Placeholder Sheet for Supplemental Content

Application Number: 18892283 Document Date: 09/20/2024

The presence of this form indicates that the following document type was received in electronic format on the date identified above. This document is stored separately from the typical case contents which are stored in image format.

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded and no paper documents or physical media exist.

- Drawing

At the time of document entry (noted above):

- USPTO employees may access this supplemental content via Docket Application Viewer (DAV) or Supplemental Content Viewer (SCV).
- External customers may access this supplemental content via Patent Center.

MICROSOFT CORP.
EXHIBIT 1002

Galvin Patent Law LLC
PO Box 2360
Silverdale, WA 98383
360-692-3078 (Work)
360-692-2617 (Fax)

RECEIVED
CENTRAL FAX CENTER
SEP 20 2024

facsimile transmittal

To:	USPTO	**Fax:**	571-273-8300
From:	Brian Galvin, Galvin Patent Law LLC	**Date:**	9/20/2024
Re:	18/892,283	**Pages:**	4
CC:			

☐ **Urgent** ☐ **For Review** ☐ **Please Comment** ☐ **Please Reply** ☐ **Please Recycle**

Notes: Applicant filed the following as Prioritized Examination application on Sept 20, 2024:

Docket No. 15388FT
Serial No. 18,892,283
Confirmation #: 7526
Patent Center #: 67266989

Applicant paid the following regular, undiscounted fees at the time of initial filing:

Request for Prioritized Examination	Fee Code 1817	$4200
Basic Filing Fee - Utility	Fee Code 1011	$320
Utility Patent Application Search Fee	Fee Code 1111	$700
Patent Application Examination Fee	Fee Code 1311	$800
Processing Fee Except in Provisional Applications	Fee Code 1830	$140

Application had 25 claims total. Applicant failed to pay the following fees:
(5) claims in excess of 20 Fee Code 1202 **Amount to pay $500**

Please find attached a Credit Card Authorization for the above-referenced matter for the $500 excess claims fee. Please process the fee payment as soon as is practicable.

Applicant is including the eFiling Acknowledgement and the ePayment Acknowledgement for your reference.

RECEIVED
CENTRAL FAX CENTER
SEP 20 2024

fax

Recipient Information

To: USPTO - MAIN FAX
Company: USPTO
Fax #: 15712738300

Sender Information

From: BRIAN GALVIN
Company: Galvin Patent Law LLC
Email address: USPTO@galvinpatentlaw.com (from 24.113.87.1)
Phone #: 3603629171
Sent on: Friday, September 20 2024 at 11:22 PM EDT

This fax was sent using the FaxZero.com fax service. Please send your response directly to the sender, not to FaxZero.

FaxZero.com has a zero tolerance policy for abuse and junk faxes. If this fax is spam or abusive, please e-mail support@faxzero.com or send a fax to 855-330-1238, or phone 707-400-6360. Specify fax #35187542. We will add your fax number to the block list.

RECEIVED
CENTRAL FAX CENTER
SEP 20 2024

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/892,283	**09/20/2024 09:26:06 PM Z ET**	**15388FT**

Title of Invention

CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	7526	FILED BY	Aura Morrey
PATENT CENTER #	67266989	FILING DATE	-
CUSTOMER #	82318	FIRST NAMED INVENTOR	Jason Crabtree
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Brian Galvin

Documents

TOTAL DOCUMENTS: 15

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
240920_15388FT_ADS_AS_FILED.pdf	10	Application Data Sheet	2225 KB
240920_15388FT_TrackOne Request_AS_FILED.pdf	2	Track One Request	112 KB
240920_15388FT_Final_AS_FILED-APP.TEXT.docx	55	Application body structured text document	65 KB
240920_15388FT_Drawings_AS_FILED.pdf	36	Drawings-only black and white line drawings	11486 KB
240920_15388FT_QOMPLX LLC_POA_AS_FILED.pdf	1	Power of Attorney	135 KB
240920_15388FT_Declaratio n_Crabtree_AS_FILED.pdf	1	Oath or Declaration filed	114 KB

