "taint analysis") with image	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 16:52
S57	3	("binary analysis" or "static analysis" or "dynamic analysis" or "taint analysis") with image AND endpoint	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 16:53
S58	392	("binary analysis" or "static analysis" or "dynamic analysis" or "taint analysis") AND endpoint	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 16:53
S59	956	("binary analysis" or "static analysis" or "dynamic analysis" or "taint analysis") SAME (endpoint or end-point or end adj point or node or server or router or host or switch or firewall)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 16:54
S60	28	("binary analysis" or "static analysis" or "dynamic analysis" or "taint analysis") SAME (endpoint or end-point or end adj point)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 16:54
S61	13	"6002869".pn. "20100058475".pn. "20110231828".pn. "20120084754".pn. "20120151592".pn. "20120233599".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 16:58
S62	105	(("binary analysis" or "static analysis" or "dynamic analysis" or "taint analysis") AND (network$3 or IDS or intru$6 adj detect$3 or firewall)).ab.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 17:00

IPR2023-01466
CrowdStrike EX1002 Page 191

S63	94	(("binary analysis" or "static analysis" or "dynamic analysis" or "taint analysis") AND (network$3 or IDS or intru$6 adj detect$3 or firewall)).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 17:01
S64	2	S62 AND S63	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 17:01
S65	51	(("binary analysis" or "static analysis" or "taint analysis") AND (network$3 or IDS or intru$6 adj detect$3 or firewall)).ab.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 17:04
S66	199	(("binary analysis" or "static analysis" or "taint analysis" or analy$6 near3 (source adj code or compiled or interpreted or byte)) AND (network$3 or IDS or intru$6 adj detect$3 or firewall)).ab.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 17:05
S67	14	S66 AND ("713" or "726" or "709").clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 17:05
S68	58	("20020004827" | "20030028257" | "20030061568" | "20030098887" | "20030115305" | "20030226131" | "20040030771" | "20040040016" | "20040111499" | "20040117624" | "20040153536" | "20040179142" | "20040205737" | "20040210654" | "20040230681" | "20050004942" | "20050015624" | "20050108387" | "20050114479" | "20050149872" | "20050174484" | "20050182969" | "20050262225" | "20060004680" | "20060195564" | "20070180432" | "4617643" | "4686623" | "4972264" | "6219706" | "6243862" | "6282546" | "6301668" | "6324656" | "6405318" | "6421719" | "6477651" | "6487666" | "6502112" | "6523172" | "6597666" | "6601059" | "6615257" | "6636972" | "6775657" | "6839850" | "6920458" | "6950865" | "6968377" | "7032014" | "7113989" | "7216298" | "7284009" | "7287069" | "7376719" | "7376969" | "7418733" | "7457884").PN. OR ("7735140").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2013/07/11 17:08
S69	11	("20020032766" | "20020075809" | "20060209794" | "20070011317" |	US-PGPUB; USPAT;	OR	ON	2013/07/11 17:12

IPR2023-01466
CrowdStrike EX1002 Page 192

		"20070192863" | "20070201359" | "20080016115" | "5774668" | "6449650" | "7290283").PN. OR ("7792959").URPN.	USOCR			
S70	0	S68 AND S69	US-PGPUB; USPAT; USOCR	OR	ON	2013/07/11 17:12
S71	5	S66 AND "717".clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/07/11 17:13
S72	69	S68 OR S69	US-PGPUB; USPAT; USOCR	OR	ON	2013/07/11 17:36
S73	6	S72 AND ("binary analysis" or "static analysis" or "dynamic analysis" or "taint analysis")	US-PGPUB; USPAT; USOCR	OR	ON	2013/07/11 17:36
S74	319	("binary analysis" or "static analysis" or "dynamic analysis" or "taint analysis") with (".iso" or image or compiled or byte)	US-PGPUB; USPAT; USOCR	OR	ON	2013/07/11 17:44
S75	287	("binary analysis" or "static analysis" or "dynamic analysis" or "taint analysis") near15 (".iso" or image or compiled or byte)	US-PGPUB; USPAT; USOCR	OR	ON	2013/07/11 17:44
S76	69	("binary analysis" or "static analysis" or "dynamic analysis" or "taint analysis") near15 (".iso" or image or compiled or byte) AND ((network or endpoint or end-point) with (secur$4 or safe$3) or ids or intru$6 adj detect$4)	US-PGPUB; USPAT; USOCR	OR	ON	2013/07/11 17:46
S77	69	("binary analysis" or "static analysis" or "dynamic analysis" or "taint analysis") near15 (".iso" or image or compiled or byte) AND ((network or endpoint or end-point) with (secur$4 or safe$3) or "ids" or intru$6 adj detect$4)	US-PGPUB; USPAT; USOCR	OR	ON	2013/07/11 17:47
S78	27	("binary analysis" or "static analysis" or "dynamic analysis" or "taint analysis") near15 (".iso" or image or compiled or byte) AND ((network or endpoint or end-point) with (secur$4 or safe$3) or intru$6 adj detect$4)	US-PGPUB; USPAT; USOCR	OR	ON	2013/07/11 17:47
S79	9672	726/22,24-25.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 17:38
S80	2467	H04L63/1433.CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 17:39

IPR2023-01466
CrowdStrike EX1002 Page 193

S81	2	"20130298244".PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 17:40
S82	827	G06F21/50.CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 17:42
S83	3474	G06F21/51.CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 17:42
S84	2658	G06F21/52.CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 17:42
S85	2002	G06F21/566.CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 17:43
S86	10652	S80 S82 S83 S84 S85	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 17:44
S87	7648	((reputation or attest$6 or integrity or fidelity or risk or trust) SAME (assess$4 or scan$4 or evaluat$4)) WITH (application or app or program or executable)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 18:34
S88	311	S87 AND S86	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 18:36
S89	486	S87 AND S79	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	ON	2014/01/08 18:36

IPR2023-01466
CrowdStrike EX1002 Page 194

			DERWENT; IBM_TDB			
S90	163	S88 and S89	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 18:36
S91	183	((endpoint or end-point) near2 (assess$4 or scan$4 or evaluat$4) SAME (assess$4 or scan$4 or evaluat$4)) WITH (application or app or program or executable)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 18:37
S92	95	S87 AND (endpoint or end-point) near2 (assess$4 or scan$4 or evaluat$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 18:37
S93	30	S92 AND S79	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 18:37
S94	11	S92 AND S86	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 18:37
S95	25	S93 NOT S94	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 18:43
S96	140	((endpoint or end-point) near2 (assess$4 or scan$4 or evaluat$4) SAME (assess$4 or scan$4 or evaluat$4)) near6 (application or app or program or executable)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 18:46
S97	140	((endpoint or end-point) near2 (assess$4 or scan$4 or evaluat$4) AND (assess$4 or scan$4 or evaluat$4)) near6 (application or app or program or executable)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/08 18:46
S98	14	S97 AND (S79 or S86)	US-PGPUB; USPAT; USOCR;	OR	ON	2014/01/08 18:46

IPR2023-01466
CrowdStrike EX1002 Page 195

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S99	27	("20060015942" | "20080276317" | "20110072506" | "20110162073" | "20110276468" | "20120011590" | "7174566" | "7370359" | "8010469" | "8214497").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/09 16:23
S100	7685	(end-point or endpoint or end adj point) near6 (security or assess$5 or trust or integrity or risk or fidelity)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/09 18:33
S101	253	(end-point or endpoint or end adj point) near15 (security or trust or integrity or risk or fidelity) near10 (assessment or profile or apparaisal or audit or rating or score)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/09 18:39
S102	2468	H04L63/1433.CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/09 18:40
S103	828	G06F21/50.CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/09 18:40
S104	3474	G06F21/51.CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/09 18:40
S105	2658	G06F21/52.CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/09 18:40
S106	2002	G06F21/566.CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/09 18:40
S107	10654	S102 S103 S104 S105 S106	US-PGPUB;	OR	ON	2014/01/09

IPR2023-01466
CrowdStrike EX1002 Page 196

			USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			18:40
S108	9682	726/22,24-25.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/09 18:41
S109	40	S101 AND S108	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/09 18:41
S110	20	S101 AND S107	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/09 18:41
S111	81	S101 AND (third adj party or third-party)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/09 18:42
S112	24	S111 AND (S107 or S108)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/09 18:43
S113	17	(US-20090328222-$ or US-20080229422-$ or US-20050044418-$ or US-20120110174-$ or US-20130042317-$ or US-20120137375-$ or US-20120102458-$ or US-20070192863-$ or US-20120260342-$ or US-20120072968-$ or US-20100251000-$ or US-20080244748-$).did. or (US-8214497-$ or US-8272061-$ or US-6742128-$ or US-7735140-$).did. or (US-20090138939-$).did.	US-PGPUB; USPAT; DERWENT	OR	ON	2014/01/09 20:28
S114	7	S113 AND (third adj party or third-party)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/09 20:28

IPR2023-01466
CrowdStrike EX1002 Page 197

EAST Search History (Interference)

<This search history is empty>

1/10/2014 8:17:06 PM
C:\Users\vsavenkov\Documents\EAST\Workspaces\13559766.wsp

IPR2023-01466
CrowdStrike EX1002 Page 198

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13559766	KUMAR ET AL.
	Examiner	**Art Unit**
	VADIM SAVENKOV	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	07/12/2013	01/10/2014							
	1	✓	✓							
	2	✓	✓							
	3	✓	✓							
	4	✓	✓							
	5	✓	✓							
	6	✓	✓							
	7	✓	✓							
	8	✓	✓							
	9	✓	✓							
	10	✓	✓							
	11	✓	✓							
	12	✓	✓							
	13	✓	✓							
	14	✓	✓							
	15	✓	✓							
	16	✓	✓							
	17	✓	✓							
	18	✓	✓							
	19	✓	✓							
	20	✓	✓							

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/559,766	07/27/2012	Srinivas KUMAR	0079152-000016

CONFIRMATION NO. 9330

21839
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

PUBLICATION NOTICE

OC000000064874153

Title:SYSTEMS AND METHODS FOR THREAT IDENTIFICATION AND REMEDIATION

Publication No.US-2013-0298244-A1
Publication Date:11/07/2013

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

IPR2023-01466
CrowdStrike EX1002 Page 200

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	**MAIL STOP AMENDMENT**
Kumar, Srinivas	Group Art Unit: 2431
Application No.: 13/559,766	Examiner: SAVENKOV, Vadim
Filed: July 27, 2012	Confirmation No.: 9330
For: Systems and Methods for Threat Identification and Remediation	

REPLY AND AMENDMENT UNDER 37 C.F.R. §1.111

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Madam:

In response to the non-final Office Action dated July 18, 2013, the non-extended due date for response being October 18, 2012, Applicants hereby timely submit the following Amendments and Remarks.

Applicants do not believe that fees are required for this submission. However, if fees are required for any reason, please charge Deposit Account No. 02-4800 the necessary amount.

AMENDMENTS TO THE SPECIFICATION:

Please replace paragraph [0019] of the original specification with the following amended paragraph.

[0019] In other exemplary embodiments, methods, apparatuses, systems and computer readable media comprise a plurality of services that enable visibility, control, and/or compliance in a cloud computing environment with a runtime dashboard **[[**to**]]** capable of displaying operational integrity metrics of systems based on a plurality of threat vectors.

Please replace paragraph [0080] of the original specification with the following amended paragraph.

[0080] In the embodiment shown in FIG. 5, the endpoint events 520 are generated by a component of the endpoint trust agent 510, and represent alerts based **[[**an**]]** on endpoint sensor resident on the device 560. The alerts are mapped to a cell in the risk correlation matrix 411 grid by the system event correlator 410. In one embodiment, the format (schema) of the endpoint events 520 is a standard Extensible Markup Language (XML) notation. Additional features of the endpoint events 520 are described below with reference to FIG. 6.

Please replace paragraph [0108] of the original specification with the following amended paragraph.

[0108] According to the embodiments of FIGs. 4 and 8, the trust orchestrator 430 is an aggregation that includes functional components such as the trust broker 407, system event correlator 410, the trust supervisor 846, and remediation controller 848. In embodiments, the

trust orchestrator 430 is configured to receive sensory threat intelligence from network analyzers 830, endpoint assessment services 820 and endpoint trust agents 510 on devices 560. Through a sequence of normalization, collation and risk correlation of events, directives 849 in the form of directives are dispatched to orchestration services to initiate remediation actions to deal with identified threats on devices 560. The directives are specific to the orchestration service and can include the use of vendor APIs. Examples of such vendor APIs include VMWARE™ vCloud APIs, BMC Atrium™ APIs for accessing a BMC Atrium™ configuration management database (CMDB) from BMC Software, Inc., Hewlett Packard Software Operations Orchestration (HP-OO) APIs, and standard protocols such as OpenFlow™ (i.e., computer network protocol that facilitates the control of network switches, routers and wireless access points), among others.

Please replace paragraph [0116] of the original specification with the following amended paragraph.

[0116] A user's (1014) device D (560) may become infected with a form of an advanced persistent threat (e.g., malware $M_{(benign)}$) while **[[**he**]]** the device D is still connected to an enterprise network of an organization 2303. The connection of the device D to the enterprise network can occur through user activity, for example, when the user 1014 connects a plug-and-play portable universal serial bus (USB) device with the malware $M_{(benign)}$ to the device D while it is connected to the enterprise network, as the result of the user 1014 opening an email attachment infected with the malware $M_{(benign)}$, when the user 1014 accesses a social network application from the device D, or when the user 1014 unwittingly transfers a file with the malware $M_{(benign)}$ to device D while accessing a file sharing service.

Please replace paragraph [0140] of the original specification with the following amended paragraph.

[0140] According to exemplary embodiments, the event correlator 1007 receives endpoint events 1033 from the event processor 1006 ~~correlator 1007~~, maps the alerts 1032 using the event correlation matrix 1013, generates and sends endpoint warnings 1034 to the threat classifier 1008.

Please replace paragraph [0161] of the original specification with the following amended paragraph.

[0161] Referring to FIG. 12, the exemplary network flow remediation system1200 may include an endpoint trust agent 1201 on a device 560 that may execute an application 1203, a trust orchestrator 1205, a plurality of collaboration services 1207 that may include malware analyzers, network endpoint assessment services, and reputation services, a network service 1230 that may include a network trust agent 1209 and [[an]] a computer network protocol (e.g., OpenFlow™) security framework 1211, [[an]] a computer network protocol (e.g., OpenFlow™) controller 1214, and [[an]] a computer network protocol (e.g., OpenFlow™) enabled network element 1216 (for example, a switch or router).

Please replace paragraph [0163] of the original specification with the following amended paragraph.

[0163] In certain exemplary embodiments, the network trust agent 1209 sends messages 1210 to the computer network protocol (e.g., OpenFlow™) security framework 1211 middleware to send

directives 1213 to [[an]] a computer network protocol (e.g., OpenFlow™) controller 1214, or send directives 1212 to [[an]] a computer network protocol (e.g., OpenFlow™) controller 1214, to notify by means of a protocol 1215 [[an]] a computer network protocol (e.g., OpenFlow™) enabled network element 1216 to apply access controls 1217 to block or divert traffic flows.

Please replace paragraph [0239] of the original specification with the following amended paragraph.

[0239] In step 2106, the remediation controller 848 at the trust orchestrator 1205 sends to the network trust agent 1209 a system warning 1208 for the network device 560. In step 2107, the network trust agent 1209 may generate and send to the computer network protocol (e.g., OpenFlow™) security framework 1211 directives 1210 to formulate commands 1213 for the computer network protocol (e.g., OpenFlow™) controller 1214.

Please replace paragraph [0240] of the original specification with the following amended paragraph.

[0240] In step 2108, the computer network protocol (e.g., OpenFlow™) controller 1214 sends rules 1215 to the computer network protocol (e.g., OpenFlow™) enabled network element (switch) 1216 to divert or block traffic flows to/from the forewarned network device 560.

Please replace paragraph [0241] of the original specification with the following amended paragraph.

[0241] In step 2109, the computer network protocol (e.g., OpenFlow™) enabled network element (switch) 1216 may enforce received access restrictions (controls) 1217 for the forewarned network device 560 before control is passed to step 2110.

Please replace paragraph [0243] of the original specification with the following amended paragraph.

[0243] In step 2112, the network trust agent 1209 may generate and send to the computer network protocol (e.g., OpenFlow™) security framework 1211 directives 1210 to formulate commands 1213 for the computer network protocol (e.g., OpenFlow™) controller 1214 to restore normal flows to/from the forewarned network device 560.

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) A method of providing an attestation service for providing runtime operational integrity of a system using a computing platform comprising a network trust agent, an endpoint trust agent, and a trust orchestration server, the method comprising:

receiving, at the trust orchestration server, a dynamic context including endpoint events of a monitored device and applications executing thereon;

analyzing, by the trust orchestration server, the received endpoint events;

receiving, by the trust orchestration server, third party network endpoint assessments;

generating, by the trust orchestration server, temporal events based at least in part on analyzing the third party network endpoint assessments;

correlating, by the trust orchestration server, the received endpoint events and the generated temporal events; and

generating, by the trust orchestration server, an integrity profile for the system.

2. (Original) The method of claim 1, wherein the dynamic context is sent by the endpoint trust agent.

3. (Currently Amended) The method of claim 1, wherein the third party network endpoint assessments are received from an endpoint assessment service.

4. (Currently Amended) The method of claim 3, further comprising:

receiving, by the trust orchestration server, integrity measurement and verification reports from the endpoint assessment service.

5. (Currently Amended) The method of claim 1, wherein the third party network endpoint assessments are received from one or more collaboration services.

6. (Currently Amended) The method of claim 5, further comprising:

receiving, by the trust orchestration server, integrity measurement and verification reports from the one or more collaboration services.

7. (Currently Amended) The method of claim 1, wherein

the endpoint events of the monitored device are received by a system event correlator of the trust orchestration server from endpoint trust agents, and

the temporal events are generated by a trust broker of the trust orchestration server and are received by [[a]] the system event correlator from ~~endpoint trust agents and a~~ the trust broker~~, respectively~~.

8. (Currently Amended) A method of providing flow level remediation to isolate infected or compromised systems and platforms from a computing network fabric using a network trust agent, an endpoint trust agent, and a trust orchestrator, the method comprising:

generating, by the endpoint trust agent, runtime system integrity alerts regarding execution anomalies and risks based on rulesets and a calculus of risk hypothesized by runtime actions and activities of monitored applications executing on an endpoint device;

sending, by the endpoint trust agent, runtime system integrity warnings as endpoint events of the endpoint device to the trust orchestrator;

generating, by the trust orchestrator, a system integrity profile for the endpoint device based on analysis of the received endpoint events;

processing and correlating, by the trust orchestrator, one or more of:

a system integrity profile generated based on a calculus of risk,

a plurality of temporal events generated based on a normalization and collation of elements in endpoint assessment reports received from a plurality of collaboration services, and

a system infection profile received from a network analyzer;

sending, by the trust orchestrator to the network trust agent, system warnings based on endpoint execution state assessments; and

sending, by the network trust agent, messages or directives to computer network protocol ~~OpenFlow~~ security frameworks and/or controllers to apply flow controls based on the received execution state as a threat posture of a connection endpoint.

9. (Original) The method of claim 8, wherein the integrity warnings comprise warnings regarding data events and content events; and wherein the endpoint events comprise data events and content events.

10. (Original) The method of claim 8, wherein the remediation of an infected system is achieved without adversely reducing the total operating capacity or availability of the computing platform through on-demand instantiation and scaling of workloads.

11. (Currently Amended) The method of claim 10, further comprising forwarding a notification conveying by a service accessed by a user from a mobile computing device an infected or compromised state of a mobile computing application on the mobile computing device ~~to a user~~ associated with the user ~~the mobile computing device~~, wherein the notification is one or more of:

an asynchronous push notification to an account associated with the user;

a short messaging service (SMS) text alert message forwarded to a phone number associated with the mobile computing device;

an email alert message forwarded to an email address associated with the user; and

a warning message displayed by a service on a display of the mobile computing device during initiation of a transaction with a service from the mobile computing device.

12. (Currently Amended) The method of claim 11, wherein one or more services accessed by ~~features or capabilities of~~ a mobile device are configured to be denied or restricted ~~are de-activated or activated~~ as a remediation action by a service provider.

13. (Currently Amended) The method of claim 12, wherein the remediation action is based on the geo-location of the device, user and associated service accessed by the user.

14. (Currently Amended) The method of claim 1, further comprising:

generating, by a trust supervisor, one or more tiered ~~flow~~ remediation actions based on real time warning associated with the operational runtime integrity of applications executing on an infected system ~~to be performed on a network fabric~~;

receiving, at a remediation controller of the trust orchestrator, the ~~flow~~ tiered remediation actions; and

sending, by the trust orchestrator, to the network trust agent, one or more system warnings pertaining to a network device associated with the one or more ~~flow~~ tiered remediation actions.

15. (Currently Amended) The method of claim 14, further comprising:

generating and sending, by the network trust agent, directives to formulate commands for an computer network protocol ~~OpenFlow~~ controller;

sending, by the computer network protocol ~~OpenFlow~~ controller, rules to computer network protocol ~~an OpenFlow~~ enabled network element or switch of the network fabric to divert or block traffic flow to/from the network device; and

enforcing, by the computer network protocol ~~OpenFlow~~ enabled network element or switch, received access restrictions or controls for the network device.

16. (Currently Amended) The method of claim 15, further comprising:

monitoring and sending, by the trust supervisor, reputation score updates for the network device to the remediation controller;

sending, by the trust orchestrator, system security posture status updates for the network device to the network trust agent; and

generating and sending, by the network trust agent, to the computer network protocol ~~OpenFlow~~ security framework, directives to formulate commands for the computer network protocol ~~OpenFlow~~ controller to restore normal flows to/from the network device.

17. (Currently Amended) The method of claim 8, further comprising:

determining, by the network analyzer, threat behaviors ~~anomalies~~ based on network activity correlation and malware detection based on a threat life cycle model; and

dispatching, by the trust orchestrator, the image files and attributes of an application for binary analysis, wherein the image files comprise compiled, intermediate, or interpreted code or scripts;

receiving a result of the binary analysis result identifying malicious activity as a set of threats identified based on the analysis; and

caching, by the trust broker, the results of the analysis indexed by a unique identifier for the image; and

generating and returning an image profile to the endpoint trust agent comprising assertions of malicious capabilities of the image to be monitored at runtime for subsequent generation of endpoint events by the endpoint trust agent.

18. (Original) The method of claim 17, wherein the binary analysis is performed by one or more third party malware analyzers, and wherein the dispatch mechanism uses trigger filter expressions that specify a set of criteria that warrant initiation of image analysis such as frequency and volume of requests for analysis associated with the application image across deployed endpoint trust agents.

19. (Original) The method of claim 18, wherein the third party malware analyzers are configured to perform static and dynamic analysis of application images based on policies specified by the trust broker.

20. (Currently Amended) A system for providing runtime operational integrity by determining execution anomalies and a threat posture of applications executing on computing platforms including mobile devices and client-server systems, the system comprising:

(i) an endpoint trust agent including:

a process monitor configured to observe the runtime execution context of ~~local execution context of the~~ applications executing on the computer platforms and transient operating states,

a socket monitor configured to observe runtime network activities of the applications for transient states, and

a resource utilization module monitor configured to observe the types and extent of system and platform resources consumed by the applications that may provide evidence of infected systems; and

an application integrity module configured to assess runtime operational ~~integrities~~ integrity of a monitored application instance running on an instrumented device ~~the computing platforms~~ based on a ruleset to deem local actions and activities of the application to be at risk;

wherein native machine instrumentation for the computing platform is configured to[[:]] (a) represent event subscriptions, callbacks, notification mechanisms provided by an operating system (OS) on the computing platforms, and (b) generate raw events;

(ii) extended trust instrumentation;

(iii) a runtime monitor configured to:

subscribe to and receive near real time asynchronous notifications of runtime operation invocations by applications executing on the computer platforms ~~application events for the applications~~ from the extended trust instrumentation, and

generate and send dynamic expressions or rules as application activity filters linked to runtime operation invocations of running instances of the applications;

(iv) a system event correlator configured to correlate system events of the computing platforms to determine a calculus of risk;

(v) a trust orchestrator configured to orchestrate actionable intelligence based on the calculus of risk by integrating security intelligence about the computing platforms and the applications; and

(vi) an endpoint trust sensor configured to measure runtime operational integrity of the computing platforms by evaluating risk based on actions of an application executing on, or a user of, the computing platforms and receiving the raw events from the native machine instrumentation.

REMARKS

This communication is a full and timely response to the non-final Office Action dated July 18, 2013. Claims 1-20 remain pending, of which claims 1, 8 and 20 are the independent claims. By this communication, claims 1, 3-8, 11-17 and 20 amended. Favorable reconsideration and allowance of the present application are respectfully requested in view of the foregoing Amendments and following Remarks.

Priority

Applicants appreciate the Office's acknowledgement of Applicant's claim for Foreign Priority.

Information Disclosure Statement

Applicants acknowledge with appreciation the Office's consideration of the Information Disclosure Statement filed in the Patent Office On November 11, 2012 and its consideration of the documents cited thereon.

Specification

In numbered paragraph 1 on page 2 of the Office Action, the Office noted that the trademark OpenFlow had been used throughout the specification and requested that the trademark be capitalized and accompanied by the generic terminology. In response thereto, paragraphs [0108], [0161], [0163], [0239], [0240] and [0243] have been amended such that the term OpenFlow is replaced with OpenFlow™ and is accompanied by the generic terminology.

Paragraph [0108] is also amended to include the known definition of OpenFlow™ (e.g., from the Trademark registration provided by the Examiner).

In numbered paragraph 2 on page 2 of the Office Action, the Office objected to the Specification for minor informalities. Applicants have amended the original specification at paragraphs [0019], [0080], [0116], and [0140], as provided on pages 2 and 3 of this filing, to correct minor typographical errors in order to remove this issue. Accordingly, the Objection to the Specification should be withdrawn.

Claim Objections

In numbered paragraph 3 on page 3 of the Office Action, the Office objected to claim 8 for reciting both "runtime system integrity alerts" and "runtime system integrity warnings". In particular, the Office alleges that since "alerts" and "warnings" are synonymous terms and that the terms were, therefore, interpreted as "referring to the same thing". Applicants respectfully disagree.

Applicants respectfully submit that "alerts" and "warnings" are described separately throughout the specification. In particular, FIG. 2, items 230, 250, 270 and 280, illustrate that alerts are "events" raised by sensors and that warnings are "threat classifications" issued based on event correlation 240 or activity correlation 260. Moreover, the relevance of a set of "alerts" to a specific type of "warning class" is the calculus that is performed by the correlation function illustrated, e.g., in FIG. 7C (items 720 and 723). Thus, "runtime system integrity alerts" and "runtime system integrity warnings" are two separate features and should be examined as such.

Accordingly, Applicants respectfully request the objection be withdrawn.

Examiner's Comment

On page 3 of the Office Action, the Examiner notes that claims 14-16 depend on claim 1 and not claim 8 and is unsure if this dependency is accurate. Applicants note that claims 14-16 accurately reflect their dependence (i.e., upon claim 1).

35 U.S.C. §112 Rejections

In numbered paragraph 5, on page 4 of the Office Action, claims 1-7 are rejected under 35 U.S.C. § 112(b) or 35 U.S.C. § 112 (pre-AIA), second paragraph, for allegedly being indefinite. In particular, the Office alleges that it is unclear as to which elements are performing the method steps of claim 1.

While not acquiescing to this rejection, Applicants have amended independent claim 1 to expedite prosecution of this application. Independent claim 1, from which claims 2-7 depend, has been amended to recite that steps central to the respective method claim are performed by a specific device. For example, independent claim 1 is amended herein to recite that the receiving step, generating steps and correlating step are performed by the trust orchestration server. Accordingly, Applicants respectfully submit that claim 1, as amended, clearly indicates the device performing the method steps and, thus, removes the issue. Applicants respectfully submit that independent claim 1, and its dependent claims, are clear and definite under the guidelines of 35 U.S.C. §112, second paragraph and request the rejection be withdrawn.

Claim 7 is further rejected for alleged indefiniteness because it is unclear how the trust broker obtains the temporal events. As recited in amended claim 1, from which claim 7 depends, the temporal events are generated by the trust orchestration server. In amended claim 7, the trust

orchestration server is further defined as including a system event correlator and a trust broker, wherein the trust broker generates the temporal events. While the temporal events are generated, in general, by the trust orchestration server (as recited in claim 1), claim 7 further specifies the actual components of the trust orchestration server that generate and subsequently receive the generated temporal events. In particular, as recited in amended claim 7, the temporal events are generated by the trust broker of the trust orchestration server and then are received by the system event correlator of the trust orchestration server. Support for this amended subject matter can be found, for example, in paragraphs [0244]-[0249] and FIGS. 5 and 22. Applicants respectfully submit that claim 6, as amended, is clear and definite under the provisions of 35 U.S.C. §112, second paragraph and request the rejection be withdrawn.

In numbered paragraph 6, on page 5 of the Office Action, the Office rejected claims 8, 15 and 16 for containing the trademark/trade name OpenFlow. Applicants have amended claims 8, 15 and 16 to recite the generic terminology in place of the term OpenFlow. Accordingly, the rejection should be withdrawn.

Claim 20 is rejected under 35 U.S.C. § 112(b) or 35 U.S.C. § 112 (pre-AIA), second paragraph, for alleged indefiniteness. In particular, the Office alleges that the grammatical structure of claim 20 following the recitations of (i) "wherein native machine instrumentation for the computing platform is configured to:…extended trust instrumentation…" and (ii) wherein native machine instrumentation for the computing platform is configured to:…a runtime monitor configured to: subscribe to and receive…generate and send…" is confusing. Applicants note that proper indentations were inadvertently omitted in the claim as originally filed. Thus, Applicants have amended claim 20 such that proper indentation and recitation identifiers (e.g.,

(i), (ii), (iii), etc.) are provided. Applicants respectfully submit that the inclusion of such indentations and identifiers addresses the Office's concerns and removes the issue. Accordingly, the rejection should be withdrawn.

Rejections of the Claims based on Prior Art

Claims 1-7 are rejected under 35 U.S.C. 102(b) for alleged anticipation by U.S. Patent Publication No. 2009/0328222 A1 to Helman ("*Helman*").

Claim 14 is rejected under pre-AIA 35 U.S.C. 103(a) for alleged unpatentability over *Helman* as applied to claims 1-7 above, and further in view of Official Notice.

Claims 8-10 are rejected under pre-AIA 35 U.S.C. 103(a) for alleged unpatentability over *Helman* in view of U.S. Patent No. 8,214,497 to Alperovitch ("*Alperovitch*").

Claims 11-13 are rejected under pre-AIA 35 U.S.C. 103(a) for alleged unpatentability over *Helman* and *Alperovitch* as applied to claims 8-10 above, and further in view of U.S. Patent Publication No. 2012, 0110174 A1 to Wootton ("*Wootton*").

Claim 17 is rejected under pre-AIA 35 U.S.C. 103(a) for alleged unpatentability over *Helman* and *Alperovitch* as applied to claims 8-10 above, and further in view of "Static Analysis of executables for Collaborative Malware Detection on Android" to Schmidt ("*Schmidt*"); further in view of U.S. Patent Publication No. 2012/0072968 A1 to Wysopal ("*Wysopal*").

Claims 18 and 19 are rejected under pre-AIA 35 U.S.C. 103(a) for alleged unpatentability over *Helman*, *Alperovitch, Schmidt* and *Wysopal* as applied to claim 17 above, and further in view of *Official Notice*.

Claim 20 is rejected under pre-AIA 35 U.S.C. 103(a) for alleged unpatentability over *Helman* in view of "Windows Management Instrumentation: Create WMI Providers to Notify Applications of System Events" to MSDN ("*MSDN*").

Applicants respectfully traverse each of the above-identified rejections.

Independent Claim 1 and Its Dependent Claims are Allowable Over Helman

Claims 1-7 are rejected for alleged unpatentability over *Helman*. Applicants respectfully traverse this rejection. Independent claim 1 recites, *inter alia*, "A method of providing an attestation service for providing runtime operational integrity of a system…comprising: receiving, at the trust orchestration server, a dynamic context *including endpoint events of a monitored device and applications executing thereon*; analyzing…the received endpoint events; receiving, by the trust orchestration server, *third party* network *endpoint* assessments; generating…temporal events based at least in part on analyzing the *third party network endpoint assessments*; correlating…the *received endpoint events* and the generated temporal events; and generating…an integrity profile for the system."

The premise of claim 1 pertains to a solution for detecting infected systems based on (1) observed malicious behaviors *of applications* (e.g., malware or compromised non-malware) and indicators of compromise *at a monitored endpoint device* (e.g. laptop, desktop, server, mobile devices, etc.) and (2) identified stages in the life cycle observed through network dialogs with internal and external entities over the network. The claimed applications are programs executing at the monitored endpoint device; ***not*** applications on a networked device along a data path that processes single flows on received data. An integrity profile for the system is then generated (on

a basis of the endpoint events of the monitored device and applications executing thereon) in order to, e.g., initiate corrective actions to remediate an infected device (e.g., tiered at machine, flow and transaction levels). Thus, any corrective action would be based on endpoint device state and *not* flow based detection of threats in progress. Further, any corrective action would not be triggered by a network flow, intrusion or attack alert. Rather, it would be based on a runtime integrity of the applications executing on the endpoint device, including applications that may not be communicating over the network.

As recited in claim 1, a trust orchestration server receives and analyzes network endpoint assessments and endpoint events *of a monitored device (and applications running thereon)*. This enables an assessment of whether application behaviors are malicious. Based on at least the analysis of the network endpoint assessments, the trust orchestration server generates temporal events (time-based events), which provides assertions of operational parameters of the monitored system. The trust orchestration server then correlates the received endpoint events *of the monitored endpoint device and applications executing thereon* and the temporal events and generates an integrity profile for the system. Therefore, any remediation (based on the integrity profile) will be based at least in part *on a state of the monitored device and applications running thereon* and, thus, remediation actions would not be *not* flow level intervention in the data path. This improves upon conventional systems and methods which initiate remediation actions based on a network flow, intrusion or attack (in progress).

Moreover, because the claimed system is endpoint device and/or application centric, it does not require a methodology pertaining to network applications, such as IDS/IPS, firewalls, anti-virus scans, etc. And, since an integrity profile is generated on a basis of at least *endpoint*

events of a device that is being monitored, a confidence level is not determined merely on a basis of statistics, metrics or content associated with a single flow that the device is engaged in *at a single point in time* (e.g., no active network flows, intrusions or attacks in progress is necessary to determine that the endpoint device is infected). Thus, the method of claim 1 enables an increase in reliability of detection. Moreover, a specific problem with the system and monitored device (e.g., what is actually wrong) can be identified, as opposed to indicating that a problem merely exists.

The system and method of *Helman*, in contrast with claim 1, uses correlation rules on event logs generated by security products, such as firewalls, HIDS and HIPS. Moreover, the ESAS Central Server, of *Helman*, serves as an aggregator of received security assessments from multiple security products, wherein the security products do *not* instrument a user device to perform runtime monitoring of any endpoint device (or applications running thereon) to assess operational runtime integrity. New security assessments may be used to decrease the fidelity of the assessment as a means to reduce false positives and noise.

In making the rejection, the Office alleges that *Helman's* disclosure pertaining to correlation rules applied to incoming security data corresponds to the claimed "analyzing…the received endpoint events…" Applicants respectfully disagree. As discussed in detail above, endpoint events pertain to a monitored endpoint device and applications executing thereon. Because the claimed method is *endpoint device and/or application centric* (e.g., *monitors an endpoint device and applications executing thereon*), the method of claim 1 does *not* require a methodology pertaining to network applications, such as IDS/IPS, firewalls, etc. *Helman,* in direct contrast, uses incoming security data to trigger an appropriate action based on correlation

of event logs *generated by security products, such as firewalls, HIDS and HIPS*. Moreover, in *Helman*, regardless of whether network activity is monitored, at no point is an endpoint device, or applications executing thereon, monitored, as in the present claims. Thus, a detection of some abnormal behavior of the system can be detected in *Helman*, however, identification of specific actions and activities (e.g., at a particular device) cannot be identified/obtained. In fact, *Helman* expressly states that "An endpoint has a general suspicion about a machine without the ability to pin point what is wrong". See, e.g., Table 1 and paragraph [0070].

Further, in making the rejection, the Office alleges that "new assessments" of *Helman* are interpreted as a form of the claimed temporal events. Applicants respectfully disagree. In *Helman*, cross-mapping relationships are used between users and machines to determine risk, and the assessment category is based on ***non***-application object types. The document expressly indicates that security assessments are performed on five main object groups: Host, User, Service (URL), Enterprise (department, subnet, site, branch), and Data (email, document, database), but **NOT** Applications (e.g., not monitored device and applications executing thereon) as in the present claims. See, e.g., paragraph [0061] of *Helman*. Contrary to *Helman*, the temporal events of the present claims, can, e.g., expose vulnerability, with *application level* granularity through policy based scans by third party services *that monitor the endpoint devices* (*and the applications executing thereon*).

As a result of the above-discussed distinctions, claim 1 substantively differs from *Helman* in that the method of claim 1 monitors an endpoint device and the applications executing thereon in order to generate a system integrity profile and, for example, identify application instances on the monitored endpoint device that may be engaging in the malicious activity. Because *Helman*

does not monitor applications executing on an endpoint device, as in the present claims, the system and method of *Helman* does not and cannot generate a system integrity profile (that is based on such the monitored endpoint device and applications), as in the present claims.

To properly anticipate a claim, the document must disclose, explicitly or implicitly, each and every feature recited in the claim. See *Verdegaal Bros. v. Union Oil Co. of Calif.*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). For at least the reasons set forth above, Applicants respectfully submit that *Helman* does not meet this requirement. Accordingly, Applicants respectfully submit that independent claim 1 is patentably distinct from *Helman* and request that the rejection be withdrawn.

Moreover, based at least upon their dependence from independent claim 1, claims 2-7 are also patentably distinct from *Helman*. Thus, Applicants respectfully request that the rejection be withdrawn

Claim 14 is rejected for alleged unpatentability over *Helman* in view of Official Notice. Claim 14 depends from independent claim 1 and is therefore patentable at least due to its dependence from an allowable base claim. Moreover, the Office acknowledges that *Helman* fails to disclose the features of claim 14 and therefore relies upon Official Notice. However, the Examiner's Official Notice does not remedy the deficiencies of *Helman* for failing to disclose or suggest at least the above-discussed features of claim 1. Accordingly, Applicants respectfully submit that claim 14 is patentably distinct from the applied documents and request the rejection be withdrawn.

Regarding dependent claims 15 and 16, on page 5 of the Office Action, the Office indicates that examination of these claims has not been performed with respect to the prior art as

a result of the use of the trademark "OpenFlow" rendering the claim indefinite (previously addressed in this filing). Regardless of whether examination of these claims has been performed, claims 15 and 16 indirectly depend from independent claim 1 and are, therefore, patentable at least due to their dependence from an allowable base claim.

Independent Claim 8 and Its Dependent Claims are Allowable Over Helman and Alperovitch

Claims 8-10 are rejected for alleged unpatentability over *Helman* and *Alperovitch*. Applicants respectfully traverse this rejection. Independent claim 8, although different in scope, recites at least some of the same distinguishing features noted above with respect to claim 1. Therefore arguments similar to those presented above with respect to the *Helman* document are also applicable to claim 8. Accordingly, Applicants respectfully submit that independent claim 8 is also patentably distinct from *Helman* (and *Alperovitch*) and request the rejection be withdrawn.

Similar to the method of claim 1, claim 8 recites a method of providing flow level remediation to isolate infected or compromised systems and platforms. The method comprises the steps of "generating, by the endpoint trust agent, runtime system integrity alerts regarding execution anomalies and risks based on rulesets and a calculus of risk hypothesized by runtime actions and activities of monitored applications executing on an endpoint device; sending, by the endpoint trust agent, runtime system integrity warnings as endpoint events *of the endpoint device* to the trust orchestrator; generating, by the trust orchestrator, a system integrity profile for the endpoint device *based on analysis of the received endpoint events*.

The method of claim 8 also includes the steps of "processing and correlating…a system integrity profile generated based on a calculus of risk, a plurality of temporal events generated based on a normalization and collation of elements in endpoint assessment reports…and a system infection profile received from a network analyzer…and sending, by the network trust agent, messages or directives to computer network protocol security frameworks and/or controllers to apply flow controls based on the received execution state as a threat posture of a connection endpoint."

Similar to the method of claim 1, the method of claim 8 pertains to a solution for detecting infected systems based on observed malicious behaviors o*f monitored applications executing on an endpoint device* and identified stages in the life cycle observed through network dialogs with internal and external entities over the network.

Helman fails to disclose the features of claim 8 for at least the reasons discussed above with respect to claim 1.

Alperovitch, in contrast with claim 1 (and similar to *Helman*), discloses a *network based* intrusion detection, prevention and/or testing system and method, and refers to applications as embodiments of traditional network applications (e.g., network firewalls, load balancers, network intrusion detection systems (NIDS), network intrusion prevention systems (NIPS), anti-virus scanners, email scanners, and web access gateways). The document describes such applications as deployed *in the data path* and processing *single flows* (e.g., using *deep packet content inspection, signatures, regular expressions, and activity logs* to detect threats and analyze events *in the context of single flow)*. The flow processing system of *Alperovitch* inspects network traffic (packet streams) to make a determination.

In making the rejection, the Office alleges that *Alperovitch* discloses the claimed "sending, by the endpoint trust agent, runtime system integrity warnings as endpoint events *of the endpoint device* to the trust orchestrator; generating, by the trust orchestrator, a system integrity profile for the endpoint device based on analysis of the received endpoint events," and refers to FIG. 10, col. 13-14, ll. 51-67 and 1-56, which pertain to the operation of a reputation based load balancer. Applicants respectfully disagree. The reputation engine of *Alperovitch* operates at the machine/IP address level, and **not** at an application level at the endpoints and across multiple flows at the network level, as recited in claim 8. Moreover, the reputation engine of *Alperovitch* analyzes communications data on a single flow by inspecting packet headers and content using signatures, regular expressions and blacklists to identify an attack or intrusion in progress. As noted above, *Alperovitch* does not use the execution state of applications running at the endpoint to determine threat posture of the endpoint to assess infections. The method of claim 8, in contrast with *Alperovitch*, identifies threats at the endpoint based on execution state of the applications engaged in the communications and reputation based on a forensic evidence and confidence score that life cycle stages of malware have been detected.

Thus, *Alperovitch* (like *Helman)* fails to disclose or suggest the monitoring of applications executing on an endpoint device, as in the present claims and, rather, focuses on a network based IDS/IPS method wherein applications as deployed *in the data path* and process *single flows*. Thus, *Alperovitch* does not remedy the deficiencies of *Helman*.

Accordingly, for at least the foregoing reasons, Applicants respectfully submit that the applied documents, whether taken individually or in proper combination, fail to disclose or suggest the claimed subject matter, and therefore, cannot support a *prima facie* case for rejecting

claim 8 under 35 U.S.C. §103(a). Thus, Applicants respectfully submit that independent claim 8 is patentably distinct from *Helman* and *Alperovitch* and request that the rejection be withdrawn.

Moreover, based at least upon their dependence independent claim 8, claims 9 and 10 are also patentably distinct from *Helman* and *Alperovitch*. Thus, Applicants respectfully request that the rejection be withdrawn

Claims 11-13 and 17-19 are rejected for alleged unpatentability over *Helman* and *Alperovitch* in view of various additional documents/sources (e.g., *Wootton, Schmidt, Wysopal,* and *Official Notice*). Claims 11-13 and 17-19 depend, directly or indirectly, from independent claim 8 and are therefore patentably distinct from the applied documents at least due to their dependence from an allowable base claim. Moreover, the Office acknowledges that *Helman* and *Alperovitch* fail to disclose the features of claims 11-13 and 17-19 and therefore relies upon one of the additional documents/sources. However, the additional documents/sources do not remedy the deficiencies of *Helman* and *Alperovitch* for failing to disclose or suggest at least the above-discussed features of claim 8. Accordingly, Applicants respectfully submit that claims 11-13 and 17-19 are patentably distinct from the applied documents and request the rejection be withdrawn.

Independent Claim 20 is Allowable over Helman and MSDN

Claim 20 is rejected for alleged unpatentability over *Helman* and *MSDN*. Applicants respectfully traverse this rejection. Independent claim 20, although different in scope, recites at least some of the same distinguishing features noted above with respect to claim 1. Therefore arguments similar to those presented above with respect to the *Helman* document are also

applicable to claim 20. Accordingly, Applicants respectfully submit that independent claim 20 is also patentably distinct from *Helman* (and *MSDN*) and request the rejection be withdrawn.

In particular, claim 20 recites a "system for providing runtime operational integrity by determining execution anomalies and a threat posture of applications executing on computing platforms…the system comprising: (i) an endpoint trust agent including: a process monitor configured to observe the *runtime execution* context of applications executing on the computing platforms and transient operating states, a socket monitor configured to observe runtime network activities of the applications for transient states, and a resource utilization module monitor configured to observe the types and extent of system and platform resources *consumed by the applications* that may provide evidence of infected systems, and an application integrity module configured to assess runtime operational integrity of a monitored application instance running on an instrumented device based on a ruleset to deem local actions and activities of the application to be at risk…"

The system also includes a runtime monitor configured to subscribe to and receive near real time notifications of *runtime operation invocations* by applications executing on the endpoint device, a system event correlator configured to correlate system events of the computing platforms to determine a calculus of risk, a trust orchestrator configured to orchestrate actionable intelligence based on the calculus of risk by integrating security intelligence about the computing platforms *and the applications*, and an endpoint trust sensor configured to measure runtime operational integrity of the computing platforms by evaluating risk based on actions *of an application executing on, or a user of, the computing platform*s and receiving the raw events from the native machine instrumentation.

Similar to claims 1 and 8, discussed above, claim 20 pertains to the monitoring of runtime operational integrity of applications *executing on computer platforms (e.g., an endpoint device)*. For example, (1) *runtime execution* context of the applications are observed, (2) runtime network activities of the applications for transient states are observed, (3) the types and extent of system and platform resources consumed by the applications are observed, (4) *runtime operational integrity* of a monitored application instance running on an instrumented device is assessed, etc. The system of claim 20 anchors a calculus of risk based on continuous runtime operational integrity measurements to increase the fidelity to a threshold at which a high forensic confidence score is reached. Thus, claim 20 (similar to claims 1 and 8) pertains to the continuous monitoring of, e.g., an endpoint device, and all applications executing thereon in order to detect infected systems based on observed malicious behaviors of monitored applications in order to initiate corrective action.

Helman fails to disclose the features of claim 20 for at least the reasons discussed above with respect to claim 1. *MSDN*, upon which the Office also relies, fails to reconcile these deficiencies of *Helman*.

Moreover, contrary to claim 20, *MSDN* describes Microsoft Windows WMI, which does ***not*** expose runtime activities. Microsoft Windows WMI, as described by *MSDN*, provides native query expressions that are *limited* to audit and performance metrics that are inadequate for the evaluation of whether an application's actions are malicious in intent. Claim 20 improve upon *MSDN by extending the instrumentation to capture runtime activities*. This feature is clearly not taught by *MSDN*.

Accordingly, for at least the reasons set forth above, Applicants respectfully submit that the applied documents, whether taken individually or in proper combination, fail to disclose or suggest the claimed subject matter, and therefore, cannot support a *prima facie* case for rejecting claim 20 under 35 U.S.C. §103(a). Thus, Applicants respectfully submit that independent claim 20 is patentably distinct from *Helman* and *MSDN* and request that the rejection be withdrawn.

CONCLUSION

All of the stated grounds of rejection have been properly traversed or rendered moot. Applicants therefore respectfully request that the Examiner reconsider and withdraw all presently outstanding rejections. Applicants believe that a full and complete response has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Amendment is respectfully requested.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: October 1, 2013

By: /Jennifer A. Wilson/
Jennifer A. Wilson
Registration No. 62,604

Customer No. 21839
703 836 6620

Electronic Acknowledgement Receipt	
EFS ID:	17004372
Application Number:	13559766
International Application Number:	
Confirmation Number:	9330
Title of Invention:	SYSTEMS AND METHODS FOR THREAT IDENTIFICATION AND REMEDIATION
First Named Inventor/Applicant Name:	Srinivas KUMAR
Customer Number:	21839
Filer:	Jennifer A. Wilson/Rosemary Shelton
Filer Authorized By:	Jennifer A. Wilson
Attorney Docket Number:	0079152-000016
Receipt Date:	01-OCT-2013
Filing Date:	27-JUL-2012
Time Stamp:	15:01:35
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		0079152016AMD.pdf	145048 c2bcce75dc1a6516359dc27fef7fcbb3cd36cab9	yes	32

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Specification	2	6
	Claims	7	15
	Applicant Arguments/Remarks Made in an Amendment	16	32
Warnings:			
Information:			
	Total Files Size (in bytes):	145048	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/559,766	Filing Date 07/27/2012	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)		
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)		
AMENDMENT	10/01/2013	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0	X $80 =	0
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $420 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	**0**

		(Column 1)		(Column 2)	(Column 3)		
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/TERRY MALLOY/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	13559732
Filing Date	2012-07-27
First Named Inventor	Srinivas, KUMAR
Art Unit	2492
Examiner Name	MEJIA, FELICIANO S.
Attorney Docket Number	0079152-000016

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7174566	B2	2007-02-06	YADAV	
	2	7370359	B2	2008-05-06	HRABIK et al.	
	3	8010469	B2	2011-08-30	KAPOOR et al.	
	4	8214497	B2	2012-07-03	ALPEROVITCH et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20060015942	A1	2006-01-19	JUDGE et al.	
	2	20080276317	A1	2008-11-06	CHANDOLA et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13559732
	Filing Date	2012-07-27
	First Named Inventor	Srinivas, KUMAR
	Art Unit	2492
	Examiner Name	MEJIA, FELICIANO S.
	Attorney Docket Number	0079152-000016

	3	20110072506	A1	2011-03-24	LAW et al.	
	4	20110162073	A1	2011-06-30	JESCHKE et al.	
	5	20110276468	A1	2011-11-10	LEWIS et al.	
	6	20120011590	A1	2012-01-12	DONOVAN	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	20110027386	KR	A	2011-03-16	MOZENSOFT INC.		☒

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	International Search Report and Written Opinion dated August 27, 2013, issued in corresponding International Application No. PCT/US2013/039033; 16 pp	☐
	2	Office Action issued in copending U.S. Patent Application No. 13/559,732, mailed June 20, 2013; 32 pp	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

IPR2023-01466
CrowdStrike EX1002 Page 237

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13559732
	Filing Date	2012-07-27
	First Named Inventor	Srinivas, KUMAR
	Art Unit	2492
	Examiner Name	MEJIA, FELICIANO S.
	Attorney Docket Number	0079152-000016

EXAMINER SIGNATURE			
Examiner Signature		Date Considered	
*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.			

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13559732
	Filing Date	2012-07-27
	First Named Inventor	Srinivas, KUMAR
	Art Unit	2492
	Examiner Name	MEJIA, FELICIANO S.
	Attorney Docket Number	0079152-000016

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☒ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Jennifer A. Wilson/	Date (YYYY-MM-DD)	2013-09-19
Name/Print	Jennifer A. Wilson	Registration Number	62,604

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	)	**MAIL STOP**
Srinivas KUMAR et al.	)	Group Art Unit: 2431
Application No.: 13/559,766	)	Examiner: SAVENKOV, Vadim
Filed: July 27, 2012	)	Confirmation No.: 9330
For: SYSTEMS AND METHODS FOR THREAT IDENTIFICATION AND REMEDIATION	)	

SECOND INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Madam:

In accordance with the duty of disclosure as set forth in 37 C.F.R. § 1.56, the accompanying information is being submitted in accordance with 37 C.F.R. §§ 1.97 and 1.98.

Pursuant to 37 C.F.R. § 1.98, a copy of each of the cited documents, other than U.S. patents and U.S. patent application publications, is enclosed.