240920_15388FT_Declaration_Kelley_FOR AS_FILED.pdf	1	Oath or Declaration filed	121 KB
240920_15388FT_Declaration_Sellers_AS_FILED.pdf	1	Oath or Declaration filed	117 KB
240920_15388FT_IDS_AS_FILED.pdf	11	Information Disclosure Statement (IDS) Form (SB08)	1333 KB
240920_15388FT_NPL_Eberle_Incremental Anomaly Detection in Graphs_AS_FILED.pdf	8	Non Patent Literature	7483 KB
240920_15388FT_NPL_Huang_Comparison of Value at Risk Approaches_AS_FILED.pdf	34	Non Patent Literature	10606 KB
240920_15388FT_NPL_Marozzo_P2P MapReduce Parallel Data Processing...Environments_AS_FILED.pdf	21	Non Patent Literature	16172 KB
240920_15388FT_IntCommAuth_AS_FILED.pdf	2	Internet Communications Authorization	83 KB
240920_15388FT_NPL_Simonian_Robust Value at Risk_AS_FILED.pdf	3	Non Patent Literature	608 KB
240920_15388FT_Final_AS_FILED.pdf	55	Auxiliary PDF of Application	275 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
240920_15388FT_ADS_AS_FILED.pdf	8A170F2B839C5295B480A60375FDA4AE91580B24FA6C1066B3680FFC0CD98F0A61439E2E0D66EC585191AAA1679E523B4684C25EDA5C3F589F589C30688CED7C
240920_15388FT_TrackOneRequest_AS_FILED.pdf	24F90B30F92A47B0F7A3FB489FCFE19DB7AA769C454BD897FE8A979EA11ED78A069A6A4497518AC76AEFB509165A867C10BB19998C2F2475DC82F4785EEDFA6D
240920_15388FT_Final_AS_FILED-APP.TEXT.docx	35EE9B96F5FA00FD6B1266DBF1BE29C4A13AD44299DB514497759F79A2CB11AB6E58852B14845693AA552867B59E3265FD7473B9321022D018333AD6EE0599DE

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

RECEIVED
CENTRAL FAX CENTER
SEP 20 2024

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/892,283	**09/20/2024 09:26:06 PM Z ET**	**15388FT**

Title of Invention

CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	7526	FILED BY	Aura Morrey
PATENT CENTER #	67266989	AUTHORIZED BY	Brian Galvin
CUSTOMER #	82318	FILING DATE	-
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	Jason Crabtree

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 1009	**E20249JL27129906**	**Aura Morrey**

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
1830	PROCESSING FEE, EXCEPT IN PROVISIONAL APPLICATIONS	140.00	1	140.00
1817	REQUEST FOR PRIORITIZED EXAMINATION	4200.00	1	4200.00
1111	UTILITY PATENT APPL. SEARCH FEE	700.00	1	700.00
1011	BASIC FILING FEE - UTILITY (PAPER FILING ALSO REQUIRES NON-ELECTRONIC FILING FEE UNDER 1.16(T))	320.00	1	320.00
1311	PATENT APPL. EXAMINATION FEE	800.00	1	800.00
			TOTAL	**$6,160.00**

PTO/AIA/01 (06-12)
Approved for use through 11/30/2020. 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.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [x] The attached application, or
- [ ] United States application or PCT international application number _____

filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Richard Kelley Date (Optional) :_____

Signature: Richard Kelley

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. 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 1 minute 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/AIA/01 (06-12)
Approved for use through 11/30/2020. 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.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [x] The attached application, or
- [ ] United States application or PCT international application number _____

filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Andrew Sellers Date (Optional) :_____

Signature: Andrew Sellers

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. 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 1 minute 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.

Doc ID: 86b050c96467e80244e1af4c79e0a77605d374bd

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/892,283	**09/20/2024 09:26:06 PM Z ET**	**15388FT**

Title of Invention

CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	7526	FILED BY	Aura Morrey
PATENT CENTER #	67266989	FILING DATE	-
CUSTOMER #	82318	FIRST NAMED INVENTOR	Jason Crabtree
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Brian Galvin

Documents

TOTAL DOCUMENTS: 15

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
240920_15388FT_ADS_AS_FILED.pdf	10	Application Data Sheet	2225 KB
240920_15388FT_TrackOne Request_AS_FILED.pdf	2	Track One Request	112 KB
240920_15388FT_Final_AS_FILED-APP.TEXT.docx	55	Application body structured text document	65 KB
240920_15388FT_Drawings_AS_FILED.pdf	36	Drawings-only black and white line drawings	11486 KB
240920_15388FT_QOMPLX LLC_POA_AS_FILED.pdf	1	Power of Attorney	135 KB
240920_15388FT_Declaration_Crabtree_AS_FILED.pdf	1	Oath or Declaration filed	114 KB

240920_15388FT_Declaration_Kelley_FOR AS_FILED.pdf	1	Oath or Declaration filed	121 KB
240920_15388FT_Declaration_Sellers_AS_FILED.pdf	1	Oath or Declaration filed	117 KB
240920_15388FT_IDS_AS_FILED.pdf	11	Information Disclosure Statement (IDS) Form (SB08)	1333 KB
240920_15388FT_NPL_Eberle_Incremental Anomaly Detection in Graphs_AS_FILED.pdf	8	Non Patent Literature	7483 KB
240920_15388FT_NPL_Huang_Comparison of Value at Risk Approaches_AS_FILED.pdf	34	Non Patent Literature	10606 KB
240920_15388FT_NPL_Marozzo_P2P MapReduce Parallel Data Processing...Environments_AS_FILED.pdf	21	Non Patent Literature	16172 KB
240920_15388FT_IntCommAuth_AS_FILED.pdf	2	Internet Communications Authorization	83 KB
240920_15388FT_NPL_Simonian_Robust Value at Risk_AS_FILED.pdf	3	Non Patent Literature	608 KB
240920_15388FT_Final_AS_FILED.pdf	55	Auxiliary PDF of Application	275 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
240920_15388FT_ADS_AS_FILED.pdf	8A170F2B839C5295B480A60375FDA4AE91580B24FA6C1066B3680FFC0CD98F0A61439E2E0D66EC585191AAA1679E523B4684C25EDA5C3F589F589C30688CED7C
240920_15388FT_TrackOneRequest_AS_FILED.pdf	24F90B30F92A47B0F7A3FB489FCFE19DB7AA769C454BD897FE8A979EA11ED78A069A6A4497518AC76AEFB509165A867C10BB19998C2F2475DC82F4785EEDFA6D
240920_15388FT_Final_AS_FILED-APP.TEXT.docx	35EE9B96F5FA00FD6B1266DBF1BE29C4A13AD44299DB514497759F79A2CB11AB6E58852B14845693AA552867B59E3265FD7473B9321022D018333AD6EE0599DE

240920_15388FT_Drawings_AS_FILED.pdf	4B7066B4ABEF96D62D544847324BE30C155E13FD4DCE2957C98E267107E1B586AFFC299796B6D834CDFC5BB6EC45C86540C13BEBC72BE5BFDB50C7C3D4C2791D
240920_15388FT_QOMPLX LLC_POA_AS_FILED.pdf	EDC005E6378BCF5F1E3532F6F080D77BF62CF956498DCFCF05F68CF3E6FE88E498D69439B5E1B5BEC51EFDC1BB57AB8C5733AC2A8E33F048C1244E71134F132C
240920_15388FT_Declaration_Crabtree_AS_FILED.pdf	920F6E96B78F1534E15E4FA2B5A1B009F68F4A3AD8C0E2113EA268B67B05EFBA99D9EC55ADF346DB01729E0A395DB8D83CAE2E8709B5F31482387C2B51C4853A
240920_15388FT_Declaration_Kelley_FOR AS_FILED.pdf	BE6CA5026762012A677782554B34A4D887A059685E07CA57A9186DAAD3E05509B6C4B52CDF4DC9F74F2F447A277A453B12BDF94D423E4BE3805E17EB930191DE
240920_15388FT_Declaration_Sellers_AS_FILED.pdf	E9D89135F36B495670D6AC8DFFD332909FB892A01F55AD103B9928D53A13CE162A51A47861904FE4C3A3D9120F0B327DA85674035D199F09611A2728262D51F7
240920_15388FT_IDS_AS_FILED.pdf	A452A056EB0E5453F6CB5F9D7347A1C0D618296AE2F0DFD77C15C847E93EECF07431A4F3D7DDB7A0AC48A9CDD739C9FA3FE079D7847A3CA3DF9766BC49322D74
240920_15388FT_NPL_Eberle_Incremental Anomaly Detection in Graphs_AS_FILED.pdf	399E59134BB3EF0BA5AA42F342D4976C7109003CB8FDE2EFE6DB0F6448B403D506E2B212E6C0AA823999B44A13720C59CFC239DFB5FDD134B8E4DB84BADAB056
240920_15388FT_NPL_Huang_Comparison of Value at Risk Approaches_AS_FILED.pdf	8E90B3CCD95F8E55857D086509B80F0FF6F28D125F3D69724ACF3272F8742003AF31C5CAAF8E8E11D35002797D40BF7DC988E6BE932BA9D3351A1A559F88B3A8
240920_15388FT_NPL_Marozzo_P2P MapReduce Parallel Data Processing...Environments_AS_FILED.pdf	817C3F53CF2F765BCC8C6D969AE1E0119BDCA3D9198A1AE08E10646F11FB23D4591A766BDFE46139D154AC357375DCF4B0A6E70F964272314FA4927E04BB76CD
240920_15388FT_IntCommAuth_AS_FILED.pdf	E6E2B6BDD1C030625396072AFF9DF42365CB0F2F4B247DE9559A7416CE73737C5EBED3232C79EA0492592FBCD18E086B0305E9B02713DB5683811AE67298FECA
240920_15388FT_NPL_Simonian_Robust Value at Risk_AS_FILED.pdf	7F0E2610827EF5534F3B356EF8F6DBF58714E4557D2EFDF079D938C2BF3EC1FDE4D3847D45F221F6804E036788ECF4C6CDBC90299A8210071FA3C94C42F46AAD
240920_15388FT_Final_AS_FILED.pdf	304749CD8DFD3D70E3340A405EA3C68F03476912688CF47797071D63FB2270ABF7B97FF79E0A52D6E27D2090105EFF2938725DCE6FC373085FFC59ACD35D6E0E