Applicants hereby submit the International Search Report and Written Opinion dated August 27, 2013, issued in corresponding International Application No. PCT/US2013/039033, and documents cited therein. These documents were first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

In addition, Applicants also submit herewith the Office Action dated June 20, 2013 issued in co-pending U.S. Application Number 13/559,732, as well as documents cited therein. To the knowledge of the person signing the certification after making reasonable inquiry, the above-identified U.S Office Action, and documents cited therein, were not known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

To assist the Examiner, the documents are listed on the attached citation form. It is respectfully requested that an Examiner initialed copy of this form be returned to the undersigned.

The Director is hereby authorized to charge any appropriate fees under 37 C.F.R. §§ 1.16, 1.17 and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 02-4800.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: September 19, 2013

By: _____
Jennifer A. Wilson
Registration No. 62,604

Customer No. 21839
703 836 6620

Espacenet

Bibliographic data: KR20110027386 (A) — 2011-03-16

APPARATUS, SYSTEM AND METHOD FOR PROTECTING MALICIOUS PACKETS TRANSMITTED OUTSIDE FROM USER TERMINAL

No documents available for this priority number.

Inventor(s): ROH CHUL HEE [KR] ± (ROH, CHUL HEE)

Applicant(s): MOZENSOFT INC [KR] ± (MOZENSOFT INC)

Classification: **- international:** ***G06F21/00; H04L12/22***
- cooperative:

Application number: KR20090085455 20090910

Priority number(s): KR20090085455 20090910

Abstract of KR20110027386 (A)

PURPOSE: An apparatus for blocking a malicious packet, a system thereof and a method thereof are provided to confirm a user about a protocol of a packet, which is not modulated, and to block the attack of DoS/DDoS or worm virus. CONSTITUTION: A user terminal(100) installs a malicious packet blocking unit. A central managing server collects log information of the user terminal. A log storing database calculates statics by using the stored log information.

Last updated: 13.03.2013 Worldwide Database 5.8.11.1; 92p

IPR2023-01466
CrowdStrike EX1002 Page 243

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2011-0027386
(43) 공개일자 2011년03월16일

(51) Int. Cl.
H04L 12/22 (2006.01) *G06F 21/00* (2006.01)
(21) 출원번호 10-2009-0085455
(22) 출원일자 2009년09월10일
심사청구일자 2009년09월10일

(71) 출원인
모젠소프트 (주)
서울 광진구 군자동 98 세종대학교 충무관 311A
(72) 발명자
노철희
경기도 의정부시 호원동 현대아이파크 201-602
(74) 대리인
오세중

전체 청구항 수 : 총 17 항

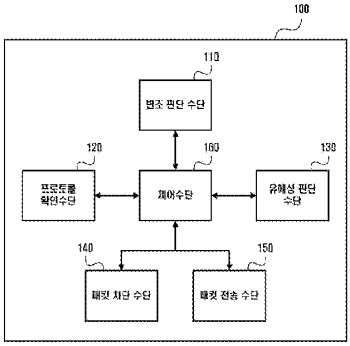
(54) 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치, 시스템 및 방법

(57) 요 약

사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치, 시스템 및 방법이 제공된다.

본 발명의 실시예에 따른 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치는, 사용자 단말로부터 나가는 패킷의 출발지 인터넷 프로토콜 주소가 변조되었는지 여부를 판단하는 변조 판단 수단; 상기 변조 판단 수단의 판단 결과 상기 출발지 인터넷 프로토콜 주소가 변조된 경우에는 상기 패킷을 차단하는 패킷 차단 수단을 포함한다.

대 표 도 - 도2



IPR2023-01466
CrowdStrike EX1002 Page 244

특허청구의 범위

청구항 1

사용자 단말로부터 나가는 패킷의 출발지 인터넷 프로토콜 주소가 변조되었는지 여부를 판단하는 변조 판단 수단;

상기 변조 판단 수단의 판단 결과 상기 출발지 인터넷 프로토콜 주소가 변조된 경우에는 상기 패킷을 차단하는 패킷 차단 수단을 포함하는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치.

청구항 2

제 1 항에 있어서,

상기 변조 판단 수단의 판단 결과 상기 출발지 인터넷 프로토콜 주소가 변조되지 않은 경우에는 상기 패킷의 프로토콜을 확인하는 프로토콜 확인 수단;

상기 확인된 프로토콜 별로 유해성 여부를 판단하는 유해성 판단 수단;

상기 유해성 판단 수단의 판단 결과 유해하지 않은 경우에는 상기 패킷을 외부로 전송하는 패킷 전송 수단을 더 포함하며,

상기 유해성 판단 수단의 판단 결과 유해한 경우에는 상기 패킷 차단 수단이 상기 패킷을 차단하는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치.

청구항 3

제 2 항에 있어서,

상기 변조 판단 수단은,

상기 사용자 단말로부터 나가는 패킷의 헤더 영역의 인터넷 프로토콜 주소와 상기 사용자 단말에 설정되어 있는 인터넷 프로토콜 주소를 비교함으로써 변조되었는지 여부를 판단하는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치.

청구항 4

제 2 항 또는 제 3 항에 있어서,

상기 유해성 판단 수단은,

상기 사용자 단말로부터 분당 전송되는 패킷의 수가 임계치를 초과하는지 여부를 판단하여 상기 임계치를 초과하는 경우에는 상기 패킷이 유해하다고 판단하고, 상기 임계치 이하인 경우에는 상기 패킷이 유해하지 않는 것으로 판단하는 임계치 초과 판단 수단;

상기 임계치 초과 판단 수단의 판단 결과 상기 임계치 이하인 경우 상기 패킷의 프래그먼트를 검사하여 프래그먼트 공격이 있는지를 탐지하여 상기 프래그먼트 공격이 있는 경우에는 상기 패킷이 유해하다고 판단하고, 상기 프래그먼트 공격이 없는 경우에는 상기 패킷이 유해하지 않는 것으로 판단하는 프래그먼트 검사 수단을 포함하는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치.

청구항 5

제 4 항에 있어서,

상기 프로토콜 확인 수단의 확인 결과 상기 패킷이 UDP(User Datagram Protocol) 패킷인 경우에,

상기 임계치 초과 판단 수단은, 분당 전송되는 UDP 패킷의 수가 UDP 임계치를 초과하는지 여부를 판단하여 상기 UDP 임계치를 초과하는 경우 상기 UDP 패킷이 유해하다고 판단하며,

상기 프래그먼트 검사 수단은, 상기 임계치 초과 판단 수단의 판단 결과 상기 UDP 임계치 이하인 경우에는 상기 UDP 패킷의 프래그먼트를 검사하여 상기 프래그먼트 공격이 있는 경우에는 상기 UDP 패킷이 유해하다고 판단하고, 상기 프래그먼트 공격이 없는 경우에는 상기 UDP 패킷이 유해하지 않는 것으로 판단하는, 사용자 단말로부

IPR2023-01466
CrowdStrike EX1002 Page 245

터 외부로 나가는 유해 패킷을 차단하는 장치.

청구항 6

제 4 항에 있어서,

상기 프로토콜 확인 수단의 확인 결과 상기 패킷이 TCP 패킷인 경우에,

상기 임계치 초과 판단 수단은,

분당 전송되는 TCP Syn/Ack 패킷의 수가 TCP Syn/Ack 임계치를 초과하는지 여부를 판단하여 상기 TCP Syn/Ack 임계치를 초과하는 경우 상기 TCP Syn/Ack 패킷이 유해하다고 판단하며, 상기 TCP Syn/Ack 임계치 이하인 경우에는 분당 전송되는 TCP Get 패킷의 수가 TCP Get 임계치를 초과하는지 여부를 판단하여 상기 TCP Get 임계치를 초과하는 경우 상기 TCP Get 패킷이 유해하다고 판단하며, 상기 TCP Get 임계치 이하인 경우에는 분당 전송되는 TCP RST/FIN 패킷의 수가 TCP RST/FIN 임계치를 초과하는지 여부를 판단하여 상기 TCP RST/FIN 임계치를 초과하는 경우 상기 TCP RST/FIN 패킷이 유해하다고 판단하며,

상기 프래그먼트 검사 수단은, 상기 임계치 초과 판단 수단의 판단 결과 상기 TCP RST/FIN 임계치 이하인 경우에는 상기 TCP RST/FIN 패킷의 프래그먼트를 검사하여 상기 프래그먼트 공격이 있는 경우에는 상기 TCP RST/FIN 패킷이 유해하다고 판단하고, 상기 프래그먼트 공격이 없는 경우에는 상기 TCP RST/FIN 패킷이 유해하지 않는 것으로 판단하는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치.

청구항 7

제 4 항에 있어서,

상기 프로토콜 확인 수단의 확인 결과 상기 패킷이 ICMP(Internet Control Message Protocol) 패킷인 경우에,

상기 임계치 초과 판단 수단은, 분당 전송되는 ICMP 패킷의 수가 ICMP 임계치를 초과하는지 여부를 판단하여 상기 ICMP 임계치를 초과하는 경우 상기 ICMP 패킷이 유해하다고 판단하며,

상기 프래그먼트 검사 수단은, 상기 임계치 초과 판단 수단의 판단 결과 상기 ICMP 임계치 이하인 경우에는 상기 ICMP 패킷의 프래그먼트를 검사하여 상기 프래그먼트 공격이 있는 경우에는 상기 ICMP 패킷이 유해하다고 판단하고, 상기 프래그먼트 공격이 없는 경우에는 상기 ICMP 패킷이 유해하지 않는 것으로 판단하는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치.

청구항 8

외부로 전송되는 패킷의 출발지 인터넷 프로토콜 주소의 변조 여부를 파악하여 변조된 패킷을 차단하고, 변조되지 않은 패킷의 전송 개수와 임계치의 비교 결과에 따라 유해한 패킷을 차단하는 유해 패킷 차단 장치가 설치된 사용자 단말;

복수의 사용자 단말에 각각 설치되어 있는 상기 유해 패킷 차단 장치를 관리하며, 상기 사용자 단말의 보안 정책을 설정하고, 상기 사용자 단말의 로그 정보를 수집하는 중앙 관리 서버;

상기 수집된 로그 정보를 저장하고, 상기 저장된 로그 정보를 이용하여 통계를 산출하는 로그 저장 데이터베이스를 포함하는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 시스템.

청구항 9

제 8 항에 있어서,

상기 유해 패킷 차단 장치는,

상기 사용자 단말로부터 나가는 패킷의 출발지 인터넷 프로토콜 주소가 변조되었는지 여부를 판단하는 변조 판단 수단;

상기 판단 결과 상기 출발지 인터넷 프로토콜 주소가 변조되지 않은 경우에는 상기 패킷의 프로토콜을 확인하는 프로토콜 확인 수단;

상기 확인된 프로토콜 별로 유해성 여부를 판단하는 유해성 판단 수단;

IPR2023-01466
CrowdStrike EX1002 Page 246

상기 변조 판단 수단의 판단 결과 상기 출발지 인터넷 프로토콜 주소가 변조된 경우 또는 상기 유해성 판단 수단의 판단 결과 유해한 경우에는 상기 패킷을 차단하는 패킷 차단 수단;

상기 유해성 판단 수단의 판단 결과 유해하지 않은 경우에는 상기 패킷을 외부로 전송하는 패킷 전송 수단을 포함하는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 시스템.

청구항 10

제 8 항에 있어서,

상기 변조 판단 수단은,

상기 사용자 단말로부터 나가는 패킷의 헤더 영역의 인터넷 프로토콜 주소와 상기 사용자 단말에 설정되어 있는 인터넷 프로토콜 주소를 비교함으로써 변조되었는지 여부를 판단하는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 시스템.

청구항 11

제 8 항에 있어서,

상기 중앙 관리 서버는,

상기 출발지 인터넷 프로토콜 주소가 변조된 패킷 또는 상기 유해성 판단 수단의 판단 결과 유해하다고 판단된 패킷의 활동 통계를 산출하고, 상기 산출된 활동 통계의 분석 결과 위험하다고 판단되는 경우 상기 사용자 단말에게 실시간으로 통지하는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 시스템.

청구항 12

사용자 단말로부터 나가는 패킷의 출발지 인터넷 프로토콜 주소가 변조되었는지 여부를 판단하는 단계;

상기 판단 결과 상기 출발지 인터넷 프로토콜 주소가 변조된 경우에는 상기 패킷을 차단하는 단계를 포함하는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 방법.

청구항 13

제 12 항에 있어서,

상기 판단 결과 상기 출발지 인터넷 프로토콜 주소가 변조되지 않은 경우에는 상기 패킷의 프로토콜을 확인하는 단계;

상기 확인된 프로도콜 별로 유해성 여부를 판단하는 단계;

상기 유해성 여부의 판단 결과 유해한 경우에는 상기 패킷을 차단하고, 유해하지 않은 경우에는 상기 패킷을 외부로 전송하는 단계를 포함하는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 방법.

청구항 14

제 12 항 또는 제 13 항에 있어서,

상기 출발지 인터넷 프로토콜 주소가 변조되었는지 여부를 판단하는 단계는,

상기 사용자 단말로부터 나가는 패킷의 헤더 영역의 인터넷 프로토콜 주소와 상기 사용자 단말에 설정되어 있는 인터넷 프로토콜 주소를 비교함으로써 변조되었는지 여부를 판단하는 단계인, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 방법.

청구항 15

제 13 항에 있어서,

상기 유해성 여부를 판단하는 단계는,

상기 패킷의 프로토콜을 확인한 결과 상기 패킷이 UDP(User Datagram Protocol) 패킷인 경우에는,

분당 전송되는 UDP 패킷의 수가 UDP 임계치를 초과하는지 여부를 판단하는 단계;

IPR2023-01466
CrowdStrike EX1002 Page 247

상기 UDP 임계치를 초과하는 경우에는 상기 UDP 패킷이 유해하다고 판단하고, 상기 UDP 임계치 이하인 경우에는 상기 UDP 패킷의 프래그먼트를 검사하여 프래그먼트 공격이 있는지를 탐지하는 단계;

상기 프래그먼트 공격이 있는 경우에는 상기 UDP 패킷이 유해하다고 판단하고, 상기 프래그먼트 공격이 없는 경우에는 상기 UDP 패킷이 유해하지 않는 것으로 판단하는 단계를 포함하는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 방법.

청구항 16

제 13 항에 있어서,

상기 유해성 여부를 판단하는 단계는,

상기 패킷의 프로토콜을 확인한 결과 상기 패킷이 TCP 패킷인 경우에는,

분당 전송되는 TCP Syn/Ack 패킷의 수가 TCP Syn/Ack 임계치를 초과하는지 여부를 판단하는 단계;

상기 TCP Syn/Ack 임계치를 초과하는 경우에는 상기 TCP Syn/Ack 패킷이 유해하다고 판단하고, 상기 TCP Syn/Ack 임계치 이하인 경우에는 분당 전송되는 TCP Get 패킷의 수가 TCP Get 임계치를 초과하는지 여부를 판단하는 단계;

상기 TCP Get 임계치를 초과하는 경우에는 상기 TCP Get 패킷이 유해하다고 판단하고, 상기 TCP Get 임계치 이하인 경우에는 분당 전송되는 TCP RST/FIN 패킷의 수가 TCP RST/FIN 임계치를 초과하는지 여부를 판단하는 단계;

상기 TCP RST/FIN 임계치를 초과하는 경우에는 상기 TCP RST/FIN 패킷이 유해하다고 판단하고, 상기 TCP RST/FIN 임계치 이하인 경우에는 상기 TCP RST/FIN 패킷의 프래그먼트를 검사하여 프래그먼트 공격이 있는지를 탐지하는 단계;

상기 프래그먼트 공격이 있는 경우에는 상기 TCP RST/FIN 패킷이 유해하다고 판단하고, 상기 프래그먼트 공격이 없는 경우에는 상기 TCP RST/FIN 패킷이 유해하지 않는 것으로 판단하는 단계를 포함하는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 방법.

청구항 17

제 13 항에 있어서,

상기 유해성 여부를 판단하는 단계는,

상기 패킷의 프로토콜을 확인한 결과 상기 패킷이 ICMP(Internet Control Message Protocol) 패킷인 경우에는,

분당 전송되는 ICMP 패킷의 수가 ICMP 임계치를 초과하는지 여부를 판단하는 단계;

상기 ICMP 임계치를 초과하는 경우에는 상기 ICMP 패킷이 유해하다고 판단하고, 상기 ICMP 임계치 이하인 경우에는 상기 ICMP 패킷의 프래그먼트를 검사하여 프래그먼트 공격이 있는지를 탐지하는 단계;

상기 프래그먼트 공격이 있는 경우에는 상기 ICMP 패킷이 유해하다고 판단하고, 상기 프래그먼트 공격이 없는 경우에는 상기 ICMP 패킷이 유해하지 않는 것으로 판단하는 단계를 포함하는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 방법.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치, 시스템 및 방법에 관한 것으로서, 더욱 상세하게는, 사용자 단말로부터 나가는 패킷의 출발지 IP 주소가 변조되었는지 여부를 판단하여 출발지 IP 주소가 변조된 패킷을 차단하며, 변조되지 않은 패킷의 프로토콜을 확인하여 프로토콜 별로 유해성 여부를 판단하여 패킷을 차단할 수 있는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치, 시스템 및 방법에

IPR2023-01466
CrowdStrike EX1002 Page 248

관한 것이다.

배경기술

[0002] 서비스 거부 공격(Denial of Service Attack, 이하 'DoS 공격'이라 한다)이란 외부 공격자가 특정 컴퓨터 시스템과 그 시스템이 속한 네트워크에 과다한 데이터를 보냄으로써 시스템과 네트워크의 성능을 급격히 저하시켜 정상적인 운영을 방해하여 그 컴퓨터 시스템이 사용자에 대한 서비스의 제공을 거부하도록 하는 공격 방법이다.

[0003] 또한, 분산 서비스 거부 공격(Distributed Denial of Service Attack, 이하 'DDoS 공격'이라 한다)이란 많은 수의 호스트들에 패킷을 범람시킬 수 있는 서비스 거부 공격용 프로그램들이 분산 설치되어 이들이 서로 통합된 형태로 어느 목표의 컴퓨터 시스템이나 네트워크의 성능을 저하시키거나 시스템을 마비시키는 것을 말한다.

[0004] 이러한 DoS 및 DDoS 공격은 TCP SYN 플러딩 공격, UDP 플러딩 공격, ICMP(Internet Control Message Protocol) 반향 요구(echo requesting) 공격, ICMP 동보(broadcasting) 공격의 형태로 나뉘어 진다. 이를 다시 크게 분류하면 플러딩 공격, IP 패킷의 부적절한 단편화를 기반으로 하는 공격, 부적절한 패킷 헤더 포맷 기반 공격으로 나눌 수 있다.

[0005] 일반적으로, DoS 공격이 이루어지는 과정을 살펴보면, DoS 에이전트(Agent)가 심어진 컴퓨터(공격자)에서 대량의 패킷을 발생시켜 호스트 컴퓨터를 공격함으로써, 호스트 컴퓨터가 정당한 다른 사용자들에게 서비스를 제대로 제공하지 못하도록 하여 서비스 거부 공격이 이루어진다.

[0006] 이러한 서비스 거부 공격은 공격자 컴퓨터가 IP 주소를 위장하면서 공격 목표 호스트 컴퓨터에 TCP 접속을 위한 동기 신호를 무한으로 되풀이하여 보냄으로써 이루어지는데, 이 경우 호스트 컴퓨터는 이 위장된 IP 주소에 접속을 위한 신호를 응답하여 접속 준비가 되었음을 무한으로 되풀이하여 알리는 동작을 수행하므로 호스트 컴퓨터에 과부하가 걸려서 정당 사용자에게 서비스를 제공할 수 없게 된다.

[0007] 그런데, 기존의 DoS 또는 DDoS 방어 시스템 기술은 외부에서 내부 서버 또는 Victim 네트워크로 유입되는 공격을 차단하는 방향으로 개발되었다. 또한, IPS 시스템들도 외부에서 유입되는 Worm 바이러스 유입을 차단하도록 네트워크 경계선 상에서 방어를 한다. 하지만, 다양한 경로를 통해 Worm 바이러스에 감염되거나 부트 프로그램이 감염되어 대량의 좀비 PC가 양산되고 각 좀비 PC 단에서 공격이 시작되는 경우에는 효율적으로 대처하지 못하였다.

[0008] 이를 게이트웨이 보안의 측면에서 살펴보면, 변조된 IP 주소를 이용한 내부 사용자의 DoS 또는 DDoS 공격이나 웜 바이러스 확산을 원천적으로 탐지 및 차단하지 못하며, 이로 인하여 내부 네트워크의 안정성 확보가 어렵게 된다. 또한, 변조된 IP 주소를 이용한 내부 네트워크에서의 좀비 PC의 활동을 막기가 어렵다는 문제가 있었다.

[0009] 또한, 사용자 PC의 보안의 측면에서 살펴보면, 첫째, 기존의 백신 프로그램의 경우 DDoS 공격이나 웜 바이러스 공격이 발생한 후 활동 내역을 분석하여 백신이 개발되는 바, 이는 공격이 발생한 이후의 사후 처리를 위한 해결책은 되지만 사전에 DoS/DDoS나 웜 바이러스의 활동을 제한하거나 예방하는 역할은 못하였다. 둘째, 기존의 PC 방화벽의 경우 사용자 PC로부터 나가는 패킷에 대해서는 웹 서비스에 대한 접속을 무제한으로 허용하기 때문에 DoS/DDoS 공격에 가담하는 좀비 PC를 구분해 내지 못하였다.

발명의 내용

해결 하고자하는 과제

[0010] 따라서, 상술한 문제점을 해결하기 위하여 본 발명이 해결하고자 하는 과제는, 게이트웨이 단에서 방어하는 기존의 백신 프로그램의 한계를 극복하기 위해 공격에 가담하는 사용자 PC 단에서 원천적으로 DoS/DDoS나 웜 바이러스의 공격을 차단하고자 하는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치, 시스템 및 방법을 제공하는 것이다.

[0011] 또한, 본 발명이 해결하고자 하는 다른 기술적 과제는, 자기 복제 기능을 통해 다른 컴퓨터나 내부 네트워크의 전산 시스템 등을 감염시키는 유해 트래픽의 확산을 사전에 감염된 PC에서 탐지하여 차단할 수 있는, 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치, 시스템 및 방법을 제공하는 것이다.

[0012] 본 발명이 해결하고자 하는 과제들은 이상에서 언급한 과제들로 제한되지 않으며, 언급되지 않은 또 다른 과제들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

IPR2023-01466
CrowdStrike EX1002 Page 249

과제 해결수단

[0013] 전술한 기술적 과제를 달성하기 위한 본 발명의 실시예에 따른 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치는, 사용자 단말로부터 나가는 패킷의 출발지 인터넷 프로토콜 주소가 변조되었는지 여부를 판단하는 변조 판단 수단; 상기 변조 판단 수단의 판단 결과 상기 출발지 인터넷 프로토콜 주소가 변조된 경우에는 상기 패킷을 차단하는 패킷 차단 수단을 포함한다.

[0014] 또한, 전술한 기술적 과제를 달성하기 위한 본 발명의 다른 실시예에 따른 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 시스템은, 외부로 전송되는 패킷의 출발지 인터넷 프로토콜 주소의 변조 여부를 파악하여 변조된 패킷을 차단하고, 변조되지 않은 패킷의 전송 개수와 임계치의 비교 결과에 따라 유해한 패킷을 차단하는 유해 패킷 차단 장치가 설치된 사용자 단말; 복수의 사용자 단말에 각각 설치되어 있는 상기 유해 패킷 차단 장치를 관리하며, 상기 사용자 단말의 보안 정책을 설정하고, 상기 사용자 단말의 로그 정보를 수집하는 중앙 관리 서버; 상기 수집된 로그 정보를 저장하고, 상기 저장된 로그 정보를 이용하여 통계를 산출하는 로그 저장 데이터베이스를 포함한다.

[0015] 또한, 전술한 기술적 과제를 달성하기 위한 본 발명의 또 다른 실시예에 따른 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 방법은, 사용자 단말로부터 나가는 패킷의 출발지 인터넷 프로토콜 주소가 변조되었는지 여부를 판단하는 단계; 상기 판단 결과 상기 출발지 인터넷 프로토콜 주소가 변조된 경우에는 상기 패킷을 차단하는 단계를 포함한다.

[0016] 기타 실시예들의 구체적인 사항들은 상세한 설명 및 도면들에 포함되어 있다.

효 과

[0017] 상기한 바와 같은 본 발명의 실시예에 따른 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치, 시스템 및 방법에 의하면, 다음과 같은 효과가 하나 이상 존재한다.

[0018] 첫째, 게이트웨이 단에서 방어하는 기존의 백신 프로그램의 한계를 극복하여 사용자 PC 단에서 원천적으로 DoS/DDoS나 웜 바이러스의 공격을 차단할 수 있다.

[0019] 둘째, 자기 복제 기능을 통해 다른 컴퓨터나 내부 네트워크의 전산 시스템 등을 감염시키는 유해 트래픽의 확산을 사전에 감염된 PC에서 탐지하여 차단할 수 있다.

[0020] 본 발명의 효과들은 이상에서 언급한 효과들로 제한되지 않으며, 언급되지 않은 또 다른 효과들은 청구범위의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

발명의 실시를 위한 구체적인 내용

[0021] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 명세서 전체에 걸쳐 동일 참조 부호는 동일 구성 요소를 지칭한다.

[0022] 본 명세서에서 사용된 용어는 실시예들을 설명하기 위한 것이며 본 발명을 제한하고자 하는 것은 아니다. 본 명세서에서, 단수형은 문구에서 특별히 언급하지 않는 한 복수형도 포함한다. 명세서에서 사용되는 "포함한다(comprises)" 및/또는 "포함하는(comprising)"은 언급된 구성요소, 단계, 동작 및/또는 소자는 하나 이상의 다른 구성요소, 단계, 동작 및/또는 소자의 존재 또는 추가를 배제하지 않는다. 다른 정의가 없다면, 본 명세서에서 사용되는 모든 용어(기술 및 과학적 용어를 포함)는 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 공통적으로 이해될 수 있는 의미로 사용될 수 있을 것이다. 또 일반적으로 사용되는 사전에 정의되어 있는 용어들은 명백하게 특별히 정의되어 있지 않는 한 이상적으로 또는 과도하게 해석되지 않는다.

[0023] 이하, 본 발명을 보다 구체적으로 설명하기 위하여 본 발명에 따른 실시예들을 첨부 도면을 참조하면서 보다 상세하게 설명하고자 한다.

[0024] 도 1은 본 발명의 일 실시예에 따른 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 시스템의 전체 구성도를 나타내는 도면이다.

IPR2023-01466
CrowdStrike EX1002 Page 250

[0025] 도 1을 참조하면, 상기 시스템은 사용자 단말(100), 중앙 관리 서버(200), 관리 콘솔(300), 로그 저장 데이터베이스(400)을 포함하여 구성된다.

[0026] 사용자 단말(100)은 본 발명의 실시예에서의 유해 패킷 차단 장치가 구비된 단말로서, 네트워크의 종단에 위치한 개인용 컴퓨터나 네트워크 내부의 서버 등 네트워크에 연결되어 있는 전산 장치이기만 하면 되고, 연결 방식이 유선이든 무선이든 무관하다.

[0027] 본 발명에서 유해 패킷 차단 장치가 구비된 사용자 단말(100)은 자신에게서 외부로 나가는 패킷의 출발지 IP(Internet Protocol) 주소의 변조 여부를 파악하여 변조된 패킷에 대해서는 외부로 내보내지 않고 차단하며, 변조되지 않은 패킷에 대해서는 변조되지 않은 패킷의 분당 전송수가 소정의 임계치를 초과하는 경우에는 유해한 트래픽이 존재한다고 보아 차단하는 역할을 한다. 사용자 단말(100)에 구비된 유해 패킷 차단 장치의 구성과 역할에 대해서는 후술할 도 2에서 설명하기로 한다.

[0028] 그 밖에도 사용자 단말(100)은 자신의 네트워크 활동 상황을 모니터링하여 중앙 관리 서버(200)로 보고하며, 변조되지 않은 패킷의 전송에 대해서는 정상적인 연결을 보장하며, 보안 감사 기록을 중앙 관리 서버(200)로 전송할 수 있다.

[0029] 중앙 관리 서버(200)는 전술한 사용자 단말(100)에 각각 설치되어 있는 상기 유해 패킷 차단 장치를 관리하는 서버로서, 사용자 단말(100)의 보안 정책을 설정하여 제어하고, 사용자 단말(100)의 개별적인 로그 정보를 수집하여 통계를 산출할 수 있다. 또한, 사용자 단말(100)의 보안 상태를 실시간으로 모니터링하여 각 사용자 단말(100) 별 보고서를 작성할 수 있으며, 전사적으로 DDoS나 웜 바이러스와 같은 유해 트래픽의 활동을 기간별로 분석하여 기간별 보고서를 생성할 수도 있다.

[0030] 또한, 중앙 관리 서버(200)는 출발지 IP 주소가 변조된 패킷 또는 IP 주소가 변조되지 않았으나 유해하다고 판단된 패킷의 활동 통계를 산출하고, 상기 산출된 활동 통계의 분석 결과 위험하다고 판단되는 경우 사용자 단말(100)에게 실시간으로 통지할 수 있다.

[0031] 관리 콘솔(300)은 중앙 관리 서버(200)에 접근하기 위한 장치로서, 사용자 단말(100) 내부에 설치된 유해 패킷 차단 장치의 정책을 수립하는 역할을 할 수 있다.

[0032] 로그 저장 데이터베이스(400)는 중앙 관리 서버(200)에 의해 수집된 사용자 단말(100)의 로그 정보를 저장하고, 상기 저장된 로그 정보를 이용하여 통계를 산출하는 역할을 한다.

[0033] 도 2는 본 발명의 실시예에 따른 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치의 구성을 나타내는 도면이다.

[0034] 상기 도 2를 참조하면, 유해 패킷을 차단하는 장치는 변조 판단 수단(110), 프로토콜 확인 수단(120), 유해성 판단 수단(130), 패킷 차단 수단(140), 패킷 전송 수단(150) 및 제어 수단(160)을 포함하여 구성된다.

[0035] 변조 판단 수단(110)은 사용자 단말(100)로부터 나가는 패킷의 출발지 IP 주소가 변조되었는지 여부를 판단하는 역할을 한다. 여기서, 패킷의 출발지 IP 주소의 변조 여부는 도 5를 참조하여 설명하기로 한다.

[0036] 도 5는 본 발명의 실시예에 따른 사용자 단말로부터 나가는 패킷의 출발지 IP 주소의 변조 여부를 판단하는 원리를 나타내는 도면이다. 즉, 도 5에서 알 수 있듯이, 사용자 단말로부터 나가는 패킷의 헤더 영역에는 출발지(Source) IP, 출발지 포트 번호, 목적지(Destination) IP, 및 목적지 포트 번호에 대한 정보가 기재되어 있는데, 이 중 출발지 IP 주소와 상기 사용자 단말에 설정되어 있는 IP 주소(도 5에서는 192.168.2.7)를 비교함으로써 변조되었는지 여부를 판단하게 된다.

[0037] 일반적으로, DDoS 공격이나 웜 바이러스의 확산시 발생하는 유해 트래픽의 내용 중 거의 대부분이 출발지 IP 주소를 변조하여 공격하므로 출발지 IP 주소가 변조되었는지 여부를 탐지하여 차단하는 것은 DDoS 공격이나 웜 바이러스의 확산에 대한 초기 대응에서 매우 중요하다고 할 수 있다.

[0038] 다시 도 2를 참조하면, 프로토콜 확인 수단(120)은 변조 판단 수단(110)의 확인 결과 상기 출발지 IP 주소가 변조되지 않은 경우에는 상기 패킷의 프로토콜을 확인하는 역할을 한다.

[0039] 유해성 판단 수단(130)은 프로토콜 확인 수단(120)에 의해 확인된 프로토콜 별로 유해성 여부를 판단하는 역할을 한다.

[0040] 유해성 판단 수단의 구성을 나타내는 도 3을 참조하면, 유해성 판단 수단(130)은 임계치 초과 판단 수단(131)

IPR2023-01466
CrowdStrike EX1002 Page 251

및 프래그먼트 검사 수단(132)를 포함하여 구성됨을 알 수 있다.

[0041] 임계치 초과 판단 수단(131)은 사용자 단말로부터 분당 전송되는 패킷의 수가 임계치를 초과하는지 여부를 판단하여 상기 임계치를 초과하는 경우에는 상기 패킷이 유해하다고 판단하고, 상기 임계치 이하인 경우에는 상기 패킷이 유해하지 않는 것으로 판단하게 된다. 여기서, 상기 임계치는 프로토콜 확인 수단(120)에 의해 확인된 프로토콜에 따른 통신에 대해 중앙 관리 서버(200)로부터 내려받은 정책을 기반으로 설정할 수 있다.

[0042] 프래그먼트 검사 수단(132)은 상기 임계치 초과 판단 수단(131)의 판단 결과 상기 임계치 이하인 경우 상기 패킷의 프래그먼트를 검사하여 프래그먼트 공격이 있는지를 탐지하는 역할을 하는데, 상기 프래그먼트 공격이 있는 경우에는 상기 패킷이 유해하다고 판단하고, 상기 프래그먼트 공격이 없는 경우에는 상기 패킷이 유해하지 않는 것으로 판단하게 된다.

[0043] 여기서, 유해성 판단 수단(130)이 프로토콜 별로 유해성 여부를 판단하는 것을 좀 더 구체적으로 살펴보기로 한다.

[0044] 첫째, 프로토콜 확인 수단(120)의 확인 결과 사용자 단말(100)에서 나가는 패킷이 UDP(User Datagram Protocol) 패킷인 경우에는, 임계치 초과 판단 수단(131)은, 분당 전송되어 나가는 UDP 패킷의 수가 UDP 임계치를 초과하는지 여부를 판단하여 상기 UDP 임계치를 초과하는 경우 상기 UDP 패킷이 유해하다고 판단한다. 여기서, 상기 UDP 임계치는 UDP 통신에 대해 중앙 관리 서버(200)로부터 내려받은 정책을 기반으로 설정할 수 있다.

[0045] 또한, 프래그먼트 검사 수단(132)은, 임계치 초과 판단 수단(131)의 판단 결과 상기 UDP 임계치 이하인 경우에는 상기 UDP 패킷의 프래그먼트를 검사하여 상기 프래그먼트 공격이 있는 경우에는 상기 UDP 패킷이 유해하다고 판단하고, 상기 프래그먼트 공격이 없는 경우에는 상기 UDP 패킷이 유해하지 않는 것으로 판단하게 된다.

[0046] 둘째, 프로토콜 확인 수단(120)의 확인 결과 사용자 단말(100)에서 나가는 패킷이 TCP 패킷인 경우에는, 임계치 초과 판단 수단(131)은, 분당 전송되어 나가는 TCP Syn/Ack 패킷의 수가 TCP Syn/Ack 임계치를 초과하는지 여부를 판단하여 상기 TCP Syn/Ack 임계치를 초과하는 경우 상기 TCP Syn/Ack 패킷이 유해하다고 판단한다. 또한, 상기 TCP Syn/Ack 임계치 이하인 경우에는 분당 전송되어 나가는 TCP Get 패킷의 수가 TCP Get 임계치를 초과하는지 여부를 판단하여 상기 TCP Get 임계치를 초과하는 경우 상기 TCP Get 패킷이 유해하다고 판단한다. 또한, 상기 TCP Get 임계치 이하인 경우에는 분당 전송되어 나가는 TCP RST/FIN 패킷의 수가 TCP RST/FIN 임계치를 초과하는지 여부를 판단하여 상기 TCP RST/FIN 임계치를 초과하는 경우 상기 TCP RST/FIN 패킷이 유해하다고 판단한다.

[0047] 이 경우, 상기 임계치 초과 판단 수단(131)의 판단 결과 상기 TCP RST/FIN 임계치 이하인 경우에는, 프래그먼트 검사 수단(132)이 상기 TCP RST/FIN 패킷의 프래그먼트를 검사하여 상기 프래그먼트 공격이 있는 경우에는 상기 TCP RST/FIN 패킷이 유해하다고 판단하고, 상기 프래그먼트 공격이 없는 경우에는 상기 TCP RST/FIN 패킷이 유해하지 않는 것으로 판단한다.

[0048] 셋째, 프로토콜 확인 수단(120)의 확인 결과 사용자 단말(100)에서 나가는 패킷이 ICMP(Internet Control Message Protocol) 패킷인 경우에는, 임계치 초과 판단 수단(131)은 분당 전송되어 나가는 ICMP 패킷의 수가 ICMP 임계치를 초과하는지 여부를 판단하여 상기 ICMP 임계치를 초과하는 경우 상기 ICMP 패킷이 유해하다고 판단한다. 여기서, 상기 ICMP 임계치는 ICMP 통신에 대해 중앙 관리 서버(200)로부터 내려받은 정책을 기반으로 설정할 수 있다.

[0049] 또한, 프래그먼트 검사 수단(132)은, 상기 임계치 초과 판단 수단(131)의 판단 결과 상기 ICMP 임계치 이하인 경우에는 상기 ICMP 패킷의 프래그먼트를 검사하여 상기 프래그먼트 공격이 있는 경우에는 상기 ICMP 패킷이 유해하다고 판단하고, 상기 프래그먼트 공격이 없는 경우에는 상기 ICMP 패킷이 유해하지 않는 것으로 판단하게 된다.

[0050] 다시 도 2로 돌아오면, 패킷 차단 수단(140)은 변조 판단 수단(110)의 판단 결과 상기 출발지 IP 주소가 변조된 경우 또는 상기 유해성 판단 수단(130)의 판단 결과 유해한 패킷이라고 판단된 경우에는 그 패킷을 차단하는 역할을 할 수 있다.

[0051] 패킷 전송 수단(150)은 유해성 판단 수단(130)의 판단 결과 유해하지 않다고 판단된 경우에는 상기 패킷을 외부로 전송하는 역할을 한다.

[0052] 제어 수단(160)은 전술한 각 수단들을 제어하고 각 수단들 간에 상호 작용할 수 있도록 신호를 전달하는 역할을

IPR2023-01466
CrowdStrike EX1002 Page 252

한다.

[0053] 도 4는 본 발명의 실시예에 따른 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 방법의 전체 흐름을 나타내는 도면이다.

[0054] 먼저, 사용자 단말(100)로부터 나가는 패킷의 출발지 IP 주소가 변조되었는지 여부를 판단한다(S110).

[0055] 상기 판단 결과 변조된 경우에는 상기 패킷을 차단하고(S170), 변조되지 않은 경우에는 상기 패킷의 프로토콜을 확인하여 프로토콜 별로 유해성 여부를 판단한다(S120).

[0056] 여기서, 패킷의 프로토콜로는 크게 3가지로 나눌 수 있는 바, UDP, TCP 및 ICMP로 분류할 수 있다.

[0057] 먼저, 상기 패킷이 UDP(User Datagram Protocol) 패킷인 경우에는, 분당 전송되는 UDP 패킷의 수가 UDP 임계치를 초과하는지 여부를 판단한다(S132). 상기 UDP 임계치를 초과하는 경우에는 상기 UDP 패킷이 유해하다고 판단하고(S170), 상기 UDP 임계치 이하인 경우에는 상기 UDP 패킷의 프래그먼트를 검사하여 프래그먼트 공격이 있는지를 탐지한다(S134). 상기 프래그먼트 공격이 있는 경우에는 상기 UDP 패킷이 유해하다고 판단하고(S170), 상기 프래그먼트 공격이 없는 경우에는 상기 UDP 패킷이 유해하지 않는 것으로 판단하여 패킷을 외부로 전송한다(S160).

[0058] 둘째, 상기 패킷이 TCP 패킷인 경우에는, 분당 전송되는 TCP Syn/Ack 패킷의 수가 TCP Syn/Ack 임계치를 초과하는지 여부를 판단한다(S142). 여기서, TCP Syn/Ack 패킷의 정상적인 통신 과정에서는 도 6a에서와 같이, 사용자 PC와 서버가 통신을 위해 TCP 연결을 위해 서로의 응답을 확인하고 다음 연결 단계를 거쳐 안전하게 통신을 하게 된다. 하지만, 비정상적인 통신 과정에서는 도 6b에서와 같이, Victim 서버로의 연결 시도 후 응답 확인 과정을 거치지 않고 대량의 연결 시도를 반복적으로 수행함으로써, Victim 서버의 대기 큐를 고갈시키는 피해가 발생된다.

[0059] 이러한 Syn/Ack 공격은 중앙 관리 서버(200)로부터 내려받은 임계치 정책을 기반으로 대량의 단 방향성 연결시도를 차단 할 수 있다. 즉, 상기 TCP Syn/Ack 임계치를 초과하는 경우에는 상기 TCP Syn/Ack 패킷이 유해하다고 판단하고(S170), 상기 TCP Syn/Ack 임계치 이하인 경우에는 분당 전송되는 TCP Get 패킷의 수가 TCP Get 임계치를 초과하는지 여부를 판단한다(S144).

[0060] 여기서, TCP Get 패킷의 정상적인 통신 과정에서는 도 7a에서와 같이, 사용자 PC와 서버가 통신을 위해 서로의 응답을 확인하고 다음 연결 단계를 거쳐 안전하게 통신을 하게 된다. 하지만, 비정상적인 통신 과정에서는 도 7b에서와 같이, Victim 서버로의 연결 시도 후 응답 확인 과정을 거치지 않고 데이터 요청을 반복적으로 수행함으로써 Victim 자원을 고갈시키게 된다.

[0061] 이러한 서버 부하 유발 공격에 대해 중앙 관리 서버(200)로부터 내려받은 Get 패킷에 대한 임계치 정책을 기반으로 대량의 데이터 요청 공격인 Get 플러딩 공격을 차단할 수 있다. 즉, 상기 TCP Get 임계치를 초과하는 경우에는 상기 TCP Get 패킷이 유해하다고 판단하고(S170), 상기 TCP Get 임계치 이하인 경우에는 분당 전송되는 TCP RST/FIN 패킷의 수가 TCP RST/FIN 임계치를 초과하는지 여부를 판단한다(S146).

[0062] 상기 TCP RST/FIN 임계치를 초과하는 경우에는 상기 TCP RST/FIN 패킷이 유해하다고 판단하고(S170), 상기 TCP RST/FIN 임계치 이하인 경우에는 상기 TCP RST/FIN 패킷의 프래그먼트를 검사하여 프래그먼트 공격이 있는지 여부를 탐지한다(S148). 상기 프래그먼트 공격이 있는 경우에는 상기 TCP RST/FIN 패킷이 유해하다고 판단하고(S170), 상기 프래그먼트 공격이 없는 경우에는 상기 TCP RST/FIN 패킷이 유해하지 않는 것으로 판단하여 패킷을 외부로 전송한다(S160).

[0063] 셋째, 상기 패킷이 ICMP(Internet Control Message Protocol) 패킷인 경우에는, 분당 전송되는 ICMP 패킷의 수가 ICMP 임계치를 초과하는지 여부를 판단한다(S152). 상기 ICMP 임계치를 초과하는 경우에는 상기 ICMP 패킷이 유해하다고 판단하고(S170), 상기 ICMP 임계치 이하인 경우에는 상기 ICMP 패킷의 프래그먼트를 검사하여 프래그먼트 공격이 있는지를 탐지한다(S154). 상기 프래그먼트 공격이 있는 경우에는 상기 ICMP 패킷이 유해하다고 판단하고(S170), 상기 프래그먼트 공격이 없는 경우에는 상기 ICMP 패킷이 유해하지 않는 것으로 판단하여 패킷을 외부로 전송한다(S160).

[0064] 한편, 본 발명의 실시예에 따른 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 방법은 이 방법을 실행하기 위한 프로그램을 기록한 컴퓨터로 판독 가능한 기록매체에 저장되어 구현 가능하다.

[0065] 이상과 같이 본 발명을 도면에 도시한 실시예를 참고하여 설명하였으나, 이는 발명을 설명하기 위한 것일 뿐이

IPR2023-01466
CrowdStrike EX1002 Page 253

며, 본 발명이 속하는 기술 분야의 통상의 지식을 가진 자라면 발명의 상세한 설명으로부터 다양한 변형 또는 균등한 실시예가 가능하다는 것을 이해할 수 있을 것이다. 따라서 본 발명의 진정한 권리범위는 특허청구범위의 기술적 사상에 의해 결정되어야 한다.

도면의 간단한 설명

[0066] 도 1은 본 발명의 일 실시예에 따른 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 시스템의 전체 구성도를 나타내는 도면이다.

[0067] 도 2는 본 발명의 실시예에 따른 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 장치의 구성을 나타내는 도면이다.

[0068] 도 3은 상기 도 2에 도시된 유해성 판단 수단의 구성을 나타내는 도면이다.

[0069] 도 4는 본 발명의 실시예에 따른 사용자 단말로부터 외부로 나가는 유해 패킷을 차단하는 방법의 전체 흐름을 나타내는 도면이다.

[0070] 도 5는 본 발명의 실시예에 따른 사용자 단말로부터 나가는 패킷의 출발지 IP 주소의 변조 여부를 판단하는 원리를 나타내는 도면이다.

[0071] 도 6a는 TCP Syn/Ack 패킷의 정상적인 통신 과정을 나타내는 도면이다.

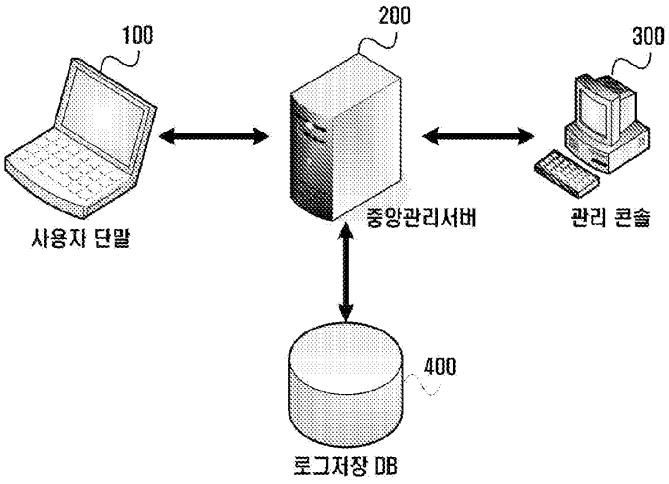
[0072] 도 6b는 TCP Syn/Ack 패킷의 공격 과정을 나타내는 도면이다.

[0073] 도 7a는 TCP Get 패킷의 정상적인 통신 과정을 나타내는 도면이다.

[0074] 도 7b는 TCP Get 패킷의 공격 과정을 나타내는 도면이다.

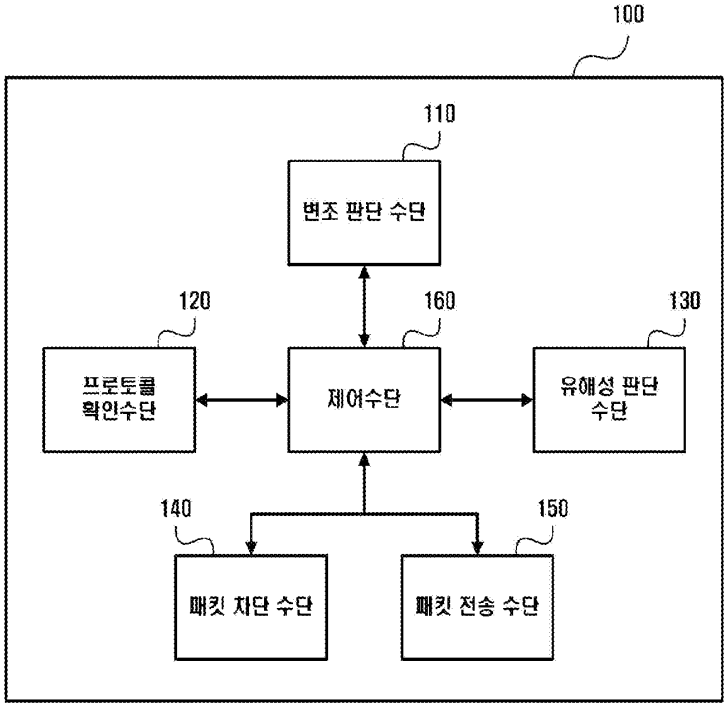
도면

도면1

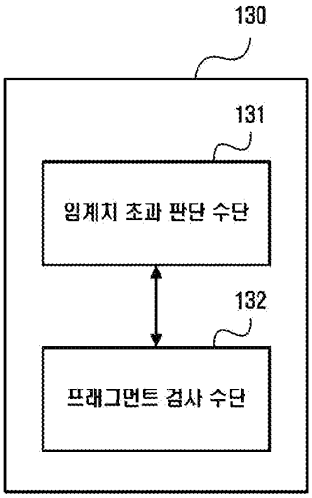


IPR2023-01466
CrowdStrike EX1002 Page 254

도면2

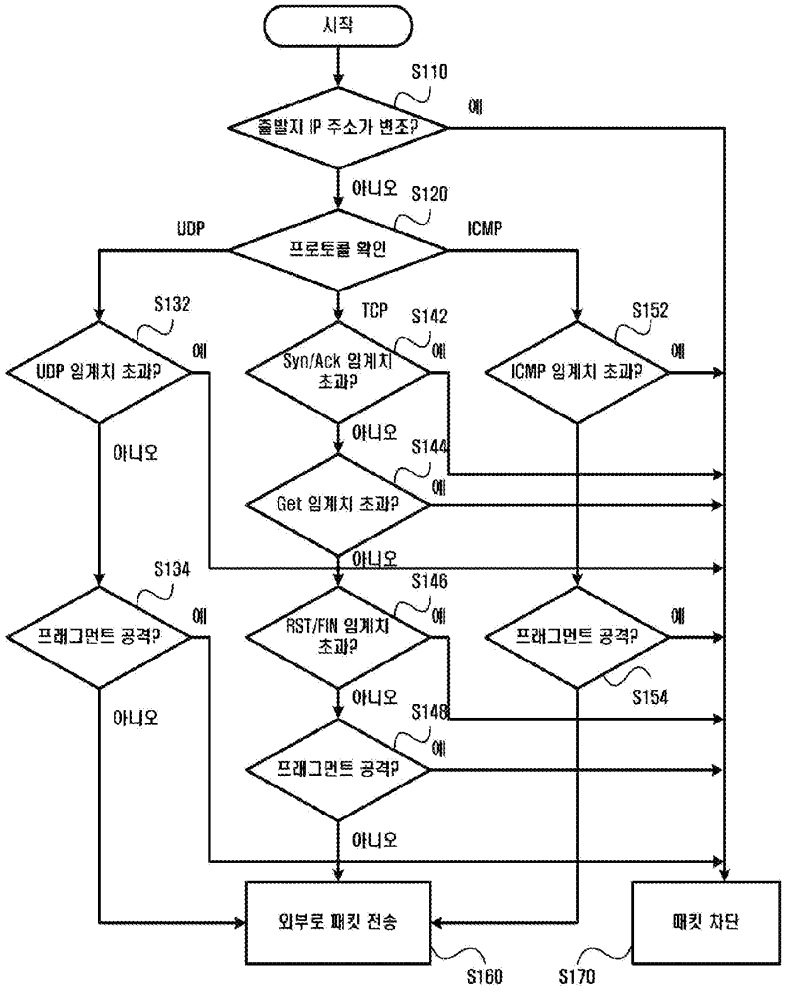


도면3

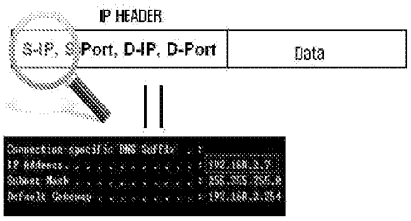


IPR2023-01466
CrowdStrike EX1002 Page 255

도면4

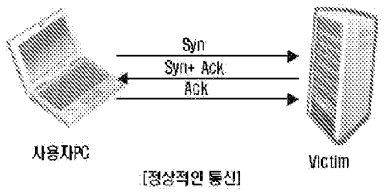


도면5

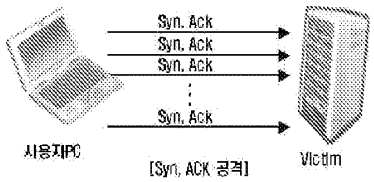


IPR2023-01466
CrowdStrike EX1002 Page 256

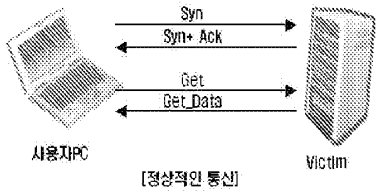
도면6a



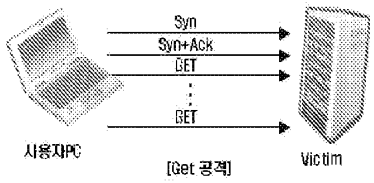
도면6b



도면7a



도면7b



IPR2023-01466
CrowdStrike EX1002 Page 257

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
WIELAND, CHARLES F., III

BUCHANAN INGERSOLL & ROONEY PC CUSTOMER NO. 21839 P. O. BOX 1404 ALEXANDRIA VA 22313-1404 USA

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

Date of mailing *(day/month/year)*	27 August 2013 (27.08.2013)
Applicant's or agent's file reference 0079152-0018	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. **PCT/US2013/039033**	International filing date *(day/month/year)* **01 May 2013 (01.05.2013)**
Applicant **TAASERA, INC.**	

1. ☒ The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:

   The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Facsimile No.: +41 22 338 82 70

   For more detailed instructions, see *PCT Applicant's Guide*, International Phase, paragraphs 9.004 . 9.011.

2. ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. ☐ **With regard to any protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with any request to forward the texts of both the protest and the decision thereon to the designated Offices.

   ☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.

Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before the completion of the technical preparations for international publication (Rules 90bis.1 and 90bis.3).

Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.
In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19months.

For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the PCT Applicant's Guide, National Chapters.

Name and mailing address of the ISA/KR Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer COMMISSIONER Telephone No. 82-42-481-8753

Form PCT/ISA/220 (July 2010)

* Attention

Copies of the documents cited in the international search report can be searched in the following Korean Intellectual Property Office English website for three months from the date of mailing of the international search report.

http://www.kipo.go.kr/en/ => PCT Services => PCT Services

ID : PCT international application number
PW : **XF7ED7CJ**

Inquiries related to PCT International Search Report or Written Opinion prepared by KIPO as an International Searching Authority can be answered not only by KIPO but also through IPKC (Intellectual Property Korea Center), located in Vienna, VA, which functions as a PCT Help Desk for PCT applicants.

Homepage: http://www.ipkcenter.com

Email: ipkc@ipkcenter.com

IPR2023-01466
CrowdStrike EX1002 Page 259

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 0079152-0018	FOR FURTHER ACTION	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. **PCT/US2013/039033**	International filing date *(day/month/year)* **01 May 2013 (01.05.2013)**	(Earliest) Priority Date *(day/month/year)* 01 May 2012 (01.05.2012)
Applicant **TAASERA, INC.**		

This International search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 3 sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language**, the international search was carried out on the basis of:
      ☒ the international application in the language in which it was filed
      ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).
   c. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.
2. ☐ **Certain claims were found unsearchable** (See Box No. II)
3. ☐ **Unity of invention is lacking** (See Box No. III)
4. With regard to the **title,**
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:
5. With regard to the **abstract,**
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.
6. With regard to the drawings,
   a. the figure of the **drawings** to be published with the abstract is Figure No. 1
      ☒ as suggested by the applicant.
      ☐ as selected by this Authority, because the applicant failed to suggest a figure.
      ☐ as selected by this Authority, because this figure better characterizes the invention.
   b. ☐ none of the figure is to be published with the abstract.

IPR2023-01466
CrowdStrike EX1002 Page 260

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2013/039033

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/50(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F 21/50; G06Q 40/00; G06F 11/00; G06F 21/00; H04L 12/22

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & keywords: cloud, mobile, integrity, alert, calculate, risk, rule, profile, trust, agent and similar terms.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2011-0162073 A1 (KONIKAYE JESCHKE) 30 June 2011 See paragraphs 20-49, 54; and figures 1-8.	1-106
A	US 2012-0011590 A1 (JOHN JOSEPH DONOVAN) 12 January 2012 See paragraphs 77-79; and figures 1, 8.	1-106
A	US 2011-0276468 A1 (MICHAEL LEWIS et al.) 10 November 2011 See paragraphs 44-49; and figure 3.	1-106
A	US 2011-0072506 A1 (GARY K. LAW et al.) 24 March 2011 See paragraphs 62-64; and figures 2, 15-16.	1-106
A	KR 10-2011-0027386 A (MOZENSOFT INC.) 16 March 2011 See paragraphs 33-35, 53-63; and figures 2-4.	1-106

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 August 2013 (26.08.2013)	**27 August 2013 (27.08.2013)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. +82-42-472-7140	Authorized officer BYUN Sung Cheal Telephone No. +82-42-481-8262

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2013/039033

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011-0162073 A1	30/06/2011	AU 2007-349278 A1	25/09/2008
		CA 2681013 A1	25/09/2008
		CN 101681328 A	24/03/2010
		CN 101681328 B	21/03/2012
		EP 2137630 A1	30/12/2009
		EP 2137630 A4	13/04/2011
		US 2008-0229420 A1	18/09/2008
		US 7900259 B2	01/03/2011
		US 8141155 B2	20/03/2012
		WO 2008-115257 A1	25/09/2008
US 2012-0011590 A1	12/01/2012	None	
US 2011-0276468 A1	10/11/2011	US 2008-140576 A1	12/06/2008
		US 7403922 B1	22/07/2008
		US 7970701 B2	28/06/2011
		US 8244629 B2	14/08/2012
US 2011-0072506 A1	24/03/2011	CN 102299909 A	28/12/2011
		DE 102010037740 A1	05/05/2011
		GB 201015884 D0	27/10/2010
		GB 2474545 A	20/04/2011
		JP 2011-100443 A	19/05/2011
KR 10-2011-0027386 A	16/03/2011	None	

IPR2023-01466
CrowdStrike EX1002 Page 262

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
WIELAND, CHARLES F., III

BUCHANAN INGERSOLL & ROONEY PC CUSTOMER NO. 21839 P. O. BOX 1404 ALEXANDRIA VA 22313-1404 USA

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

Date of mailing *(day/month/year)*	**27 August 2013 (27.08.2013)**
Applicant's or agent's file reference 0079152-0018	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2013/039033	**01 May 2013 (01.05.2013)**	01 May 2012 (01.05.2012)

International Patent Classification (IPC) or both national classification and IPC

G06F 21/50(2013.01)i

Applicant
TAASERA, INC.

I. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☒ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.
For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/KR	Date of completion of this opinion	Authorized officer
Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. +82-42-472-7140	26 August 2013 (26.08.2013)	BYUN Sung Cheal Telephone No. +82-42-481-8262

Form PCT/ISA/237 (cover sheet) (July 2011)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2013/039033

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of :

   ☒ the international application in the language in which it was filed

   ☐ a translation of the international application into _____ , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of:

   a. a sequence listing filed or furnished
      ☐ on paper
      ☐ in electronic form

   b. time of filing or furnishing
      ☐ contained in the international application as filed.
      ☐ filed together with the international application in electronic form.
      ☐ furnished subsequently to this Authority for the purposes of search.

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additioanl copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

IPR2023-01466
CrowdStrike EX1002 Page 264

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2013/039033

Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-106	YES
	Claims	NONE	NO
Inventive step (IS)	Claims	1-106	YES
	Claims	NONE	NO
Industrial applicability (IA)	Claims	1-106	YES
	Claims	NONE	NO

2. Citations and explanations :

Reference is made to the following documents:

D1: US 2011-0162073 A1 (KONIKAYE JESCHKE) 30 June 2011
D2: US 2012-0011590 A1 (JOHN JOSEPH DONOVAN) 12 January 2012
D3: US 2011-0276468 A1 (MICHAEL LEWIS et al.) 10 November 2011
D4: US 2011-0072506 A1 (GARY K. LAW et al.) 24 March 2011
D5: KR 10-2011-0027386 A (MOZENSOFT INC.) 16 March 2011

2.1 Novelty and Inventive Step (PCT Article 33(2) and (3))

2.1.1 Claims 1-19

The subject matter of claim 1 differs from these prior art documents in that a method comprises the steps of: determining a calculus of risk for a mobile device based at least upon integrity alerts and identified risks; sending, by an endpoint trust agent, a plurality of endpoints events comprising data and content of runtime integrity warnings to a trust orchestrator and generating, by the trust orchestrator, an integrity profile based on received endpoint events. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 1 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 2-19 are directly or indirectly dependent on claim 1. Consequently, claims 2-19 are also considered to be novel and to involve an inventive step under PCT Article 33(2) and (3).

2.1.2 Claim 20

The subject matter of claim 20 differs from these prior art documents in that a system comprises: a computing platform including a network trust agent, and endpoint trust agent, and a trust orchestrator, wherein the computing platform is configured to: generate, by a trust orchestrator, an integrity profile for an endpoint based on received endpoint events pertaining to data and content; process and correlate, by the trust orchestrator one or more of: a system

Continued on Supplemental Box

IPR2023-01466
CrowdStrike EX1002 Page 265

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2013/039033

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

1. Claim 38 is referring to itself, thereby rendering the definition of the subject matter of said claim unclear (PCT Article 6). (Note: This international search report and written opinion have been established on the assumption that claim 38 is dependent on claim 29.)

2. Claim 100 is unclear because "the trust orchestrator" has not been previously defined. Therefore, claim 100 does not meet the requirements of PCT Article 6. (Note: This international search report and written opinion have been established on the assumption that claim 100 is dependent on claim 94.)

IPR2023-01466
CrowdStrike EX1002 Page 266

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of : Box No. V

integrity profile generated based on a calculus of risk; a plurality of temporal events generated based on a normalization and collation of elements in endpoint assessment reports from a plurality of collaboration services; a system infection profile received from a network analyzer; send, by the trust orchestrator, system warnings based on an endpoint execution state of the mobile application or mobile computing device as a threat posture assesment to one or more of: a network trust agent, a mobile policy manager, and a mobile device manager; and send, by the network trust agent, messages or directives to network security frameworks and/or wireless access points to apply flow controls based on the received execution state of a mobile endpoint. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 20 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

2.1.3 Claim 21

The subject matter of claim 21 differs from these prior art documents in a non-transitory computer readable medium having instructions comprising: determining a predicate score based upon a deviation from a prescribed attribute constraint or metric; calculating a score that is inversely proportional to the deviation; determining a sample rate needed to achieve a required measurement frequency; determining a recurrence of successive deviations; identifying a weight for the attribute constraint; and identifying outlying integrity confidence scores as exceptions across a plurality of client applications or client mobile devices. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 21 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

2.1.4 Claims 22-28

The subject matter of claim 22 differs from these prior art documents in an architecture comprising: native machine instrumentation for a mobile device is configured to: represent event subscriptions, callbacks, notification mechanisms provided by an operating system (OS) on the mobile device, and generate raw events; extended trust instrumentation; a runtime monitor configured to: subscribe to and receive near real time asynchronous notifications of application events for the applications from the extended trust instrumentation, and generate and send dynamic expressions or rules as application filters linked to running instances of the applications; a system event correlator configured to correlate system events of the mobile device to determine a calculus of risk; a trust orchestrator configured to orchestrate actionable intelligence based on the calculus of risk by integrating security intelligence about the mobile device and the applications; and an endpoint trust sensor configured to measure runtime operational integrity of the mobile device by evaluating risk based on actions of an application

Continued on The Next Page

IPR2023-01466
CrowdStrike EX1002 Page 267

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of: Previous Page

executing on, or a user of, the mobile device and receiving the raw events from the native machine instrumentation. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 22 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 23-28 are directly or indirectly dependent on claim 22. Consequently, claims 23-28 are also considered to be novel and to involve an inventive step under PCT Article 33(2) and (3).

2.1.5 Claims 29-48

The subject matter of claim 29 differs from these prior art documents in a system comprising a reputation broker configured to: process a query for a reputation score of the subject received at a trust broker from a service provider; and dispatch a request to a trust orchestrator to generate a hierarchical reputation score for the subject, wherein the trust orchestrator is configured to process a received request for a hierarchical reputation score by: initiating a plurality of directed queries to information management systems internal or external to an organization to interrogate attributes associated with the subject; analyzing received query responses; receiving a generated hierarchical reputation score for the subject based on a calculus of risk; and sending the received hierarchical reputation score for the subject to the reputation broker; receive a reputation token from the reputation broker for the subject in response to the dispatched request; and send the reputation token to the service provider as a response to the query. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 29 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 30-48 are directly or indirectly dependent on claim 29. Consequently, claims 30-48 are also considered to be novel and to involve an inventive step under PCT Article 33(2) and (3).

2.1.6 Claims 49-52

The subject matter of claim 49 differs from these prior art documents in a method comprising: receiving, at the trust orchestrator by the reputation broker, from a service provider, a query for the reputation score of a subject; dispatching, at the trust orchestrator by the reputation broker, a request to generate a just-in-time reputation score for a subject; and processing, at the trust orchestrator by the trust broker, the received reputation request by: initiating, a plurality of directed queries to external information management systems to interrogate attributes associated with a subject, analyzing, received query responses and generate

Continued on The Next Page

IPR2023-01466
CrowdStrike EX1002 Page 268

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of: Previous Page

a reputation score for a subject based on a calculus of risk, sending, a reputation score for a subject to the reputation broker, and sending, by the reputation broker at the trust orchestrator, as a query response to a service provider, a reputation token for a subject. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 49 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 50-52 are directly or indirectly dependent on claim 49. Consequently, claims 50-52 are also considered to be novel and to involve an inventive step under PCT Article 33(2) and (3).

2.1.7 Claims 53-58

The subject matter of claim 53 differs from these prior art documents in a system comprising: a trust orchestration server configured to: perform a calculus of risk on a global security context including endpoint assessment reports received from collaboration services, and send system warnings based upon the endpoint threat intelligence to the network trust agent; and a remediation engine configured to receive real time directives for control of the computing device or application. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 53 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 54-58 are directly or indirectly dependent on claim 53. Consequently, claims 54-58 are also considered to be novel and to involve an inventive step under PCT Article 33(2) and (3).

2.1.8 Claims 59-60

The subject matter of claim 59 differs from these prior art documents in a method comprising: determining, by the network analyzer, anomalies based on network activity correlation and network malware detection; determining, by the trust broker, system configuration anomalies based on system level normalization and collation of assessments; determining, by the endpoint trust agent, resource utilization anomalies based on rulesets associated with central processing unit(CPU), memory, storage, and network resources usage; determining, by the endpoint trust agent, application integrity anomalies based on the rulesets associated with static and dynamic image analysis; correlating, by the trust orchestrator, network activity and endpoint events and behaviors characterized through continuous local and remote monitoring of network endpoints for risk analysis and detection of infected systems; and mitigating, by the trust orchestrator, infected systems through automated machine, network flow,

Continued on The Next Page

IPR2023-01466
CrowdStrike EX1002 Page 269

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of: Previous Page

or transaction-level remediation controls. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 59 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claim 60 is dependent on claim 59. Consequently, claim 60 is also considered to be novel and to involve an inventive step under PCT Article 33(2) and (3).

2.1.9 Claims 61-72

The subject matter of claim 61 differs from these prior art documents in a method comprising: generating, by a trust broker, temporal events related to an endpoint system; receiving, at the trust orchestrator, by the trust supervisor: infection profiles from the network analyzer, and integrity profiles from the system event correlator; identifying and categorizing, by the trust supervisor, threats and infections diagnosed at the endpoint system; receiving, by the remediation controller, at the trust orchestrator, directives from the trust supervisor to initiate a remediation sequence; and sending, by the remediation controller, at the trust orchestrator, actions to network elements for orchestration and policy enforcement services based on established thresholds and triggers. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 61 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 62-72 are directly or indirectly dependent on claim 61. Consequently, claims 62-72 are also considered to be novel and to involve an inventive step under PCT Article 33(2) and (3).

2.1.10 Claims 73-75

The subject matter of claim 73 differs from these prior art documents in a method comprising: displaying, in the GUI, a status and progress of initiated remediation actions; and displaying, in the GUI, details of malware analytics comprising one or more of: infection summaries, infection diagnosis, threat categorization and identification based on a signatureless infection life-cycle model, an address and geo-location for a source or attacker, an identification of one or more infected victims, forensic evidence chain of detected malicious activities and intent, and compute, memory, storage and network level anomalies detected on the victim machine or infected system. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 73 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 74-75 are dependent on claim 73. Consequently, claims 74-75 are also considered to

Continued on The Next Page

IPR2023-01466
CrowdStrike EX1002 Page 270

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of: Previous Page

be novel and to involve an inventive step under PCT Article 33(2) and (3).

2.1.11 Claim 76

The subject matter of claim 76 differs from these prior art documents in a method comprising: correlating, by a trust orchestrator, network activity and endpoint events and behaviors characterized through continuous local and remote monitoring of network endpoints for risk analysis and detection of infected systems; and mitigating, by the trust orchestrator, an infected system using inputs received from a real time threat visualization dashboard to implement flow level or transaction level remediation controls. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 76 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

2.1.12 Claims 77-81

The subject matter of claim 77 differs from these prior art documents in a method comprising: correlating, by an event and behavior correlation engine, risk based on monitoring; and displaying, in a plurality of runtime dashboards of an administrative console of the computing platform, real time status indications for operational integrity of the system and application. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 77 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 78-81 are directly or indirectly dependent on claim 77. Consequently, claims 78-81 are also considered to be novel and to involve an inventive step under PCT Article 33(2) and (3).

2.1.13 Claims 82-86

The subject matter of claim 82 differs from these prior art documents in a system comporising: a reputation broker configured to: process a query from a service provider for a reputation score of the subject, and dispatch a request to generate a hierarchical reputation score for the subject; a trust orchestrator configured to: process a received request from the reputation broker for a hierarchical reputation score by: initiating a plurality of directed queries to information management systems external to an organization to interrogate attributes associated with the subject, analyzing received query responses, receiving a generated hierarchical reputation score for the subject based on a calculus of risk; and sending the received hierarchical reputation score for the subject to the reputation broker; receive a reputation token from the reputation broker for the subject in response to the dispatched

Continued on The Next Page

IPR2023-01466
CrowdStrike EX1002 Page 271

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of : Previous Page

request; and send the reputation token to the service provider as a response to the query. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 82 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 83-86 are dependent on claim 82. Consequently, claims 83-86 are also considered to be novel and to involve an inventive step under PCT Article 33(2) and (3).

2.1.14 Claims 87-93

The subject matter of claim 87 differs from these prior art documents in a method comprising: generating temporal events based at least in part on analyzing network endpoint assessments; correlating received endpoint events and generated temporal events; and generating an integrity profile for the system. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 87 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 88-93 are directly or indirectly dependent on claim 87. Consequently, claims 88-93 are also considered to be novel and to involve an inventive step under PCT Article 33(2) and (3).

2.1.15 Claims 94-105

The subject matter of claim 94 differs from these prior art documents in a method comprising: processing and correlating, by the trust orchestrator, one or more of: a system integrity profile generated based on a calculus of risk, a plurality of temporal events generated based on a normalization and collation of elements in endpoint assessment reports received from a plurality of collaboration services, and a system infection profile received from a network analyzer; sending, by the trust orchestrator to the network trust agent, system warnings based on endpoint execution state assessments; and sending, by the network trust agent, messages or directives to OpenFlow security frameworks and/or controllers to apply flow controls based on the received execution state as a threat posture of a connection endpoint. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 94 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 95-105 are directly or indirectly dependent on claim 94. Consequently, claims 95-105 are also considered to be novel and to involve an inventive step under PCT Article 33(2) and (3).

Continued on The Next Page

IPR2023-01466
CrowdStrike EX1002 Page 272

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of: Previous Page

2.1.16 Claim 106

The features of independent claim 106 essentially correspond to those of claim 22. Thus, the same reasoning as in claim 22 applies to claim 106. Therefore, claim 106 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

2.2 Industrial Applicability (PCT Article 33(4))

Claims 1-106 are industrially applicable under PCT Article 33(4).

IPR2023-01466
CrowdStrike EX1002 Page 273

Electronic Acknowledgement Receipt	
EFS ID:	16901408
Application Number:	13559766
International Application Number:	
Confirmation Number:	9330
Title of Invention:	SYSTEMS AND METHODS FOR THREAT IDENTIFICATION AND REMEDIATION
First Named Inventor/Applicant Name:	Srinivas KUMAR
Customer Number:	21839
Filer:	Jennifer A. Wilson/Taya M. Hawkins
Filer Authorized By:	Jennifer A. Wilson
Attorney Docket Number:	0079152-000016
Receipt Date:	19-SEP-2013
Filing Date:	27-JUL-2012
Time Stamp:	15:04:21
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS_KUMAR016.PDF	612983 d761385b45d9ede590a03d1af6ed1e3f8c42e134	no	5

Warnings:
Information:

2	Transmittal Letter	016.pdf	245757 f33be0e00abddebd36a8797fbe8bf7e85b814513	no	2
Warnings:					
Information:					
3	Foreign Reference	KR_20110027386.PDF	1655084 43f263341030fce51de88d200f3464977aa389bc	no	15
Warnings:					
Information:					
4	Non Patent Literature	ISR.PDF	620829 d9ea61b90857ebc6dd503f8edeae5784c1ae3404	no	16
Warnings:					
Information:					
5	Non Patent Literature	OA6202013.PDF	1098646 9a2b6a3acc32402c0a2bf484c6429694e03d8f71	no	32
Warnings:					
Information:					
		Total Files Size (in bytes):	4233299		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/559,766	07/27/2012	Srinivas KUMAR	0079152-000016	9330

21839 7590 07/18/2013

BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
SAVENKOV, VADIM	
ART UNIT	**PAPER NUMBER**
2431	

NOTIFICATION DATE	DELIVERY MODE
07/18/2013	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPDOC1@BIPC.com

IPR2023-01466
CrowdStrike EX1002 Page 276

Office Action Summary	Application No. 13/559,766	Applicant(s) KUMAR ET AL.	
	Examiner VADIM SAVENKOV	Art Unit 2431	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 July 2012*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-20* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-20* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☒ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *27 July 2012* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some * c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *11/09/2012*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☒ Other: *Trademark Information*.

DETAILED ACTION

This office action is in response to the application which was filed on July 27th of 2012.

Claims 1-20 are pending.

Priority

Acknowledgement is made of Applicant's claim to priority to provisional Application No. 61/641007, filed 5/1/2012.

Information Disclosure Statement

Examiner has considered Applicant's IDS, filed 11/9/2012.

Specification

1. The use of the trademark **OPENFLOW™** has been noted in this application. It should be capitalized wherever it appears and be accompanied by the generic terminology.

Although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks.

2. The disclosure is objected to because of the following informalities:

"…*with a runtime dashboard* ***to*** *capable of displaying*…" [0019] of Specification

"…*and represent alerts based* ***an*** *endpoint sensor resident on*…" [0080] of Specification

"…*while* ***he*** *device D is still connected*…" [0116] of Specification

"*According to exemplary embodiments,* ***the event correlator 1007*** *receives endpoint events 1033 from the* ***event correlator 1007***..."[0140] of Specification

Appropriate correction is required.

Examiner's Comment

Claims 14-16 depend on claim 1, and not on claim 8. Since there are no antecedent errors regarding this claim dependency, Examiner is unsure if this dependency is intended or not. Examiner has therefore treated claims 14-16 as being dependent on claim 1.

Claim Objections

3. Claim 8 is objected to because of the following informalities: Claim 8 recites both "*runtime system integrity* ***alerts***" and "*runtime system integrity* ***warnings***." Since "alerts" and "warnings" are known synonyms, and because the context of claim 8 appears to intend so, Examiner has interpreted "*runtime system integrity* ***alerts***" and "*runtime system integrity* ***warnings***" as referring to the same thing. However, in the interest of providing clarity, a single word should be chosen. Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of 35 U.S.C. 112(b):
(b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:
The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1-7 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention. Claim 1 recites: "***receiving*** *network endpoint assessments,*" "***generating*** *temporal events…,*" "***correlating*** *the received endpoint events…,*" "***generating*** *an integrity profile…,*" which render claim 1 indefinite because it is unclear as to which element(s) of Applicant's invention is(are) performing said ***receiving***, ***generating***, ***correlating***, and ***generating*** steps. Since claims 2-7 depend on claim 1, but do not cure its deficiencies, they are likewise rejected.

Furthermore, claim 7 recites: "*wherein the… temporal events are received by a system event coordinator from... a trust broker...,*" which renders claim 7 indefinite because it is unclear as to how said trust broker obtains said temporal events. This is because the temporal events are not claimed as being generated, stored on, or transferred to the trust broker (refer to the "generating temporal events…" limitation in claim 1). As such, claim 7 is rejected as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

6. Claims 8, 15, and 16 contain the trademark/trade name **OPENFLOW™**. Where a trademark or trade name is used in a claim as a limitation to identify or describe a particular material or product, the claim does not comply with the requirements of 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph. See *Ex parte Simpson*, 218 USPQ 1020 (Bd. App. 1982). The claim scope is uncertain since the trademark or trade name cannot be used properly to identify any particular material or product. A trademark or trade name is used to identify a source of goods, and not the goods themselves. Thus, a trademark or trade name does not identify or describe the goods associated with the trademark or trade name. In the present case, the trademark/trade name is used to identify/describe computer network protocols that facilitate the control of network switches, routers and wireless access points and, accordingly, the identification/description is indefinite.

As such, examination of claims 15 and 16 has not been performed with respect to the prior art, as the recited limitations regarding OPENFLOW™ controllers and/or network elements or switches are indefinite as claimed. With regard to claim 8, its last limitation reciting OPENFLOW™ security frameworks has been interpreted as performing the claimed step(s) without specificity to OPENFLOW™.

7. Claim 20 is rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards

as the invention. Claim 20 recites: "*wherein native machine instrumentation for the computing platform is* **configured to***: …extended trust instrumentation*." This language renders claim 20 indefinite by virtue of its confusing grammatical structure, said structure making interpretation difficult. Examiner has interpreted this claim language as potentially being intended to mean that the computing platform comprises extended trust instrumentation, or that the computing platform is configured for extended trust instrumentation.

Claim 20 furthermore recites: "*wherein native machine instrumentation for the computing platform is* **configured to***: …a runtime monitor configured to: subscribe to and receive…generate and send…,*" which renders this claim indefinite by virtue of confusing grammatical structure, said structure making interpretation difficult. Examiner has interpreted this claim language as being intended to mean that the computing platform comprises the runtime monitor.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of pre-AIA 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. Claims 1-7 are rejected under pre-AIA 35 U.S.C. 102(b) as being anticipated by **Helman (US 2009/0328222 A1)**.

Regarding claim 1, Helman discloses: ***A method of providing an attestation service for providing runtime operational integrity of a system using a computing platform comprising a network trust agent, an endpoint trust agent, and a trust orchestration server*** (refer to **FIG. 1** and **2** of **Helman** regarding system implementation)***, the method comprising:***

receiving, at the trust orchestration server, a dynamic context including endpoint events;

- Refer to at least **[0060]** and **FIG. 3** of **Helman** regarding the contents which are sent as part of a Security Assessment. As such, the whole of contents expressed in **FIG. 3** may be interpreted as a form of claimed dynamic context. Furthermore, Data such as Failed Login **305** may be interpreted as a form of claimed endpoint event. Finally, the Host Security Endpoint **135 (FIG.1 of Helman)** may be interpreted as a form of claimed trust orchestration server.

analyzing, by the trust orchestration server, the received endpoint events;

- Refer to at least **[0098]** of **Helman** regarding subscribing endpoints applying their specific security expertise through the application of their own correlation rules. Furthermore, it is extremely old and well known in the art to analyze incoming security data, as indicated by **[0047]**-**[0048]** of **Helman**.

receiving network endpoint assessments;

- Refer to at least **FIG. 3** of **Helman** regarding content which is received by a subscribing endpoint such as the Host Security Endpoint. Furthermore, refer to

Assessment **316** which may be interpreted as a form of claimed endpoint assessment.

generating temporal events based at least in part on analyzing the network endpoint assessments;

- Refer to at least **[0007]** and **[0101]** of **Helman** regarding the Host Security Endpoint receiving a Security Assessment interpreted previously as a form of claimed dynamic context, said dynamic context including both endpoint events and endpoint assessments, wherein the Host Security Endpoint generates one or more additional Security Assessments in turn; said generation encompassing use of data which is local to the Host Security Endpoint. These new assessments are interpreted as a form of claimed temporal events.

correlating the received endpoint events and the generated temporal events;

- Refer to at least **[0035]** and **[0098]** of **Helman** regarding combination or correlation of evidence from Security Assessments received from a variety of different sources, and across object types. As in **[0007]** and **[0101]** of **Helman**, these sources and object types may include the Host Security Endpoint.

and generating an integrity profile for the system.

- Refer to **FIG. 8A**, **FIG. 11-12**, and **[0110]** of **Helman** regarding actualization of security assessment information for a system which is monitored.
- Also Refer to **[0037]** of **Helman** regarding a comprehensive centralized view of system context.

Regarding claim 2, Helman discloses: ***The method of claim 1, wherein the dynamic context is sent by the endpoint trust agent.***

- Refer to **[0051]-[0056]** of **Helman** regarding exemplary endpoints which are used for generation of a security assessment, said exemplary endpoints comprising hardware and/or software. Furthermore, refer to **FIG. 5** and **[0085]-[0096]** of **Helman**). Software executing on these endpoints may be interpreted as endpoint trust agent(s).

Regarding claim 3, Helman discloses: ***The method of claim 1, wherein the network endpoint assessments are received from an endpoint assessment service.***

- Refer to **[0051]-[0056]** of **Helman** regarding exemplary endpoints which are used for generation of a security assessment, said exemplary endpoints comprising hardware and/or software. Furthermore, refer to **FIG. 5** and **[0085]-[0096]** of **Helman**). Software executing on these endpoints may be interpreted as endpoint assessment service(s).

Regarding claim 4, Helman discloses: ***The method of claim 3, further comprising: receiving integrity measurement and verification reports from the endpoint assessment service.***

- Refer to **[0070]-[0078]** of **Helman** regarding exemplary contents of a security assessment. Health information assessments are interpreted as a form of claimed integrity measurement and verification reports.

Regarding claim 5, Helman discloses: ***The method of claim 1, wherein the network endpoint assessments are received from one or more collaboration services.***

- Refer to **[0050]** of **Helman** regarding potential additional different types of security products/endpoints that may be utilized by the ESAS system of Helman.

Regarding claim 6, Helman discloses: ***The method of claim 5, further comprising: receiving integrity measurement and verification reports from the one or more collaboration services.***

- Refer to **[0050]** of **Helman** regarding potential additional different types of security products/endpoints that may be utilized by the ESAS system of Helman. More specifically, refer to the operational health monitoring and configuration management products and the variety of security evaluation products mentioned.

Regarding claim 7, Helman discloses: ***The method of claim 1, wherein the endpoint events and temporal events are received by a system event correlator from endpoint trust agents and a trust broker, respectively.***

- Refer to the ESAS central server in at least **FIG. 2** of **Helman**, said central server interpreted as a form of claimed system event correlator. Furthermore, refer to [0037] regarding the ESAS central server's system event correlation capacity.
- The Security Assessment Channel **205** in **FIG. 2** of **Helman** may be interpreted as a form of claimed trust broker, since it facilitates communication between

endpoints **([0057]; Helman)**. Since said channel is used for transmission of endpoint Security Assessments, then the previously mentioned ESAS central server would inherently receive its incoming Security Assessments from this channel.

Claim Rejections - 35 USC § 103

10. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claim 14 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over **Helman (US 2009/0328222 A1)** as applied to claims 1-7 above, and further in view of **Official Notice**.

Regarding claim 14, Helman discloses: ***The method of claim 1, further comprising: sending, by the trust orchestrator, to the network trust agent, one or more system warnings pertaining to a network device associated with the one or more flow remediation actions.***

- Refer to **725** and **728** in **FIG. 7** and **[0101]-[0103]** of **Helman** regarding generation of new Security Assessments by the Host Security Endpoint, wherein said Security Assessments inform future remediation actions which are taken by

endpoint security products. Said future remediation actions are outlined in **730** in **FIG. 7** and **[0104]** of **Helman**.

Helman does disclose: ***generating, by a trust supervisor, one or more flow remediation actions to be performed on a network fabric; receiving, at a remediation controller of the trust orchestrator, the flow remediation actions.*** This is because the ESAS endpoints and their security products prepare tailored local actions in accordance with a set of response policies **([0036]; Helman)**. As such, the ESAS endpoints are not informed of local actions to be taken by an endpoint which would be a form of the claimed trust supervisor. As an aside, since the Host Security Endpoint is deployed to protect, assess, and monitor endpoints in the ESAS system **([0051]; Helman)**, then it would inherently receive any form of the claimed flow remediation actions which are sent by said trust supervisor. However, since it is extremely old and well known in the art for a form of claimed trust supervisor to send security instructions to endpoints for addressing security threats, then it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to combine these teachings with the ESAS system of Helman such that a specific trust supervisor serves the role of publishing local actions to be taken by endpoints. One of ordinary skill in the art would have been motivated to combine these teachings to reduce processing at the local endpoints.

12. Claims 8-10 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over **Helman (US 2009/0328222 A1)** in view of **Alperovitch (8,214,497 B2)**.

Regarding claim 8, Helman discloses: ***A method of providing flow level remediation to isolate infected or compromised systems and platforms from a computing network fabric using a network trust agent, an endpoint trust agent, and a trust orchestrator, the method comprising:***

generating, by the endpoint trust agent, runtime system integrity alerts regarding execution anomalies and risks based on rulesets and a calculus of risk;

- Refer to at least DATA in **FIG. 3** and **[0060]** of **Helman** regarding generation of alerts based on the current or near-current runtime state of a monitored system. Inherently, this information is generated based on a predetermined ruleset for identifying potential security hazards. Refer to **Table 1** residing between [0063] and [0064] of **Helman** with respect to both execution anomalies and risks. Finally, refer to **[0096]** of Helman regarding a calculus of risk.

sending, by the endpoint trust agent, runtime system integrity warnings as endpoint events to the trust orchestrator;

- Security Assessments generated by endpoints are published to the ESAS system at large **([0057]; Helman)**, whereupon they are received by the subscribing Host Security Endpoint **([0051], [0098]; Helman)**. Said Host Security Endpoint may be interpreted as a form of claimed trust orchestrator.

generating, by the trust orchestrator, a system integrity profile for the endpoint based on analysis of the received endpoint events;

- Refer to at least **[0098]** and **[0101]** of **Helman**, wherein the Host Security Endpoint evaluates the received Security Assessment further in view of its local data and ESAS data about the target endpoint. The new security assessments are interpreted as a form of claimed system integrity profile for the endpoint.

processing and correlating, by the trust orchestrator, one or more of:

a system integrity profile generated based on a calculus of risk,

- The Host Security Endpoint processes and correlates received Security Assessments **([0035], [0098]; Helman)**, which are generated based at least partly on a calculus of risk (as was discussed above, see **[0096]** of **Helman**).

a plurality of temporal events generated based on a normalization and collation of elements in endpoint assessment reports received from a plurality of collaboration services, and

a system infection profile received from a network analyzer;

sending, by the trust orchestrator to the network trust agent, system warnings based on endpoint execution state assessments;

- Refer to **[0037]** of **Helman** regarding an ESAS central server, which is interpreted as a form of the claimed network trust agent. Once the Host Security Endpoint publishes its new Security Assessments **([0102]; Helman)**, they are received by the subscribing ESAS central server **([0037]; Helman)**. The ESAS central server provides a comprehensive view of the history and current status of the enterprise as a whole and of each endpoint.

Helman does not disclose: ***sending, by the network trust agent, messages or directives to OpenFlow security frameworks and/or controllers to apply flow controls based on the received execution state as a threat posture of a connection endpoint.*** However, Alperovitch in the same field of endeavor discloses: ***sending, by the network trust agent, messages or directives to*** [load balancing] ***security frameworks and/or controllers to apply flow controls based on the received execution state as a threat posture of a connection endpoint.***

- Refer to **FIG. 10** and **Col. 13-14**, **Lines 51-67** and **1-56** of **Alperovitch**, which regard operation of a reputation based load balancer. A reputation engine of a network security system provides the load balancer with a reputation vector indicating the reputation of an entity. The load balancer directs data transfers based on the reputation vector.
- "***a threat posture of a connection endpoint***" has been interpreted as its reputation, wherein the reputation is based at least in part on the riskiness of association with said endpoint.

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to combine the teachings of Helman's ESAS system with the teachings of Alperovitch regarding load balancing based on received security/risk assessment analogues. These teachings are combinable because they both regard endpoint-agent based network security. One of ordinary skill in the art would have been motivated to combine these teachings for the purpose of more efficiently utilizing security resources.

Regarding claim 9, Helman-Alperovitch discloses: ***The method of claim 8, wherein the integrity warnings comprise warnings regarding data events and content events; and wherein the endpoint events comprise data events and content events.***

- Refer to **FIG. 3** and at least **[0060]** of **Helman** regarding the context of a Security Assessment. Furthermore, refer to **Table 1** on page 5 of **Helman**.

Regarding claim 10, Helman-Alperovitch discloses: ***The method of claim 8, wherein the remediation of an infected system is achieved without adversely reducing the total operating capacity or availability of the computing platform through on-demand instantiation and scaling of workloads.***

- Refer to **Col. 11**, **Lines 7-56** in **Alperovitch** regarding load balancing analysis and remediation of potentially hazardous items based on the reputation of entities associated with said items.

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to combine the teachings of Helman's ESAS system with the teachings of Alperovitch regarding load balancing analysis and remediation of potentially hazardous items. These teachings are combinabel for primary the same reasons as expressed in claim 8 above. One of ordinary skill in the art would have been motivated to combine these teachings for the purpose of increasing system efficiency.

13. Claims 11-13 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Helman-Alperovitch as applied to claims 8-10 above, and further in view of **Wootton (US 2012/0110174 A1)**.

Regarding claim 11, Helman-Alperovitch discloses: ***The method of claim 10, further comprising forwarding a notification conveying an infected or compromised state of a mobile computing device to a user associated with the mobile computing device, wherein the notification is one or more of*** [Helman discloses displaying security information to an administrator in at least [0037], however a mobile device is not specifically disclosed (but it is extremely old and well known in the art that teachings applicable to a generalized computing device would further be applicable to a mobile computing device)].

Helman-Alperovitch does not disclose:

an asynchronous push notification to an account associated with the user;

a short messaging service (SMS) text alert message forwarded to a phone number associated with the mobile computing device;

an email alert message forwarded to an email address associated with the user; and

a warning message displayed by a service on a display of the mobile computing device during initiation of a transaction with a service from the mobile computing device.

However, Wootton in the same field of endeavor discloses at least: ***a short messaging service (SMS) text alert message forwarded to a phone number associated with the mobile computing device;***

- If server 151 determines the data object to be undesirable based on universal undesirability characteristics or characteristics for the user, the server transmits a notification… The notification may take a variety of forms, such as an email, SMS message, or user interface dialog displayed on a web page, on a PC, or on a mobile communication device **([0210]; Wootton)**.

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to combine the teachings of Helman-Alperovitch's ESAS system with load balancing with the teachings of Wootton regarding the specificities of a security notification associated with a user. These teachings are combinable because they both regard informing a user of a security issue associated with a computing device. One of ordinary skill in the art would have been motivated to combine these teachings to allow for alternative ways to inform a user of potential security issues.

Regarding claim 12, Helman-Alperovitch-Wootton discloses: ***The method of claim 11, wherein one or more features or capabilities of a mobile device are de-activated or activated as a remediation action.***

- In block 207, mobile communication device 101 receives the notification, and in block 209, the mobile communication device 101 takes action based upon the notification. As will be discussed in more detail below, such actions may include

deactivating one or more features or applications on the mobile communication device 101 **([0047]; Wootton)**.

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to combine the teachings of Helman-Alperovitch's ESAS system with load balancing with the teachings of Wootton regarding deactivating features of a mobile device in response to a security issue. These teachings are combinable for substantially the same reasons as expressed in claim 11 above. One of ordinary skill in the art would have been motivated to combine these teachings to reduce the avenues of attack or infection for a potentially hazardous entity.

Regarding claim 13, Helman-Alperovitch-Wootton discloses: ***The method of claim 12, wherein the remediation action is based on the geo-location.***

- Refer to at least FIG. 11A-C of Alperovitch, as well as their corresponding descriptions in **Col. 14-16**, **Lines 57-19**, regarding geo-location based operational scenarios.

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to combine the teachings of Helman, Alperovitch, and Wootton such that geolocational data is used in determining remediation actions. These teachings are combinable for substantially the same reasons as expressed in claim 11 above. One of ordinary skill in the art would have been motivated to combine these teachings to provide for additional analysis mechanisms and therefore increase security.

14. Claims 17 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over **Helman-Alperovitch** as applied to claims 8-10 above, and further in view of "**Static Analysis of Executables for Collaborative Malware Detection on Android**," hereinafter **Schmidt**; further in view of **Wysopal (US 2012/0072968 A1)**.

Regarding claim 17, Helman-Alperovitch discloses: ***The method of claim 8, further comprising:***

determining, by the network analyzer, anomalies based on network activity correlation and malware detection;

- Refer to at least **[0035]** and the **Abstract** of **Helman** regarding the capabilities of ESAS-enabled endpoints to determine anomalies based on malware detection and network activity correlation.

Helman-Alperovitch does not disclose: ***dispatching, by the trust orchestrator, the image files and attributes of an application for binary analysis, wherein the image files comprise compiled, intermediate, or interpreted code or scripts;***

receiving a result of the binary analysis result identifying malicious activity as a set of threats identified based on the analysis; and caching, by the trust broker, the results of the analysis indexed by a unique identifier for the image; and generating and returning an image profile to the endpoint trust agent comprising assertions of malicious capabilities of the image to be monitored at runtime for subsequent generation of endpoint events by the endpoint trust agent.

However, Schmidt in the same field of endeavor disclose: ***dispatching, by the trust orchestrator, the image files and attributes of an application for binary analysis, wherein the image files comprise compiled, intermediate, or interpreted code or scripts;***

- Refer to "**B. Creating a Training Set With Readelf**" in **Schmidt** regarding image files and attributes of an application, wherein the image files comprise compiled, intermediate, or interpreted code or scripts. Furthermore, refer to "**IV. CLASSIFY EXECUTABLES BY STATIC ANALYSIS**" in **Schmidt** regarding the specificities of testing said image files and attributes. Finally, refer to at least **Fig. 3** and its corresponding description in **Schmidt** regarding dispatch of said image files and attributes.

receiving a result of the binary analysis result identifying malicious activity as a set of threats identified based on the analysis;

- Refer to the following in the description of **Fig. 3** in **Schmidt**: "V-The initiating node is informed about the results."

Helman-Alperovitch in view of Schmidt does not specifically disclose:

caching, by the trust broker, the results of the analysis indexed by a unique identifier for the image; and

However, Wysopal in the same field of endeavor discloses:

caching, by the trust broker, the results of the analysis indexed by a unique identifier for the image;

- Refer to at least **[0017]** of **Wysopal** regarding a set of analysis-derived security data which may be associated with the image file using a secure identifier.

Furthermore, while Helman-Alperovitch alone does not disclose: ***generating and returning an image profile to the endpoint trust agent comprising assertions of malicious capabilities of the image to be monitored at runtime for subsequent generation of endpoint events by the endpoint trust agent,*** Helman-Alperovitch in view of Schmidt and Wysopal discloses this preceding limitation for the following reasons: Helman states that his ESAS-enabled endpoints are liable to enhance the quality of their detection of potential security threats via combination or correlation of published Security Assessments with their local rules **([0035]; Helman)**. Since a combination of the aforementioned prior art would use the publish and subscribe system of Security Assessments disclosed in Helman, then the image file analysis of Helman-Alperovitch in view of Schmidt and Wysopal would naturally be published as a Security Assessment following its determination.

As to the distinction between binary and static analysis, refer to **[0013]** of **US 2012/0102458** regarding their interchangeability with regard to obviousness.

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention combine the teachings of Helman-Alperovitch with the teachings of Schmidt and the teachings of Wysopal as expressed above. These teachings are combinable because Schmidt concerns distributed malware detection on devices within a network; as well, the teachings of Wysopal are applicable to the image file and attribute analysis of Schmidt because both concern a form static analysis in use for

malware detection. One of ordinary skill in the art would have been motivated to combine the teachings of Helman-Alperovitch with the teachings of Schmidt and the teachings of Wysopal for the purpose of extending the network security ESAS system of Helman to use static analysis methods, whose benefits are expressed in the disclosures of both Schmidt and Wyspoal.

15. Claims 18-19 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over **Helman-Alperovitch-Schmidt-Wysopal** as applied to claim 17 above, and further in view of **Official Notice**.

Regarding claim 18, Helman-Alperovitch-Schmidt-Wysopal discloses: ***The method of claim 17, wherein the binary analysis is performed by one or more third party malware analyzers, and wherein the dispatch mechanism uses trigger filter expressions that specify a set of criteria that warrant initiation of image analysis such as frequency and volume of requests for analysis associated with the application image across deployed endpoint trust agents.***

- It is extremely old and well known in the art that a network security system may be configured to access and make use of third part malware analyzers. Furthermore, the claimed dispatch mechanism which is described above is simply a form of previously mentioned rulesets inherent to the endpoint security software of Helman.

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to combine the teachings of Helman-Alperovitch-Schmidt-Wysopal with the teachings of Official Notice regarding third party malware analysis. These teachings are combinable because it is well known in the art to use third party malware analyzers in combination with a network security system. The reason for doing so may be to reduce the amount of infrastructure necessary for the abovementioned network security system.

Regarding claim 19, it is substantially the same as claim 18 above, but with regard to static and dynamic analysis. Since both static and dynamic analysis are disclosed in the teachings of Helman-Alperovitch-Schmidt-Wysopal in view of Official Notice, claim 19 is rejected for substantially the same reasons as expressed in rejecting claim 18 above.

16. Claim 20 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over **Helman (US 2009/0328222 A1)** in view of "**Windows Management Instrumentation: Create WMI Providers to Notify Applications of System Events**," hereinafter **msdn**.

Regarding claim 20, Helman discloses: ***A system for providing runtime operational integrity by determining execution anomalies and a threat posture of applications executing on computing platforms including mobile devices and client-server systems, the system comprising:***

an endpoint trust agent [Refer to software executing on hardware in FIG. 1 of Helman]

including:

a process monitor configured to observe local execution context of the applications, a socket monitor configured to observe network activities of the applications,

- Refer to at least **Table 1** residing between [0063] and [0064] in **Helman** regarding the multiple types of assessment categories, which inherently imply monitoring of application execution contexts and network activities.

a resource utilization module monitor configured to observe system and platform resources consumed by the applications;

- It is extremely old and well known in the art for anti-malware/IDS/etc. systems to monitor application resource usage. For instance, refer to chapter 2, “Monitoring your system's performance” of “Norton Antivirus Product Manual”.

an application integrity module configured to assess operational integrities of the computing platforms based on a ruleset;

- Refer to at least **Table 1** residing between [0063] and [0064] in **Helman** regarding the multiple types of assessment categories, namely those referring to detecting that a portion of a system or network is compromised. Inherently, there must be a ruleset to assess a system or network thusly.

a system event correlator configured to correlate system events of the computing platforms to determine a calculus of risk;

- Refer to at least **[0035]** of **Helman** regarding the capability of ESAS-enabled endpoints to combine or correlate evidence from Security Assessments in order to significantly enhance the quality of its detection of potential security incidents, wherein detection is associated with publishing a Security Assessment comprising fidelity and severity ratings **(FIG. 3 and [0060]; Helman)**.

a trust orchestrator configured to orchestrate actionable intelligence based on the calculus of risk by integrating security intelligence about the computing platforms and the applications;

- Refer to **[0098]** and **[0101]** of **Helman** regarding a Host Security Endpoint which receives published Security Assessments and applies its specific security expertise through application of its own correlation rules and locally-available data to trigger an appropriate action.

an endpoint trust sensor configured to measure runtime operational integrity of the computing platforms by evaluating risk based on actions of an application executing on, or a user of, the computing platforms and receiving the raw events from the native machine instrumentation.

- Refer to at least **Table 1** residing between [0063] and [0064] in **Helman** regarding the multiple types of assessment categories, which inherently implies a sensor module which monitors a system for compromise during runtime.

Helman does not specifically disclose: ***wherein native machine instrumentation for the computing platform is configured to: represent event subscriptions, call backs, notification mechanisms provided by an operating system (OS) on the***

computing platforms, and generate raw events; extended trust instrumentation; a runtime monitor configured to: subscribe to and receive near real time asynchronous notifications of application events for the applications from the extended trust instrumentation, and generate and send dynamic expressions or rules as application filters linked to running instances of the applications;

However, msdn in the same field of endeavor discloses: ***wherein native machine instrumentation for the computing platform is configured to:***

represent event subscriptions, call backs, notification mechanisms provided by an operating system (OS) on the computing platforms,

- In **[0077]** of their **Specification**, Applicant states: "In embodiments, the native machine instrumentation 511 can represent any event subscription, callback, notification mechanism provided by the supported operating system (OS) on the device 560 (e.g., MICROSOFTTM WINDOWS® Machine Instrumentation (WMI)."

generate raw events;

- Refer to the **first paragraph** of "**Building an Event Provider**" in **msdn** regarding a WMI event provider that generates events.

extended trust instrumentation;

- In **[0269]** of their **Specification**, Applicant states: "The extended trust instrumentation 2501 may be layered extensions to native machine instrumentation 610, such as, for example, the WINDOWS® Management Instrumentation (WMI) on MICROSOFTTM WINDOWS® platforms."

a runtime monitor configured to:

subscribe to and receive near real time asynchronous notifications of application events for the applications from the extended trust instrumentation,

- Refer to the **first paragraph** in the **Conclusion** of **msdn** regarding event filters and permanent subscribers which are inherent to WMI.

generate and send dynamic expressions or rules as application filters linked to running instances of the applications;

- Refer to the **first paragraph** in the **Conclusion** of **msdn** regarding event filters and permanent subscribers which are inherent to WMI.

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to combine the teachings of Helman's ESAS system with the teachings of msdn regarding the inherencies of WMI. These teachings are combinable for substantially similar reasons as expressed regarding exemplary software in **[0050]** of **Helman**. One of ordinary skill in the art would have been motivated to combine these teachings because of WMI's flexibility and manageability **(second paragraph in the Summary of msdn)**.

Conclusion

17. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. US 2012/0260342 A1 is believed to be indicative of the state of technology in the field of malware detection by static analysis. US 2012/0137375 A1 is a network security system which makes use of OPENFLOW™ protocols in assessing how

to distribute network information flows. Finally, US 6,742,128 B1 is an exemplary network security system.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to VADIM SAVENKOV whose telephone number is (571)270-5751. The examiner can normally be reached on Monday - Friday 10:00 AM - 6:30 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, NATHAN J. FLYNN can be reached on (571) 272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/V. S./
Examiner, Art Unit 2431

/NATHAN FLYNN/

Supervisory Patent Examiner, Art Unit 2431

Notice of References Cited	Application/Control No. 13/559,766	Applicant(s)/Patent Under Reexamination KUMAR ET AL.	
	Examiner VADIM SAVENKOV	Art Unit 2431	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,742,128 B1	05-2004	Joiner, Herbert V.	726/25
*	B	US-2009/0328222 A1	12-2009	Helman et al.	726/25
*	C	US-2012/0072968 A1	03-2012	Wysopal et al.	726/1
*	D	US-2012/0102458 A1	04-2012	Meijer et al.	717/123
*	E	US-2012/0110174 A1	05-2012	Wootton et al.	709/224
*	F	US-2012/0137375 A1	05-2012	RAMACHANDRAN et al.	726/28
*	G	US-8,214,497 B2	07-2012	Alperovitch et al.	709/226
*	H	US-2012/0260342 A1	10-2012	Dube et al.	726/24
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Norton Antivirus Product Manual Copyright © 2011 Symantec Corporation. All rights reserved.
	V	Windows Management Instrumentation: Create WMI Providers to Notify Applications of System Events msdn magazine As crawled by the Wayback Machine on 2/1/2009
	W	Static Analysis of Executables for Collaborative Malware Detection on Android Aubrey-Derrick Schmidt et al. ICC'09 Proceedings of the 2009 IEEE international conference on Communications Pages 631-635
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.