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 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.

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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	15388FT
	Application Number	
Title of Invention	CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2:

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Jason		Crabtree	

Residence Information (Select One) ◉ US Residency ◯ Non US Residency ◯ Active US Military Service

City	Vienna	State/Province	VA	Country of Residence	US

Mailing Address of Inventor:

Address 1	10208 Westford Drive		
Address 2			
City	Vienna	State/Province	VA
Postal Code	22182	Country	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Andrew		Sellers	

Residence Information (Select One) ◉ US Residency ◯ Non US Residency ◯ Active US Military Service

City	Monument	State/Province	CO	Country of Residence	US

Mailing Address of Inventor:

Address 1	16258 Windsor Creek Dr.		
Address 2			
City	Monument	State/Province	CO
Postal Code	80132	Country	US

Inventor 3 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Richard		Kelley	

Residence Information (Select One) ◉ US Residency ◯ Non US Residency ◯ Active US Military Service

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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	15388FT
	Application Number	
Title of Invention	CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION	

City	Woodbridge	State/Province	VA	Country of Residence i	US

Mailing Address of Inventor:

Address 1	12904 Valleywood Dr		
Address 2			
City	Woodbridge	**State/Province**	VA
Postal Code	22192	**Country** i	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	82318		
Email Address	uspto@galvinpatentlaw.com	Add Email	Remove Email

Application Information:

Title of the Invention	CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION		
Attorney Docket Number	15388FT	**Small Entity Status Claimed**	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	36	**Suggested Figure for Publication (if any)**	1

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country i

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	15388FT
	Application Number	
Title of Invention	CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION	

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	82318		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Continuation of	17237346	2021-04-22

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
17237346	Continuation in part of	16777270	2020-01-30	11025674	2021-06-01

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
16777270	Continuation in part of	16720383	2019-12-19	10944795	2021-03-09

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
16720383	Continuation of	15823363	2017-11-27	10560483	2020-02-11

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
15823363	Continuation in part of	15725274	2017-10-04	10609079	2020-03-31

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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	15388FT
	Application Number	
Title of Invention	CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION	

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
15725274	Continuation in part of	15655113	2017-07-20	10735456	2020-08-04
Prior Application Status	Abandoned				Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)		
15655113	Continuation in part of	15616427	2017-06-07		
Prior Application Status	Abandoned				Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)		
15616427	Continuation in part of	14925974	2015-10-28		
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
15655113	Continuation in part of	15237625	2016-08-15	10248910	2019-04-02
Prior Application Status	Abandoned				Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)		
15237625	Continuation in part of	15206195	2016-07-08		
Prior Application Status	Abandoned				Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)		
15206195	Continuation in part of	15186453	2016-06-18		
Prior Application Status	Abandoned				Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)		
15186453	Continuation in part of	15166158	2016-05-26		
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
15166158	Continuation in part of	15141752	2016-04-28	10860962	2020-12-08
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
15141752	Continuation in part of	15091563	2016-04-05	10204147	2019-02-12