Trademarks > Trademark Electronic Search System (TESS)

TESS was last updated on Thu Jul 11 03:20:58 EDT 2013

TESS Home | New User | Structured | Free Form | Browse Dict | Search OG | Bottom | Help | Prev List | Curr List | Next List | First Doc | Prev Doc | Next Doc | Last Doc

Logout Please logout when you are done to release system resources allocated for you.

Start List At: OR Jump to record: **Record 1 out of 5**

TSDR [redacted] [redacted] *(Use the "Back" button of the Internet Browser to return to TESS)*

OPENFLOW

Word Mark	**OPENFLOW**
Goods and Services	IC 009. US 021 023 026 036 038. G & S: Computer network switches; computer software implementing a computer network protocol that facilitates the control of network switches, routers and wireless access points; all of the aforesaid goods not intended to be marketed, sold or used in the fields of oil exploration and production or in the fields of receiving and storage of carbon dioxide IC 042. US 100 101. G & S: Design and development of computer hardware and software; design and development of computer network protocols that facilitate the control of network switches, routers and wireless access points; consultancy in the field of computer hardware and software for purposes of encouraging computer networking innovation; all of the aforesaid services not intended to be marketed, sold or used in the fields of oil exploration and production or in the field of receiving and storage of carbon dioxide
Standard Characters Claimed	
Mark Drawing Code	(4) STANDARD CHARACTER MARK
Serial Number	85319202
Filing Date	May 12, 2011
Current Basis	1B
Original Filing Basis	1B
Published for	

IPR2023-01466
CrowdStrike EX1002 Page 308

Opposition	January 8, 2013
Owner	(APPLICANT) Open Networking Foundation non-profit corporation OREGON 3855 SW 153rd Drive Beaverton OREGON 97006
Attorney of Record	Matthew R. Wilmot
Type of Mark	TRADEMARK. SERVICE MARK
Register	PRINCIPAL
Live/Dead Indicator	LIVE

IPR2023-01466
CrowdStrike EX1002 Page 309

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13559766	KUMAR ET AL.
	Examiner	**Art Unit**
	VADIM SAVENKOV	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	07/12/2013								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								

IPR2023-01466
CrowdStrike EX1002 Page 310

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 9330

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/559,766	07/27/2012	726	2431	0079152-000016

APPLICANTS

Srinivas KUMAR, Cupertino, CA;
Dennis Pollutro, Clymer, NY;

**** CONTINUING DATA ***************************

This appln claims benefit of 61/641,007 05/01/2012

**** FOREIGN APPLICATIONS **************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****

08/08/2012

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /VADIM SAVENKOV/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		CA	29	20	3

ADDRESS

BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404
UNITED STATES

TITLE

SYSTEMS AND METHODS FOR THREAT IDENTIFICATION AND REMEDIATION

FILING FEE RECEIVED		
1250	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13559766
	Filing Date	2012-07-27
	First Named Inventor	Srinivas KUMAR et al.
	Art Unit	2431
	Examiner Name	Unassigned
	Attorney Docket Number	0079152-000016

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20050289072	A1	2005-12-29	Sabharwal	
	2	20070143474	A1	2007-06-21	Sheng et al.	
	3	20070174406	A1	2007-07-26	Morris et al.	
	4	20090094584	A1	2009-04-09	Dheap et al.	
	5	20090144818	A1	2009-06-04	Kumar et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.S./

Receipt date: 11/09/2012	Application Number	13559766	13559766 - GAU: 2431
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Filing Date	2012-07-27	
	First Named Inventor	Srinivas KUMAR et al.	
	Art Unit	2431	
	Examiner Name	Unassigned	
	Attorney Docket Number	0079152-000016	

	6	20090138939	A1	2009-05-28	Kumar et al.	
	7	20090276204	A1	2009-11-05	Kumar et al.	
	8	20090241170	A1	2009-09-24	Kumar et al.	
	9	20090133110	A1	2009-05-21	Kumar et al.	
	10	20090328186	A1	2009-12-31	Pollutro et al.	
	11	20120216244	A1	2012-08-23	Kumar et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.S./

Receipt date: 11/09/2012	Application Number	13559766 13559766 - GAU: 2431
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Filing Date	2012-07-27
	First Named Inventor	Srinivas KUMAR et al.
	Art Unit	2431
	Examiner Name	Unassigned
	Attorney Docket Number	0079152-000016

	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE

Examiner Signature	/Vadim Savenkov/	Date Considered	07/11/2013

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.S./

Receipt date: 11/09/2012	Application Number	13559766	13559766 - GAU: 2431
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Filing Date	2012-07-27	
	First Named Inventor	Srinivas KUMAR et al.	
	Art Unit	2431	
	Examiner Name	Unassigned	
	Attorney Docket Number	0079152-000016	

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/ R. K. Baldwin /	Date (YYYY-MM-DD)	2012-11-09
Name/Print	Randall K. Baldwin	Registration Number	59713

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.S./

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.S./

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13559766	KUMAR ET AL.
	Examiner	Art Unit
	VADIM SAVENKOV	2431

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	25	7/12/2013	VS

SEARCH NOTES		
Search Notes	Date	Examiner
See attached EAST search history of all the relevant databases.	7/12/2013	VS
Double Patenting search: Inventor/Assignee in PALM/EAST	7/12/2013	VS
Consulted with SPE Nathan Flynn regarding OPENFLOW claim language.	7/12/2013	VS
Class search of 726/22-25; Word search within and outside of said class/subclasses.	7/12/2013	VS
Forward and Backward citation searching relevant prior art.	7/12/2013	VS
Google and IEEE search for relevant prior art; search history not included.	7/12/2013	VS

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

/V.S./ Examiner.Art Unit 2431	

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	13559766
Filing Date	2012-07-27
First Named Inventor	Srinivas KUMAR et al.
Art Unit	2431
Examiner Name	Unassigned
Attorney Docket Number	0079152-000016

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20050289072	A1	2005-12-29	Sabharwal	
	2	20070143474	A1	2007-06-21	Sheng et al.	
	3	20070174406	A1	2007-07-26	Morris et al.	
	4	20090094584	A1	2009-04-09	Dheap et al.	
	5	20090144818	A1	2009-06-04	Kumar et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13559766
	Filing Date	2012-07-27
	First Named Inventor	Srinivas KUMAR et al.
	Art Unit	2431
	Examiner Name	Unassigned
	Attorney Docket Number	0079152-000016

	6	20090138939	A1	2009-05-28	Kumar et al.	
	7	20090276204	A1	2009-11-05	Kumar et al.	
	8	20090241170	A1	2009-09-24	Kumar et al.	
	9	20090133110	A1	2009-05-21	Kumar et al.	
	10	20090328186	A1	2009-12-31	Pollutro et al.	
	11	20120216244	A1	2012-08-23	Kumar et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13559766
	Filing Date	2012-07-27
	First Named Inventor	Srinivas KUMAR et al.
	Art Unit	2431
	Examiner Name	Unassigned
	Attorney Docket Number	0079152-000016

	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13559766
	Filing Date	2012-07-27
	First Named Inventor	Srinivas KUMAR et al.
	Art Unit	2431
	Examiner Name	Unassigned
	Attorney Docket Number	0079152-000016

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/ R. K. Baldwin /	Date (YYYY-MM-DD)	2012-11-09
Name/Print	Randall K. Baldwin	Registration Number	59713

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt	
EFS ID:	14188959
Application Number:	13559766
International Application Number:	
Confirmation Number:	9330
Title of Invention:	SYSTEMS AND METHODS FOR THREAT IDENTIFICATION AND REMEDIATION
First Named Inventor/Applicant Name:	Srinivas KUMAR
Customer Number:	21839
Filer:	Randall K. Baldwin/Kevin Chanthakhoune
Filer Authorized By:	Randall K. Baldwin
Attorney Docket Number:	0079152-000016
Receipt Date:	09-NOV-2012
Filing Date:	27-JUL-2012
Time Stamp:	11:09:00
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	PTO_SB08.PDF	612594 c013e77717723fea2ef59827df7a41a4f6ba285f	no	5

Warnings:
Information:

Total Files Size (in bytes):	612594

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 13/559,766

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	380
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	620
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	250
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20 =	*			OR	x 60 =	0.00
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*				x 250 =	0.00
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	1250

APPLICATION AS AMENDED - PART II

AMENDMENT A

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
Application Size Fee (37 CFR 1.16(s))									
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

AMENDMENT B

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
Application Size Fee (37 CFR 1.16(s))									
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/559,766	07/27/2012	2431	1250	0079152-000016	20	3

CONFIRMATION NO. 9330

21839
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

FILING RECEIPT

OC000000055899035

Date Mailed: 08/14/2012

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Srinivas KUMAR, Cupertino, CA;
Dennis Pollutro, Clymer, NY;

Assignment For Published Patent Application

Taasera, Inc., Erie, PA

Power of Attorney: The patent practitioners associated with Customer Number 21839

Domestic Priority data as claimed by applicant

This appln claims benefit of 61/641,007 05/01/2012

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)

If Required, Foreign Filing License Granted: 08/08/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/559,766**

Projected Publication Date: 11/07/2013

Non-Publication Request: No

Early Publication Request: No

IPR2023-01466
CrowdStrike EX1002 Page 326

Title

SYSTEMS AND METHODS FOR THREAT IDENTIFICATION AND REMEDIATION

Preliminary Class

726

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as

IPR2023-01466
CrowdStrike EX1002 Page 327

set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage, facilitate, and accelerate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

Patent
Attorney Docket No. 0079152-000016

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

UTILITY PATENT APPLICATION TRANSMITTAL LETTER
FOR ELECTRONICALLY FILED UTILITY APPLICATION

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Customer Number **2 1 8 3 9**

Sir:

Enclosed for filing is the utility patent application entitled:

SYSTEMS AND METHODS FOR THREAT IDENTIFICATION AND REMEDIATION

by the following named inventors:

Srinivas KUMAR; and Dennis Vance POLLUTRO

☒ Applicant(s) suggests Figure 1 for inclusion on the front page of the patent application publication and patent.

☒ Applicant(s) requests that the published application include the following assignment information: TAASERA, INC., Cupertino, California, USA.

☐ Small entity status is claimed.

Also enclosed are:

DRAWINGS: 29 sheets of drawings

DECLARATION: ☐ will follow ☒ executed, is enclosed ☐ unexecuted, is enclosed

ASSIGNMENT: ☒ is being filed electronically concurrent with the electronic filing of the application.
☐ will follow.

CLAIM FOR PRIORITY UNDER 35 USC § 119 and/or 365: ☐ is made in the declaration ☒ is hereby made as follows:

Country	Appl. No.	Filing Date MM-DD-YYYY
US	61/641,007	05-01-2012

OTHER PAPERS:
☒ A General Authorization for Petitions for Extensions of Time and Payment of Fees
☐ An Information Disclosure Statement
☒ An Application Data Sheet
☐ Other:

☒ The filing fee has been calculated as follows:

☐ and in accordance with the enclosed Preliminary Amendment:

					FEES
Basic Patent Application Filing Fee (1011)					$380.00
Examination Fee (1311)					$250.00
Search Fee (1111)					$620.00
	No. of Claims		Extra Claims	Rate	
Total Claims	20	Minus 20=		x $ 60.00 (1202)	
Independent Claims	3	Minus 3=		x $ 250.00 (1201)	
If multiple dependent claims are presented, add $450.00 (1203)					
App. Size Fee (app + dwgs. exceeding 100 sheets) - $310.00 / each add'l. 50 sheets (1081)					
TOTAL APPLICATION FEE DUE					**$1,250.00**

☒ Charge $1,250.00 to credit card. Filing fee is being paid electronically concurrent with filing of application.

☒ The Director is hereby authorized to charge any appropriate fees under 37 C.F.R. §§ 1.16, 1.17 and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 02-4800.

Please address all correspondence concerning this application to:

Buchanan Ingersoll & Rooney PC
Customer Number **2 1 8 3 9**

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: July 27, 2012

By: _____
Charles F. Wieland III
Registration No. 33,096

Customer Number 21839
703.836.6620

Attorney Docket No. 0079152-000016

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	
Srinivas KUMAR et al.	Group Art Unit: Unassigned
Application No.: Unassigned	Confirmation No.: Unassigned
Filed: July 27, 2012	
For: SYSTEMS AND METHODS FOR THREAT IDENTIFICATION AND REMEDIATION	

GENERAL AUTHORIZATION FOR PETITIONS FOR EXTENSIONS OF TIME AND PAYMENT OF FEES

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with 37 C.F.R. § 1.136(a)(3), the U.S. Patent and Trademark Office is hereby provided with a general authorization to treat any concurrent or future reply requiring a petition for an extension of time for its timely submission as containing a request therefor for the appropriate length of time.

The Commissioner is hereby authorized to charge any appropriate fees that may be required by this paper, or any other submissions in this application, and to credit any overpayment, to Deposit Account No. 02-4800.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: July 27, 2012

By: _____
Charles F. Wieland III
Registration No. 33,096

Customer Number 21839
703.836.6620

APPLICATION DATA SHEET

Application Information

Application Number::	
Filing Date::	
Application Type::	Nonprovisional
Subject Matter::	Utility
CD-ROM or CD-R?::	None
Computer Readable Form (CRF)?::	No
Title::	SYSTEMS AND METHODS FOR THREAT IDENTIFICATION AND REMEDIATION
Attorney Docket Number::	0079152-000016
Request for Early Publication?::	No
Request for Non-Publication?::	No
Total Drawing Sheets::	29
Small Entity?::	No
Petition Included?::	No
Secrecy Order in Parent Appl.?::	No

Applicant Information

Applicant Authority Type::	Inventor
Primary Citizenship Country::	USA
Status::	Full Capacity
Given Name::	Srinivas
Family Name::	KUMAR
City of Residence::	Cupertino
State or Province of Residence::	California

IPR2023-01466
CrowdStrike EX1002 Page 332

Country of Residence::	USA
Street of Mailing Address::	10926 Northridge Square
City of Mailing Address::	Cupertino
State or Province of Mailing Address::	California
Country of Mailing Address::	USA
Postal or Zip Code of Mailing Address::	95014
Applicant Authority Type::	Inventor
Primary Citizenship Country::	USA
Status::	Full Capacity
Given Name::	Dennis
Middle Name::	Vance
Family Name::	POLLUTRO
City of Residence::	Clymer
State or Province of Residence::	New York
Country of Residence::	USA
Street of Mailing Address::	8613 Knowlton Road
City of Mailing Address::	Clymer
State or Province of Mailing Address::	New York
Country of Mailing Address::	USA
Postal or Zip Code of Mailing Address::	14724

Correspondence Information

Correspondence Customer Number::	21839
Phone Number::	(703) 836-6620

Fax Number: (703) 836-2021

Representative Information

Representative Customer Number:: 21839

Domestic Priority Information

Application::	Continuity Type::	Parent Application::	Parent Filing Date::
This Application	Claiming benefit under 35 USC 119(e)	61/641,007	05/01/12

Assignee Information

Assignee Name::	Taasera, Inc.
Street of Mailing Address::	1030 State Street
City of Mailing Address::	Erie
State or Province of Mailing Address::	Pennsylvania
Country of Mailing Address::	USA
Postal or Zip Code of Mailing Address::	16501

Signature	/Charles F. Wieland III/	Date	July 27, 2012
Name	Charles F. Wieland III	Registration No.	33,096

IPR2023-01466
CrowdStrike EX1002 Page 334

Electronic Patent Application Fee Transmittal	
Application Number:	
Filing Date:	
Title of Invention:	SYSTEMS AND METHODS FOR THREAT IDENTIFICATION AND REMEDIATION
First Named Inventor/Applicant Name:	Srinivas KUMAR
Filer:	Charles F. Wieland III/Beverly Caraway
Attorney Docket Number:	0079152-000016
Filed as Large Entity	

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility application filing	1011	1	380	380
Utility Search Fee	1111	1	620	620
Utility Examination Fee	1311	1	250	250
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**1250**

Electronic Acknowledgement Receipt	
EFS ID:	13356009
Application Number:	13559766
International Application Number:	
Confirmation Number:	9330
Title of Invention:	SYSTEMS AND METHODS FOR THREAT IDENTIFICATION AND REMEDIATION
First Named Inventor/Applicant Name:	Srinivas KUMAR
Customer Number:	21839
Filer:	Charles F. Wieland III/Beverly Caraway
Filer Authorized By:	Charles F. Wieland III
Attorney Docket Number:	0079152-000016
Receipt Date:	27-JUL-2012
Filing Date:	
Time Stamp:	11:17:14
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$1250
RAM confirmation Number	9939
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1		SPEC.pdf	315744 37c732a05824c1f3a109c82c97d09678e1577411	yes	72

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Specification	1	65
	Claims	66	71
	Abstract	72	72

Warnings:					
Information:					
2	Drawings-only black and white line drawings	DRAW.pdf	9379314 3894323d7faec091ecec8c59c6fc3eb368901360	no	29
Warnings:					
Information:					
3	Oath or Declaration filed	DEC.pdf	195470 2f77a7d3a134f1b53840fe3af2ba094d9c5a11ce	no	4
Warnings:					
Information:					
4	Transmittal of New Application	TL.pdf	81923 5f14107ba4cad959f2a365718fd1bd11239950f2	no	2
Warnings:					
Information:					
5	Authorization for Extension of Time all replies	GENAUTH.pdf	35396 04e5b20b4a2be27d73c2330e6363a36ff225ce62	no	1
Warnings:					
Information:					
6	Application Data Sheet	ADS.pdf	16527 1c3b50bde6500768c86bbbc19ca741ea2f368f6c	no	3
Warnings:					
Information:					
This is not an USPTO supplied ADS fillable form					
7	Fee Worksheet (SB06)	fee-info.pdf	33177 2a88d5f3fb4a0e33e9aba7ab0fc86d8f8b65eb7a	no	2
Warnings:					
Information:					

Total Files Size (in bytes):	10057551

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

APPLICATION FOR
UNITED STATES LETTERS PATENT

FOR

SYSTEMS AND METHODS FOR THREAT IDENTIFICATION AND REMEDIATION

by

SRINIVAS KUMAR
and
DENNIS POLLUTRO

Attorney Docket No. 0079152-000016
BUCHANAN INGERSOLL & ROONEY PC
CUSTOMER NO. 21839
P.O. Box 1404
Alexandria, VA 22313-1404

SYSTEMS AND METHODS FOR THREAT IDENTIFICATION AND REMEDIATION

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application claims the benefit of U.S. Provisional Appl. No. 61/641,007 entitled "System and Method for Operational Integrity Attestation," filed May 1, 2012, incorporated by reference herein in its entirety.

BACKGROUND OF THE DISCLOSURE

FIELD OF THE DISCLOSURE

[0002] The present disclosure relates to the field of data center virtualization and, more particularly, to systems and methods for providing dynamic operational integrity attestation of application security and a user reputation at runtime.

DESCRIPTION OF THE RELATED ART

[0003] One recent trend in computing is the trend towards virtualization and cloud computing in which, for example, enterprise software is no longer owned by the customer, but instead the enterprise's Information Technology (IT) infrastructure can be provided by a third party and enterprise software applications are sold as service offerings.

[0004] Traditional legacy and currently available security technologies, such as next-generation anti-virus software, network firewalls, and intrusion detection/prevention systems, operate based on signatures, protocol anomalies or virtual execution in a sandbox to monitor threats and attacks. However, once a target of an attack or threat (i.e., a 'target system' or 'target platform') becomes infected or compromised, many of these technologies have been proven relatively ineffective in protecting systems and preventing data breaches or service disruptions. Emerging threats and attacks can exhibit a low and slow mode of operation and can be signature-less in order to evade traditional detection and defense technologies. Further, these technologies are often agnostic to the runtime

operational integrity of computer workloads on the target (victim) systems and therefore often do not offer any level of remediation to service the affected target systems. As such, many traditional security technologies merely provide coarse-grained access controls limited to a simple allow or deny decision logic.

[0005] Many enterprises and organizations are moving there IT infrastructures to cloud computing environments (from self-managed on-premise data centers to service-provider managed outsourced virtual data centers), wherein which third parties may provide shared computing resources and applications running on those resources. They are being offered as services to a plurality of customers. The move by companies to cloud computing environments are increasing for various reasons, including the need for increased computing power, increased storage capacity, and/or increased network bandwidth, among others. Enterprise applications and mission critical applications may be executed in the cloud. Without adequate device, system, and application security, the cloud can compromise these applications, potentially causing large financial losses. Data confidentiality, data integrity and data availability can be maintained in the cloud computing environment even when such applications may be controlled by these third parties. The cloud may enable traditional information technology devices, systems and applications to transparently execute from these service-providers managed outsourced virtual data centers. As newer technologies emerge, the cloud infrastructure may evolve transparent to and scalable with enterprise operations. Security in such environments may be an emerging challenge. For example, virtualized, cloud computing on-demand, and elastic models require dynamic security orchestration at both the device and network level that is lacking in traditional security approaches and technologies.

[0006] A significant metric that relates to the lack of remediation controls in current security controls is the high rate of false positives and negatives in the detection of threats. False positives are unproductive and reduce operating capacity in data centers. False negatives lead to the bypass of security controls and compromise of the target systems and services. Existing signature-based approaches to security control are vulnerable to improvised attacks staged at targeted systems.

[0007] The proliferation of applications (business, social networking and gaming software) in Enterprise and cloud computing ecosystems has significantly increased the attack surface and window of exposure. Application runtime operational integrity is a critical factor in building end-to-end trust from device to service. The proliferation of unmanaged devices such as mobile computing devices (i.e., tablets and smart phones) and Bring Your Own Device (BYOD) policies in Enterprise network environments has increased the risk of advanced coordinated threats.

[0008] The current predominant security paradigm is based on a hard edge and soft core architecture. Security appliances such as network firewalls and intrusion detection/prevention systems deploy at the edge (perimeter). Antivirus and network based integrity measurement and verification services scan and audit the soft-core that comprises business critical systems, services and high value data silos. Once the edge is breached, defensive methods are largely ineffective in protecting vulnerable or compromised systems. In this paradigm, the hard edge does not generally provide any level of assurance of the runtime operational integrity of the soft core.

[0009] The heavy reliance on extensive application whitelists/blacklists(based on file hash digests and/or configuration), Internet Protocol (IP) address reputation lists, signatures, protocol anomalies and virtual execution in a sandbox, provides targeted and coordinated attacks a large staging surface to maneuver around with meticulously engineered evasion methods exploiting the gaps. Irrespective of the method of break-in, the post-infection behaviors during the window of exposure on a victim machine or environment are difficult to conceal, but may be obscured from timely detection and diagnosis by security administrators and virtual execution (sandbox) environments through evasion techniques. Various exemplary embodiments include an early warning system for threat identification and diagnosis with high forensic confidence and infection summaries for manual and/or automated intervention.

[0010] Current identity management (IdM) approaches are typically aimed at domain level authentication of users for the use of a security token in a transaction or business process wherein the issuance of the token is strictly based on proof of

possession of credentials and not the reputation of the user. While the industry has adopted multi-factor authentication technologies for increased protection from malicious users whose intent is to steal credentials for the purpose of impersonation or delegation, these security controls do not provide a means for incorporating attribution of an authenticated user's risk posture, independent of provisioned entitlements (i.e., user account privileges and roles). Thus, existing security controls do not incorporate a complete view of a user's risk posture as a component of an access policy, based on correlation of location and device agnostic global threat intelligence about the user. Accordingly, what is needed are systems and methods for runtime operational integrity monitoring of applications by providing dynamic operational integrity attestation of application security and user reputation at runtime that take into account a subject's (such as a device, application, or user) risk posture. What is further needed are systems and methods for performing post infection diagnoses, threat identification via signature-less anomalous behavior recognition using non-intrusive platform instrumentation without requiring 'hooks' into an operating system (OS) Kernel by security vendors that leverages OS vendor application programming interfaces (APIs).

[0011] The emerging cloud based application-hosting model requires a higher level of scrutiny of device and user security posture. Threats can be posed by both external and internal users, and therefore it has become harder to determine whether an authenticated user is a trustworthy operative. Application and network layer entitlements are largely static in nature. While role based access control (RBAC) systems are positioned to offer dynamic policies, these are not based on any form of aggregation of external threat intelligence in the context of the user in the transaction.

[0012] Tokenization of identities by Security Token Services (STS) intended to facilitate in Identity Federation and Single Sign On (SSO) for web and Enterprise applications have only aggravated the threat vectors by expanding the scope of resources that an authenticated user may access implicitly without granular context. Along with the coarse access policies offered by traditional security controls, such as firewalls and intrusion prevention systems, this increases the attack surface for

application exploits by malicious users leveraging the excessive privileges granted by default to most users (and groups) today, in the absence of strict Separation of Duties (SoD) and Principle of Least Privilege (PoLP) enforcement.

[0013] Several studies have uncovered conclusive evidence that the largest risk, associated with malicious activities resulting in theft of confidential data, intellectual property or financial losses for enterprises and consumers, arises from insider rather than outsider or man-in-the-middle attacks. Threat assessment systems have been predominantly focused on the means and methods rather than the adversary or operator (i.e., a user). There has been no emphasis on the reputation score of a user in the transaction or business process as a real time integrity metric for integration with access policy decision logic. Accordingly, what is further needed are systems and methods that employ a user reputation score that can serve either as a punitive or corrective method of intervention for the proactive prevention of exploits and data breaches.

[0014] One goal of trusted computing is to provide a resource owner or service provider with reliable knowledge about a target system. Current attestation systems are components of computer systems that permit reliable statements of evidence about those systems to be conveyed to remote parties, including other computers. Through evaluation of the identity and integrity of components of a system (i.e., a target system being evaluated), evidence is produced that the target system will not engage in defined classes of misbehaviors. As the users accessing a system and the requirements of applications running on a system generally cannot be known a priori, attestation systems and measurement systems alike must be flexible, providing for privacy, completeness of measurement, and trust in the basic collection and reporting mechanisms.

[0015] Existing attestation systems are often narrowly focused and generally aimed at specific use-cases limited to system components such as hardware and applications and therefore typically lack flexibility to dynamically address more general attestation problems. Further, existing definitions of attestation focus primarily on describing specific, narrow, and particular properties desirable in specific use-cases. Additionally, current attestation systems are created to work with one

particular measurement system targeting one particular system of interest without considering the reputations of users or operators of the system of interest.

[0016] Accordingly, what the present inventors have identified as desirable are technology based attestation architectures, systems, and methods that perform a calculus of risk to determine a level of trust of systems that are not necessarily monolithic and can be made up of diverse hardware and software platforms and can be accessed by users with varying credentials and reputations. Accordingly, what the inventors have identified as being desirable are attestation architectures, systems, and methods that can be flexible enough to accommodate varying concepts of attestation, including taking the reputation of users that access targeted systems into account. What the present inventors also see as desirable are attestation systems and architectures that can dynamically handle complex attestation scenarios and provide more complete runtime attestation than is currently achievable. What the present inventors additionally see as desirable are methods and systems for performing evidence based automated application binary analysis.

SUMMARY OF THE DISCLOSURE

[0017] Exemplary methods and systems are disclosed for continuously monitoring one or more systems and/or to correlate events and behavior of systems on an instrumented target platform at runtime using or based on a plurality of assertions (or statements).

[0018] In exemplary embodiments, methods, apparatus, systems and computer readable media perform infection diagnosis based on reconnaissance based intelligence correlation and a threat life cycle model of advanced low-and-slow attacks wherein malware may operate through a series of benign actions at an endpoint device.

[0019] In other exemplary embodiments, methods, apparatuses, systems and computer readable media comprise a plurality of services that enable visibility, control, and/or compliance in a cloud computing environment with a runtime dashboard to capable of displaying operational integrity metrics of systems based on a plurality of threat vectors.

[0020] In yet other exemplary embodiments, methods, apparatuses, systems and computer readable media establish device-to-network flows based on dynamic attestation of device integrity, and/or security controls provisioned based on integrity and context aware business logic instead of, for example, topology based coordinates associated with encapsulation headers in network packets.

[0021] Exemplary systems and methods for dynamic attestation of application integrity are described in U.S. Non-Provisional Patent Application No. 13/399,065 entitled "System and Method for Application Attestation," filed February 16, 2012, and U.S. Provisional Patent Application No. 61/443,854 entitled "System and Method for Application Attestation," filed February 17, 2011, both of which are incorporated herein by reference in their entireties.

[0022] According to exemplary embodiments, methods, apparatuses, systems and computer readable media authorize user-to-application transactions and/or data exchange in an established connection, during the authentication phase based on dynamic attestation of devices.

[0023] In accordance with further exemplary embodiments, methods, apparatuses, systems, and computer readable media determine a calculus of risk based on a plurality of sensory inputs from network and endpoint sensors to correlate network activity, system configuration, resource utilization and application integrity.

[0024] According to an exemplary embodiment, the network and endpoint sensors may be configured to measure runtime operational integrity and/or detect anomalous deviations in behavior from baseline based on rule sets to generate tiered alerts.

[0025] In accordance with exemplary embodiments, methods, apparatuses, systems and computer readable media comprise an event and behavior correlation engine configured to receive alerts, calculate risks and generate warnings.

[0026] In other exemplary embodiments, methods, apparatuses, systems and computer readable media remediate systems that are deviated, vulnerable, in duress or compromised based on a calculus of risk.

[0027] In accordance with yet other exemplary embodiments, methods, apparatuses, systems and computer readable media include: (1) a correlation engine configured to receive scan reports from vulnerability, configuration, compliance, and

patch scan services; (2) a risk correlation matrix configured to store elements of the scan reports that are used to analyze the elements; and (3) a module configured to generate an integrity profile of systems.

[0028] The presently disclosed exemplary technical solutions also may be embodied as methods, apparatuses, systems and computer readable media comprising: (1) event correlation logic that correlates temporal system events based on multiple predicate scores; (2) logic to determine a predicate score based upon a deviation from a prescribed value constraint per attribute (or metric, i.e., an attribute constraint); (3) logic for calculating a score that is inversely proportional to the deviation; (4) logic for determining a sample rate needed to achieve a required measurement frequency; (5) logic for determining a recurrence of successive deviations; (6) logic for identifying a weight for the attribute constraint; (7) logic for determining an integrity confidence for the system or process (or application) entity as a weighted average of predicate scores; and (8) logic for determining identifying outliers as exceptions (across multiple systems or processes).

[0029] The exemplary methods, apparatuses, architectures, systems and computer readable media disclosed herein may also use threat identification categories including, but not limited to:

[0030] (1) static image analysis (i.e., static analysis of binary files, intermediate code, and/or scripts);

[0031] (2) dynamic image (binary, intermediate code, or script) analysis with process, platform and network monitors;

[0032] (3) malware analysis for evasion techniques (multiple packing, obfuscated application programming interfaces (APIs), anti-debugging, anti-memory, anti-tracing, virtual machine monitor/manager (VMM) or hypervisor/emulator detection;

[0033] (4) dynamic system analysis of performance metrics harvested through native machine instrumentation, registry, and file system monitors; and

[0034] (5) temporal system analysis with consolidated integrity measurement and verification assessments and scan reports.

[0035] The presently disclosed exemplary technical solutions may be embodied as a method, apparatus and/or system for integrity confidence measurement including:

(1) a weighted average of system (or platform) predicate scores; (2) system (or platform) outliers; (3) weighted average of process (or application package) predicate scores; (4) process outliers.

[0036] The presently disclosed exemplary technical solutions also may be embodied methods, apparatuses, architectures, systems and computer readable media for generating user reputation scores for a plurality of users based on one or more of: (1) threat vectors modeled by actions of the plurality of users; (2) risk correlation with aggregation of intelligence related to accessed object (resource) attribution, subject roles, globally unique subject identifiers, security information and event management analytics, and geo-location services.

BRIEF DESCRIPTION OF THE DRAWING FIGURES

[0037] The presently disclosed exemplary technical solutions are best understood from the following detailed description when read in connection with the accompanying drawings, to which the claimed invention is not limited. According to common practice, various features/elements of the drawings may not be drawn to scale. Common numerical references represent like features/elements. The following figures are included in the drawings:

FIG. 1 is an architecture diagram of an exemplary system for providing operational integrity attestation of application security and user reputation, according to an embodiment of the present disclosure;

FIG. 2 is a schematic diagram illustrating an exemplary system for endpoint and network activity correlation, according to an exemplary embodiment of the present disclosure;

FIG. 3A is a flowchart illustrating steps by which early warning and response automation is performed through monitoring, orchestration and remediation, according to an exemplary embodiment of the present disclosure;

FIG. 3B is a data flow diagram for intersystem risk assessment and remediation, according to an exemplary embodiment of the present disclosure;

FIG. 4 is a data flow diagram for configuring an attestation system by consolidating and normalizing network endpoint assessments, according to an exemplary embodiment of the present disclosure;

FIG. 5 illustrates communications between components of a system for measuring and evaluating application operational integrity, according to an exemplary embodiment of the present disclosure;

FIG. 6 is a block diagram illustrating data flows for instrumenting and measuring network endpoint risk, according to an exemplary embodiment of the present disclosure;

FIG. 7A depicts exemplary endpoint events that can be monitored by the systems and methods disclosed herein;

FIG. 7B depicts exemplary endpoint alerts that can be generated by the systems and methods disclosed herein;

FIG. 7C is a block diagram illustrating a method for correlating endpoint alerts and generating endpoint warnings, according to an exemplary embodiment of the present disclosure;

FIG. 8 is a block diagram of a trust orchestration architecture for correlating a plurality of events for determining operational integrity of a system, according to an exemplary embodiment of the present disclosure;

FIG. 9 is a block diagram of a system for consolidating and correlating a plurality of identity, inventory and log management systems for determining a reputation of a user, according to an exemplary embodiment of the present disclosure;

FIG. 10 is a block diagram of a system for determining a calculus of risk, according to an exemplary embodiment of the present disclosure;

FIG. 11 is block diagram of a of a system for generating subject reputation scores based on a calculus of risk, according to an exemplary embodiment of the present disclosure;

FIG. 12 is a block diagram of a system for network flow remediation based on a calculus of risk, according to an exemplary embodiment of the present disclosure;

FIG. 13 a block diagram illustrating of a system for providing mobile security by remediating mobile devices and wireless network flows based on a calculus of risk, according to an exemplary embodiment of the present disclosure;

FIGs. 14-18 depict a graphical user interface (GUI) for an exemplary trust management console including dashboards for operational runtime integrity, system configuration, resource, application integrity, and network activity, in accordance with various exemplary embodiments;

FIGs. 19-22 are flowcharts illustrating methods for threat identification and remediation, providing a user reputation service, and providing network flow level remediation in accordance with various exemplary embodiments of the presently disclosed technology;

FIG. 23 is an entity-relationship diagram (ERD) illustrating relationships between entities of a reputation scoring system, according to an embodiment of the present disclosure;

FIG. 24 illustrates a hierarchical representation of a subject reputation score, according to an embodiment of the present disclosure;

FIG. 25 is a block diagram of an architecture for monitoring application events with extensions to native machine instrumentation, according to an exemplary embodiment of the present disclosure; and

FIG. 26 is a diagram of an example computer system in which embodiments can be implemented.

DETAILED DESCRIPTION

[0038] Although the invention is illustrated and described herein with reference to certain exemplary embodiments, the invention is not intended to be limited thereto. Rather, various modifications may be made that are within the scope and range of equivalents of the claims and without departing from the invention. Various features, attributes and advantages described herein may or may not be present in various embodiments of the claimed invention.

[0039] In the detailed description herein, references to “one embodiment,” “an embodiment,” “an example embodiment,” etc., indicate that the embodiment described may include a particular feature, structure, or characteristic, but every

embodiment may not necessarily include the particular feature, structure, or characteristic. Moreover, such phrases are not necessarily referring to the same embodiment. Further, when a particular feature, structure, or characteristic is described in connection with an embodiment, it is submitted that it is within the knowledge of one skilled in the art to affect such feature, structure, or characteristic in connection with other embodiments whether or not explicitly described.

[0040] In certain exemplary embodiments, behavior deviations from a baseline healthy operational state to a vulnerable or compromised state may be detected, and the infection identified, before there is further propagation of the threat across interconnected systems, or information is exfiltrated resulting in data loss or theft.

[0041] The proliferation of unmanaged smart phones and Bring Your Own Device (BYOD) initiatives in the Enterprise ecosystem has increased the ability of advanced malware to evade traditional network and endpoint security controls and propagate to connected systems over standard protocols. Various exemplary embodiments include determination of the operational integrity of the device and/or the user in a transaction with an on-premise or off-premise service, based on the calculus of risk from a plurality of sensory inputs, for transaction and/or flow level remediation of infected devices.

Network for Monitoring and Dynamic Analysis of Events and Activities

[0042] FIG. 1 is an architecture diagram for an exemplary network 100 configured to continuously monitor and dynamically analyze events and network activity to ascertain the integrity of a monitored system (i.e., a target system).

[0043] Referring to the exemplary embodiment provided in FIG. 1, the network 100 includes an event and behavior correlation engine 130 configured to perform risk correlation 120 based on continuous monitoring 110 using a plurality of sensory inputs. In the embodiment of FIG. 1, the sensory inputs can include, but are not limited to, one or more of: network activity 111; system configuration 113; resource utilization 115; and application integrity 117. The network 100 also comprises a runtime dashboard 150 configured to receive real time status indications 131 for visibility of operational integrity of systems and a remediation engine 170 configured to receive real time directives 132 for control of infected systems.

[0044] The event and behavior correlation engine 130 is configured to receive network events and infection profiles 112 from a network activity sensor 111, integrity measurement and verification reports 114 of scans performed by a system configuration sensor 113. According to an embodiment, the scans are performed by the configuration sensor 113 according to a schedule. In embodiments, the scans can be scheduled to run daily, weekly, bi-weekly, monthly, or at other time increments as needed.

[0045] As shown in FIG. 1, the event and behavior correlation engine 130 is also configured to receive endpoint events 116 of computing, network and storage resource consumption from a resource utilization sensor 115, and endpoint events of image profiles and local execution context 118 from an application integrity sensor 117. Details of exemplary implementations of the system configuration sensor 113, the resource utilization sensor 115, the application integrity sensor 117, and the endpoint events 116, 118 are described below with reference to FIGs. 4-7.

[0046] The remediation engine 170 may perform actions 171 on a virtual machine (VM) 172, actions 173 on a network flow controller 174, or actions 175 on a transaction 176 based on configured trigger controls.

[0047] As will be appreciated by persons skilled in the relevant art(s), a VM is a software implementation of a machine such as a server, personal computer, mobile computing device, or other computing device that supports the execution of an operating system (OS) and executes applications as a physical machine running that OS would. A VM is a software implementation that duplicates the functionality of a physical machine implemented in hardware and software. Software applications and the OS running on a VM are limited to the resources and abstractions provided by the VM. Virtual machines (VMs) can be viewable within an overall virtual infrastructure. As will be appreciated by those skilled in the relevant art, a VMM or hypervisor can be used to start up, monitor, and manage VMs. Such hypervisors can be, but are not limited to VMMs such as the VMWARE™ Player, MICROSOFT™ VirtualPC, SUN™ VirtualBox, VMWARE™ ESX/ESXi, MICROSOFT™ Hyper-V, CITRIX™ XENServer, PARALLELS™ and others. As it would be apparent to one of

skill in the art, other hypervisors and VMs/virtualization solutions can be used for VM 172 in network 100 as well.

Example System and Method for Endpoint and Network Activity Correlation

[0048] FIG. 2 is a schematic diagram illustrating an exemplary system 200 for endpoint and network activity correlation. In particular, the system 200 shown in FIG. 2 is configured to receive inputs for endpoint events, correlate the events, and generate outputs such as, but not limited to, warnings and reports.

[0049] As shown in FIG. 2, the exemplary system 200 may include an endpoint event correlation module 240 configured to receive endpoint alerts 230 from an instrumented system 210 with a plurality of sensors configured to detect endpoint events related to one or more of application integrity 211, resource utilization 212, and system configuration 213. The system 200 also comprises a network activity correlation module 260 configured to receive network alerts 250 from a network activity sensor 220.

[0050] With continued reference to FIG. 2, the network activity correlation module 260 is further configured to produce network warnings 270 resulting from the network activity correlation and output the network warnings 270 to an orchestrator 290. The orchestrator 290 is configured to receive network warnings 270 from network activity correlation module 260 and endpoint warnings 280 from the endpoint event correlation module 240. According to embodiments depicted in FIG. 2, the received network warnings 270 and endpoint warnings 280 can be used by orchestrator 290 to coordinate manual or automated actions on infected systems.

[0051] With continued reference to FIG. 2, the orchestrator 290 can similarly receive warnings produced by one or more additional instrumented systems (see, e.g., VM #N) with respective pluralities of sensors and endpoint event correlation modules.

[0052] As shown in FIG. 2, the instrumented systems can include multiple virtual machines (VMs, i.e., VM 1 … VM #N) with respective pluralities of sensors configured to detect endpoint events related to one or more of application integrity 211, resource utilization 212, and system configuration 213.

[0053] FIG. 3A is a flowchart illustrating steps by which early warning and response automation is performed using monitoring, orchestration and remediation, in accordance with an exemplary method.

[0054] As shown in FIG. 3A, an exemplary method 300 comprises receiving communications from an early warning system 301 configured to continuously monitor the runtime integrity of systems. This continuous monitoring enables near-real time determinations and detections of deviated, vulnerable, in duress, and compromised systems 307.

[0055] The method 300 can operate in conjunction with legacy security technologies 305 to fill in the security holes or gaps inherent in traditional security solutions. As illustrated in FIG. 3A, such legacy security technologies 305 can include anti-virus software, network firewalls, and intrusion detection/prevention systems (IDS/IPS). Unlike the early warning system 301 and the automated and rapid response 303, the legacy security technologies 305 are limited to using signatures, detecting protocol anomalies or virtual execution in a sandbox to monitor threats and attacks. As shown in FIG. 3A once a target of an attack or threat (i.e., a 'target system' or vulnerable system 307) becomes infected or compromised, these technologies 305 can be ineffective in protecting the compromised/infected systems 307 and preventing data breaches or service disruptions.

[0056] Example limitations of legacy security technologies 305 are shown in FIG. 3A. For example, as depicted in FIG. 3A, a traditional network firewall technology 305 using access control lists (ACLs) cannot reliably block every threat. This is because firewalls are typically limited to monitoring well-known, default open ports used as listening ports for web protocols such as the Transmission Control Protocol/Internet Protocol (TCP/IP), email protocols such as the Simple Mail Transfer Protocol (SMTP) and the Post Office Protocol (POP), and other protocols such as the File Transfer Protocol (FTP), the Secret File Transfer Protocol (SSH), Secure FTP (SFTP), telnet, and the Remote Desktop Protocol (RDP). IDS and IDP technologies using rulesets cannot detect every zero-day signature/anomaly attack and have issues with regarding false negatives and leaving platforms/systems

vulnerable to backdoor attacks. Similarly, anti-virus software cannot detect zero-day, mutant, and low-and-slow infections.

[0057] The method 300 can also supplement security audit scans 308 and manual IT process that may be in place. For example, an organization may periodically run security audit scans (i.e., on a weekly or bi-weekly basis). Such security audit scans may be National Institute of Standards and Technology (NIST)/Security Content Automation Protocol (SCAP) compliant checks for common vulnerability exposures to identify deviated and vulnerable systems 307. The results from these scans may be used as part of manual IT processes for ticketing (i.e., creating 'trouble tickets' for deviated/vulnerable systems 307) and security/compliance review boards. However, as shown in FIG. 3A these manual processes triggered by merely periodic scans can takes days or weeks to react to threats, thus leaving target systems open to a long window of exposure.

[0058] The method 300 improves upon the legacy technologies 305, periodic audit scans 308, and manual IT processes 309 and makes up for their above-noted shortcomings by carrying out an automated and rapid response 303 for orchestration and remediation of infected systems 307. In an embodiment, automated and rapid response 303 can be performed by monitoring and orchestration systems (not shown). In the example of FIG. 3, a protocol 302 is used for data exchange between the early warning system 301 and monitoring and orchestration systems.

[0059] In an embodiment, the early warning system 301 monitors instrumented systems to measure and evaluate runtime operational integrity to determine whether a system 307 has deviated, become vulnerable, is in duress or has been compromised. Once this determination has been made, the system 307 is marked by the early warning system 301 as one or more of a deviated system, a vulnerable system, an in duress system, or a compromised/infected system. The early warning system 301 can then issue warnings regarding the system 307 via the protocol 302 so that an automated and rapid response 303 can be carried out by monitoring and orchestration systems.

[0060] FIG. 3B is a schematic diagram illustrating an exemplary method 310 for determining a calculus of risk, in accordance with exemplary embodiments.

[0061] Referring to FIG. 3B, the exemplary method 310 may include determining or performing a calculus of risk 320 for the data center application and data silos, that receives sensory inputs 314 from instrumentation 313 including integrity measurement and verification scan correlation 315, network activity correlation 316 and endpoint event correlation 317, and may generate integrity metrics for security orchestration 321, and may dispatch directives to an edge device 323 (for example, network firewall) for user access controls 322, to a load balancer 325 for session controls 324, or to a network fabric element 327 (for example, a switch or router) for flow controls 326.

[0062] With continued reference to FIG. 3B, the security orchestration 321 may include user access controls 322 as a remediation or mitigation means to block the infected device or malicious user from accessing protected data center centers, session controls 324 to divert users from infected systems or infected devices from protected systems, flow controls 326 to quarantine infected systems, divert traffic away from protected systems, or redirect traffic from attackers to pure, high-interaction or low-interaction honeypots.

[0063] FIG. 4 illustrates data flows used to configure an attestation system. In particular, FIG. 4 depicts a data flow for consolidating and normalizing network endpoint assessments as part of a configuration for an exemplary attestation system 400.

[0064] Referring to FIG. 4, the exemplary attestation system 400 includes a trust orchestrator 430, a trust broker 407 configured to receive integrity reports 406 published by endpoint assessment services 401.

Trust Broker and Integrity Report

[0065] With continued reference to FIG. 4, the trust broker 407 can be configured to receive sensory data feeds that represent the configuration state of the system based on a remotely administered scan of a device, such as device 560 described with reference to FIG. 5 below, by endpoint assessment services 401. These scans provide a snapshot in time of the state of the system and are agnostic to runtime aspects of the system including applications thereon.

[0066] In an embodiment, the sensory data is represented in a markup language such as, but not limited to, Extensible Markup Language (XML). An integrity report 406 incudes this sensory data. In embodiments, the integrity report 406 is generated by third party endpoint assessment services at platform- and application-level granularities. According to embodiments, the integrity report 406 may be received by the trust broker 407 either: (a) programmatically through outbound application programming interfaces (APIs) provided by respective application vendors; or (b) manually through importing the integrity report 406 as a file provided by an administrator through a dashboard of an administrative console user interface (UI) in a specified file format. Examples of an administrative console UI are discussed below with reference to FIGs. 14-18.

[0067] The trust broker 407 can also be configured to parse, normalize and collate received integrity reports 406. In accordance with embodiments, the parsing, normalizing, and/or collating can be based on one or more object identifiers. Exemplary object identifiers can include, but are not limited to, machine hostnames, IP addresses, application names, and package names. This parsing, normalization, and collation (collectively, processing) generates temporal events 409 that annotate the state of the endpoints (devices) at scan time. Additional embodiments of the trust broker are described with reference to FIGs. 5, 9, and 11 below.

Temporal Events

[0068] According to embodiments, the temporal events 409 can be expressed as assertions about operational parameters (e.g., vulnerabilities, compliance, patch level, etc.) based on enterprise policies established for a baseline configuration. The trust broker 407 serves as a moderator that aggregates endpoint operational state measurements for situation awareness and threat identification by the trust orchestrator 430.

[0069] With continued reference to FIG. 4, the temporal events 409 can be an annotation (e.g., an XML representation) of the configuration state of the system (including device, application and package) and include trust and severity scores as generated by third party security vendors based on integrity measurement and verification, in accordance with standards established by organizations. These

organizations can include NIST, the MITRE Corporation, and the United States Computer Emergency Readiness Team (US-CERT). The temporal events can be assertions about operational parameters expressed in the Open Vulnerability and Assessment Language (OVAL) to convey system details representing configuration information and a system/machine state including vulnerability, configuration, patch level, etc. Alternatively, the system details can be conveyed using the SCAP protocol. According to embodiments, the state representation includes schema attributes to measure configuration, vulnerability (exposures), compliance, and patch level based on severity. Compliance can be expressed in terms of the Extensible Configuration Checklist Description Format (XCCDF) using XCCDF checklists for devices attached to a system's Peripheral Component Interconnect (PCI) bus, and data security/system integrity compliance with the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), and/or the Gramm–Leach–Bliley Act (GLBA).

[0070] As shown in FIG. 4, the integrity reports 406 can be generated by performing one or more scans, including, but not limited to, a vulnerability scan 402, a configuration scan 403, a compliance scan 404, and a patch scan 405 of networked endpoints. In an embodiment, the trust broker 407 can be implemented as the Trust-as-a-Service (TaaS) Broker from TAASERA, Inc. In one exemplary embodiment, the trust orchestrator 430 can be implemented as the TaaS Orchestrator from TAASERA, Inc.

[0071] With continued reference to FIG. 4, the attestation system 400 further comprises a normalizer and collator 408 and a system event correlator 410 configured to receive temporal events 409 associated with an endpoint and use a risk correlation matrix 411 to correlate and generate an integrity profile 420 for an endpoint. According to embodiments, the system event correlator 410 shown in FIG. 4 can be configured to receive temporal events 409 generated by the trust broker 407 that measure the integrity of the system at last scan. Additional exemplary features of the system event correlator 410 are described below with reference to FIG. 5.

Integrity Profile

[0072] In the embodiments of FIGs. 4-6, the integrity profile 420 represents an aggregation of system warnings (threats such as malware) identified based on the received temporal 409 and endpoint 520 events. In one embodiment, the format (schema) of the integrity profile 420 is a standard Extensible Markup Language (XML) notation.

Risk Correlation Matrix

[0073] In embodiments, the risk correlation matrix 411 depicted in FIGs 4-6 and the risk correlation matrix 721 described with reference to 7A-7C are embodied as grids that represent an exemplary dynamic model of measurement and identification based on clustering and classification of independent endpoint events (alerts) to generate system warnings that may be mapped to warning categories or classes. Additional details of the risk correlation matrices 411 and 721 are provided below with reference to FIGs. 6, 7B, and 7C.

System for Evaluating Operational Integrity of Applications

[0074] FIG. 5 illustrates communications between components of a system 500 for measuring and evaluating application operational integrity. In particular, FIG. 5 depicts communications between components of the application operational integrity system 500 used to evaluate application integrity based upon executable image profiles and process monitoring, and evaluate resource utilization based upon process and system monitoring. In embodiments, image profiles are generated for executable images such as, but not limited to, binary images, intermediate images, or scripts. FIG. 5 is described with continued reference to the embodiment illustrated in FIG. 4. However, FIG. 5 is not limited to that embodiment.

[0075] As shown in FIG. 5, the exemplary application operational integrity system 500 includes an endpoint trust agent 510 on a device 560 comprising a process monitor 514 configured to observe local execution context of applications and services. The endpoint trust agent 510 further comprises a socket monitor 513 configured to observe network activities of applications and services and a system monitor 512 configured to observe system and platform resources consumed by applications and services. In the example embodiment provided in FIG. 5, the trust

agent 510 also comprises an application integrity module 516 and a resource utilization module 515 configured to assess operational integrity based on rulesets. The trust agent 510 can also comprise native machine instrumentation 511 for a computing device being monitored by the application operational integrity system 500.

Device

[0076] In embodiments, the device 560 depicted in FIG. 5 may be a desktop, server, laptop, a mobile computing device such as a smart phone or tablet, or other types of mobile computing platforms that comprise (a) an operating system (OS); (b) a user operating the device to access a service or another device 560 over a network; and (c) application packages, applications or application components that may be downloaded and installed either with or without user intervention for later execution. Non-limiting examples of the device 560 include a personal computer, server, laptop, or tablet device running a MICROSOFT™ WINDOWS® operating system (OS), a personal computer, server, or laptop running an OSX OS from Apple Inc., a personal computer, server, or laptop running a UNIX or Linux OS, a personal digital assistant (PDA), an iPhone™, an iPod™ touch, or iPad™ tablet device running an iOS from Apple Inc., a device operating the Android OS from Google Inc., device running the MICROSOFT™ WINDOWS® Mobile or Phone OS, a device running a Symbian OS, a device running a PALM OS®, a BLACKBERRY® device running a Blackberry OS from Research In Motion ("RIM"), a mobile phone, a portable game device, a gaming console, a hand held computer, a netbook computer, a palmtop computer, an ultra-mobile PC, or another similar type of computing device capable of processing instructions and receiving and transmitting data to and from users and other computing devices.

Native Machine Instrumentation

[0077] In embodiments, the native machine instrumentation 511 can represent any event subscription, callback, notification mechanism provided by the supported operating system (OS) on the device 560 (e.g., MICROSOFT™ WINDOWS® Machine Instrumentation (WMI), Transport Filter Drivers, Application Layer Enforcement Callout Drivers, Linux/Unix Network Filter Drivers, etc.). The native

machine instrumentation 511 can generate raw events, as described below with reference to the illustrative example in FIG. 7A, that may appear insignificant as an isolated occurrence, but may include notable data points as forensic evidence of behavior anomalies or malicious activity to the event and risk correlation system.

[0078] Referring to FIG. 5, the trust broker 407 can be configured to receive one or more state attributes pertaining to applications running on a device 560 and components from the endpoint trust agent 510. The trust broker 407 serves as an arbitrator configured to dispatch a request for image analysis to one or more third party malware analyzers 540. In one embodiment, the dispatch mechanism uses trigger filter expressions that specify the set of criteria that warrant initiation of image analysis (e.g., frequency and volume of requests for analysis associated with the image across deployed endpoint trust agents), and parameters configured for each available connector to a third party malware analyzer 540. According to an embodiment, the parameters include cost, latency, and platform specific analysis capabilities. Such platform specific analysis capabilities can include static and dynamic analysis of applications on mobile platforms such as, but not limited to, devices 560 running an Android operating system (OS) from Google Inc., a PALM OS®, a MICROSOFT™ WINDOWS® Mobile or Phone OS, a Symbian OS, a Blackberry OS from Research In Motion (i.e., a BLACKBERRY® device 560), or an iOS (i.e., iPhone™, an iPod™ touch, or iPad™ devices 560).

[0079] The third party malware analyzers 540 perform static and dynamic analysis of the application images based on policies specified by the trust broker. The result of the malware analysis is a set of threats identified based on the analysis. The trust broker caches the results of the analysis indexed by a unique identifier for the image. The trust broker generates and returns an image profile 519 to the endpoint trust agent 510 which comprises assertions of malicious capabilities of the image that must be monitored at runtime for subsequent generation of endpoint events 520 by the endpoint trust agent 510.

Endpoint Events

[0080] In the embodiment shown in FIG. 5, the endpoint events 520 are generated by a component of the endpoint trust agent 510, and represent alerts based an

endpoint sensor resident on the device 560. The alerts are mapped to a cell in the risk correlation matrix 411 grid by the system event correlator 410. In one embodiment, the format (schema) of the endpoint events 520 is a standard Extensible Markup Language (XML) notation. Additional features of the endpoint events 520 are described below with reference to FIG. 6

[0081] With continued reference to FIG. 5, the application operational integrity system 500 can include a trust orchestrator 430 comprising a system event correlator 410 and a trust broker 407. The application operational integrity system 500 can further include a malware analyzer 540. In an embodiment, the trust orchestrator 430 can be implemented as the TaaS Orchestrator from TAASERA, Inc.

[0082] According to the exemplary embodiment depicted in FIG. 5, the system event correlator 410 can be configured to receive endpoint events 520 from the endpoint trust agent 510 as sensory inputs to a calculus of risk. The trust broker 407 is configured to receive an image file and image attributes 518 and then send the received image file to the malware analyzer 540 for diagnosis. The trust broker can also receive an asynchronous prognosis 533 and forward an asynchronous image profile 519 to the process monitor 514 to include in ruleset processing for diagnosis at the application integrity module 516.

System Event Correlator

[0083] According to embodiments, the system event correlator 410 shown in FIG. 5 can be configured to receive temporal events 409 generated by the trust broker 407 that measure the integrity of the system at last scan, and endpoint events 520 from the endpoint trust agent 510 that measure the runtime execution state of applications. The system event correlator 410 can be further configured to map the events to a cell in the risk correlation matrix 411 grid and processes the triggered system warnings to evaluate threats by category (or vectors). In one embodiment, the categories include at least resource utilization, system configuration, and application integrity. Each category is assigned a metric that is an indicator of the level of runtime operational integrity that may be asserted based on the system warnings and threat classification produced by the risk correlation matrix 411. The system event correlator 410 can also be configured to generate an integrity profile

420 for the device 560 that describes the security risks and threats posed by the measured execution state of running applications on the device 560.

[0084] FIG. 6 depicts data flows between components of an exemplary system for correlating endpoint events. In particular, FIG. 6 illustrates data flows between components and modules of a system event correlation system 600. FIG. 6 is described with continued reference to the embodiments illustrated in FIGs. 4 and 5. However, FIG. 6 is not limited to those embodiments.

[0085] Referring to FIG. 6, the exemplary correlation system 600 includes an endpoint trust agent 510 on a device 560 that comprises runtime monitor 620 configured to register for and receive a plurality of raw events 611 from native machine instrumentation 511 on the device 560. The runtime monitor 620 is further configured to raise integrity events 621 to an integrity processor 630 that may apply rulesets 631 to generate integrity alerts 632 and generate or populate an event correlation matrix 633 that maps integrity warnings 634 to endpoint events 520 for dispatch to a trust orchestrator 430.

[0086] In the embodiments shown in FIGs. 6 and 7A-7C, the endpoint events 520 are generated by the integrity processor 630, which is a component of the endpoint trust agent 510, and represent alerts based an endpoint sensor resident on the device 560. As described above with reference to FIG. 5, the alerts can then be mapped to a cell in the risk correlation matrix 411 grid by the system event correlator 410, which can be configured to read endpoint events 520 expressed in XML notation.

[0087] With continued reference to the exemplary embodiment provided in FIG. 6, the trust orchestrator 430 comprises a system event correlator 410 configured to use a risk correlation matrix 411 to generate an integrity profile 420 for the monitored system (i.e., the target system). In one embodiment, the system event correlator 410 can be implemented as a correlation engine. In another embodiment, the trust orchestrator 430 can be implemented as the TaaS Orchestrator from TAASERA, Inc.

[0088] For the risk correlation matrix 411 shown in FIG. 6, each cell in the grid is a set of alerts triggered through an event correlation matrix 633 and rulesets 631 (rule expressions) by the endpoint trust agent 510.

[0089] In certain exemplary embodiments, the application integrity module 516 and the resource utilization module 515 described above with reference to FIG. 5 may be included as a subcomponent or module of the integrity processor 630 depicted in FIG. 6.

[0090] In certain exemplary embodiments, the process monitor 514, system monitor 512 and socket monitor 513 depicted in FIG. 5 and described above may be included as subcomponents or modules of the runtime monitor 620.

[0091] FIG. 7A is a diagram indicating groupings of exemplary endpoint events 700 that can be monitored and analyzed by the presently disclosed methods and systems to determine a system integrity profile. In particular, the endpoint events 700 shown in FIG. 7A can be used to determine what an attestation system can assert about the integrity of a monitored system (i.e., a target system). FIG. 7A is described with continued reference to the embodiments illustrated in FIGs. 1, 4, 5, and 6. However, FIG. 7A is not limited to those embodiments.

[0092] By continuously monitoring for the endpoint events 700 and performing dynamic analysis of detected endpoint events 700, assertions about the integrity of a target system can be made. For example, the endpoint events 700 can be included in the endpoint events 116, 118 received by the event and behavior correlation engine 130 in the network 100 described above with reference to FIG. 1.

[0093] In one embodiment, one or more of the endpoint events 700 can be included in the endpoint events 520 used by the attestation system 500, described above with reference to FIG. 5. In other embodiments, the endpoint events 700 can be included in the endpoint events 520 used by the system event correlator 410 of the correlation system 600 depicted in FIG. 6.

[0094] Referring to FIG. 7A, the exemplary endpoint events 700 may include per process events 701, per processor events 702, system events 703, and per image binary analysis events 704. According to an embodiment, the events 701-704 can include, but are not limited to, all events available through native machine instrumentation and extensible on the platform with provider plug-ins.

[0095] FIG. 7B is a block diagram 710 illustrating exemplary alerts that can be generated by the methods and systems discussed herein.

[0096] As shown in FIG. 7B, in embodiments, alerts may include platform alerts 711, per image alerts 712, grayware alerts 713 (i.e., for a watch list), and per application alerts 714. The alerts are configurable and extensible, and not limited to the alerts illustrated in FIG. 7B.

[0097] FIG. 7C is a block diagram illustrating an exemplary method 720 for correlating endpoint alerts and generating endpoint warnings using a correlation matrix. FIG. 7C is described with continued reference to the embodiments illustrated in FIGs. 4-6. However, FIG. 7C is not limited to those embodiments.

[0098] Referring to FIG. 7C, the method 720 populates a risk correlation matrix 721 based upon one or more of system warning classes 722, system warnings 723, and integrity warnings 724. As shown in FIG. 7C, an alert expression can be expressed as a function 725 of at least an attribute, an attribute value constraint, a sample rate, a recurrence, a score and a weight. The function may be specified in any programming language or construct, as compiled, intermediate or interpreted code.

[0099] The risk correlation matrix 721 can comprise a universally unique identifier (UUID) for the system, system warnings 723 mapped to at least one system warning class 722, and at least a system warning class 722 to diagnose system deviations (i.e., system deviated integrity warnings 724), system duress, system vulnerable and system infections (i.e., system infected integrity warnings 724).

[0100] In the embodiment of FIG. 7C, each alert for the risk correlation matrix 721 is generated by a program function 725 that evaluates expressions that are specific for each attribute of the device 560. Based on the occurrence of a qualifying set of alerts in each cell, the corresponding system warning is triggered. In FIG. 7C, the exemplary risk correlation matrix 721 illustrates that for each device 560 (or application) uniquely identified by a machine identifier (e.g., a virtual machine universally unique identifier (UUID), IP address) or application instance identifier (application UUID), a different set of alerts may trigger different system warnings that map to a common system warning class. By mapping alerts to a behavior model (or cluster), unknown (such as emerging or polymorphic) threats may be classified and identified without requiring image or wire level signatures. The alerts may be grouped as illustrated in FIG. 7B to represent a category of alerts (e.g., platform,

application, grayware - that includes applications that are placed on a watch list based on reports generated by third party malware analyzers, image – that are weighted by threat level based on inspections performed by the endpoint trust agent 510 or malware analyzers 540). In an embodiment, the program function 725 can be configured to use conditional expressions (operators) to generate an alert based on value constraints, sample rate for the measurement, recurrence of measured values, an assigned score and weight for the attribute. According to embodiments, the score and weight can be predefined or customizable through a graphical user interface GUI or dashboard, such as the GUIs described below with reference to FIGs. 14-18.

[0101] In accordance with embodiments, a plurality of timers may be associated in the evaluation of system warnings and system warning classes, the calculus of risk, and generation of an integrity profile for the system.

[0102] According to embodiments, the integrity profile 420 comprises at least the endpoint address and one or more of system warning class, forensic confidence of the declared warning, and the full evidence chain.

Integrity Processor

[0103] With reference to FIGs. 6 and 7A-7C, the integrity processor 630 is a functional component of the endpoint trust agent 510. The integrity processor 630 can be configured to receive integrity events 621 from the runtime monitor 620 that describes process, processor, system and binary analysis events illustrated in FIG. 7A. Applying qualifying rule expressions (illustrated in FIG. 7B) in the rulesets 631, integrity alerts 632 are generated and mapped to a cell in an event correlation matrix grid 633 (analogous to the risk correlation matrix 411 of FIG. 4 and grid 721 of FIG. 7C) to generate system level integrity warnings 634. The rows in the event correlation matrix 633 represent an application instance on the device 560 (analogous to rows in the risk correlation matrix 411 that represent a device by machine identifier). The integrity warnings 634 can be formatted as endpoint events 520 for dispatch to the system event correlator 410 of the trust orchestrator 430 for threat classification and identification and subsequent remediation.

[0104] In accordance with embodiments, a plurality of alerts 711-714 in a variety of user configurable combinations (for example, as editable settings in an XML or text

format configuration file, or through a graphical administrative dashboard or user interface) constitute a system warning, and a system warning maps to a system warning class.

[0105] In accordance with embodiments, a plurality of system warning classes can be included in the integrity profiles 420 of the attestation system 400 and correlation system 600 depicted in FIGs. 4 and 6 respectively.

Example Trust Orchestration Architecture

[0106] FIG. 8 is a block diagram of an exemplary architecture 800 for trust orchestration including a trust orchestrator 430, a network analyzer 830, and a device 560. The architecture 800 can be used to correlate a plurality of events for determining runtime operational integrity of a system. FIG. 8 is described with continued reference to the embodiments illustrated in FIGs. 4, 5, and 7C and with reference to FIGs. 12 and 13. However, FIG. 8 is not limited to those embodiments.

[0107] As shown in FIG. 8, the trust orchestration architecture 800 may include an endpoint trust agent 510 on a device 560, a network analyzer 830 that may include a network activity correlator 831, an endpoint assessment service 820, a service provider for orchestration and/or policy enforcement point services 860, and a trust orchestrator 430 that may include a trust broker 407, a system event correlator 410, a trust supervisor 846, and a remediation controller 848.

Trust Orchestrator

[0108] According to the embodiments of FIGs. 4 and 8, the trust orchestrator 430 is an aggregation that includes functional components such as the trust broker 407, system event correlator 410, the trust supervisor 846, and remediation controller 848. In embodiments, the trust orchestrator 430 is configured to receive sensory threat intelligence from network analyzers 830, endpoint assessment services 820 and endpoint trust agents 510 on devices 560. Through a sequence of normalization, collation and risk correlation of events, directives 849 in the form of directives are dispatched to orchestration services to initiate remediation actions to deal with identified threats on devices 560. The directives are specific to the orchestration service and can include the use of vendor APIs. Examples of such vendor APIs include VMWARE™ vCloud APIs, BMC Atrium™ APIs for accessing a

BMC Atrium™ configuration management database (CMDB) from BMC Software, Inc., Hewlett Packard Software Operations Orchestration (HP-OO) APIs, and standard protocols such as OpenFlow.

[0109] In certain exemplary embodiments, the system event correlator 410 receives endpoint events 520 from the endpoint trust agent 510, temporal events 409 from the trust broker 407, correlates and sends an integrity profile for a network endpoint to the trust supervisor 846 and the network activity correlator 831.

[0110] In certain exemplary embodiments, the trust supervisor 848 receives an infection profile 832 for a network endpoint from the network activity correlator 831, an integrity profile 420 for a network endpoint from the system event correlator 410, analyzes and classifies threats along with a forensic confidence score, sends real time actions 847 to the remediation controller 848, and real time status indications 850 to a dashboard controller 870. The remediation controller 848 sends directives 849 to orchestration and/or policy enforcement point services 860 for machine, flow or transaction level remediation.

Remediation Controller

[0111] In embodiments, the remediation controller 848 can be configured to receive action requests 847 from the trust supervisor 846. The remediation controller 848 can also be configured to process the received requests and perform appropriate operations on orchestration services. According to embodiments, upon processing a received action request the remediation controller 848 may perform (a) a flow level operation on a network element 1216 (e.g., a physical or virtual switch or a firewall) or wireless access point 1320; (b) a machine level operation on a device 560 (e.g., a web or database server); (c) a transaction level operation to restrict access to a service or device 560; and/or (d) an update notification to a network trust agent (see, e.g., network trust agents 1209 and 1315 depicted in FIGs. 12 and 13, respectively) to indicate a revised reputation score for a device 560.

[0112] In embodiments, the infection profile 832 comprises at least the victim endpoint address and one or more of a forensic confidence of the declared infection, the attacker source, the command and control source, the full evidence chain, and the infection time range (onset, duration).

[0113] According to embodiments, the integrity profile 420 comprises at least the endpoint address and one or more of system warning class, forensic confidence of the declared warning, and the full evidence chain.

[0114] In accordance with embodiments, the risk correlation matrices 411 and 721 of FIGs. 4 and 7C, respectively, may be included in the trust supervisor 846 to consolidate and correlate integrity profile 420 and infection profile 832 of FIG. 8.

Example Threat Detection and Mitigation Scenario

[0115] An exemplary flow of a threat detection and mitigation sequence is described below with reference to FIGs. 3A, 4-6, 7B, 8, 10, 12, 13, and 23. In the example scenario below, the exemplary threat is a user device infected with malware. The paragraphs below detail how exemplary embodiments described herein with reference to FIGs. 4-6, 7B, 8, 10, 12 and 13 can handle such 'real world' threat vectors. The multi-dimensional event and risk correlation model described in the following paragraphs illustrates an exemplary method of detecting low and slow signature-less threats that are characteristic of emerging malware and advanced persistent threats.

[0116] A user's (1014) device D (560) may become infected with a form of an advanced persistent threat (e.g., malware $M_{(benign)}$) while he device D is still connected to an enterprise network of an organization 2303. The connection of the device D to the enterprise network can occur through user activity, for example, when the user 1014 connects a plug-and-play portable universal serial bus (USB) device with the malware $M_{(benign)}$ to the device D while it is connected to the enterprise network, as the result of the user 1014 opening an email attachment infected with the malware $M_{(benign)}$, when the user 1014 accesses a social network application from the device D, or when the user 1014 unwittingly transfers a file with the malware $M_{(benign)}$ to device D while accessing a file sharing service.

[0117] The device D can also become infected with malware $M_{(benign)}$ while the device D is disconnected from the enterprise network of the organization 2303. For example, the device D can become infected as a result of user activity on a home network, or external wireless or wired network not managed by an enterprise IT administrator of the organization 2303, such as a mobile network or the Internet.

[0118] Once the device D is infected, an egg download (i.e., download of an .egg compressed archive file) that evaded traditional network edge protections (e.g., legacy security technologies 305 such as firewalls and network IPS/IDS systems) has occurred. At this stage of infection, legacy security technologies 305 such as traditional antivirus programs installed on the device D are unlikely to detect the targeted malware $M_{(benign)}$ because no signature or blacklist already exists for this threat. The malware $M_{(benign)}$ may then perform discrete (and apparently benign) surveillance operations on the device D, such as periodic process restarts, executable file property modifications (i.e., changes to file name and/or size attributes) to introduce entropy and evade detection. The malware $M_{(benign)}$ may also make registry modifications, perform keyboard/input device monitoring, screen level monitoring, memory dumps, disk navigation to inspect files without excessive resource (CPU) utilization on the device D.

[0119] At this post-infection stage, the endpoint trust agent 510 monitors the executing malware process $P_{(benign)}$, performs file and component (e.g., dynamic link library(DLL)) level integrity checks including checking a file hash digest, digital signature, and certificate chain verification by leveraging collaboration services, such as the collaboration services 1207 and 1312, described below with reference to FIGs. 12 and 13, respectively, to access intelligent whitelisting services. These collaboration services are accessed through the trust orchestrator 430. Failure of one or more of these checks immediately places process $P_{(benign)}$ on a grayware alert 713 (i.e., a watch list).

[0120] Assuming no checks fail at this stage, the process $P_{(benign)}$ is continuously monitored by the integrity processor 630 for explicit rule violations. In an embodiment, violations of a rule in a ruleset 631 are continuously monitored for and detected. These rules detect anomalous behaviors in benign processes. Once a rule trigger criteria is reached, the endpoint trust agent 410 initiates an image integrity check and leverages a remote malware analyzer 540 through the trust orchestrator 430. The purpose of this check is to avoid complete reliance on supply chain provenance and locally available evidence. The image profile 519 generated

from malware binary analysis provides the integrity processor additional local events to monitor for process $P_{(suspect)}$.

[0121] At this point, the malware analyzer 540 reports capabilities detected (present in reverse engineered code) through static and dynamic analysis of the image. Such image analysis can look for code obfuscation techniques in the reverse engineered code such as anti-debug, anti-trace, anti-memory, and anti-emulation, use of network communication protocols like SMTP, FTP or HTTP, use of embedded uniform resource locators (URLs) or IP addresses, use of encryption methods such as use of the secure sockets layer (SSL) protocol, listening on local ports, remote ports accessed, file system operations, registry operations, operations in temporary, system or non-program folders, memory peek or poke operations, and remote thread creation.

[0122] The integrity processor 630 then monitors process $P_{(suspect)}$ for related warnings 721 and triggers endpoint events such as alerts 711-714 to the system event correlator 410. Multiple endpoint assessment services 820 may be deployed in the enterprise network to perform scheduled policy based scans to detect known exposures (vulnerability, configuration, compliance and patch level exploits). The respective integrity reports 821 may contain indications of exposures on the device D. However, these reports do not affirm positive presence of a threat or an infection on the device D and may be unaware of the existence and runtime activities of process $P_{(suspect)}$. The trust broker 407 generates temporal events 409 that inform the system event correlator 410 of the damage potential (severity) on the device D should any malicious program be active on the device (e.g., a personally identifiable information (PII) violation on a database server, a buffer overflow attack on an application server, a structured query language (SQL) injection attack on a database server, a keystroke or screen element capture, a microphone or camera hijack, etc.) based on authoritative state (snapshot) information and scan policies applied in the assessment of device D.

[0123] Based on risk analysis triggered by endpoint and temporal events, an integrity profile is generated by the system event correlator 410 for the device D. The network activity correlator 831 concurrently monitors all network traffic and

activities of device D and dispatches infection profiles 832 based on forensic evidence of malicious network dialogs indicative of an infected victim (device D). The evidence may be indicative of malicious activities such as peer-to-peer propagation, command and control communications, or data exfiltration to an attacker. The trust supervisor 846 classifies the forensic evidence based on the integrity and infection profiles generated independently by the endpoint, network, and scan based assessment sensors to determine the threat risk level of the device D with high forensic confidence to warrant an immediate manual or automated remediation action to mitigate the detected infection.

System for Integrity Profile Generation

[0124] FIG. 9 is block diagram illustrating an exemplary system for generating a subject integrity profile. The system 900 shown in FIG. 9 can be used to consolidate and correlate a plurality of identity, inventory and log management systems in order to determine a reputation of a subject (e.g., a user, device, transaction, service, or organization/company). FIG. 9 is described with continued reference to the embodiments illustrated in FIGs. 4 and 5. However, FIG. 9 is not limited to those embodiments.

[0125] Referring to FIG. 9, the exemplary subject integrity profile system 900 includes a trust orchestrator 430, a trust broker 407 that can be configured to query and receive an associated response 905 from a plurality of management systems.

[0126] With continued reference to FIG. 9, the integrity profile system 900 can include a plurality of subsystems, including an inventory management system 901 configured to provide resource object attributes, a role management system 902 configured to provide subject (or user) attributes (e.g., roles and entitlements), an identity management system 903 configured to provide aggregated subject attributes, a log management system 904 configured to provide information and events categorized by subject, a system event correlator 410 that receives temporal events 409 categorized by subject, and a risk correlation matrix to generate an integrity profile 420 for a subject that comprises a unique subject identifier and a reputation score.

[0127] Within the context of the subject integrity profile system 900, the trust broker 407 is configured to query and receive responses from third party management systems regarding inventory, role, identity and logs.

Inventory Management System

[0128] The inventory management system 901 shown in FIG. 9 is configured to provide information pertinent to devices 560 (e.g., mobile devices 560, mobile applications, enterprise desktops, servers, etc.). Examples of inventory management systems 901 include commercial products available from the IBM and Oracle Corporations used for managing an inventory of Enterprise IT managed assets.

Role Management System

[0129] According to embodiments, the role management systems 902 shown in FIG. 9 can be configured to provide information pertinent to a user's organizational roles, resource level privileges, application level entitlements, and extended group memberships (i.e., project level privileges and roles). Examples of role management systems include commercial products available from Oracle, Computer Associates, IBM, and SAP for role based access controls to database objects, files, servers, directories/folders, web servers, applications, network domains/subdomains, printers, and other resources. In some of these systems, users are assigned one or more roles that aggregate a set of privileges and permissions. For example, roles in an Oracle or IBM relational database environment represent different tiers or levels of access to database objects. For example, a user account with a 'database administrator' (DBA) role may have privileges and permissions needed to delete (i.e., drop), create, and alter database objects such as tables, views, synonyms, stored procedures, triggers, user accounts, entire databases, and other roles. In contrast user accounts with lesser roles, such as a developer or user role may only be able to insert and update data in database tables and views and revise existing stored procedure and trigger code. Yet other roles may be restricted to 'read only' access to select records from database tables and views as needed to generate reports and run queries.

Identity Management System

[0130] In accordance with embodiments, the identity management systems 903 shown in FIG. 9 can be configured to provide information pertinent to a user's organizational domain accounts and group level memberships (e.g., MICROSOFT™ Active Directory, Oracle Internet Identity).

Log Management System

[0131] In embodiments, the log management systems 904 shown in FIG. 9 can be configured provide information pertinent to a user's activities at the endpoint device and at the network level of operations based on logs generated by endpoint and network elements and reported through standard system information and event management protocols (e.g., SYSLOG) and formats such as the WebTrends Enhanced Log file Format (WELF) or the Common Event Format (CEF) used for network security applications.

Systems for Determining Calculus of Risk and Subject Reputation Scores

[0132] FIG. 10 is a block diagram illustrating an exemplary system for determining a calculus of risk. FIG. 10 is described with continued reference to the embodiments illustrated in FIGs. 4, 5 and 8. However, FIG. 10 is not limited to those embodiments.

[0133] Referring to FIG. 10, the exemplary calculus of risk system 1000 includes a network endpoint assessment 1001 configured to generate a network security scan report 1025, an endpoint collator 1002 to parse a plurality of received reports for categorization by address or geo-location, a normalizer 1003 for report consolidation, an object collator 1004 for categorization by package and component, an integrity processor 630 on a device 560, for runtime system 1016, application 1015 and user 1014 context, an endpoint trust agent 510, a global object context generator 1005 for aggregation of context, an event processor 1006 for evaluation of context, a rules repository 1012 of object attributes configured to include at least constraints 1023, a sample rate 1022, a recurrence 1021, a score 1020 and a weight 1019 for integrity assessments, an event correlator 1007, an event correlation matrix 1013, a threat classifier 1008, a dashboard controller 1009, and a remediation controller 848.

Trust Supervisor

[0134] According to the exemplary embodiments of FIG. 8 and FIG. 10, the trust supervisor 846 can be configured to receive infection profiles 832 from the network analyzers 830 and integrity profiles 420 from the system event correlator 410. The trust supervisor 846 uses an event processor 1006, an event correlator 1007, a threat classifier 1008, an event correlation matrix 1013 and a rules repository 1012 to correlate events associated to a device 560 for the classification and identification of threats based on the forensic confidence of leading indicators.

[0135] In an embodiment, the network endpoint assessment 1001 comprises performing a security scan of network endpoints for vulnerability, configuration, compliance, and patch management and use the results of these scans to generate a security assessment report 1026. As shown in FIG. 10, an endpoint collator 1002 is configured to receive the generated security assessment report 1026. In embodiments depicted in FIG. 10, at this point, the endpoint collator 1002 can then sort the security assessment report 1026 by endpoint address and/or geo-location to produce categorized reports 1027.

[0136] A normalizer 1003 is configured to receive the categorized reports 1027 and then normalize the elements therein to produce normalized reports 1028.

[0137] An object collator 1004 is configured to receive the normalized reports 1028 and then sort the elements therein by object package and component to produce temporal events 1029 for the global object context generator 1005.

[0138] In certain exemplary embodiments, the global object context generator 1005 receives endpoint events 1018 that may include the local runtime object execution context from the integrity processor 630 on a device 1017, and temporal events 1029 that may include endpoint security context from the object collator 1004.

[0139] In exemplary embodiments, the event processor 1006 receives endpoint integrity profiles 420 from the global object context generator 1005, retrieves associated endpoint rules 1031 from the rules repository 1012, generates and sends endpoint alerts 1033 to the event correlator 1007.

[0140] According to exemplary embodiments, the event correlator 1007 receives endpoint events 1033 from the event correlator 1007, maps the alerts 1032 using the

event correlation matrix 1013, generates and sends endpoint warnings 1034 to the threat classifier 1008.

[0141] In accordance with exemplary embodiments, the threat classifier 1008 may categorize threats, send status indications 1024 to the dashboard controller 1009 for real time visibility of endpoint integrity, and send action requests 1025 to the remediation controller 848.

[0142] In certain exemplary embodiments, the endpoint collator 1002, normalizer 1003 and object collator 1004 may be included in the trust broker 407 as described above with reference to FIG. 4.

[0143] In certain exemplary embodiments, the global object context generator 1005 may be included in the system event correlator 410 described in FIG. 4.

[0144] In certain exemplary embodiments, the event processor 1006, event correlator 1007 and threat classifier 1008 may be included in the trust supervisor 846 as described in FIG. 8.

[0145] FIG. 11 is a block diagram illustrating an exemplary system for determining a subject reputation. FIG. 11 is described with continued reference to the embodiments illustrated in FIGs. 4, 5, 7C, and 8-10. However, FIG. 11 is not limited to those embodiments. For example, the system 1100 can be used to generate subject reputation scores based on a calculus of risk, such as the calculus of risk determined by system 1000 described above with reference to FIG. 10.

[0146] Referring to FIG. 11, the exemplary subject reputation system 1100 includes a user 1014 authenticated on a device 560 through an authentication process/ceremony 1115 with an authentication service 1103, a service provider 1104 configured to receive a service request, a managed application 1105 that may be the target service, a reputation broker 1106, a trust broker 407, a log management system 904, a role management system 902 and an identity management system 903.

[0147] Unless specifically stated differently, a user is interchangeably used herein to identify a human user, a software agent, or a group of users and/or software agents. Besides a human user who needs use devices 560 and the attestation systems described herein, a software application or agent sometimes needs to run

applications, access services or social networks, conduct online transactions, review, update, or analyze security data, and process events, alerts and warnings. Accordingly, unless specifically stated, the term "user" as used herein does not necessarily pertain to a human being.

[0148] With continued reference to FIG. 11, the exemplary subject reputation system 1100 also includes an inventory management system 901, a reputation processor 1110, a risk correlator 1111, a risk correlation matrix 1113, and a reputation score generator 1112.

[0149] In an embodiment, the reputation processor 1110 is a component of the system event correlator 410 configured to receive subject events 1123 from the trust broker 407 and includes user alerts 1124 that are analogous to integrity profiles 420 of a user 1101.

[0150] As shown in FIG. 11, the risk correlator 1111 can be configured to receive subject alerts 1124 such as alerts for a user 1014 or a device 560, and map the subject alerts 1124 to a cell in the risk correlation matrix 1113 grid analogous to the risk correlation matrix 721 in FIG. 7C. The subject warnings 1126 (i.e., user 1014 or device 560 warnings) triggered can then be processed by the reputation score generator 1112 to determine the user's 1014 reputation score 1125.

Subject Events

[0151] In embodiments, the subject events 1123 shown in FIG. 11 can be assertions about provisioned attributes, endpoint and network level activities associated with a subject, received as a response to a directed query from the respective management systems. The subject can be a user 1014, a device 560, a transaction, or an organization such as a company.

[0152] In certain exemplary embodiments, a device 560 sends a service request 1116 on behalf of a user 1014 to a service provider 1104 to access a managed application 1105. The service provider 1104 sends a reputation query 1117 to the reputation broker 1106, receives a reputation token 1118 that may include at least a reputation score for the user 1014 or device 560, and enforces a reputation-based access control 1119 to permit or deny the service request 1116 to access the managed application 1105.

[0153] Within the context of the subject reputation system 1100, the trust broker 407 is configured to process received subject attributes (e.g., entitlements, memberships of users 1014, roles for users 1014, activity information), to generate and dispatch subject events to the reputation processor 1110. The subject events represent assertions about the subject that may determine a level of security risk in a transaction (e.g., static and dynamic separation of duties, principle of least privilege, observed resource usage patterns, observed activities on the internal and external networks, etc.). In one embodiment, the queries 1121, 1130, 1122, 1128 issued by the trust broker 407 are preconfigured, but can be customized by the administrator from a graphical user interface (GUI) or dashboard, such as the exemplary GUI described below with reference to FIGs. 14-18. In embodiments, the management systems may include information systems hosted by social networking vendors such as FACEBOOK® operated by Facebook, Inc., Twitter operated by Twitter, Inc., and LinkedIn.

[0154] According to exemplary embodiments, the trust broker 407 receives a query 1120 for a reputation score for a subject (i.e., a user, device, transaction, service, or organization), sends a subject activity query 1121 to log management systems 904, sends a subject attribute query to role management systems 902 and identity management systems 903, sends a device attribute query to inventory management systems 1128, generates and sends subject events 1123 to the reputation processor 1110.

[0155] In the context of the subject reputation system 1100, the inventory management system 901 shown in FIG. 9 can be configured to provide information pertinent to subjects that are devices 560, including mobile devices 560, mobile applications, enterprise desktops, servers, etc.

[0156] With continued reference to FIG. 11, in an embodiment, associated device attributes include at least a device 560 geo-location, a device provisioned state, enabled/disabled device 560 functions, and an owner registration (i.e., a user 1014 registration or an organization registration).

[0157] In accordance with embodiments, the risk correlator 1111 is configured to receive subject alerts 1124, use the risk correlation matrix 1113 to map the subject

alerts 1124 to subject warnings 1126, and invoke the reputation score generator 1112 to establish a subject reputation score 1125, which can be included in the reputation token 1118 by the reputation broker 1106.

[0158] In the exemplary embodiment of FIG. 11, the subject alerts 1124 can be user 1014 alerts (i.e., user 1014 integrity profiles), device 560 alerts, or application alerts for an application executing on the device 560. In certain exemplary embodiments, the reputation processor 1110 may be included in the system event correlator 410 described in FIG. 4.

[0159] According to exemplary embodiments, the risk correlator 1111, the risk correlation matrix 1113 and the reputation score generator 1112, may be included in the trust supervisor 846 described in FIG. 8.

Systems for Providing Network Flow Remediation and Mobile Security

[0160] FIG. 12 is a block diagram illustrating an exemplary system for network flow remediation. FIG. 12 is described with continued reference to the embodiment illustrated in FIG. 5. However, FIG. 12 is not limited to that embodiment. The system 1200 can perform network flow remediation based on a calculus of risk.

[0161] Referring to FIG. 12, the exemplary network flow remediation system1200 may include an endpoint trust agent 1201 on a device 560 that may execute an application 1203, a trust orchestrator 1205, a plurality of collaboration services 1207 that may include malware analyzers, network endpoint assessment services, and reputation services, a network service 1230 that may include a network trust agent 1209 and an OpenFlow security framework 1211, an OpenFlow controller 1214, and an OpenFlow enabled network element 1216 (for example, a switch or router).

[0162] In certain exemplary embodiments, the endpoint trust agent 1201 sends a dynamic context 1204 that may include the local runtime execution context of an application 1203 to the trust orchestrator 1205 that may perform a calculus of risk on a global security context, that may include endpoint assessment reports 1206 received from collaboration services 1207, and sends a system warning 1208 (endpoint threat intelligence) as a subscription based reputation service to a network trust agent 1209 for network flow remediation.

[0163] In certain exemplary embodiments, the network trust agent 1209 sends messages 1210 to the OpenFlow security framework 1211 middleware to send directives 1213 to an OpenFlow controller 1214, or send directives 1212 to an OpenFlow controller 1214, to notify by means of a protocol 1215 an OpenFlow enabled network element 1216 to apply access controls 1217 to block or divert traffic flows.

[0164] FIG. 13 is a block diagram illustrating an exemplary system for providing mobile security. FIG. 13 is described with continued reference to the embodiments illustrated in FIGs. 4-6. However, FIG. 13 is not limited to those embodiments. System 1300 can provide mobile security by remediating mobile devices and wireless network flows based on a calculus of risk.

[0165] Referring to FIG. 13, the exemplary mobile security system1300 includes an endpoint trust agent 1301 on a mobile device 560 that may execute a mobile application 1303, a trust orchestrator 1310, a plurality of collaboration services 1312 that may include malware analyzers, network endpoint assessment services, and reputation services, a network service 1350 that may include a network trust agent 1315 and an network security framework 1318, a network element 1320 (for example, a switch or router), a wireless access point 1322, a mobile policy manager 1313 and a mobile device manager 1324.

Endpoint Trust Agent

[0166] Referring to FIGs. 5, 6 and 13, in an embodiment, the endpoint trust agent 510 resides on a device 560. The endpoint trust agent 510 can be configured to monitor all operations performed on the device 560 at runtime, including running applications and device functions (e.g., microphone, camera, keyboard, or display functions), and dispatches endpoint events 520 and security service requests 518 to the trust orchestrator 430. The runtime monitor 620, a functional component of the endpoint trust agent 510, includes a system monitor 512, a socket monitor 513, and a process monitor 514 that receive raw events 611 from native machine instrumentation 511 using a notification mechanism (e.g., MICROSOFT™ WINDOWS® Management Instrumentation (WMI) or the Android Application Manager). In certain exemplary embodiments, the endpoint trust agent 520 may

also receive and process messages from a mobile device manager 1324 or mobile policy manager 1313 to control device operations and/or settings. The endpoint trust agent 510 is risk and threat agnostic and merely generates events based on the evaluation of rulesets 631 and assessment of runtime behavior based on the threat correlation matrix 633. The assessment of risk, and classification and identification of threats can be delegated to the trust orchestrator 430.

[0167] In certain exemplary embodiments, the endpoint trust agent 1301 sends a dynamic context 1304 that may include the local runtime execution context of a mobile application 1303 to the trust orchestrator 1310 that may perform a calculus of risk on a global security context, that may include endpoint assessment reports 1311 received from collaboration services 1312, and sends threat intelligence as a subscription based reputation service 1314 to a network trust agent 1315 for network flow remediation.

[0168] In certain exemplary embodiments, the network trust agent 1315 sends messages 1316 to the network security framework 1318 middleware to send policies 1319 to a wireless access point 1320, or send policies 1317 to a wireless access point 1320, to apply access controls 1321 to block or divert traffic flows.

[0169] In certain exemplary embodiments, the trust orchestrator 1310 sends messages 1307 to the mobile policy manager 1313 to send directives 1308 to the mobile device manager 1324 to set feature controls 1306 on the mobile device 560 or send directives 1305 to the endpoint trust agent 1301 for the integrity processor 630 and runtime monitor 620 of FIG. 6.

[0170] In certain exemplary embodiments, the trust orchestrator 1310 is configured to send messages 1309 to the mobile device manager 1324 to set feature controls 1306 on the mobile device 560.

Example User Interface Dashboards for an Administration Console

[0171] FIGs. 14-18 illustrate exemplary graphical user interfaces (GUIs) according to embodiments of the present disclosure. The GUIs depicted in FIGs. 14-18 are described with reference to the embodiments of FIGs. 1-13. However, the GUIs are not limited to those example embodiments. FIGS. 14-18 illustrate an exemplary data center administration console interface comprising various dashboards for displaying

data related to operational integrity, resource utilization, application integrity, and network activity, in accordance with embodiments of the invention.

[0172] The terms "console display," "display," "display screen," and "screen" are used interchangeably herein to refer broadly and inclusively to any type of display device or screen coupled to or integrated with a computing device for displaying content viewable by a user of the computing device, such as administrators for the systems describe herein or a user 1014 of a device 560. In an embodiment, the device 560 is a mobile computing device 560. Such a display screen can include, for example and without limitation, a touch-screen liquid crystal display (LCD). In embodiments of the invention, the GUIs of a mobile device 560 is viewed on a display. In other embodiments, the GUIs shown in FIGs. 14-18 are viewed on a display of a server (i.e., a server console), a desktop computer (i.e., a PC monitor), or a laptop display.

[0173] In the example GUIs shown in FIGs. 14-18, the console interface and dashboards are rendered in a dedicated, native interface. In alternative embodiments, the console interface can be web based and rendered within a web browser. In other embodiments, the console interface and dashboards illustrated in FIGs. 14-18 can be displayed on server or workstation displays having a touch sensitive (i.e., touch screen) display. For ease of explanation, the operation of the console interface is discussed in the context of a computing device platform with an input device such as a mouse or pointing device (including a touch-screen), but is not intended to be limited thereto. Examples of such computing device platforms include, but are not limited to, OSX server and workstation operating systems (OSs) from Apple, Inc.; WINDOWS® server and workstation OSs from the MICROSOFT™ Corporation; UNIX-based OSs, and Linux OSs, such as, but not limited to, Linux from RedHat™ Inc.

[0174] In alternative embodiments, the GUIs of FIGs. 14-18 can be rendered on a display of a mobile computing device such as, but not limited to a personal digital assistant (PDA), an iPhone™, an iPod™ touch, or iPad™ tablet device, a device operating the Android operating system (OS) from Google Inc., a device running a MICROSOFT™ WINDOWS® Mobile or Phone OS, a device running a Symbian OS,

a device running a PALM OS®, a BLACKBERRY® device running a Blackberry OS from Research In Motion ("RIM"), a smart phone, a hand held computer, a netbook computer, a palmtop computer, a laptop computer, an ultra-mobile PC, or another similar type of mobile device capable of processing instructions and receiving and transmitting data to and from users and other computing devices.

[0175] It is to be understood that the console interface and dashboards illustrated in the exemplary embodiments of FIGs. 14-18 can be readily adapted to execute on a display of mobile device platforms and operating systems, a computer terminal, a display of a client device, a display console of a server, a display console of a monitoring device, a display of a target or subject device, or other display of a computing device. Thus, the exemplary GUIs illustrated in FIGs. 14-18 can be rendered on a display of a mobile device using an attestation application, within a web browser session, on a display console of an attestation server, or on a display of a client device running an attestation application.

[0176] Throughout FIGs. 14-18, displays are shown with various icons, folders, panes, command regions, interfaces, windows, tabs, tiles, data entry fields, drop down menus, and buttons that are used to initiate action, invoke routines, monitor and display data related to operational integrity of, monitor resource utilization, or invoke other functionality. The initiated actions include, but are not limited to, viewing events, editing events, inputting calendar preferences, a backward scroll, a forward scroll, and other calendar view navigation inputs and gestures. For brevity, only the differences occurring within the figures, as compared to previous or subsequent ones of the figures, are described below.

[0177] In an embodiment, the display used to display the GUIs and dashboards shown in FIGs. 14-18 may be a computer display 2630 shown in FIG. 26, and the console interface may be display interface 2602. According to embodiments of the present invention, a user can interact with the console interface and dashboards using input devices such as, but not limited to, a touch screen, a pointing device, a stylus, a track ball, a touch pad, a mouse, a keyboard, a keypad, a joy stick, a voice activated control system, or other input devices used to provide interaction between a user and a GUI.

[0178] FIG. 14 depicts an exemplary GUI for a data center administration console 1400 including an operational integrity dashboard 1450.

[0179] Referring to FIG. 14, the exemplary data center administration console 1400 may visually display as a single pane an operational integrity dashboard or display window 1450 to provide a 'global view' of the data center inventory 1401 (i.e., a 'global view dashboard'). The display window 1450 can include information fields including the global view of the data center inventory 1401 in a hierarchical tree view of resources, a component level view of a resource 1402, a resource name 1403, a resource platform type 1404, integrity metrics for a plurality of trust vectors that include at least the system configuration 1405, resource utilization 1406, application integrity 1407, network activity 1408, a remediation action 1409, a remediation control 1410 that may include at least a restore, quarantine and divert users function, an action summary 1413, a details pane 1411, a status pane 1412, and color coded runtime integrity indicators 1440. The console 1400 can also graphically display risk indicators as integrity indicators 1440 and indications of impact analysis based on a confidence level of received integrity metrics for the trust vectors.

[0180] The information fields may be displayed and/or updated in real time or near real time. The color coded runtime integrity indicators 1440 for each displayed trust vector 1405, 1406, 1407 and 1408 may be animated and include audio-visual effects. For example, the integrity indicators 1440 can be animated with location changes, color changes, size changes, cross-fading, blinking, beeping, or vibration (i.e., when displayed on a mobile client device). In embodiments, some or all of the integrity indicators 1440 may be hyperlinked graphics with links to detailed dialog boxes, expanded views, or reports for a drill-down or detailed view of the corresponding trust vector.

[0181] Although the integrity dashboard 1450 is shown with specific information fields and labels in a particular arrangement, it is contemplated that other information fields and arrangements are possible. For example, additional trust vectors or a custom filter based perspective view may be displayed, or the dashboard may be embedded as a plug-in control and streamlined in a third party management console.

[0182] FIG. 15 depicts an exemplary GUI for a runtime operational integrity monitoring console 1500 including a system configuration dashboard 1550.

[0183] Referring to FIG. 15, the exemplary runtime operational integrity monitoring console 1500 may visually display a system configuration dashboard or display window 1550 in a single pane. The display window 1550 may include information fields including a severity 1501, a warning or observed activity 1502, a timestamp 1503, an evaluation status 1504, a recommended action 1505, advanced details 1506 that may include a timestamp corresponding to the displayed threat details pane 1507, source location, threat identifier and victim identifier, threat details pane 1507, and machine history 1508 that may pertain to infection history.

[0184] The threat details pane 1507 may include a forensic evidence chain, a plurality of detected events that led to the infection diagnosis and threat identification.

[0185] Although the system configuration dashboard 1550 is shown with specific information fields and labels in a particular arrangement, it is contemplated that other information fields and arrangements are possible.

[0186] FIG. 16 depicts an exemplary GUI for a runtime operational integrity monitoring console 1600 including a resource utilization dashboard 1650.

[0187] Referring to FIG. 16, the exemplary runtime operational integrity monitoring console 1600 may visually display a resource utilization dashboard or display window 1650. The display window 1650 may include information fields including a severity 1601, a warning or observed activity 1602, a timestamp 1603, an evaluation status 1604, a recommended action 1605, advanced details 1606 that may include a timestamp corresponding to the displayed threat details pane 1607, source location, threat (or malware) identifier and victim identifier, threat details pane 1607, and machine history 1608 that may pertain to infection history.

[0188] The threat details pane 1607 may include a forensic evidence chain, a plurality of detected events that led to the infection diagnosis and threat identification.

[0189] Although the resource utilization dashboard 1650 is shown with specific information fields and labels in a particular arrangement, it is contemplated that other information fields and arrangements are possible.

[0190] FIG. 17 depicts an exemplary GUI for a runtime operational integrity monitoring console 1700 including an application integrity dashboard 1750.

[0191] Referring to FIG. 17, the exemplary runtime operational integrity monitoring console 1700 may visually display an application integrity dashboard or display window 1750. The display window 1750 may include information fields including a severity 1701, a warning or observed activity 1702, a timestamp 1703, an evaluation status 1704, a recommended action 1705, advanced details 1706 that may include a timestamp corresponding to the displayed threat details pane 1707, source location, threat (or malware) identifier and victim identifier, threat details pane 1707, and machine history 1708 that may pertain to infection history.

[0192] The threat details pane 1707 may include a forensic evidence chain, a plurality of detected events that led to the infection diagnosis and threat identification.

[0193] Although the application integrity dashboard 1750 is shown with specific information fields and labels in a particular arrangement, it is contemplated that other information fields and arrangements are possible.

[0194] FIG. 18 depicts an exemplary GUI for runtime operational integrity monitoring console 1800 including a network activity dashboard 1850.

[0195] As shown in FIG. 18, an exemplary runtime operational integrity-monitoring console 1800 may visually display a network activity dashboard or display window 1850. The display window 1850 may include information fields including a severity 1801, a warning or observed activity 1802, a timestamp 1803, an evaluation status 1804, a recommended action 1805, advanced details 1806 that may include a timestamp corresponding to the displayed threat details pane 1807, source location, threat (or malware) identifier and victim identifier, threat details pane 1807, and machine history 1808 that may pertain to infection history.

[0196] The threat details pane 1807 may include a forensic evidence chain, a plurality of detected events that led to the infection diagnosis and threat identification.

[0197] Although the network activity dashboard 1850 is shown with specific information fields and labels in a particular arrangement, it is contemplated that other information fields and arrangements are possible.

Methods for Threat Identification and Remediation and Subject Reputation

[0198] FIGs. 19-22 are flowcharts illustrating exemplary methods for threat identification and remediation, providing a subject reputation service, and providing network flow level remediation.

[0199] The flowcharts depicted in FIGs. 19-22 are described with reference to the embodiments of FIGs. 1-8 and 11. However, the methods 1900-2200 shown in FIGs. 1900-2200 are not limited to those example embodiments. The steps of the methods 1900-2200 shown in FIGs. 19-22 do not necessarily have to occur in the order described below. According to embodiments, some of the steps of the methods 1900-2200 are optional.

[0200] FIG. 19 is a flowchart illustrating an exemplary method for threat identification and remediation. Referring to FIG. 19, the method 1900 may provide threat identification and remediation for an infected device 560 using a trust orchestrator 430, an endpoint trust agent 510, a network analyzer 830 and an endpoint assessment service 820.

[0201] In step 1901, raw events 611 from the native device and/or platform instrumentation 610 are received. In an embodiment, the endpoint runtime monitor 620 described with reference to FIG. 6 above receives the raw events 611. After the raw events 611 are received, control is passed to step 1902.

[0202] In step 1902, image file and attributes are sent to a trust broker. According to an embodiment, this step is performed by the process monitor 514 described with reference to FIG. 5 above, that is included in the endpoint runtime monitor 620 described with reference to FIG. 6 above. In this embodiment, the process monitor 514 included in the endpoint runtime monitor 620 sends image file and attributes 518 to the trust broker 407 at the trust orchestrator 430 described with reference to FIG.

8 above so that specialized image analysis can be performed. After the image file and attributes 518 are sent, the method 1900 continues with step 1903.

[0203] In step 1903, the trust broker validates the image file based on received image attributes before passing control to step 1904. In accordance with an embodiment, the validation in step 1903 can be performed by the trust broker 407 described with reference to FIG. 5 above.

[0204] In step 1904, the trust broker (i.e., trust broker 407) sends the received image file to a malware analyzer. In one embodiment, the malware analyzer is malware analyzer 540 described with reference to FIG. 5 above and the malware analyzer is configured to perform specialized static and dynamic image introspection of the received image file.

[0205] In step 1905, a trust broker, such as, but not limited to, the trust broker 407, generates and sends, based on a received diagnosis, an image profile to an endpoint process monitor. In an embodiment, this step comprises sending an image profile 519 to the endpoint process monitor 514 described above with reference to FIG. 5. After the image profile is sent, control is passed to step 1906.

[0206] In step 1906, the endpoint runtime monitor 620 generates and sends integrity events, such as, but not limited to, integrity events 621, to an integrity processor, such as, but not limited to, the integrity processor 630 described above with reference to FIG. 6.

[0207] In step 1907, the endpoint integrity processor 630 may process and map received events to alerts using rulesets 631. In step 1908, the endpoint integrity processor 630 may generate and send warnings 634 using an event correlation matrix 633 to the trust orchestrator 430 as endpoint events 520.

[0208] In step 1909, a system event correlator, such as, but not limited to, the system event correlator 410, receives endpoint events 520 from the endpoint integrity processor 630.

[0209] In step 1910, the trust broker 407 receives network endpoint integrity measurement and verification reports 821 from an endpoint assessment service 820.

[0210] In step 1911, the system event correlator 410 receives temporal events 409 from the trust broker 407.

[0211] In step 1912, a system event correlator 410 may correlate the received endpoint and temporal events and generate an integrity profile 420 for the device 560 before passing control to step 1913.

[0212] In step 1913, the system event correlator 410 sends an integrity profile 420 of the device 560 to the trust supervisor 846.

[0213] In step 1914, the network activity correlator 831 sends infection profiles 831 to a trust supervisor, the trust supervisor 846.

[0214] In step 1915, the trust supervisor 846 may process the received integrity and infection profiles for classification of warnings based on forensic confidence for threat identification on the device 560.

[0215] In step 1916, the trust supervisor 846 sends to the remediation controller 848 actions 847 to perform on the infected device 560. In step 1917, the remediation controller 848 may process the received action request on the infected device 560 and send directives 849 based on configured thresholds and triggers to system orchestration and policy enforcement point (or network security) services 860.

[0216] FIG. 20 is a flowchart illustrating an exemplary method for providing a subject reputation service to a service provider. In the example embodiment of FIG. 20, the subject is a user and the method 2000 provides a user reputation service. However, as discussed above with reference to FIGs. 9 and 11, in alternative embodiments, the subject can also be a device, transaction, service, or an organization, such as a company.

[0217] In particular, FIG. 20 illustrates the steps by which a method 2000 provides a user reputation service for a service provider. In one embodiment, the service provider is the service provider 1104 described above with reference to FIG. 11 and the method 2000 can use a trust orchestrator, such as, but not limited to, the trust orchestrator 430 described above with reference to FIG. 8.

[0218] According to embodiments, steps of the method 2000 can also be performed using an endpoint trust agent, a network analyzer , and a network analyzer, such as, but not limited to, the endpoint trust agent 510, network analyzer

830, and the endpoint assessment service 820 described above with reference to FIG. 8.

[0219] In step 2001, an endpoint runtime monitor, such as, but not limited to, the endpoint runtime monitor 620 described above with reference to FIG. 6, receives raw events 611 from the native device and/or platform instrumentation 610, detect and identify the user 1014 authenticated by the authentication service 1103 at the device 560.

[0220] In step 2002, the endpoint runtime monitor 620 receives user activity events from the native device and/or platform instrumentation 610. After the user activity events have been received, control is passed to step 2003.

[0221] In step 2003, the endpoint runtime monitor 620 may generate and send integrity events 621 to the endpoint integrity processor 630.

[0222] In step 2004, the endpoint integrity processor 630 may process and map received events to alerts using rulesets 631.

[0223] In step 2005, the endpoint integrity processor 630 may generate and send warnings 634 using an event correlation matrix 633 to the trust orchestrator 430 as endpoint events 520. After the warnings and event correlation matrix have been generated and sent, the method 2000 continues with step 2006.

[0224] In step 2006, the trust broker 407 may query and receive user and resource attributes 1121, 1130, 1122, and 1128 from a plurality of collaboration services 904, 903, 902, 901 and generate subject events 1123. In step 2007, the reputation processor 1110 may analyze received subject events 1123 and generate subject alerts 1124 (i.e., user alerts or integrity profiles).

[0225] In step 2008, the risk correlator 1111 may correlate received subject alerts 1124, such as user 1014 alerts, to generate user warnings 1126 using the risk correlation matrix 721, and user reputation score 1125 using the reputation score generator 1112.

[0226] In step 2009, the trust supervisor 846 may process the received integrity and infection profiles for classification of warnings based on forensic confidence for threat identification of a user 1014 of the device 560. The user 1014 may be associated with the device due to currently being logged into the device 560, running

an application on the device 560, or by virtue of having account/user ID privileges to access resources such as files, data, applications, or web pages on the device 560.

[0227] In step 2010, the reputation broker 1106 receives a reputation query 1117 for the user 1014 of the device 560 from a service provider 1104.

[0228] In step 2011, the reputation broker 1106 sends a reputation token 1118 for the user 1014 of the device 560. In an embodiment, the reputation token 1118 sent in this step includes at least a user reputation score 1125. After the reputation token 1118 is sent, control is passed to step 2012.

[0229] In step 2012, the service provider 1104 applies a reputation-based access control 1119 in processing a service request 1116 received from the device 560 for the user 1014 to access a managed application 1105. After the reputation-based access control has been applied, control is passed to step 2013.

[0230] In step 2013, the trust supervisor 846 sends to the remediation controller 848 actions 847 to perform on the network fabric for sessions of the user 1014 of the device 560.

[0231] In step 2014, the remediation controller 848 may process received action request for sessions of the user 1014 of the device 560 and send directives 849 based on configured thresholds and triggers to system orchestration and policy enforcement point (network security) services 860.

[0232] FIG. 21 is a flowchart illustrating steps by which an attestation service for runtime operational integrity of systems executing on a computing platform using a network trust agent, endpoint trust agent and trust orchestration server can be provided. The steps of the method 2100 shown in FIG. 21 do not necessarily have to occur in the order described.

[0233] Referring to FIG. 21, the method 2100 can provide network flow level remediation for an infected device 560 at a network element 1216 using a trust orchestrator 1205, an endpoint trust agent 1201, a network trust agent 1209 and collaboration services 1207.

[0234] In step 2101, the endpoint runtime monitor 620 at the endpoint trust agent 1201 on the device 560 sends a dynamic context 1204 that may include endpoint events 520 to the trust orchestrator 1205.

[0235] In step 2102, the trust orchestrator 430 may analyze received endpoint events 520 from the endpoint trust agent 1201 on the device 560 before passing control to step 2103.

[0236] In step 2103, the trust broker 407 receives and analyzes network endpoint assessments (or integrity measurement and verification reports) 821 from an endpoint assessment service (or collaboration services) 820 and generate temporal events 409.

[0237] In step 2104, the system event correlator 410 may correlate endpoint 520 and temporal 409 events and generate an integrity profile 420 for the device 560.

[0238] In step 2105, the trust supervisor 846 may generate and send to the remediation controller 848 flow remediation actions 847 to perform on the network fabric.

[0239] In step 2106, the remediation controller 848 at the trust orchestrator 1205 sends to the network trust agent 1209 a system warning 1208 for the network device 560. In step 2107, the network trust agent 1209 may generate and send to the OpenFlow security framework 1211 directives 1210 to formulate commands 1213 for the OpenFlow controller 1214.

[0240] In step 2108, the OpenFlow controller 1214 sends rules 1215 to the OpenFlow enabled network element (switch) 1216 to divert or block traffic flows to/from the forewarned network device 560.

[0241] In step 2109, the OpenFlow enabled network element (switch) 1216 may enforce received access restrictions (controls) 1217 for the forewarned network device 560 before control is passed to step 2110.

[0242] In step 2110, the trust supervisor 846 may monitor and send reputation score updates 847 for the forewarned network device 560 to the remediation controller 848. In step 2111, the remediation controller 848 at the trust orchestrator 1205 sends system security posture status updates 1208 for the forewarned network device 560 to the network trust agent 1209. After the reputation score updates are monitored and sent, the method 2100 proceeds to step 2112.

[0243] In step 2112, the network trust agent 1209 may generate and send to the OpenFlow security framework 1211 directives 1210 to formulate commands 1213 for

the OpenFlow controller 1214 to restore normal flows to/from the forewarned network device 560.

[0244] FIG. 22 is a flowchart illustrating a method in accordance with various exemplary embodiments.

[0245] Referring to FIG. 22, the method 2200 can provide network flow level remediation for an infected mobile device 560 at a wireless access point 1320 using a trust orchestrator 1310, an endpoint trust agent 1301, a network trust agent 1315 and an endpoint assessment service 1312.

[0246] In step 2201, the endpoint runtime monitor 620 at the endpoint trust agent 1301 on the mobile device 560 sends a dynamic context 1304 that may include endpoint events 520 to the trust orchestrator 1310 before passing control to step 2202.

[0247] In step 2202, the trust orchestrator 430 may analyze received endpoint events 520 from the endpoint trust agent 1301 on the mobile device 560.

[0248] In step 2203, the trust broker 407 receives and analyzes network endpoint assessments (or integrity measurement and verification reports) 821 from an endpoint assessment service (or collaboration services) 820 and generate temporal events 409. After the network endpoint assessments are analyzed and the temporal events are generated, the method 2200 proceeds to step 2204.

[0249] In step 2204, the system event correlator 410 may correlate endpoint 520 and temporal 409 events and generate an integrity profile 420 for the mobile device 560.

[0250] In step 2205, the trust supervisor 846 may generate and send to the remediation controller 848 flow remediation actions 847 to perform on the network fabric.

[0251] In step 2206, the remediation controller 848 at the trust orchestrator 1310 sends to the network trust agent 1209 a system warning 1208 for the mobile device 560 before control is passed to step 2207.

[0252] In step 2207, the network trust agent 1209 generates and sends to the wireless access point 1320 policies 1317 to apply access controls 1321 for the mobile device 560, at which point control is passed to step 2208.

[0253] In step 2208, the remediation controller 848 at the trust orchestrator 1310 sends to the mobile policy manager 1313 a system warning 1307 for the mobile device 560 or to the mobile device manager 1324 directives 1309 to set feature controls on the mobile device 560.

[0254] In step 2209, the mobile policy manager 1313 generate and send to the mobile device manager 1324 directives 1309 to formulate advisories and security settings for the registered user (service subscriber) and the mobile device 560 or set feature controls on the mobile device 560.

[0255] In step 2210, the reputation broker 1106 receives a reputation query 1117 for a mobile device 560 from a service provider 1104.

[0256] In step 2211, the reputation broker 1106 sends a reputation token 1118 for the device 560 that may include at least a security posture established by the trust supervisor 846 based on the received infection 832 and integrity 420 profiles for the device 560.

[0257] In step 2212, the service provider 1104 may apply a reputation-based access control 1119 in processing a service request 1116 received from the device 560 to access a managed application 1105.

Entity Relationship Model and Hierarchical Subject Reputation

[0258] FIG. 23 is an entity relationship diagram illustrating exemplary relationships between entities and components used in a system for the calculus of a subject reputation score. For example, the entities and components depicted in the entity model 2300 can be used to generate reputation scores by the system 1100 described above with reference to FIG. 11.

[0259] Referring to FIG. 23, the exemplary reputation scoring system 2300 computes a reputation score for a user 1014 that is employed by, a member of, or otherwise associated with an organization 2303. The user 1014 can be associated with the organization temporarily (i.e., as a contractor). The user 1014 uses one or more endpoint devices 560 to perform an online transaction 2304 with a service 2305 that is rendered by an application 2306 and managed by the organization 2303, to participate in an activity 2307. In embodiments, the activity 2307 is categorized as either social 2308 or professional 1409.

[0260] According to embodiments, the organization 2303 can be, but is not limited to, a company, a government agency/division, a university or school, a hospital, a non-profit firm, or any other group that needs to secure systems, platforms, mobile computing devices, or other IT assets on behalf of its employees/members (i.e., users 1014 of devices 560). The organization's 2303 IT assets can include, but are not limited to, servers, desktop computers, laptops, tablet computers, multi-function printers/scanners/fax machines, and network devices. The IT assets can be devices 560 owned or leased by the organization and directly controlled by the organization 2303.

[0261] The IT assets can include devices 560 owned and managed by users 1014 (i.e., a user-owned mobile computing device in a BYOD environment) or the organization 2303 (i.e., a 'corporate' IT asset owned or leased by the organization 2303). In an embodiment, the reputation scoring system 2300 can operate in a mixed environment of IT assets wherein the organization 2303 owns some devices 560, leases some devices 560, and users 1014 own other devices 560. For example the organization 2303 may own enterprise servers and network devices (not shown), lease laptops, desktop computers/personal computers (PCs), and other endpoint devices 560 for users 1014 and simultaneously allow user 1014-owned mobile computing devices 560 (i.e., smart phones, laptops, and tablets in a BYOD environment) to access the organization's 2303 domain via internal or external networks. The internal networks can be, but are not limited to, an intranet, a LAN, or a WAN. The external networks can be, but are not limited to, an extranet, a wireless data networks such as Wi-Fi, and the Internet.

[0262] The servers (not shown) in the reputation scoring system 2300 may be part of a server farm and can be, but are not limited to, application servers hosting applications 2306, file servers, mail servers, database servers, proxy servers, and web servers. These servers can be enterprise servers owned by the organization 2303 or servers under a corporate lease. Alternatively, the servers can also be part of a remote, service-provider managed outsourced virtual data center (i.e., a cloud computing environment). The network devices can be networked storage devices,

routers, switches, hubs, and firewalls. These network devices can be part of the organization's 2303 local area network (LAN) or wide area network (WAN).

[0263] FIG. 24 is a block diagram illustrating an exemplary hierarchical representation of a subject reputation score. The hierarchical representation 2400 can be used to report reputation scores generated by system 1100 described above with reference to FIG. 11.

[0264] Referring to FIG. 24, the exemplary hierarchical representation of a subject reputation score 2400 includes a reputation score 2401, a transaction score 2409, a user score 2407, a service score 2408, a social score 2402, a professional score 2403, a device score 2404, an organization score 2405, and an application score 2406. In the exemplary embodiment of FIG. 24, the organization score 2405 can be, for example a company score 2405.

[0265] A reputation score may comprise one or more component scores (as an aggregation), where a component score is illustrated in FIG. 24 below an aggregate score (for example, a service score may be a component score of a transaction score). An aggregate reputation score may provide an enumerated list to annotate component scores included.

Application Event Monitoring Architecture

[0266] FIG. 25 is a block diagram illustrating an exemplary computing system architecture 2500 for monitoring application events for trusted execution with layered extensions to native machine instrumentation mechanisms. FIG. 25 is described with continued reference to the embodiments illustrated in FIGs. 4-6. However, FIG. 25 is not limited to those embodiments.

[0267] Referring to FIG. 25, the exemplary representation of the architecture 2500 instrumented for trust includes a device 560, an endpoint trust agent 510, native machine instrumentation 610, extended trust instrumentation 2501, a runtime monitor 620, a system event correlator 410, and a trust orchestrator 430.

[0268] The runtime monitor 620 subscribes for, and receives, near real time asynchronous notifications of application events 2502 from the extended trust instrumentation 2501. The application events 2502 may include registry, file system, network, storage, input (for example, keyboard), output (for example, screen

display), memory (for example, peek or poke) and process operations (for example, thread creation), and usage of any system resource (for example, microphone or camera) by running applications on the target instrumented device 560.

[0269] The extended trust instrumentation 2501 may be layered extensions to native machine instrumentation 610, such as, for example, the WINDOWS® Management Instrumentation (WMI) on MICROSOFT™ WINDOWS® platforms.

[0270] As will be appreciated by persons skilled in the relevant art, WMI is a set of extensions to the MICROSOFT™ WINDOWS® Driver Model (WDM), which is a framework for device drivers that provides an operating system interface through which instrumented components (i.e., components of an instrumented platform) provide information and notification. WMI is a MICROSOFT™ implementation of the Distributed Management Task Force (DMTF) Web-Based Enterprise Management (WBEM) and the DMTF Common Information Model (CIM) standards. WMI is preinstalled on some MICROSOFT™ WINDOWS® Operating Systems (OSs) and allows scripting languages like Visual Basic Scripting Edition (VBScript) or Windows PowerShell to manage computing devices and platforms running a MICROSOFT™ WINDOWS® OS. Such management can be performed locally (i.e., on the server or platform being managed) or remotely from a computing device external to the managed platform/device.

[0271] In certain exemplary embodiments, the runtime monitor 620 may generate and send dynamic expressions or rules as application filters 2503 linked to one or more running instances of applications on the target instrumented device 560.

[0272] The application events 2502 and application filters 2503 may be expressed using standards based schema definitions, such as for example the DMTF CIM specification. In a non-limiting embodiment, the CIM schema can be used to provide Trust-as-a-Service (TaaS).

[0273] In embodiments, the architecture 2500 can be used with APIs to subscribe for asynchronous application events such as, but not limited to, registry, file system, network, and process operations (e.g., Load Library, Remote Thread Attach, Peek/Poke Memory operations).

[0274] Embodiments of the architecture 2500 can include packaging of a TaaS endpoint comprising an endpoint trust sensor with OS updates, such as, but not limited to, MICROSOFT™ WINDOWS®, UNIX, Linux, and Apple OSX updates (i.e., OS and application upgrades and security patches for browsers, business productivity suites, device drivers, and other platform components). By using the architecture 2500, an endpoint trust sensor can measure runtime operational integrity by evaluating risk based on 'actions' and leveraging the native machine instrumentation 610.

[0275] In embodiments, the architecture 2500 also enables a network trust sensor to perform signature-less network activity correlation using a threat 'life cycle model' for clustering and classification of malware.

[0276] According to embodiments, the architecture 2500 enables trust orchestration for actionable intelligence based on real-time event correlation (i.e., a calculus of risk) by using an API collaboration bus for integration of security intelligence.

Example Computer System Implementation

[0277] Although exemplary embodiments have been described in terms of a computing device or instrumented platform, it is contemplated that it may be implemented in software on microprocessors/general purpose computers such as the computer system 2600 illustrated in FIG. 26. In various embodiments, one or more of the functions of the various components may be implemented in software that controls a computing device, such as computer system 2600, which is described below with reference to FIG. 26.

[0278] Aspects of the present invention shown in FIGS. 1-25, or any part(s) or function(s) thereof, may be implemented using hardware, software modules, firmware, non-transitory computer readable media having instructions stored thereon, or a combination thereof and may be implemented in one or more computer systems or other processing systems.

[0279] FIG. 26 illustrates an example computer system 2600 in which embodiments of the present invention, or portions thereof, may be implemented as computer-readable code. For example, the network systems and architectures of FIGS. 1, 4-6,

8-13 and 25 can be implemented in computer system 2600 using hardware, software, firmware, non-transitory computer readable media having instructions stored thereon, or a combination thereof and may be implemented in one or more computer systems or other processing systems. Hardware, software, or any combination of such may embody any of the modules and components used to implement the architectures and systems 100, 400, 500, 600, 800, 900, 1000, 1100, 1200, 1300 and 2500 of FIGS. 1, 4-6, 8-13 and 25.

[0280] If programmable logic is used, such logic may execute on a commercially available processing platform or a special purpose device. One of ordinary skill in the art may appreciate that embodiments of the disclosed subject matter can be practiced with various computer system configurations, including multi-core multiprocessor systems, minicomputers, mainframe computers, computers linked or clustered with distributed functions, as well as pervasive or miniature computers that may be embedded into virtually any device.

[0281] For instance, at least one processor device and a memory may be used to implement the above-described embodiments. A processor device may be a single processor, a plurality of processors, or combinations thereof. Processor devices may have one or more processor "cores."

[0282] Various embodiments of the invention are described in terms of this example computer system 2600. After reading this description, it will become apparent to a person skilled in the relevant art how to implement the invention using other computer systems and/or computer architectures. Although operations may be described as a sequential process, some of the operations may in fact be performed in parallel, concurrently, and/or in a distributed environment, and with program code stored locally or remotely for access by single or multi-processor machines. In addition, in some embodiments the order of operations may be rearranged without departing from the spirit of the disclosed subject matter.

[0283] Processor device 2604 may be a special purpose or a general-purpose processor device. As will be appreciated by persons skilled in the relevant art, processor device 2604 may also be a single processor in a multi-core/multiprocessor system, such system operating alone, or in a cluster of computing devices operating

in a cluster or server farm. Processor device 2604 is connected to a communication infrastructure 2606, for example, a bus, message queue, network, or multi-core message-passing scheme.

[0284] The computer system 2600 also includes a main memory 2608, for example, random access memory (RAM), and may also include a secondary memory 2610. Secondary memory 2610 may include, for example, a hard disk drive 2612, removable storage drive 2614. Removable storage drive 2614 may comprise a floppy disk drive, a magnetic tape drive, an optical disk drive, a flash memory, or the like.

[0285] The removable storage drive 2614 reads from and/or writes to a removable storage unit 2618 in a well-known manner. Removable storage unit 2618 may comprise a floppy disk, magnetic tape, optical disk, etc. which is read by and written to by removable storage drive 2614. As will be appreciated by persons skilled in the relevant art, removable storage unit 2618 includes a non-transitory computer usable storage medium having stored therein computer software and/or data.

[0286] In alternative implementations, secondary memory 2610 may include other similar means for allowing computer programs or other instructions to be loaded into computer system 2600. Such means may include, for example, a removable storage unit 2622 and an interface 2620. Examples of such means may include a program cartridge and cartridge interface (such as that found in video game devices), a removable memory chip (such as an EPROM, or PROM) and associated socket, and other removable storage units 2622 and interfaces 2620 which allow software and data to be transferred from the removable storage unit 2622 to computer system 2300.

[0287] The computer system 2600 may also include a communications interface 2624. Communications interface 2624 allows software and data to be transferred between computer system 2600 and external devices. Communications interface 2624 may include a modem, a network interface (such as an Ethernet card), a communications port, a PCMCIA slot and card, or the like. Software and data transferred via communications interface 2624 may be in the form of signals, which may be electronic, electromagnetic, optical, or other signals capable of being

received by communications interface 2624. These signals may be provided to communications interface 2324 via a communications path 2626. Communications path 2626 carries signals and may be implemented using wire or cable, fiber optics, a phone line, a cellular phone link, an RF link or other communications channels.

[0288] The computer system 2600 may also include a computer display 2630 and a display interface 2602. According to embodiments, the display used to display the GUIs and dashboards shown in FIGs. 14-18 and described above may be the computer display 2630, and the console interface may be display interface 2602.

[0289] In this document, the terms "computer program medium," "non-transitory computer readable medium," and "computer usable medium" are used to generally refer to media such as removable storage unit 2618, removable storage unit 2622, and a hard disk installed in hard disk drive 2612. Signals carried over communications path 2626 can also embody the logic described herein. Computer program medium and computer usable medium can also refer to memories, such as main memory 2608 and secondary memory 2610, which can be memory semiconductors (e.g., DRAMs, etc.). These computer program products are means for providing software to computer system 2600.

[0290] Computer programs (also called computer control logic) are stored in main memory 2608 and/or secondary memory 2610. Computer programs may also be received via communications interface 2624. Such computer programs, when executed, enable computer system 2600 to implement the present invention as discussed herein. In particular, the computer programs, when executed, enable processor device 2604 to implement the processes of the present invention, such as the stages in the methods illustrated by the flowcharts 1900, 2000, 2100 and 2200 of FIGS. 19-22, discussed above. Accordingly, such computer programs represent controllers of the computer system 2600. Where the invention is implemented using software, the software may be stored in a computer program product and loaded into computer system 2600 using removable storage drive 2614, interface 2620, and hard disk drive 2612, or communications interface 2624.

[0291] Embodiments of the invention also may be directed to computer program products comprising software stored on any computer useable medium. Such

software, when executed in one or more data processing device, causes a data processing device(s) to operate as described herein. Embodiments of the invention employ any computer useable or readable medium. Examples of computer useable mediums include, but are not limited to, primary storage devices (e.g., any type of random access memory), secondary storage devices (e.g., hard drives, floppy disks, CD ROMS, ZIP disks, tapes, magnetic storage devices, and optical storage devices, MEMS, nanotechnological storage device, etc.), and communication mediums (e.g., wired and wireless communications networks, local area networks, wide area networks, intranets, etc.).

Conclusion

[0292] It is to be appreciated that the Detailed Description section, and not the Summary and Abstract sections, is intended to be used to interpret the claims. The Summary and Abstract sections may set forth one or more but not all exemplary embodiments of the present invention as contemplated by the inventor(s), and thus, are not intended to limit the present invention and the appended claims in any way.

[0293] Embodiments of the present invention have been described above with the aid of functional building blocks illustrating the implementation of specified functions and relationships thereof. The boundaries of these functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternate boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed.

[0294] The foregoing description of the specific embodiments will so fully reveal the general nature of the invention that others can, by applying knowledge within the skill of the art, readily modify and/or adapt for various applications such specific embodiments, without undue experimentation, without departing from the general concept of the present invention. Therefore, such adaptations and modifications are intended to be within the meaning and range of equivalents of the disclosed embodiments, based on the teaching and guidance presented herein. It is to be understood that the phraseology or terminology herein is for the purpose of description and not of limitation, such that the terminology or phraseology of the

present specification is to be interpreted by the skilled artisan in light of the teachings and guidance.

[0295] Although the invention is illustrated and described herein with reference to specific embodiments, the invention is not intended to be limited to the details shown. Rather, various modifications may be made in the details within the scope and range equivalents of the claims and without departing from the invention.

What is claimed is:

1. A method of providing an attestation service for providing runtime operational integrity of a system using a computing platform comprising a network trust agent, an endpoint trust agent, and a trust orchestration server, the method comprising:

receiving, at the trust orchestration server, a dynamic context including endpoint events;

analyzing, by the trust orchestration server, the received endpoint events;

receiving network endpoint assessments;

generating temporal events based at least in part on analyzing the network endpoint assessments;

correlating the received endpoint events and the generated temporal events; and

generating an integrity profile for the system.

2. The method of claim 1, wherein the dynamic context is sent by the endpoint trust agent.

3. The method of claim 1, wherein the network endpoint assessments are received from an endpoint assessment service.

4. The method of claim 3, further comprising:

receiving integrity measurement and verification reports from the endpoint assessment service.

5. The method of claim 1, wherein the network endpoint assessments are received from one or more collaboration services.

6. The method of claim 5, further comprising:

receiving integrity measurement and verification reports from the one or more collaboration services.

7. The method of claim 1, wherein the endpoint events and temporal events are received by a system event correlator from endpoint trust agents and a trust broker, respectively.

8. A method of providing flow level remediation to isolate infected or compromised systems and platforms from a computing network fabric using a network trust agent, an endpoint trust agent, and a trust orchestrator, the method comprising:

generating, by the endpoint trust agent, runtime system integrity alerts regarding execution anomalies and risks based on rulesets and a calculus of risk;

sending, by the endpoint trust agent, runtime system integrity warnings as endpoint events to the trust orchestrator;

generating, by the trust orchestrator, a system integrity profile for the endpoint based on analysis of the received endpoint events;

processing and correlating, by the trust orchestrator, one or more of:

a system integrity profile generated based on a calculus of risk,

a plurality of temporal events generated based on a normalization and collation of elements in endpoint assessment reports received from a plurality of collaboration services, and

a system infection profile received from a network analyzer;

sending, by the trust orchestrator to the network trust agent, system warnings based on endpoint execution state assessments; and

sending, by the network trust agent, messages or directives to OpenFlow security frameworks and/or controllers to apply flow controls based on the received execution state as a threat posture of a connection endpoint.

9. The method of claim 8, wherein the integrity warnings comprise warnings regarding data events and content events; and wherein the endpoint events comprise data events and content events.

10. The method of claim 8, wherein the remediation of an infected system is achieved without adversely reducing the total operating capacity or availability of the computing platform through on-demand instantiation and scaling of workloads.

11. The method of claim 10, further comprising forwarding a notification conveying an infected or compromised state of a mobile computing device to a user associated with the mobile computing device, wherein the notification is one or more of:

an asynchronous push notification to an account associated with the user;

a short messaging service (SMS) text alert message forwarded to a phone number associated with the mobile computing device;

an email alert message forwarded to an email address associated with the user; and

a warning message displayed by a service on a display of the mobile computing device during initiation of a transaction with a service from the mobile computing device.

12. The method of claim 11, wherein one or more features or capabilities of a mobile device are de-activated or activated as a remediation action.

13. The method of claim 12, wherein the remediation action is based on the geo-location.

14. The method of claim 1, further comprising:

generating, by a trust supervisor, one or more flow remediation actions to be performed on a network fabric;

receiving, at a remediation controller of the trust orchestrator, the flow remediation actions; and

sending, by the trust orchestrator, to the network trust agent, one or more system warnings pertaining to a network device associated with the one or more flow remediation actions.

15. The method of claim 14, further comprising:

generating and sending, by the network trust agent, directives to formulate commands for an OpenFlow controller;

sending, by the OpenFlow controller, rules to an OpenFlow enabled network element or switch of the network fabric to divert or block traffic flow to/from the network device; and

enforcing, by the OpenFlow enabled network element or switch, received access restrictions or controls for the network device.

16. The method of claim 15, further comprising:

monitoring and sending, by the trust supervisor, reputation score updates for the network device to the remediation controller;

sending, by the trust orchestrator, system security posture status updates for the network device to the network trust agent; and

generating and sending, by the network trust agent, to the OpenFlow security framework, directives to formulate commands for the OpenFlow controller to restore normal flows to/from the network device.

17. The method of claim 8, further comprising:

determining, by the network analyzer, anomalies based on network activity correlation and malware detection; and

dispatching, by the trust orchestrator, the image files and attributes of an application for binary analysis, wherein the image files comprise compiled, intermediate, or interpreted code or scripts;

receiving a result of the binary analysis result identifying malicious activity as a set of threats identified based on the analysis; and

caching, by the trust broker, the results of the analysis indexed by a unique identifier for the image; and

generating and returning an image profile to the endpoint trust agent comprising assertions of malicious capabilities of the image to be monitored at runtime for subsequent generation of endpoint events by the endpoint trust agent.

18. The method of claim 17, wherein the binary analysis is performed by one or more third party malware analyzers, and wherein the dispatch mechanism uses trigger filter expressions that specify a set of criteria that warrant initiation of image analysis such as frequency and volume of requests for analysis associated with the application image across deployed endpoint trust agents.

19. The method of claim 18, wherein the third party malware analyzers are configured to perform static and dynamic analysis of application images based on policies specified by the trust broker.

20. A system for providing runtime operational integrity by determining execution anomalies and a threat posture of applications executing on computing platforms including mobile devices and client-server systems, the system comprising:

an endpoint trust agent including:

a process monitor configured to observe local execution context of the applications,

a socket monitor configured to observe network activities of the applications, and

a resource utilization module monitor configured to observe system and platform resources consumed by the applications; and

an application integrity module configured to assess operational integrities of the computing platforms based on a ruleset;

wherein native machine instrumentation for the computing platform is configured to:

represent event subscriptions, callbacks, notification mechanisms provided by an operating system (OS) on the computing platforms, and

generate raw events;

extended trust instrumentation;

a runtime monitor configured to:

subscribe to and receive near real time asynchronous notifications of application events for the applications from the extended trust instrumentation, and

generate and send dynamic expressions or rules as application filters linked to running instances of the applications;

a system event correlator configured to correlate system events of the computing platforms to determine a calculus of risk;

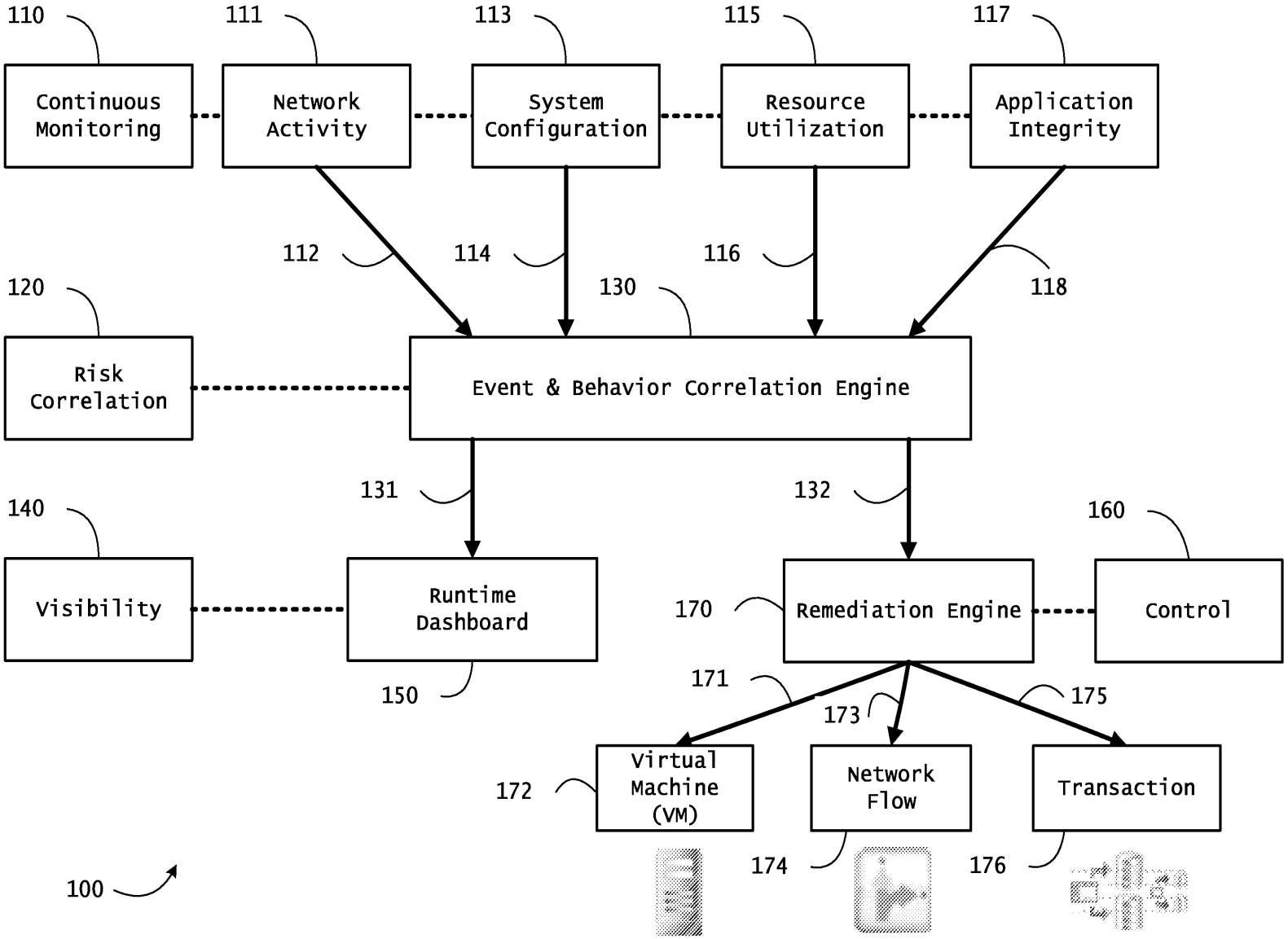
a trust orchestrator configured to orchestrate actionable intelligence based on the calculus of risk by integrating security intelligence about the computing platforms and the applications; and

an endpoint trust sensor configured to measure runtime operational integrity of the computing platforms by evaluating risk based on actions of an application executing on, or a user of, the computing platforms and receiving the raw events from the native machine instrumentation.

ABSTRACT OF THE DISCLOSURE

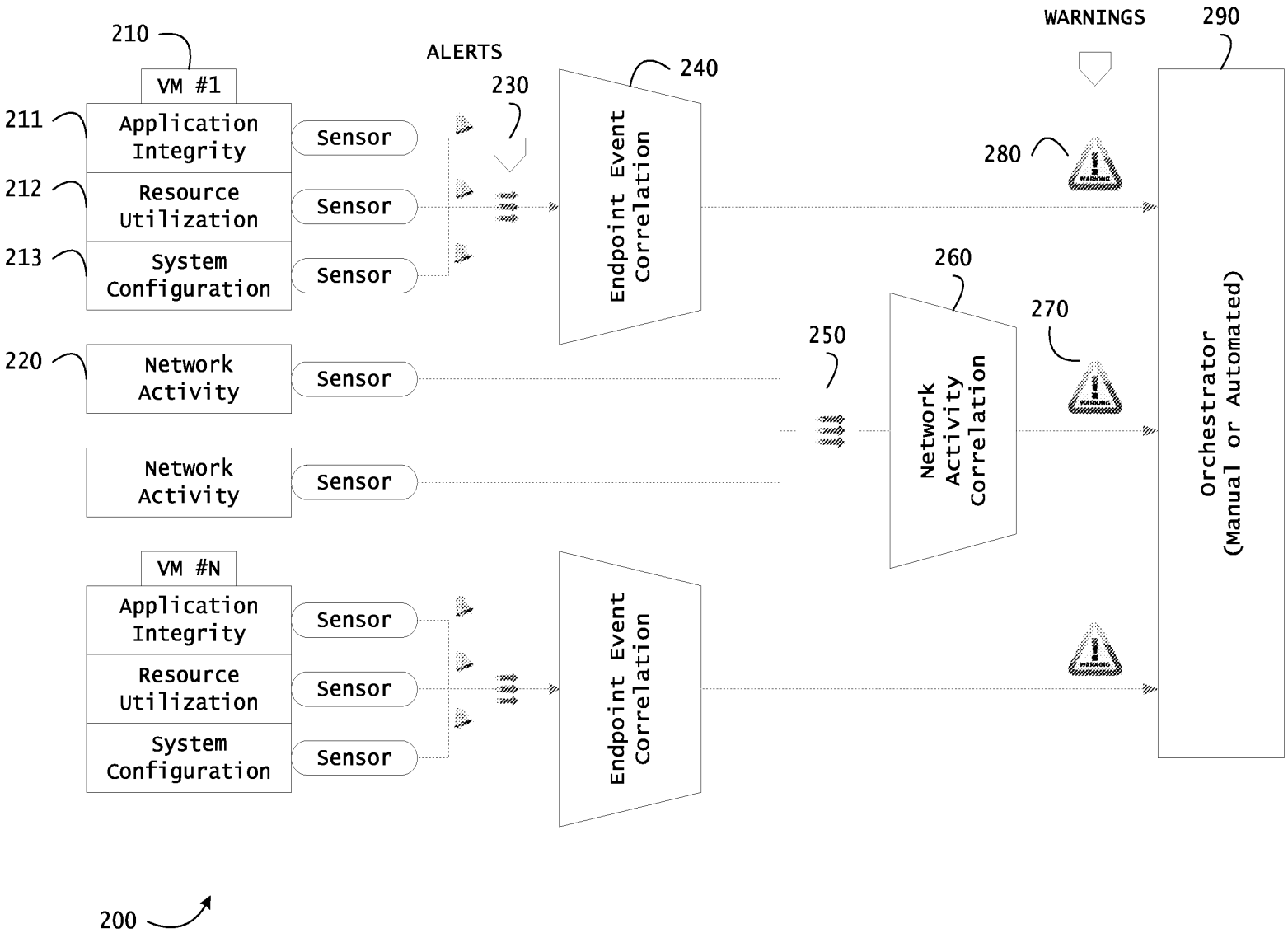
Instrumented networks and platforms having target subjects (devices, transactions, services, users, organizations) are disclosed. A security orchestration service generates runtime operational integrity profiles representing and identifying a level of threat or contextual trustworthiness, at near real time, of subjects and applications on the instrumented target platform. Systems and methods for threat identification and remediation for computing platforms based upon reconnaissance-based intelligence correlation and network/application monitoring are disclosed. In an embodiment, a method provides runtime operational integrity of a system by receiving: a dynamic context including endpoint events; and network endpoint assessments. The method generates temporal events based on the network endpoint assessments and correlates the endpoint events and temporal events before generating an integrity profile for the system. In another embodiment, flow level remediation is provided to isolate infected or compromised systems from a computing network fabric using a network trust agent, an endpoint trust agent, and a trust orchestrator.

FIG. 1



IPR2023-01466
CrowdStrike EX1002 Page 412

FIG. 2



IPR2023-01466
CrowdStrike EX1002 Page 413

FIG. 3A

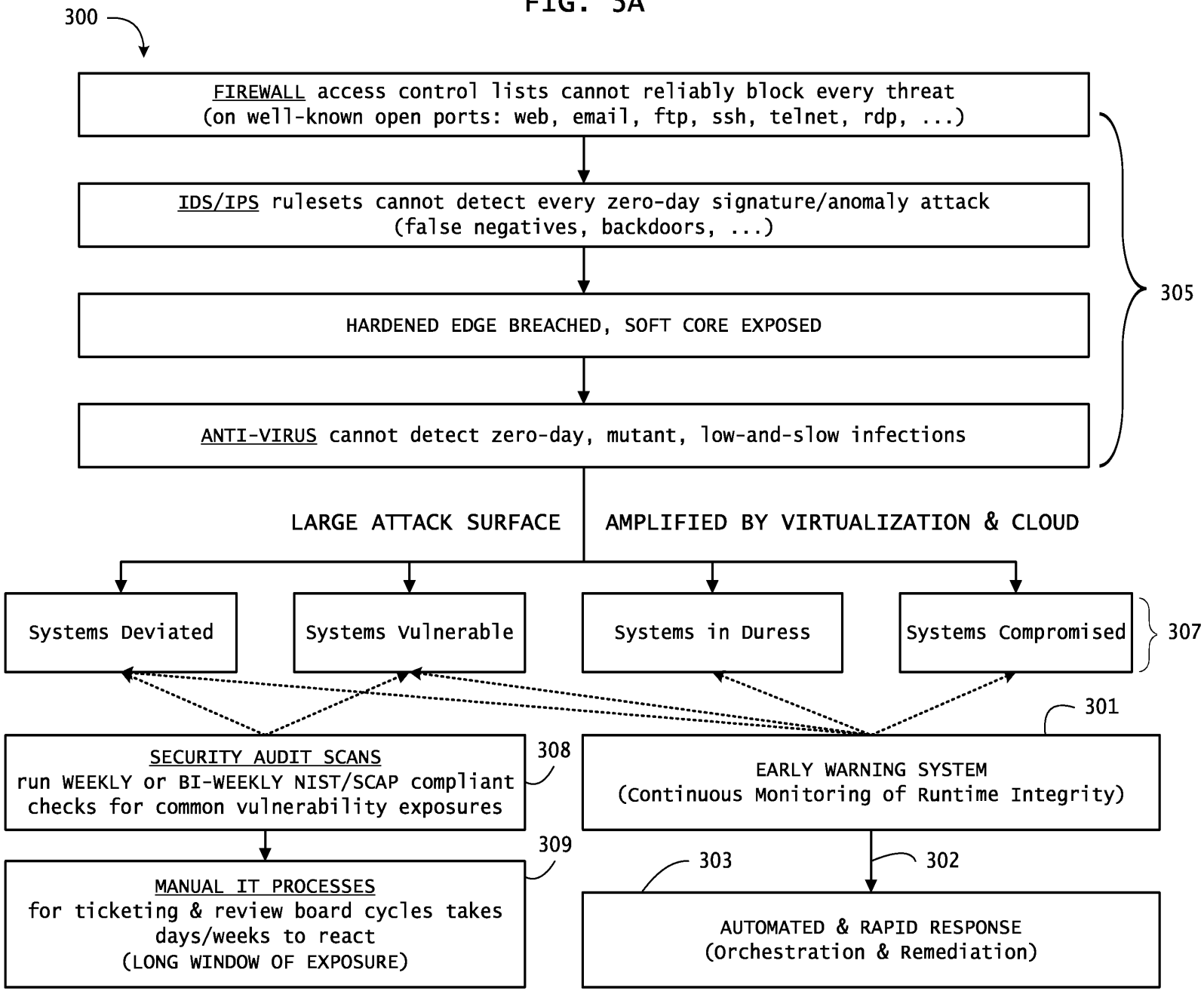
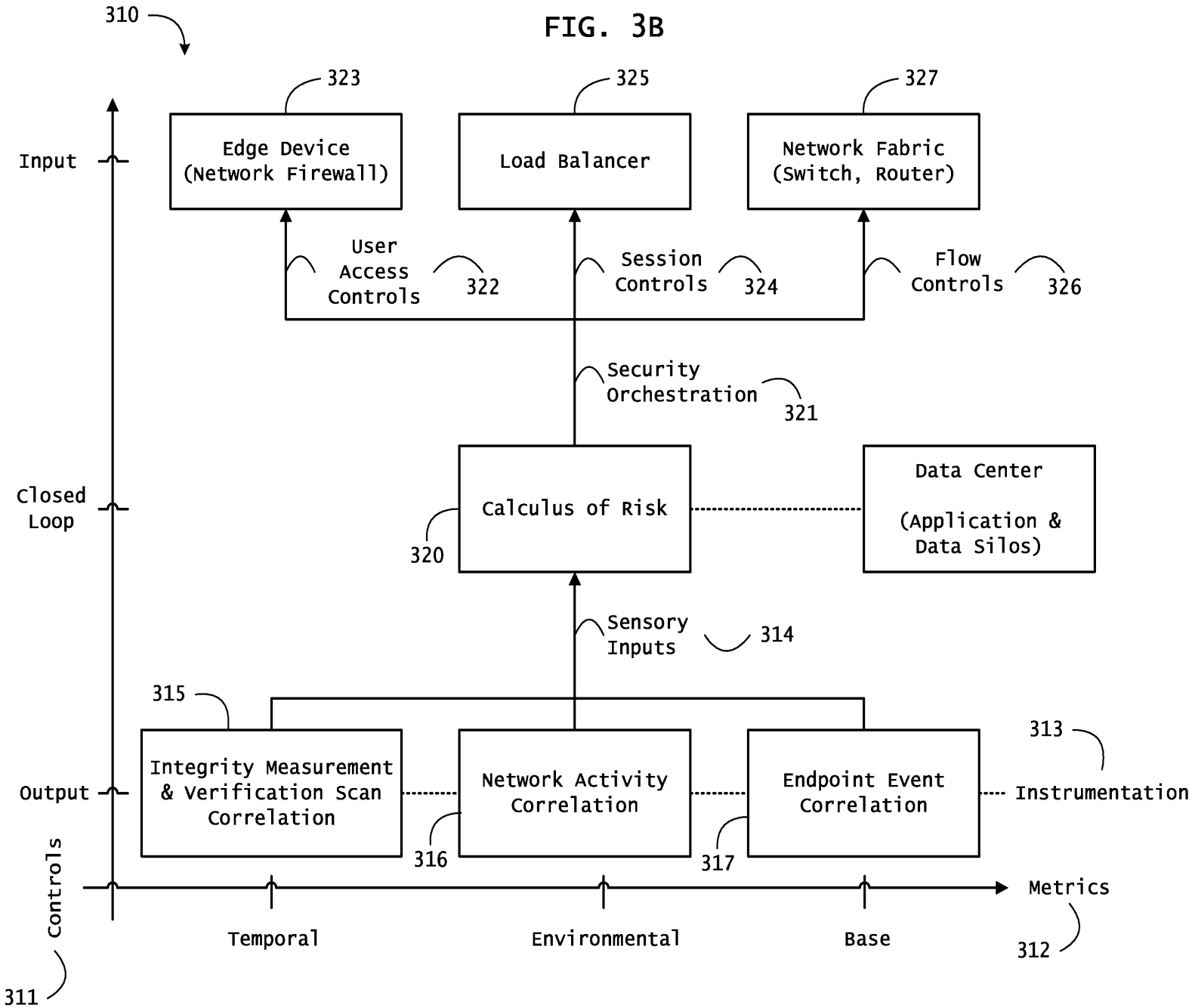
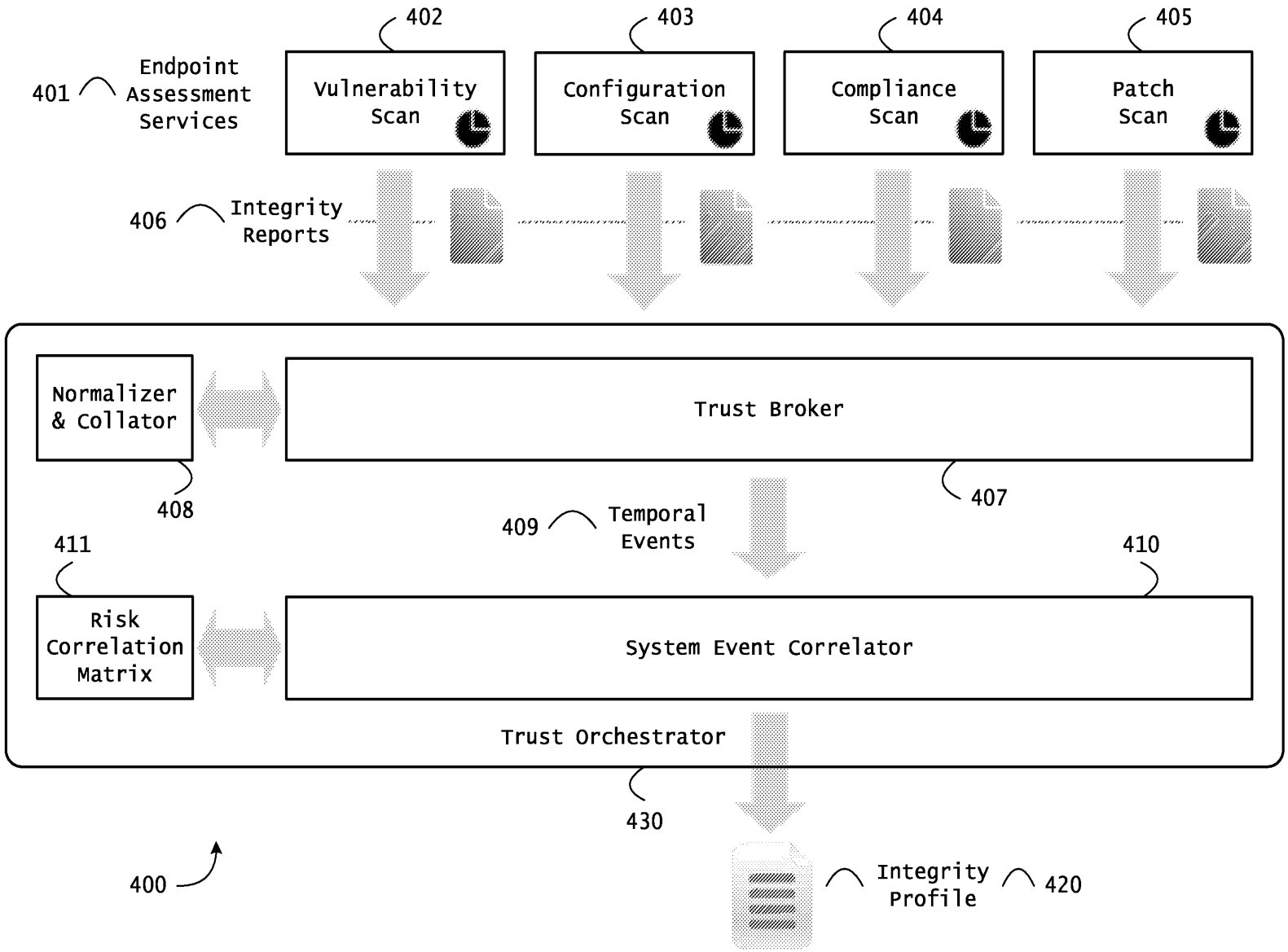

300
FIREWALL access control lists cannot reliably block every threat
(on well-known open ports: web, email, ftp, ssh, telnet, rdp, ...)
IDS/IPS rulesets cannot detect every zero-day signature/anomaly attack
(false negatives, backdoors, ...)
HARDENED EDGE BREACHED, SOFT CORE EXPOSED
ANTI-VIRUS cannot detect zero-day, mutant, low-and-slow infections
305
LARGE ATTACK SURFACE
AMPLIFIED BY VIRTUALIZATION & CLOUD
Systems Deviated
Systems Vulnerable
Systems in Duress
Systems Compromised
307
301
SECURITY AUDIT SCANS
run WEEKLY or BI-WEEKLY NIST/SCAP compliant
checks for common vulnerability exposures
308
EARLY WARNING SYSTEM
(Continuous Monitoring of Runtime Integrity)
309
303
302
MANUAL IT PROCESSES
for ticketing & review board cycles takes
days/weeks to react
(LONG WINDOW OF EXPOSURE)
AUTOMATED & RAPID RESPONSE
(Orchestration & Remediation)

FIG. 3B



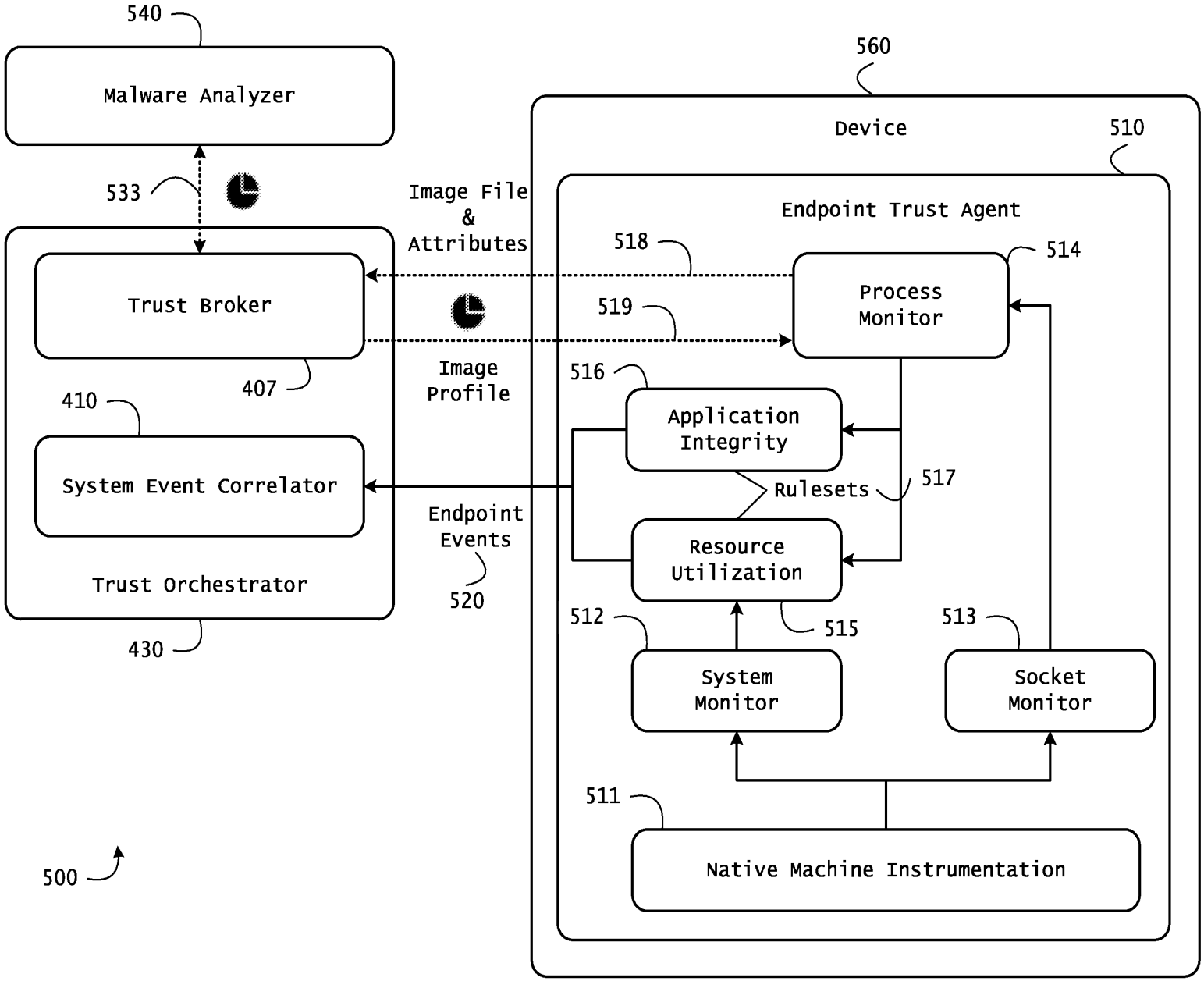
IPR2023-01466
CrowdStrike EX1002 Page 415

FIG. 4



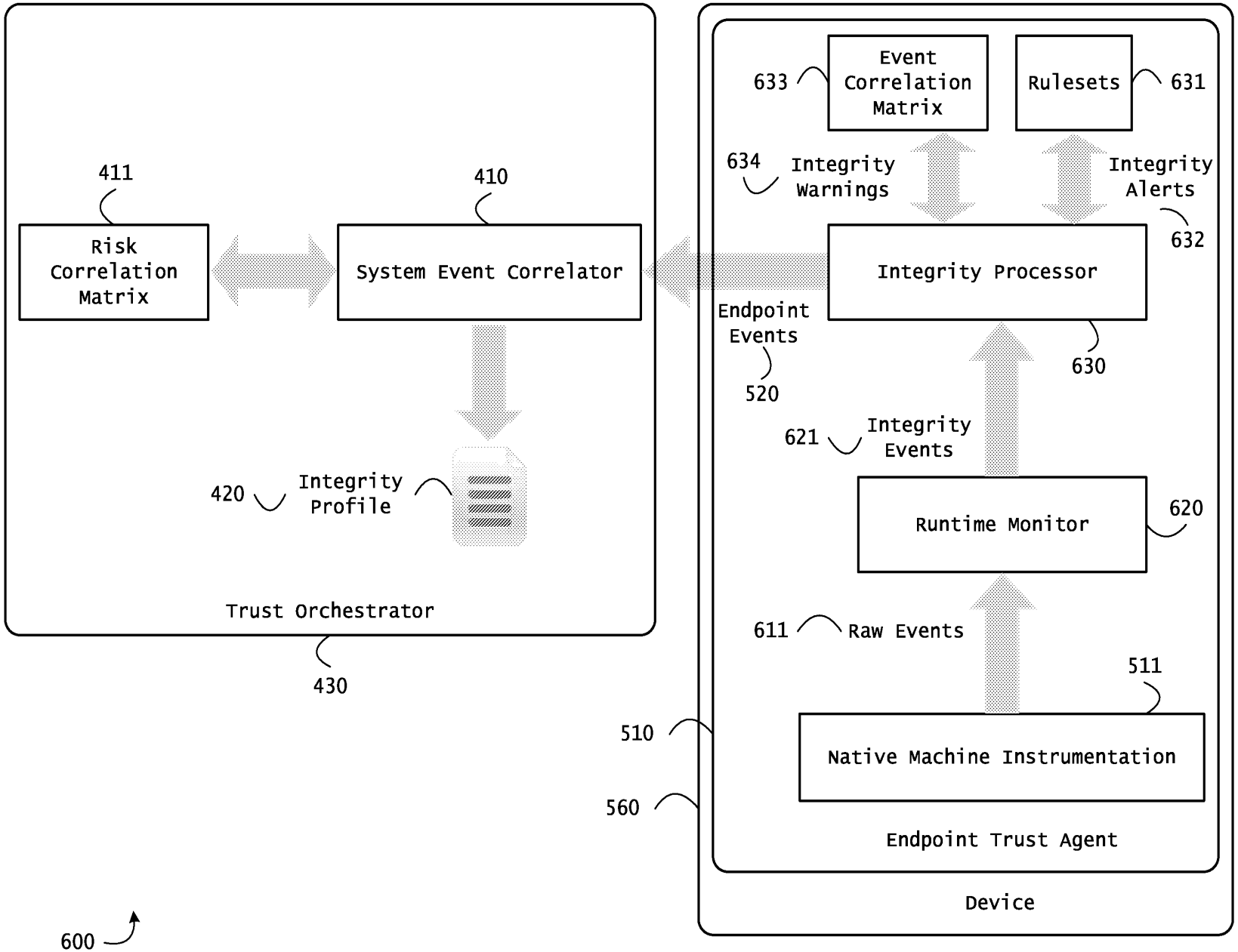
IPR2023-01466
CrowdStrike EX1002 Page 416

FIG. 5



IPR2023-01466
CrowdStrike EX1002 Page 417

FIG. 6



IPR2023-01466
CrowdStrike EX1002 Page 418

FIG. 7A

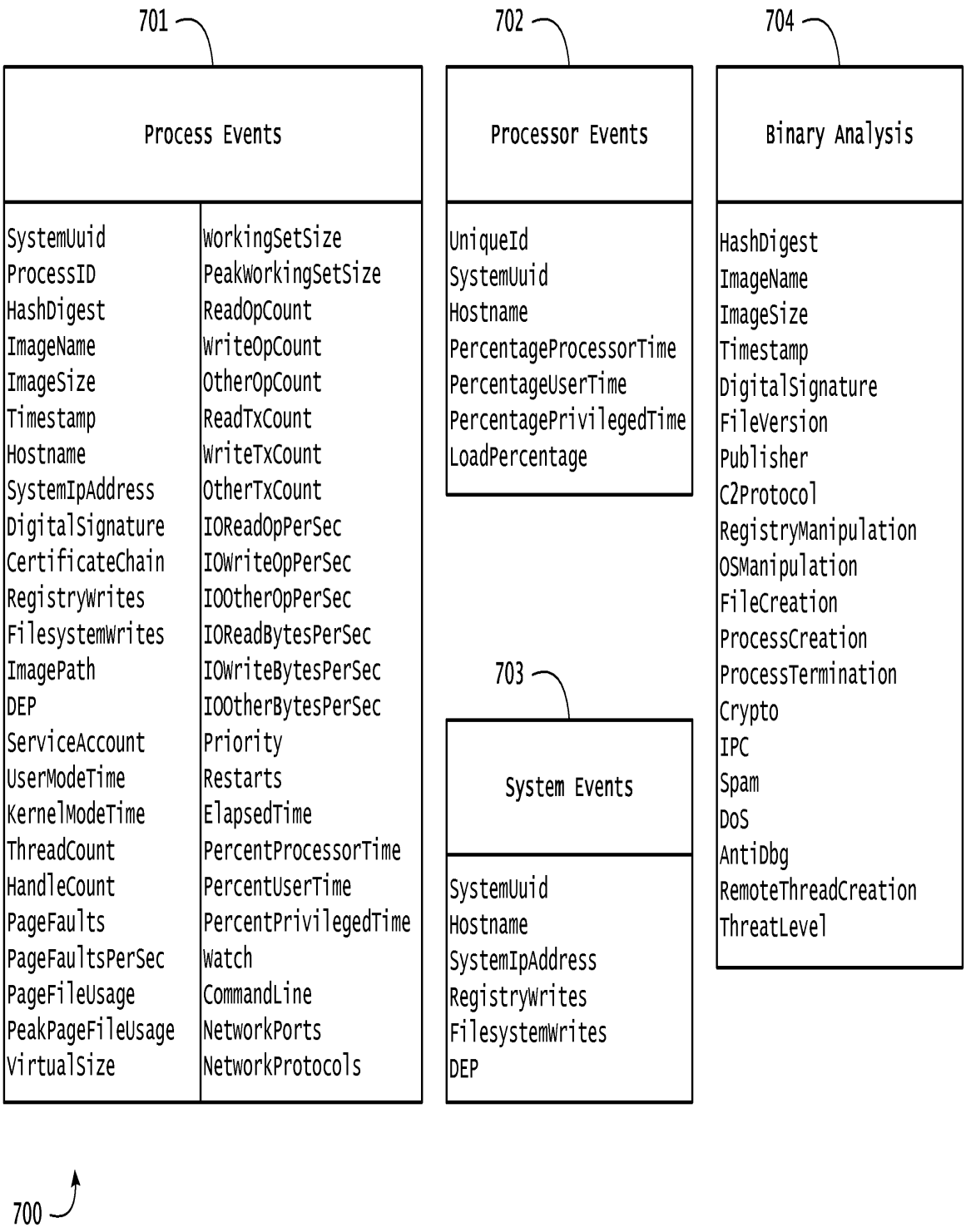

701
Process Events
SystemUuid
ProcessID
HashDigest
ImageName
ImageSize
Timestamp
Hostname
SystemIpAddress
DigitalSignature
CertificateChain
RegistryWrites
FilesystemWrites
ImagePath
DEP
ServiceAccount
UserModeTime
KernelModeTime
ThreadCount
HandleCount
PageFaults
PageFaultsPerSec
PageFileUsage
PeakPageFileUsage
VirtualSize
WorkingSetSize
PeakWorkingSetSize
ReadOpCount
WriteOpCount
OtherOpCount
ReadTxCount
WriteTxCount
OtherTxCount
IOReadOpPerSec
IOWriteOpPerSec
IOOtherOpPerSec
IOReadBytesPerSec
IOWriteBytesPerSec
IOOtherBytesPerSec
Priority
Restarts
ElapsedTime
PercentProcessorTime
PercentUserTime
PercentPrivilegedTime
Watch
CommandLine
NetworkPorts
NetworkProtocols
702
Processor Events
UniqueId
SystemUuid
Hostname
PercentageProcessorTime
PercentageUserTime
PercentagePrivilegedTime
LoadPercentage
703
System Events
SystemUuid
Hostname
SystemIpAddress
RegistryWrites
FilesystemWrites
DEP
704
Binary Analysis
HashDigest
ImageName
ImageSize
Timestamp
DigitalSignature
FileVersion
Publisher
C2Protocol
RegistryManipulation
OSManipulation
FileCreation
ProcessCreation
ProcessTermination
Crypto
IPC
Spam
DoS
AntiDbg
RemoteThreadCreation
ThreatLevel
700

FIG. 7B

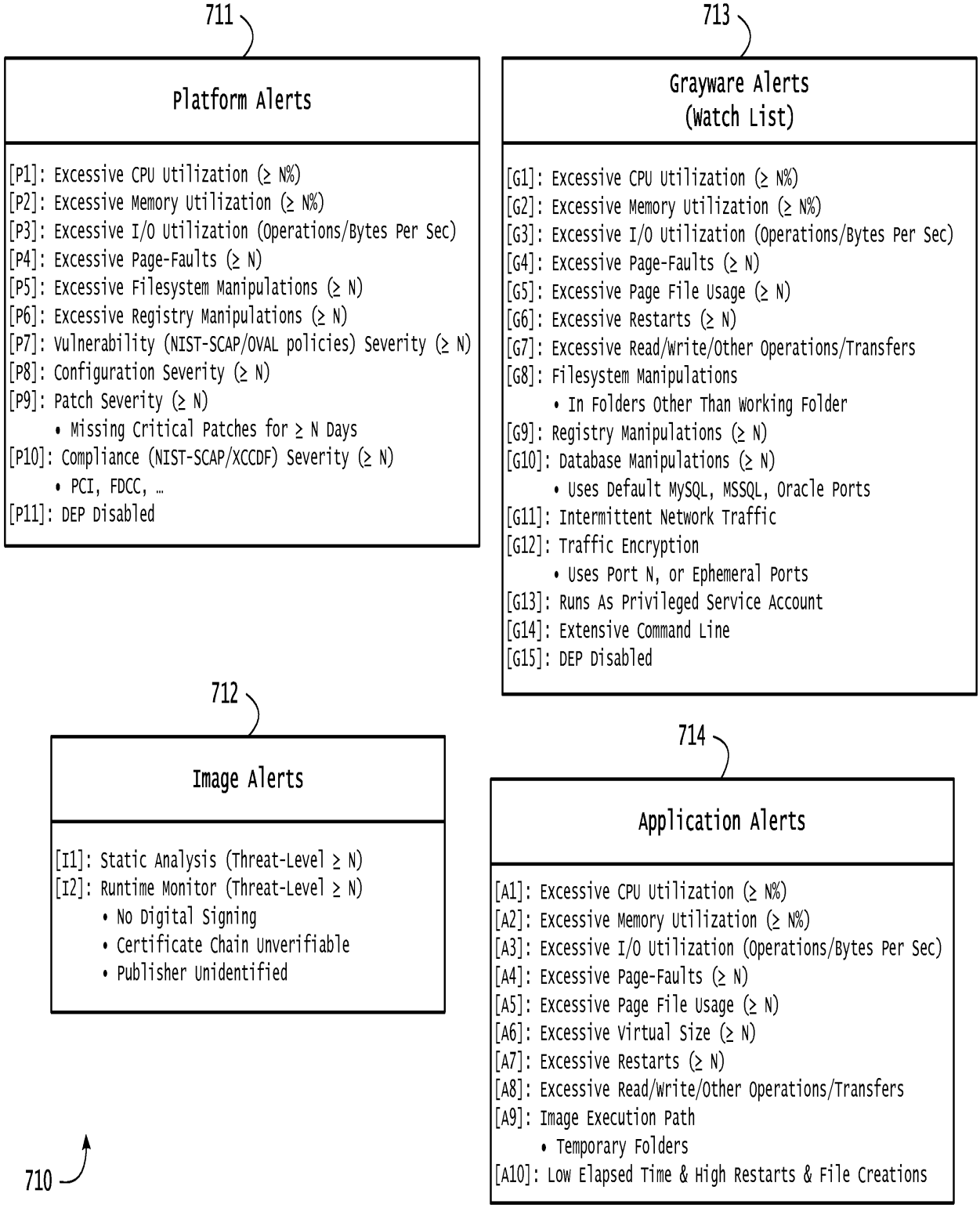
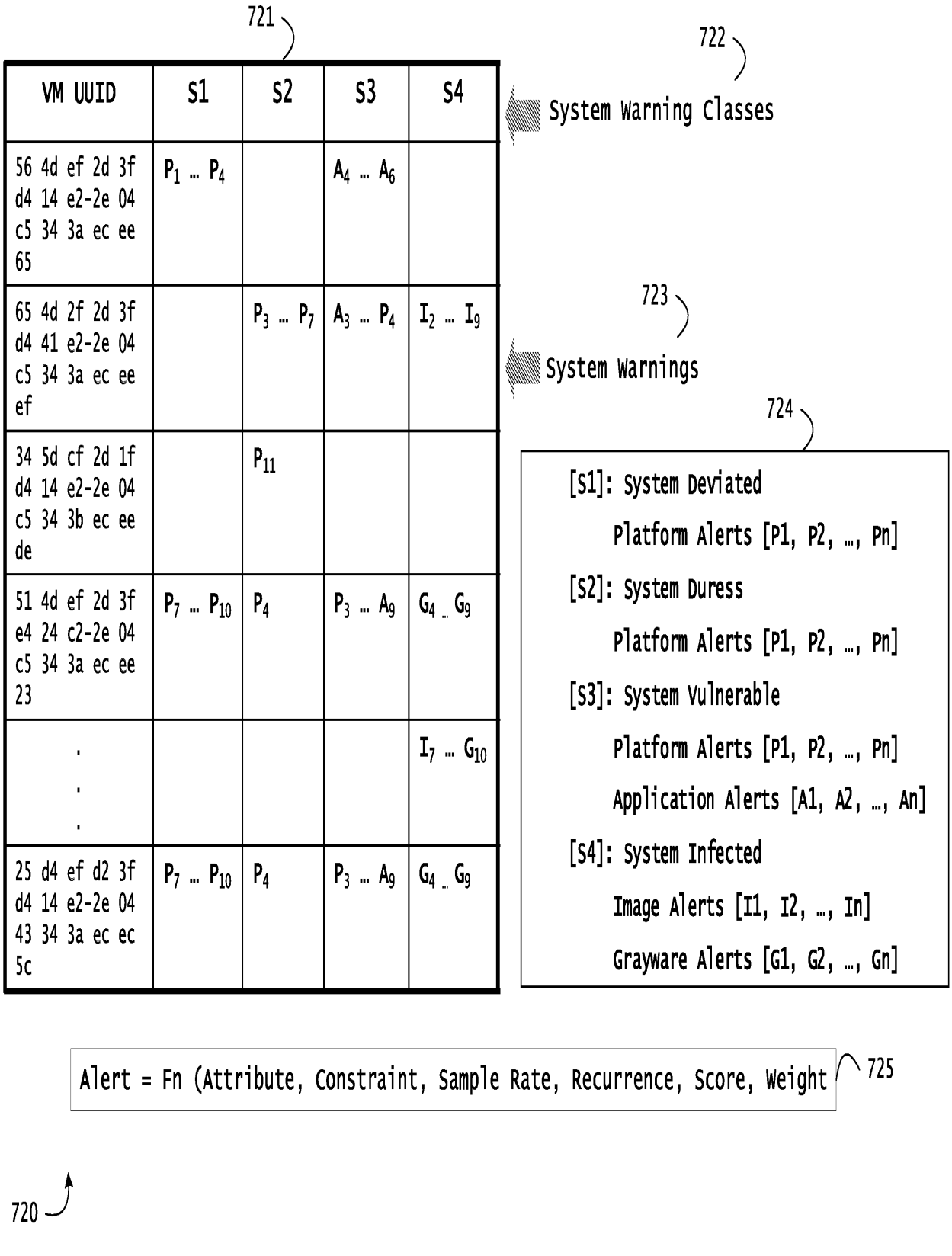
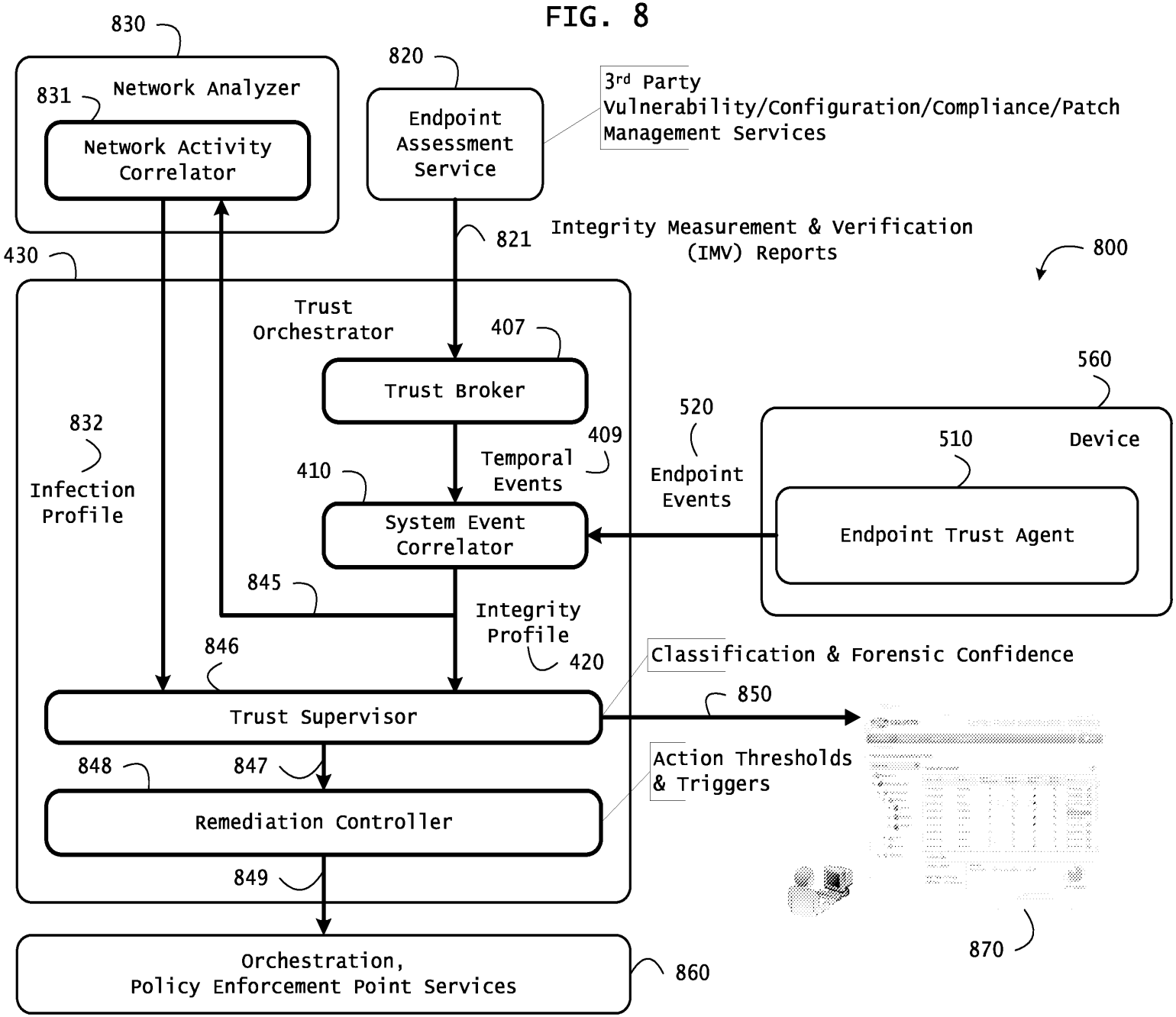

711
Platform Alerts
[P1]: Excessive CPU Utilization (≥ N%)
[P2]: Excessive Memory Utilization (≥ N%)
[P3]: Excessive I/O Utilization (Operations/Bytes Per Sec)
[P4]: Excessive Page-Faults (≥ N)
[P5]: Excessive Filesystem Manipulations (≥ N)
[P6]: Excessive Registry Manipulations (≥ N)
[P7]: Vulnerability (NIST-SCAP/OVAL policies) Severity (≥ N)
[P8]: Configuration Severity (≥ N)
[P9]: Patch Severity (≥ N)
• Missing Critical Patches for ≥ N Days
[P10]: Compliance (NIST-SCAP/XCCDF) Severity (≥ N)
• PCI, FDCC, …
[P11]: DEP Disabled
713
Grayware Alerts
(Watch List)
[G1]: Excessive CPU Utilization (≥ N%)
[G2]: Excessive Memory Utilization (≥ N%)
[G3]: Excessive I/O Utilization (Operations/Bytes Per Sec)
[G4]: Excessive Page-Faults (≥ N)
[G5]: Excessive Page File Usage (≥ N)
[G6]: Excessive Restarts (≥ N)
[G7]: Excessive Read/Write/Other Operations/Transfers
[G8]: Filesystem Manipulations
• In Folders Other Than Working Folder
[G9]: Registry Manipulations (≥ N)
[G10]: Database Manipulations (≥ N)
• Uses Default MySQL, MSSQL, Oracle Ports
[G11]: Intermittent Network Traffic
[G12]: Traffic Encryption
• Uses Port N, or Ephemeral Ports
[G13]: Runs As Privileged Service Account
[G14]: Extensive Command Line
[G15]: DEP Disabled
712
Image Alerts
[I1]: Static Analysis (Threat-Level ≥ N)
[I2]: Runtime Monitor (Threat-Level ≥ N)
• No Digital Signing
• Certificate Chain Unverifiable
• Publisher Unidentified
714
Application Alerts
[A1]: Excessive CPU Utilization (≥ N%)
[A2]: Excessive Memory Utilization (≥ N%)
[A3]: Excessive I/O Utilization (Operations/Bytes Per Sec)
[A4]: Excessive Page-Faults (≥ N)
[A5]: Excessive Page File Usage (≥ N)
[A6]: Excessive Virtual Size (≥ N)
[A7]: Excessive Restarts (≥ N)
[A8]: Excessive Read/Write/Other Operations/Transfers
[A9]: Image Execution Path
• Temporary Folders
[A10]: Low Elapsed Time & High Restarts & File Creations
710

FIG. 7C



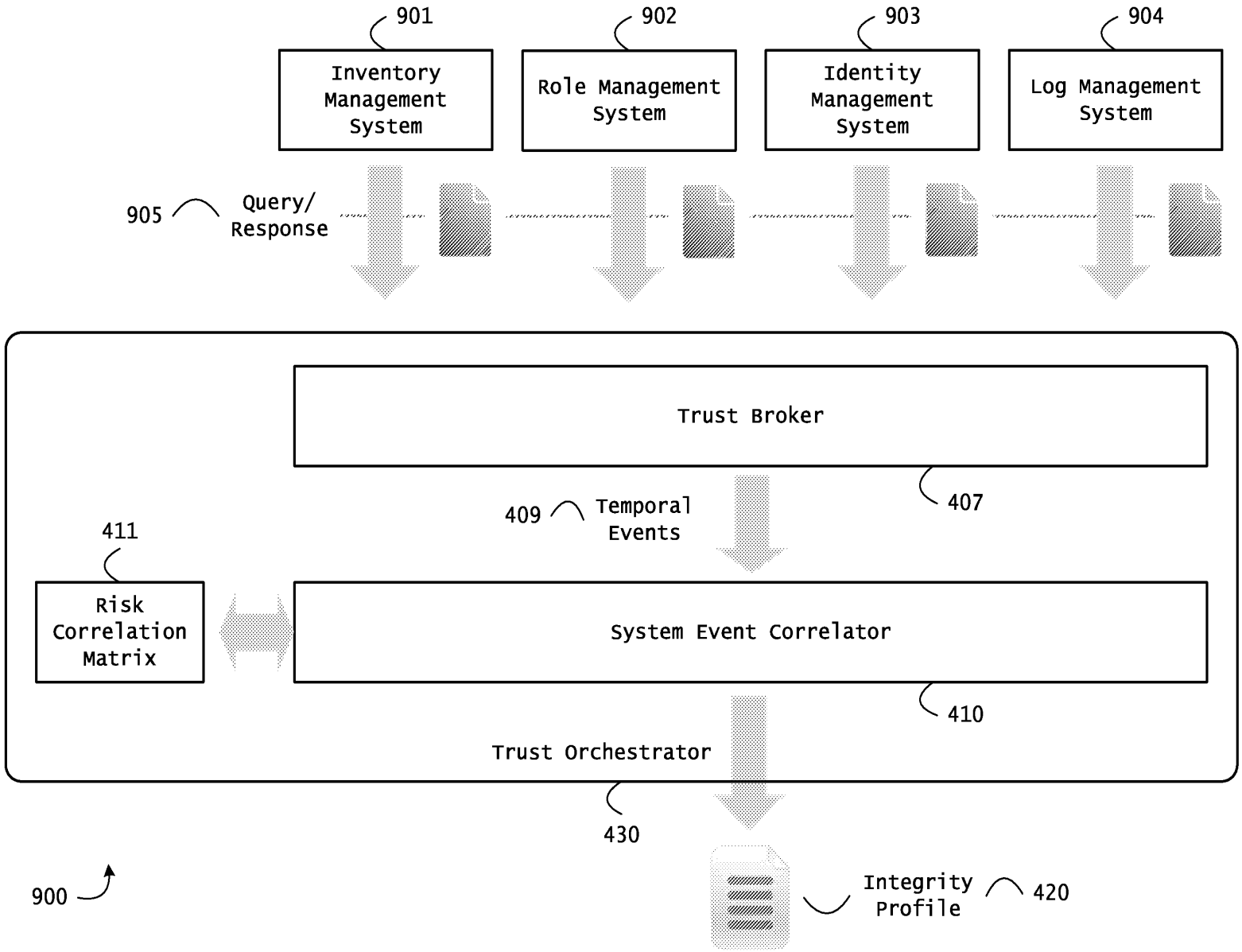
VM UUID	S1	S2	S3	S4
56 4d ef 2d 3f d4 14 e2-2e 04 c5 34 3a ec ee 65	$P_1 \ldots P_4$		$A_4 \ldots A_6$	
65 4d 2f 2d 3f d4 41 e2-2e 04 c5 34 3a ec ee ef		$P_3 \ldots P_7$	$A_3 \ldots P_4$	$I_2 \ldots I_9$
34 5d cf 2d 1f d4 14 e2-2e 04 c5 34 3b ec ee de		P_{11}		
51 4d ef 2d 3f e4 24 c2-2e 04 c5 34 3a ec ee 23	$P_7 \ldots P_{10}$	P_4	$P_3 \ldots A_9$	$G_4 \ldots G_9$
. . .				$I_7 \ldots G_{10}$
25 d4 ef d2 3f d4 14 e2-2e 04 43 34 3a ec ec 5c	$P_7 \ldots P_{10}$	P_4	$P_3 \ldots A_9$	$G_4 \ldots G_9$

FIG. 8

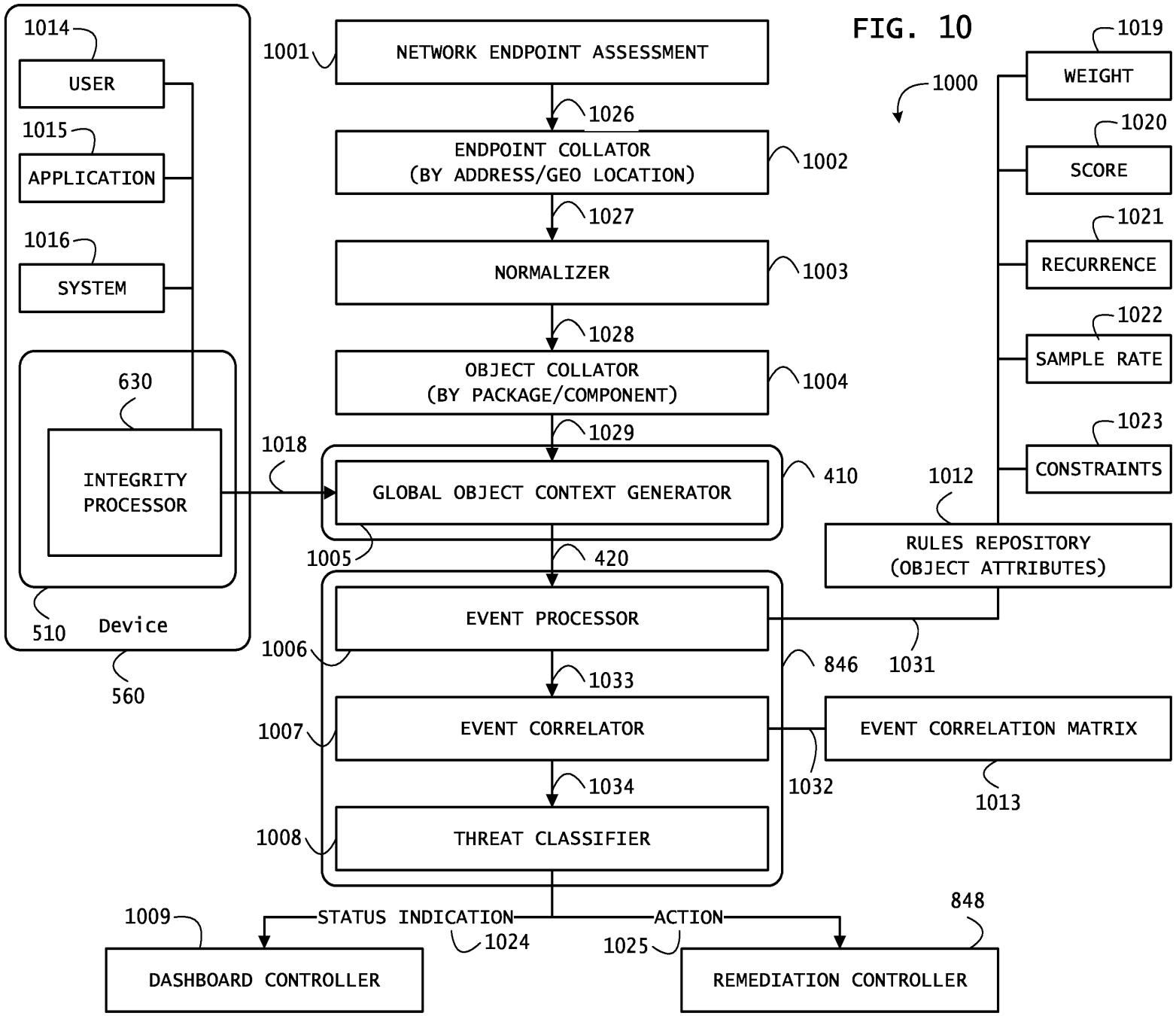


IPR2023-01466
CrowdStrike EX1002 Page 422

FIG. 9



IPR2023-01466
CrowdStrike EX1002 Page 423



IPR2023-01466
CrowdStrike EX1002 Page 424

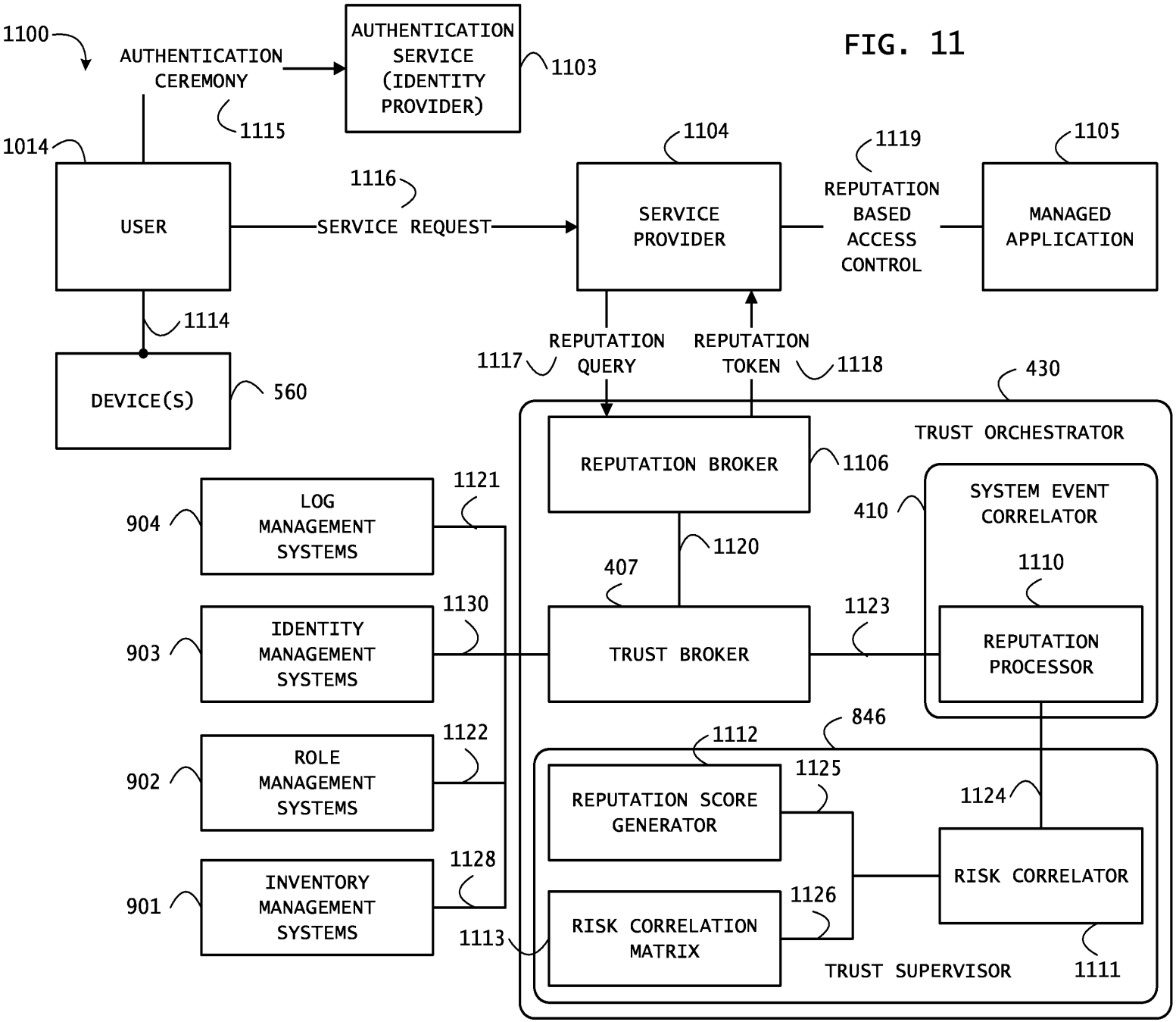
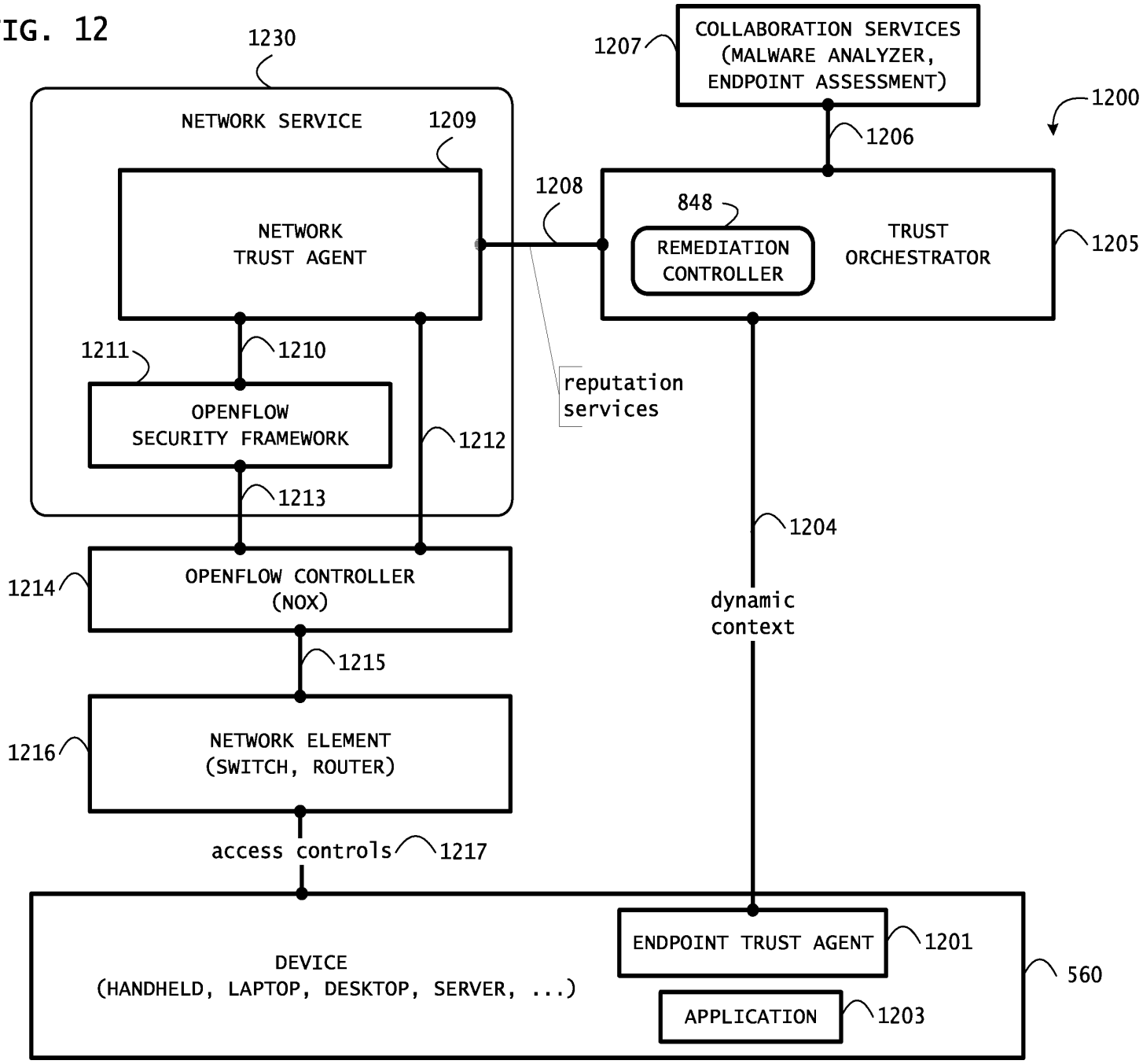


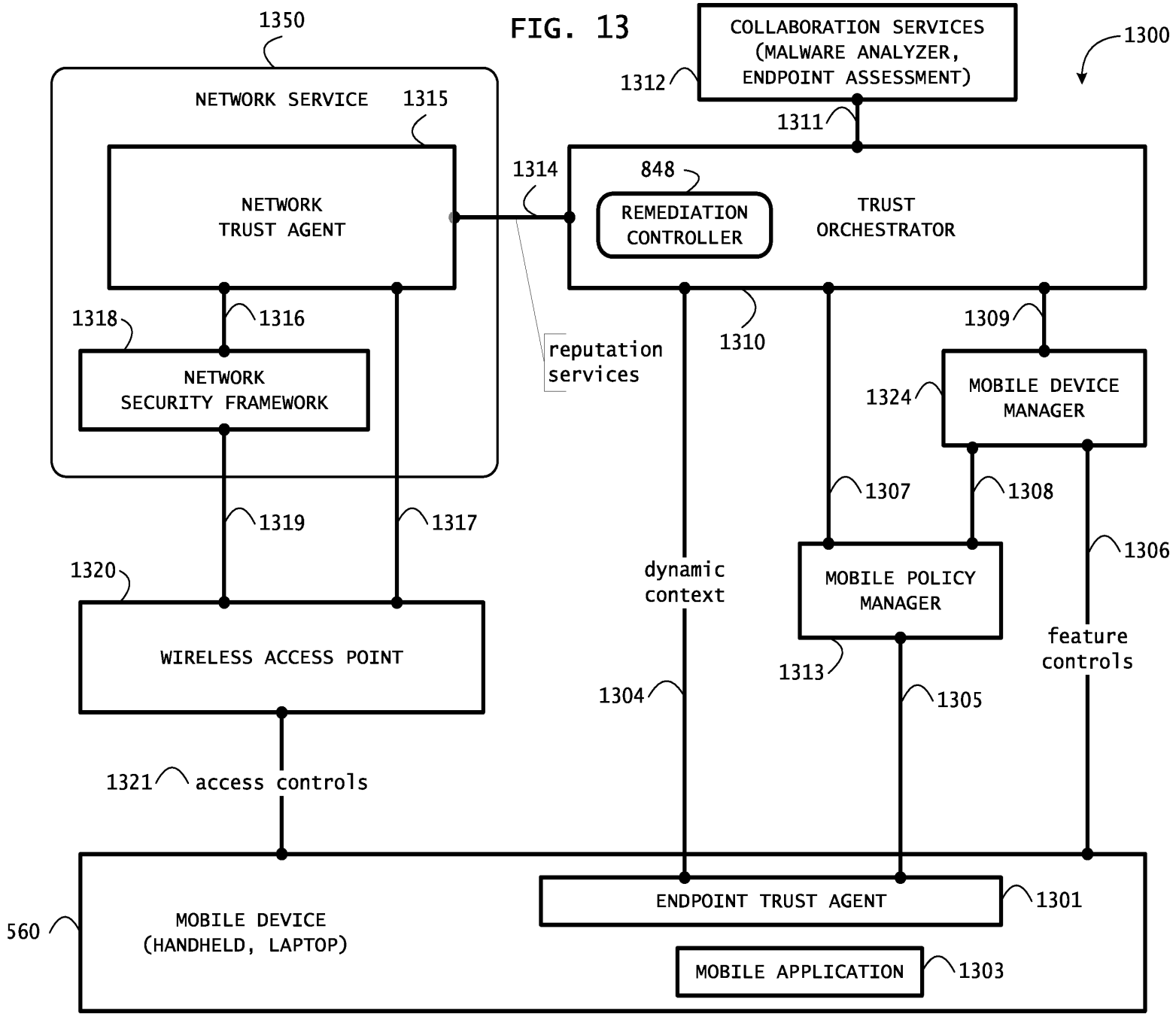
FIG. 11

IPR2023-01466
CrowdStrike EX1002 Page 425

FIG. 12



IPR2023-01466
CrowdStrike EX1002 Page 426



IPR2023-01466
CrowdStrike EX1002 Page 427

FIG. 14

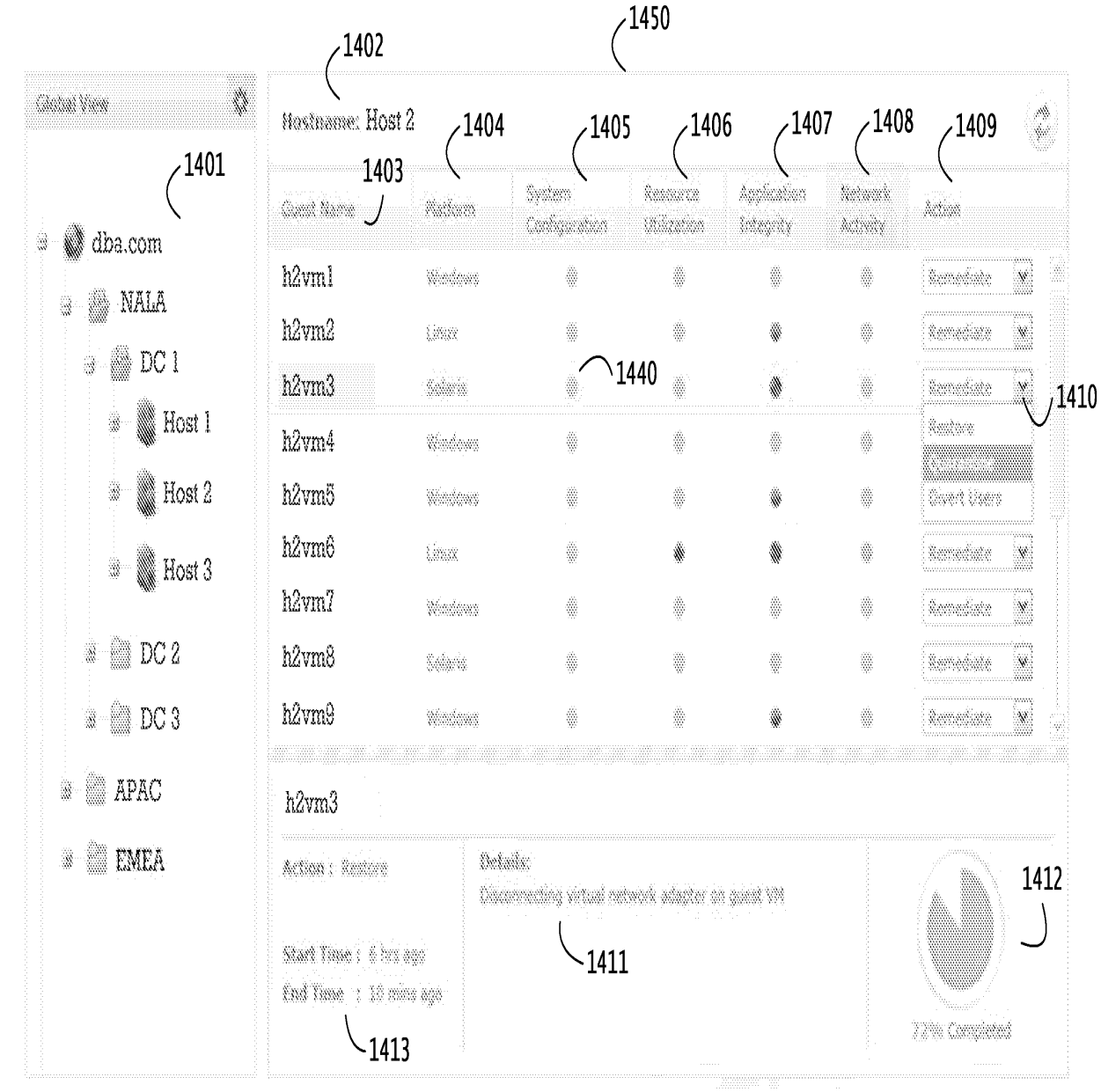

1400
1450
1402
1401
1403
1404
1405
1406
1407
1408
1409
1440
1410
1411
1412
1413
Global View
Hostname: Host 2
dba.com
NALA
DC 1
Host 1
Host 2
Host 3
DC 2
DC 3
APAC
EMEA
h2vm1
h2vm2
h2vm3
h2vm4
h2vm5
h2vm6
h2vm7
h2vm8
h2vm9
Remediate
Restore
Revert
Event Users
Details:
77% Completed

FIG. 15

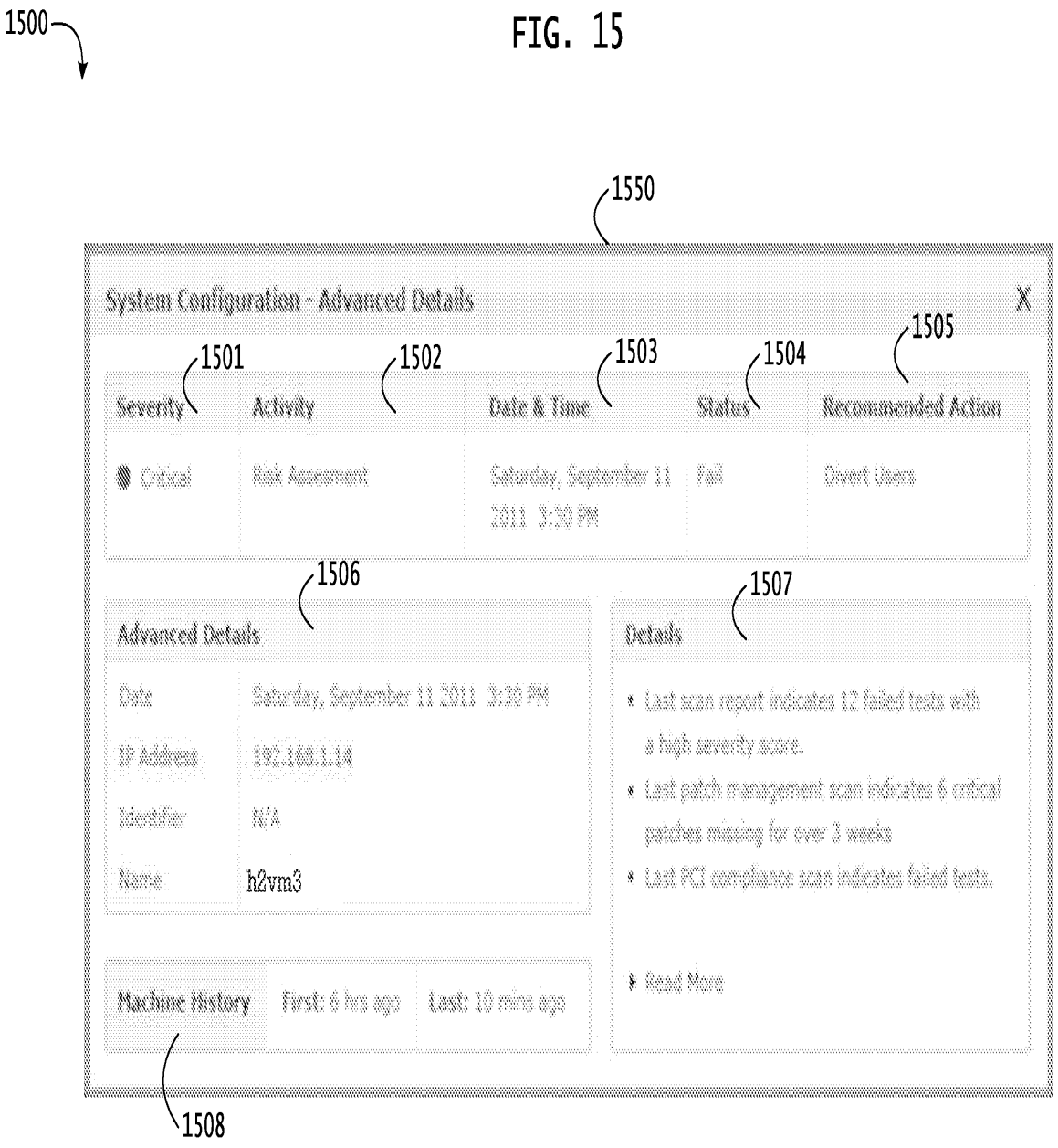
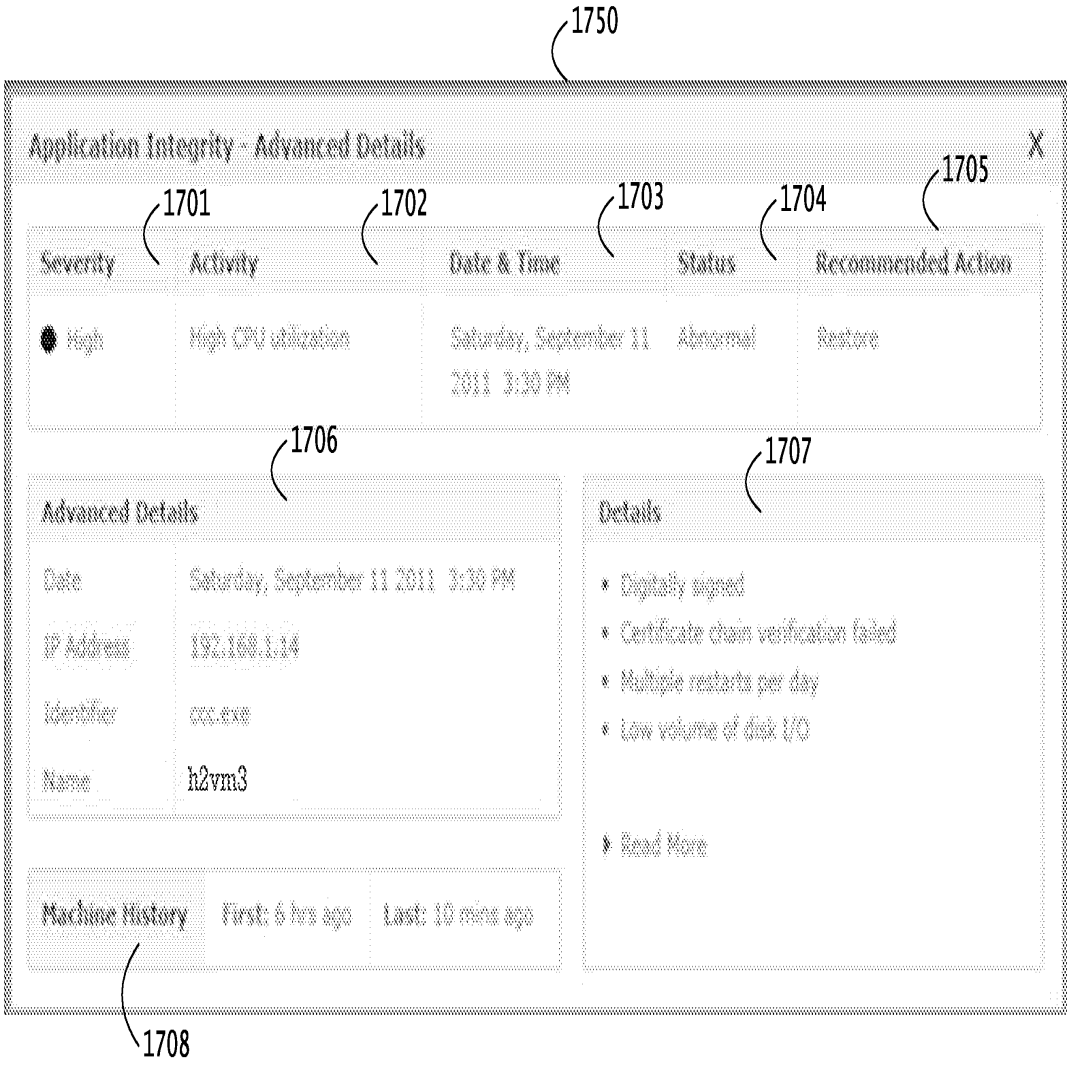

1500
1550
System Configuration - Advanced Details
X
1501
1502
1503
1504
1505
Severity
Activity
Date & Time
Status
Recommended Action
Critical
Risk Assessment
Saturday, September 11 2011 3:30 PM
Fail
Overt Users
1506
1507
Advanced Details
Details
Date
Saturday, September 11 2011 3:30 PM
IP Address
192.168.1.14
Identifier
N/A
Name
h2vm3
Last scan report indicates 12 failed tests with a high severity score.
Last patch management scan indicates 6 critical patches missing for over 3 weeks.
Last PCI compliance scan indicates failed tests.
Read More
Machine History
First: 6 hrs ago
Last: 10 mins ago
1508

FIG. 16


1600
1650
Resource Utilization - Advanced Details
X
1601
1602
1603
1604
1605
Severity
Activity
Date & Time
Status
Recommended Action
Medium
High CPU utilization
Saturday, September 11 2011 3:30 PM
Abnormal
Manual Intervention
1606
1607
Advanced Details
Details
Date
Saturday, September 11 2011 3:30 PM
IP Address
192.168.1.14
Identifier
foobar.exe
Name
h2vm3
Moderate disk read/write operations
High CPU usage over 45 min interval
Machine History
First: 6 hrs ago
Last: 10 mins ago
1608

1700

FIG. 17


1750
Application Integrity - Advanced Details
X
1701
1702
1703
1704
1705
Severity
Activity
Date & Time
Status
Recommended Action
High
High CPU utilization
Saturday, September 11 2011 3:33 PM
Abnormal
Restore
1706
1707
Advanced Details
Details
Date
Saturday, September 11 2011 3:33 PM
IP Address
192.168.1.14
Identifier
cc.exe
Name
h2vm3
Digitally signed
Certificate chain verification failed
Multiple restarts per day
Low volume of disk I/O
Read More
Machine History
First: 6 hrs ago
Last: 10 mins ago
1708

1800

FIG. 18

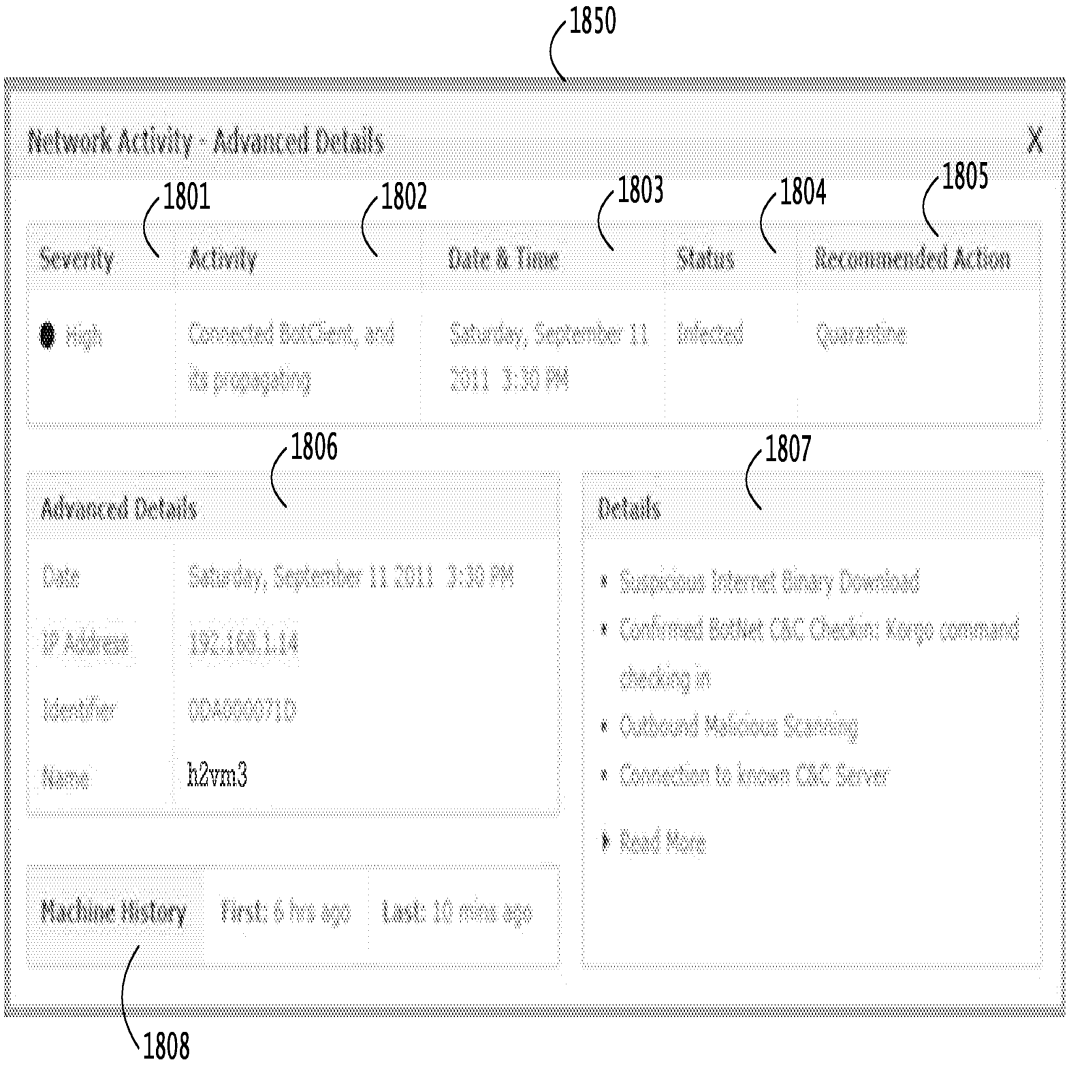

1850
Network Activity - Advanced Details
X
1801
1802
1803
1804
1805
Severity
Activity
Date & Time
Status
Recommended Action
High
Connected BotClient, and its propagating
Saturday, September 11 2011 3:30 PM
Infected
Quarantine
1806
1807
Advanced Details
Details
Date
Saturday, September 11 2011 3:30 PM
IP Address
192.168.1.14
Identifier
CRA0900710
Name
h2vm3
Suspicious Internet Binary Download
Confirmed BotNet C&C Checkin: Keys command checking in
Outbound Malicious Scanning
Connection to known C&C Server
Read More
Machine History
First: 6 hrs ago
Last: 10 mins ago
1808

FIG. 19

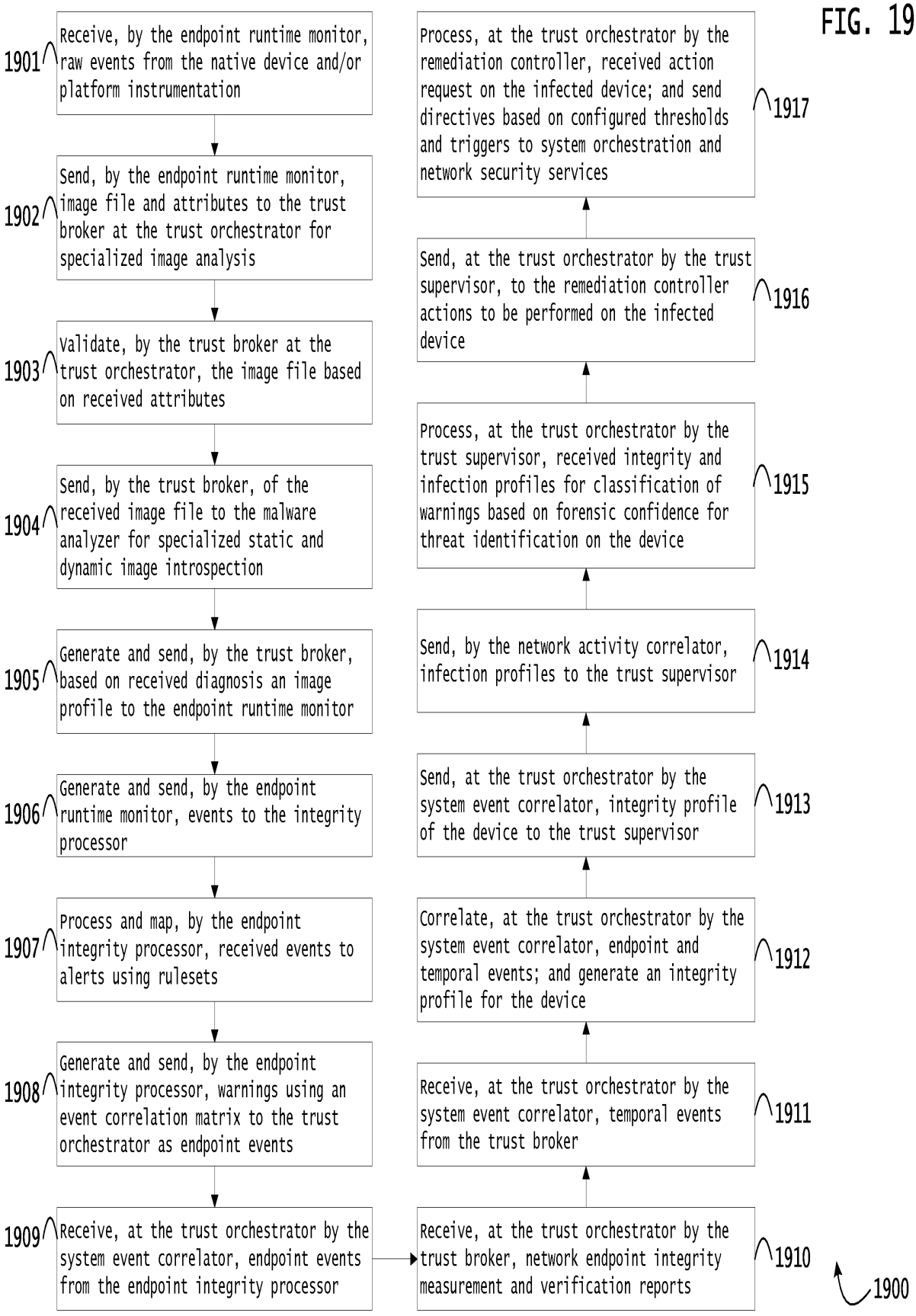

1901
Receive, by the endpoint runtime monitor, raw events from the native device and/or platform instrumentation
1902
Send, by the endpoint runtime monitor, image file and attributes to the trust broker at the trust orchestrator for specialized image analysis
1903
Validate, by the trust broker at the trust orchestrator, the image file based on received attributes
1904
Send, by the trust broker, of the received image file to the malware analyzer for specialized static and dynamic image introspection
1905
Generate and send, by the trust broker, based on received diagnosis an image profile to the endpoint runtime monitor
1906
Generate and send, by the endpoint runtime monitor, events to the integrity processor
1907
Process and map, by the endpoint integrity processor, received events to alerts using rulesets
1908
Generate and send, by the endpoint integrity processor, warnings using an event correlation matrix to the trust orchestrator as endpoint events
1909
Receive, at the trust orchestrator by the system event correlator, endpoint events from the endpoint integrity processor
1910
Receive, at the trust orchestrator by the trust broker, network endpoint integrity measurement and verification reports
1911
Receive, at the trust orchestrator by the system event correlator, temporal events from the trust broker
1912
Correlate, at the trust orchestrator by the system event correlator, endpoint and temporal events; and generate an integrity profile for the device
1913
Send, at the trust orchestrator by the system event correlator, integrity profile of the device to the trust supervisor
1914
Send, by the network activity correlator, infection profiles to the trust supervisor
1915
Process, at the trust orchestrator by the trust supervisor, received integrity and infection profiles for classification of warnings based on forensic confidence for threat identification on the device
1916
Send, at the trust orchestrator by the trust supervisor, to the remediation controller actions to be performed on the infected device
1917
Process, at the trust orchestrator by the remediation controller, received action request on the infected device; and send directives based on configured thresholds and triggers to system orchestration and network security services
1900

FIG. 20

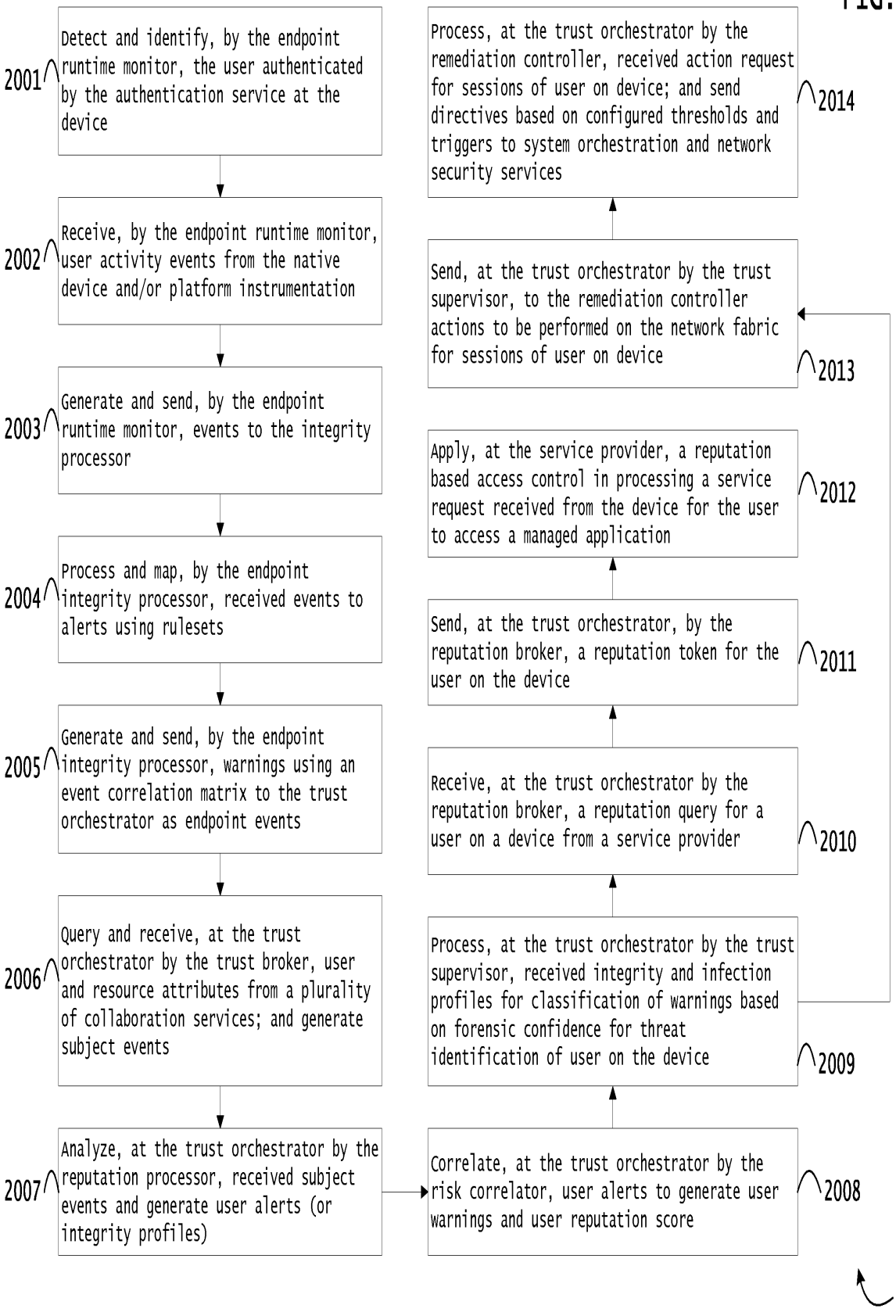

2001
Detect and identify, by the endpoint runtime monitor, the user authenticated by the authentication service at the device
2002
Receive, by the endpoint runtime monitor, user activity events from the native device and/or platform instrumentation
2003
Generate and send, by the endpoint runtime monitor, events to the integrity processor
2004
Process and map, by the endpoint integrity processor, received events to alerts using rulesets
2005
Generate and send, by the endpoint integrity processor, warnings using an event correlation matrix to the trust orchestrator as endpoint events
2006
Query and receive, at the trust orchestrator by the trust broker, user and resource attributes from a plurality of collaboration services; and generate subject events
2007
Analyze, at the trust orchestrator by the reputation processor, received subject events and generate user alerts (or integrity profiles)
2008
Correlate, at the trust orchestrator by the risk correlator, user alerts to generate user warnings and user reputation score
2009
Process, at the trust orchestrator by the trust supervisor, received integrity and infection profiles for classification of warnings based on forensic confidence for threat identification of user on the device
2010
Receive, at the trust orchestrator by the reputation broker, a reputation query for a user on a device from a service provider
2011
Send, at the trust orchestrator, by the reputation broker, a reputation token for the user on the device
2012
Apply, at the service provider, a reputation based access control in processing a service request received from the device for the user to access a managed application
2013
Send, at the trust orchestrator by the trust supervisor, to the remediation controller actions to be performed on the network fabric for sessions of user on device
2014
Process, at the trust orchestrator by the remediation controller, received action request for sessions of user on device; and send directives based on configured thresholds and triggers to system orchestration and network security services
2000

FIG. 21

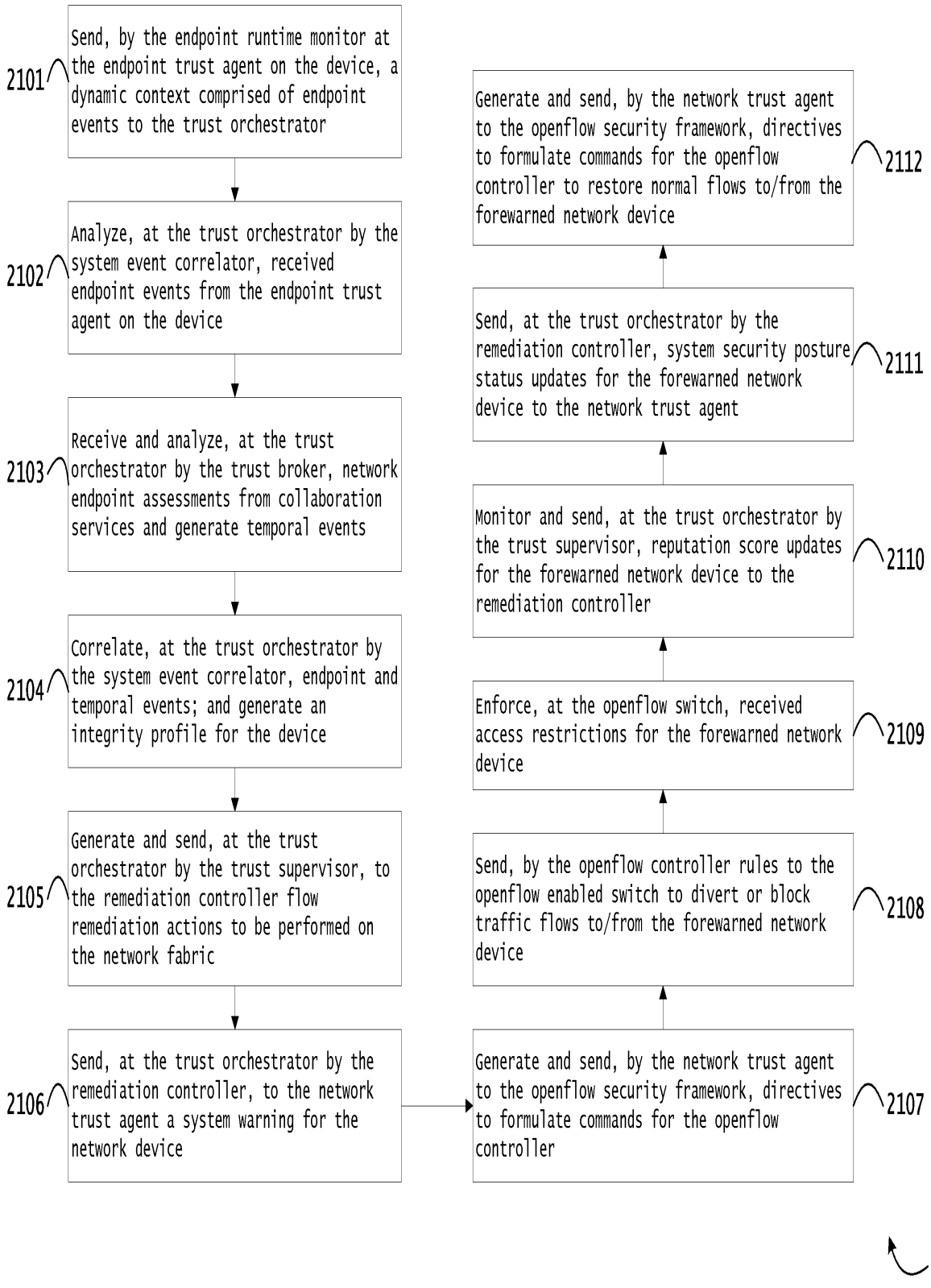

2101
Send, by the endpoint runtime monitor at the endpoint trust agent on the device, a dynamic context comprised of endpoint events to the trust orchestrator
2102
Analyze, at the trust orchestrator by the system event correlator, received endpoint events from the endpoint trust agent on the device
2103
Receive and analyze, at the trust orchestrator by the trust broker, network endpoint assessments from collaboration services and generate temporal events
2104
Correlate, at the trust orchestrator by the system event correlator, endpoint and temporal events; and generate an integrity profile for the device
2105
Generate and send, at the trust orchestrator by the trust supervisor, to the remediation controller flow remediation actions to be performed on the network fabric
2106
Send, at the trust orchestrator by the remediation controller, to the network trust agent a system warning for the network device
2107
Generate and send, by the network trust agent to the openflow security framework, directives to formulate commands for the openflow controller
2108
Send, by the openflow controller rules to the openflow enabled switch to divert or block traffic flows to/from the forewarned network device
2109
Enforce, at the openflow switch, received access restrictions for the forewarned network device
2110
Monitor and send, at the trust orchestrator by the trust supervisor, reputation score updates for the forewarned network device to the remediation controller
2111
Send, at the trust orchestrator by the remediation controller, system security posture status updates for the forewarned network device to the network trust agent
2112
Generate and send, by the network trust agent to the openflow security framework, directives to formulate commands for the openflow controller to restore normal flows to/from the forewarned network device
2100

FIG. 22

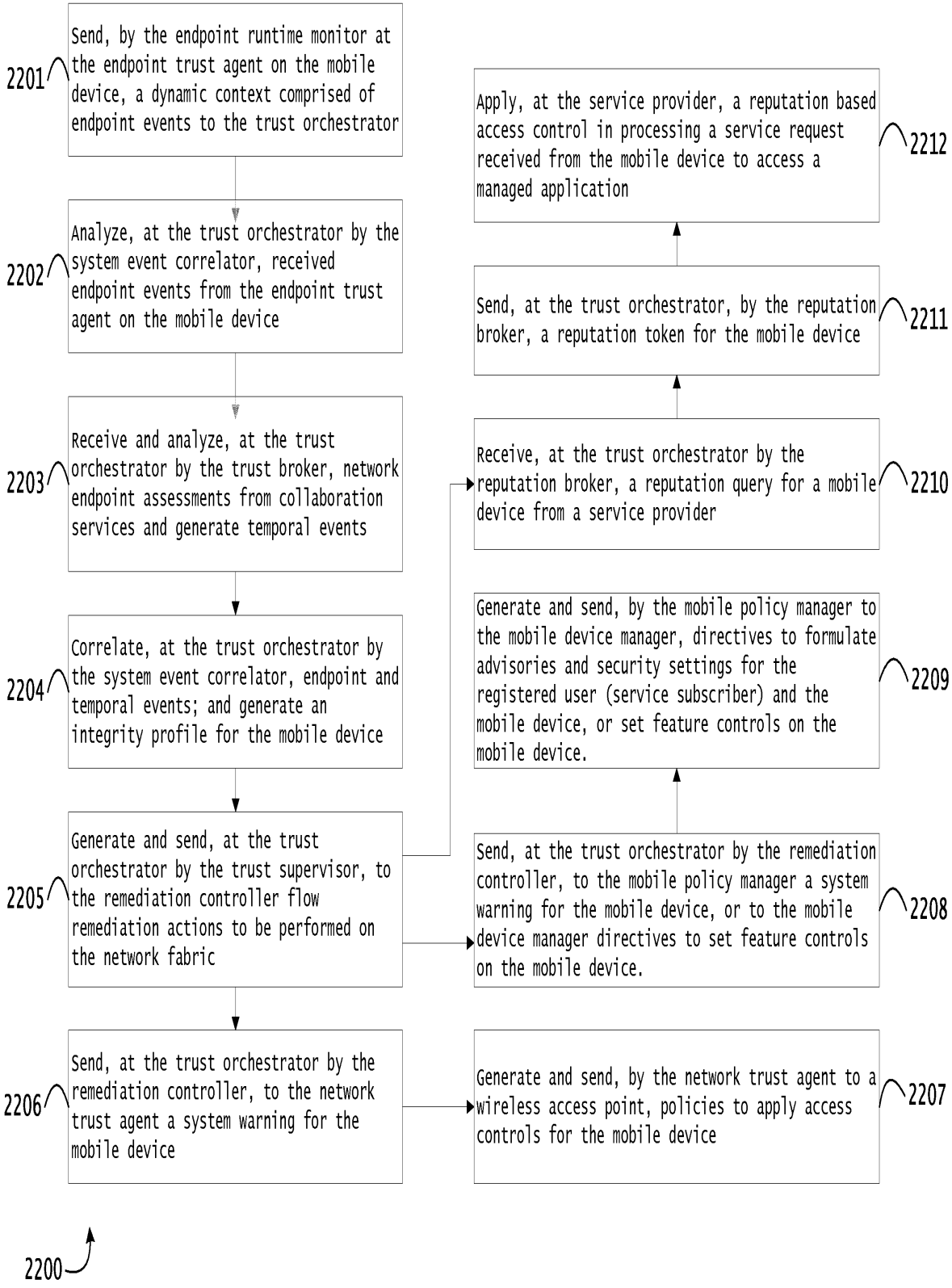

2201
Send, by the endpoint runtime monitor at the endpoint trust agent on the mobile device, a dynamic context comprised of endpoint events to the trust orchestrator
2202
Analyze, at the trust orchestrator by the system event correlator, received endpoint events from the endpoint trust agent on the mobile device
2203
Receive and analyze, at the trust orchestrator by the trust broker, network endpoint assessments from collaboration services and generate temporal events
2204
Correlate, at the trust orchestrator by the system event correlator, endpoint and temporal events; and generate an integrity profile for the mobile device
2205
Generate and send, at the trust orchestrator by the trust supervisor, to the remediation controller flow remediation actions to be performed on the network fabric
2206
Send, at the trust orchestrator by the remediation controller, to the network trust agent a system warning for the mobile device
2207
Generate and send, by the network trust agent to a wireless access point, policies to apply access controls for the mobile device
2208
Send, at the trust orchestrator by the remediation controller, to the mobile policy manager a system warning for the mobile device, or to the mobile device manager directives to set feature controls on the mobile device.
2209
Generate and send, by the mobile policy manager to the mobile device manager, directives to formulate advisories and security settings for the registered user (service subscriber) and the mobile device, or set feature controls on the mobile device.
2210
Receive, at the trust orchestrator by the reputation broker, a reputation query for a mobile device from a service provider
2211
Send, at the trust orchestrator, by the reputation broker, a reputation token for the mobile device
2212
Apply, at the service provider, a reputation based access control in processing a service request received from the mobile device to access a managed application
2200

FIG. 23

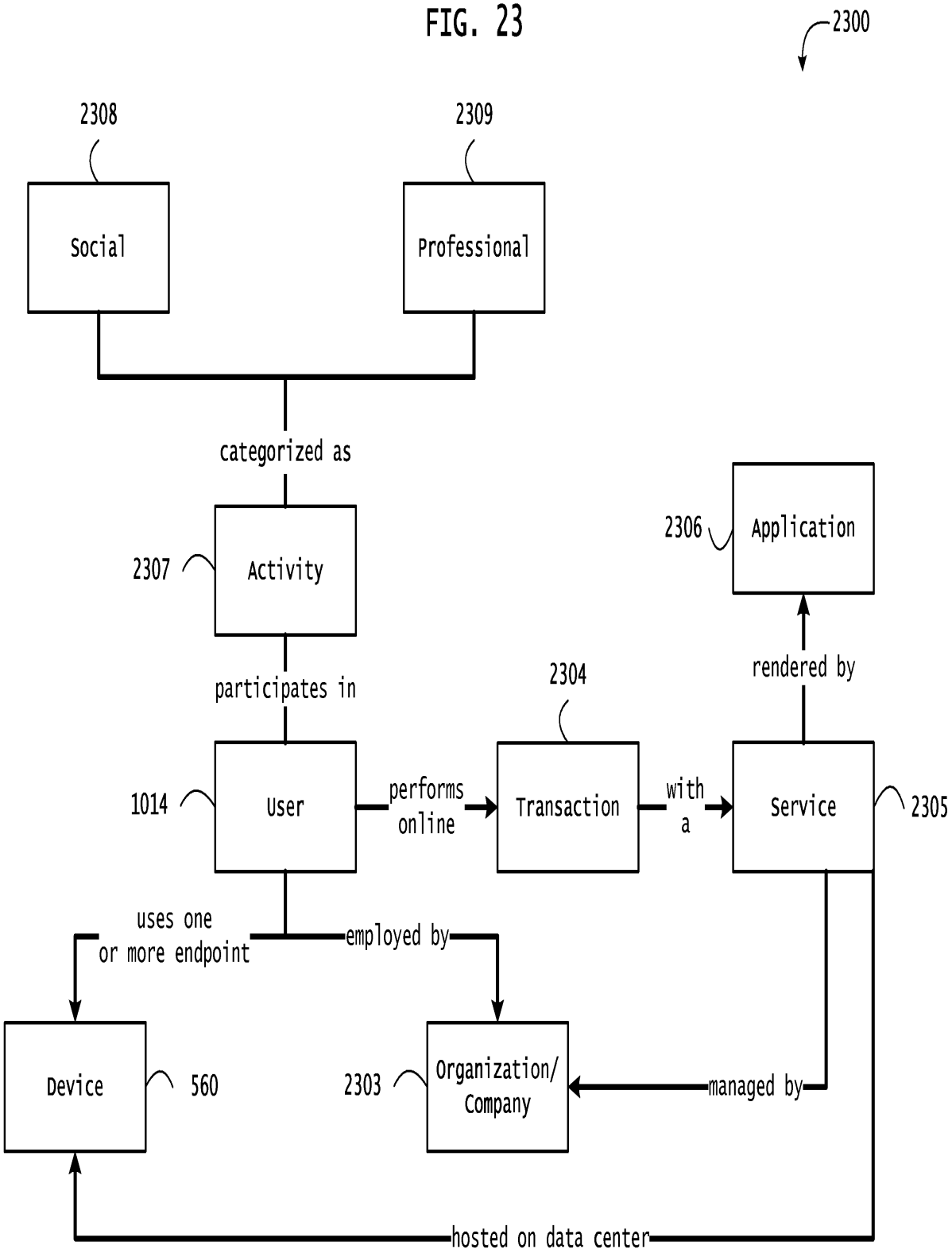
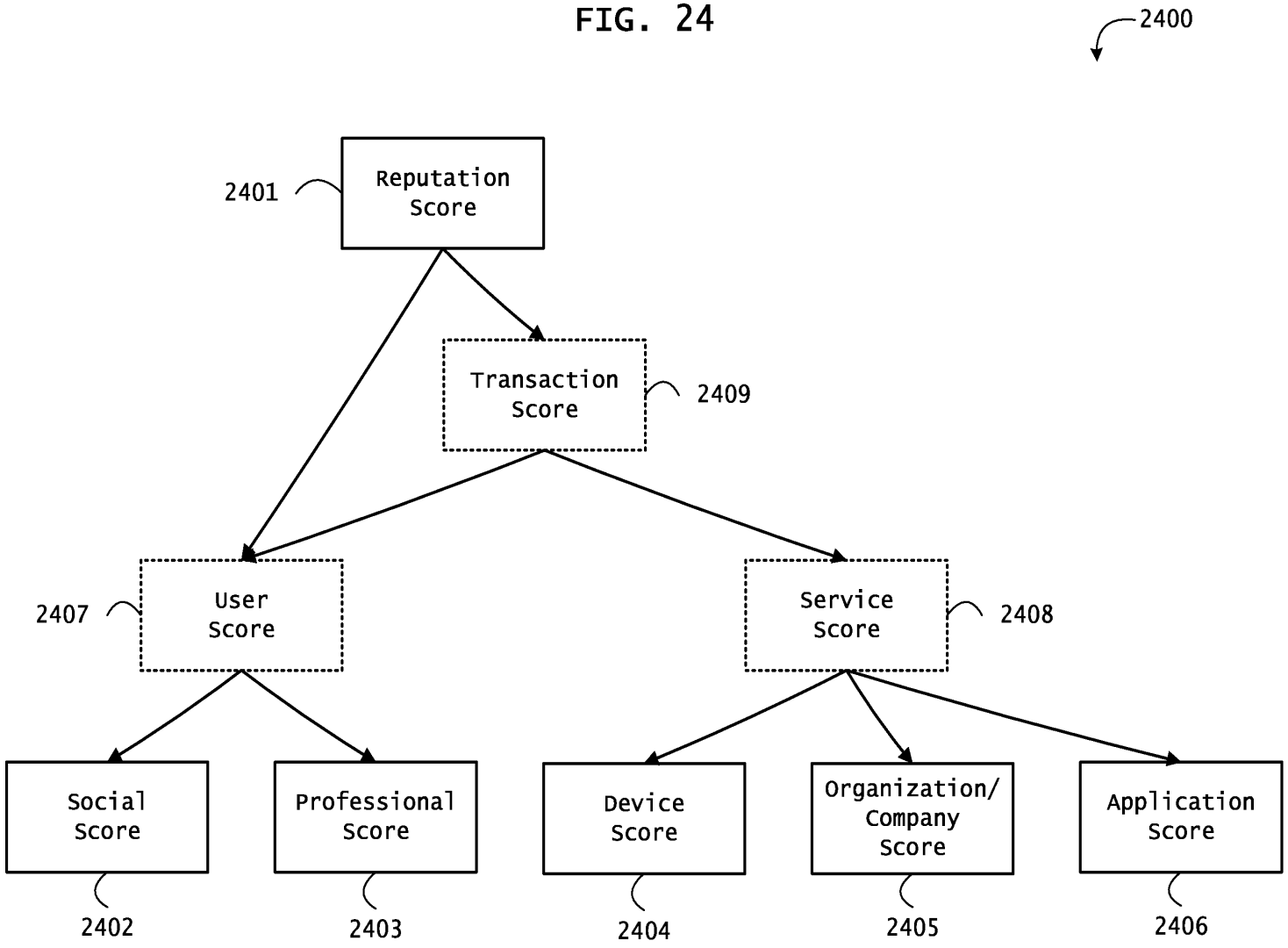
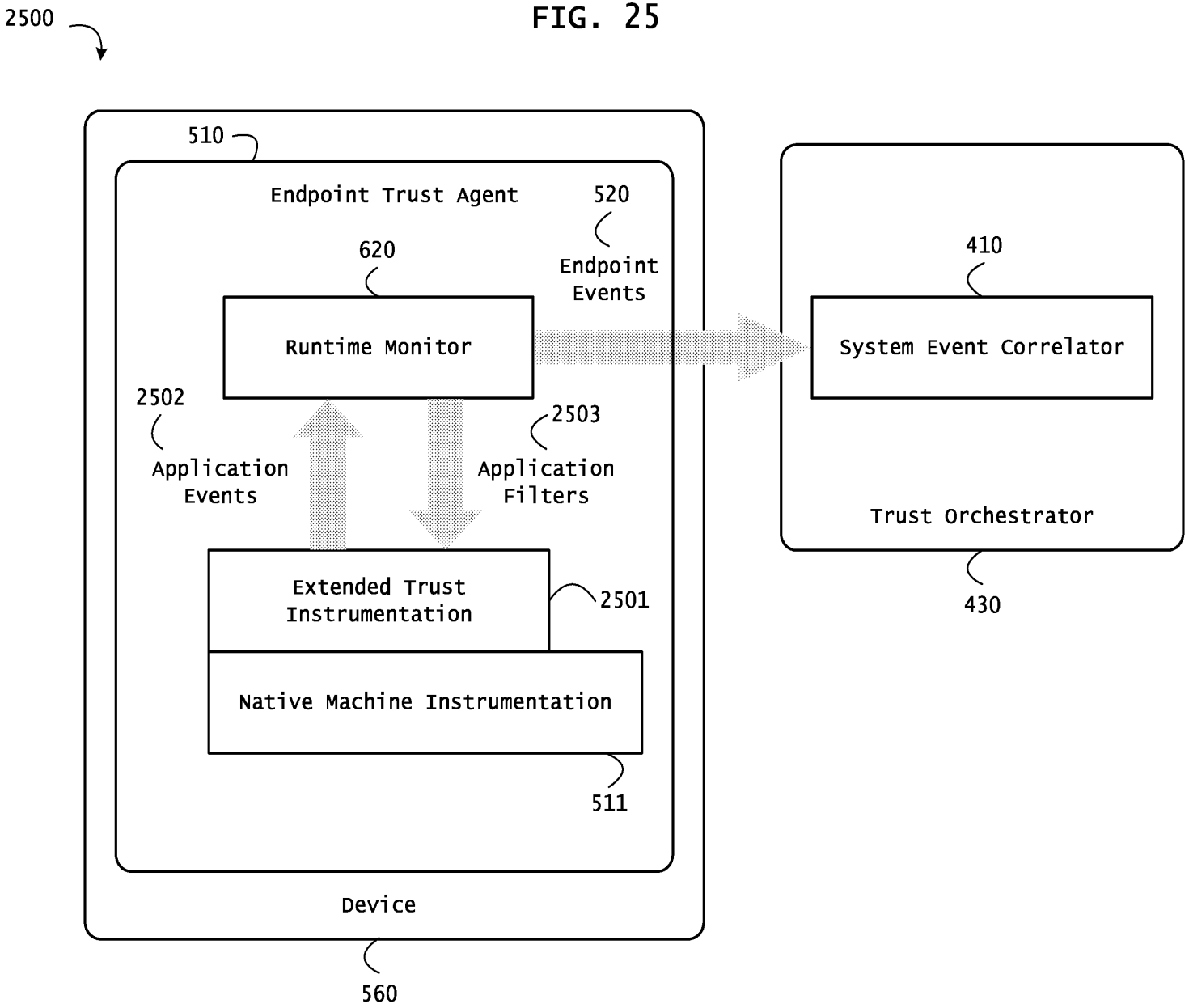

2300
2308
2309
Social
Professional
categorized as
2307
Activity
2306
Application
participates in
rendered by
2304
1014
User
performs online
Transaction
with a
Service
2305
uses one or more endpoint
employed by
Device
560
2303
Organization/ Company
managed by
hosted on data center

FIG. 24



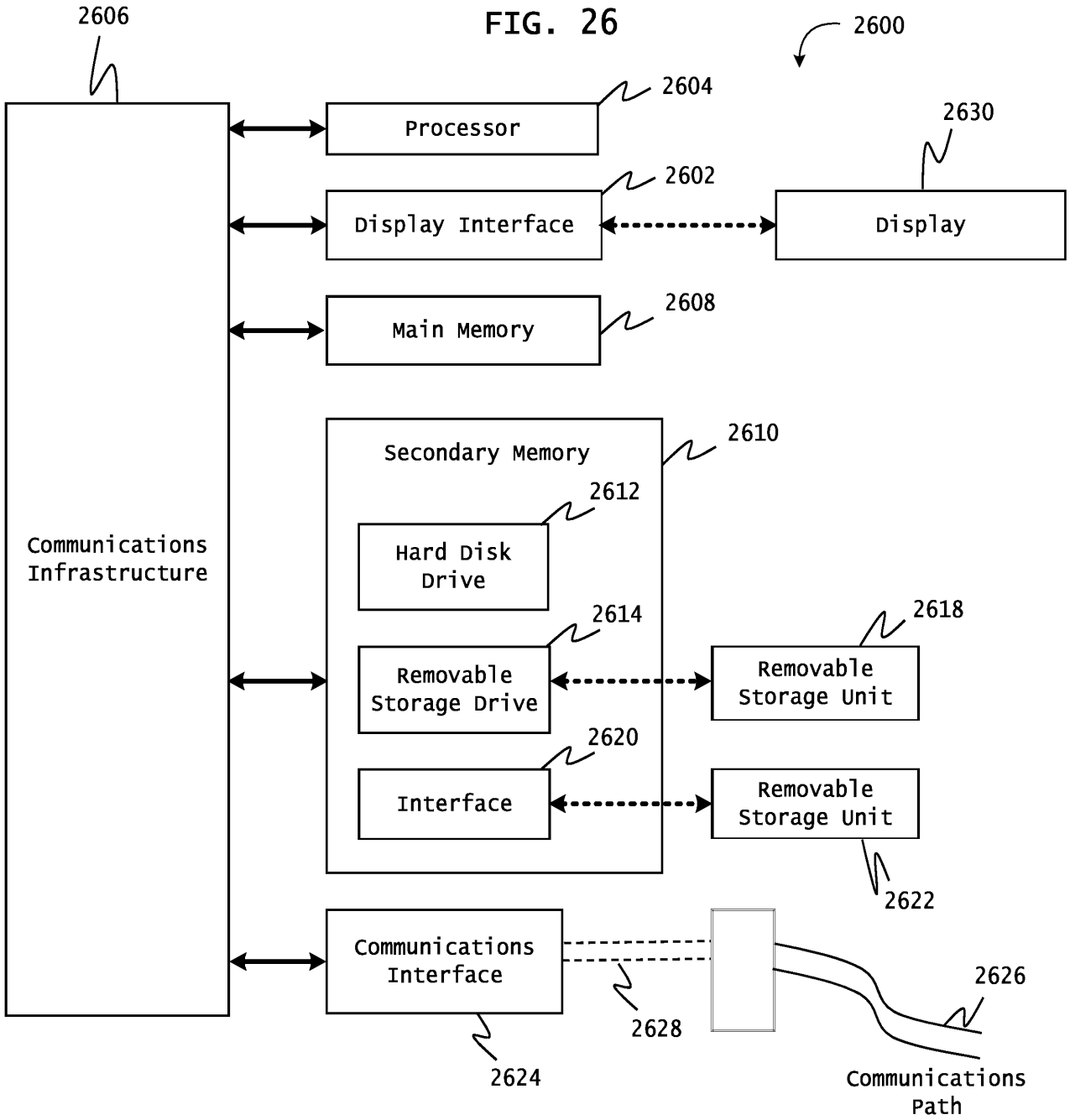
IPR2023-01466
CrowdStrike EX1002 Page 438

FIG. 25



IPR2023-01466
CrowdStrike EX1002 Page 439

FIG. 26



IPR2023-01466
CrowdStrike EX1002 Page 440

COMBINED DECLARATION AND POWER OF ATTORNEY FOR UTILITY OR DESIGN PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

SYSTEMS AND METHODS FOR THREAT IDENTIFICATION AND REMEDIATION

the application of which **(check only one item below)**:

☐ is attached hereto.

☐ was filed as United States Patent application Number _____ on _____ and was amended on _____ (if applicable).

☐ was filed as PCT International application Number _____ on _____ and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified application, including the claims, and drawings (if any), as amended by any amendment referred to above.

I acknowledge the duty to disclose to the Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §§ 119 (a)-(d), 172 or 365(a) of any foreign application(s) for patent or inventor's certificate or of any international (PCT) application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international (PCT) application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

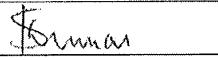
PRIOR FOREIGN/PCT APPLICATION(S) AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. §§119(a)-(d), 172 or 365(a):				
COUNTRY (if PCT, indicate "PCT")	APPLICATION NUMBER	DATE OF FILING (MM/DD/YYYY)	PRIORITY CLAIMED UNDER 35 U.S.C. §§119, 172 OR 365(a)	
			Yes	No

(7/06)

I hereby appoint the attorneys and agents associated with the following PTO Customer Number of Buchanan Ingersoll & Rooney PC to prosecute said application and to transact all business in the Patent and Trademark Office connected therewith and to file, prosecute and transact all business in connection with international applications directed to said invention:

Customer Number **21839**

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

FULL NAME OF SOLE OR FIRST INVENTOR	Srinivas KUMAR
Signature	
Date	7/25/2012
Residence (City, State, Country)	Cupertino, CA, US
Citizenship	US
Mailing Address	10926 Northridge Square
City, State, ZIP, Country	Cupertino, CA 95014, US
FULL NAME SECOND INVENTOR, IF ANY	Dennis POLLUTRO
Signature	
Date	
Residence (City, State, Country)	Clymer, NY, US
Citizenship	US
Mailing Address	8613 Knowlton Road
City, State, ZIP, Country	Clymer, NY 14724, US

COMBINED DECLARATION AND POWER OF ATTORNEY FOR UTILITY OR DESIGN PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

SYSTEMS AND METHODS FOR THREAT IDENTIFICATION AND REMEDIATION

the application of which **(check only one item below)**:

- ☐ is attached hereto.
- ☐ was filed as United States Patent application Number _____ on _____ and was amended on _____ (if applicable).
- ☐ was filed as PCT International application Number _____ on _____ and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified application, including the claims, and drawings (if any), as amended by any amendment referred to above.

I acknowledge the duty to disclose to the Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §§ 119 (a)-(d), 172 or 365(a) of any foreign application(s) for patent or inventor's certificate or of any international (PCT) application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international (PCT) application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

PRIOR FOREIGN/PCT APPLICATION(S) AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. §§119(a)-(d), 172 or 365(a):				
COUNTRY (If PCT, indicate "PCT")	APPLICATION NUMBER	DATE OF FILING (MM/DD/YYYY)	PRIORITY CLAIMED UNDER 35 U.S.C. §§119, 172 OR 365(a)	
			Yes	No

IPR2023-01466
CrowdStrike EX1002 Page 443

I hereby appoint the attorneys and agents associated with the following PTO Customer Number of Buchanan Ingersoll & Rooney PC to prosecute said application and to transact all business in the Patent and Trademark Office connected therewith and to file, prosecute and transact all business in connection with international applications directed to said invention:

Customer Number **21839**

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

FULL NAME OF SOLE OR FIRST INVENTOR	Srinivas KUMAR
Signature	
Date	
Residence (City, State, Country)	Cupertino, CA, US
Citizenship	US
Mailing Address	10926 Northridge Square
City, State, ZIP, Country	Cupertino, CA 95014, US
FULL NAME SECOND INVENTOR, IF ANY	Dennis POLUTRO
Signature	
Date	7/26/12
Residence (City, State, Country)	Clymer, NY, US
Citizenship	US
Mailing Address	8613 Knowlton Road
City, State, ZIP, Country	Clymer, NY 14724, US

IPR2023-01466
CrowdStrike EX1002 Page 444

DocCode - SCORE

SCORE Placeholder Sheet for IFW Content

Application Number: 13559766 Document Date: 7/27/2012

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

- Drawings – Other than Black and White Line Drawings

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

To access the documents in the SCORE database, refer to instructions developed by SIRA.

At the time of document entry (noted above):

- Examiners may access SCORE content via the eDAN interface.
- Other USPTO employees can bookmark the current SCORE URL (http://es/ScoreAccessWeb/).
- External customers may access SCORE content via the Public and Private PAIR interfaces.

Form Revision Date: February 8, 2006