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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	15388FT
	Application Number	
Title of Invention	CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION	

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
15141752	Continuation in part of	14986536	2015-12-31	10210255	2019-02-19

Prior Application Status	Abandoned		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
15141752	Continuation in part of	14925974	2015-10-28

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)[i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Remove

Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	15388FT
	Application Number	
Title of Invention	CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION	

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	15388FT
	Application Number	
Title of Invention	CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION	

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1 Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section. Clear

- (●) Assignee
- ( ) Legal Representative under 35 U.S.C. 117
- ( ) Joint Inventor
- ( ) Person to whom the inventor is obligated to assign.
- ( ) Person who shows sufficient proprietary interest

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor:

If the Applicant is an Organization check here. [X]

Organization Name	QOMPLX LLC		
Mailing Address Information For Applicant:			
Address 1	1900 Reston Metro Plaza		
Address 2	Ste. 600		
City	Reston	**State/Province**	VA
Country	US	Postal Code	20190
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	15388FT
	Application Number	
Title of Invention	CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION	

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).**

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/BRIAN R. GALVIN/			Date (YYYY-MM-DD)	2024-09-20
First Name	Brian	Last Name	Galvin	Registration Number	50966

Additional Signature may be generated within this form by selecting the Add button. Add

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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	15388FT
	Application Number	
Title of Invention	CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION	

This collection of information is required by 37 CFR 1.76. 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 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet 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 records.

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 CooperationTreaty.

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.

PTO/AIA/82B (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
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

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 82,318

OR

☐ I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:

☑ The address associated with the above-mentioned Customer Number

OR

☐ The address associated with Customer Number:

OR

Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

QOMPLX LLC

☐ Inventor or Joint Inventor (title not required below)

☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)

☑ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature	Jason Crabtree	Date (Optional)	
Name	Jason Crabtree		
Title	CEO		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☑ Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. 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 3 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.

CERTIFICATION AND REQUEST FOR PRIORITIZED EXAMINATION UNDER 37 CFR 1.102(e) (Page 1 of 1)

First Named Inventor:	Jason Crabtree	Nonprovisional Application Number (if known):	
Title of Invention:	CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION		

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS PRIORITIZED EXAMINATION FOR THE ABOVE-IDENTIFIED APPLICATION.

1. The processing fee set forth in 37 CFR 1.17(i)(1) and the prioritized examination fee set forth in 37 CFR 1.17(c) have been filed with the request. The publication fee requirement is met because that fee, set forth in 37 CFR 1.18(d), is currently $0. The basic filing fee, search fee, and examination fee are filed with the request or have been already been paid. I understand that any required excess claims fees or application size fee must be paid for the application.

2. I understand that the application may not contain, or be amended to contain, more than four independent claims, more than thirty total claims, or any multiple dependent claims, and that any request for an extension of time will cause an outstanding Track I request to be dismissed.

3. The applicable box is checked below:

I. ☑ Original Application (Track One) - Prioritized Examination under § 1.102(e)(1)

i. (a) The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a). This certification and request is being filed with the utility application via EFS-Web.

---OR---

(b) The application is an original nonprovisional plant application filed under 35 U.S.C. 111(a). This certification and request is being filed with the plant application in paper.

ii. An executed inventor's oath or declaration under 37 CFR 1.63 or 37 CFR 1.64 for each inventor, **or** the application data sheet meeting the conditions specified in 37 CFR 1.53(f)(3)(i) is filed with the application.

II. ☐ Request for Continued Examination - Prioritized Examination under § 1.102(e)(2)

i. A request for continued examination has been filed with, or prior to, this form.
ii. If the application is a utility application, this certification and request is being filed via EFS-Web.
iii. The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a), or is a national stage entry under 35 U.S.C. 371.
iv. This certification and request is being filed prior to the mailing of a first Office action responsive to the request for continued examination.
v. No prior request for continued examination has been granted prioritized examination status under 37 CFR 1.102(e)(2).

Signature /BRIAN R. GALVIN/	Date September 20, 2024
Name (Print/Typed) Brian R. Galvin	Practitioner Registration Number 50966

Note: *This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. Submit multiple forms if more than one signature is required.**

☑ *Total of 1 forms are submitted.

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.

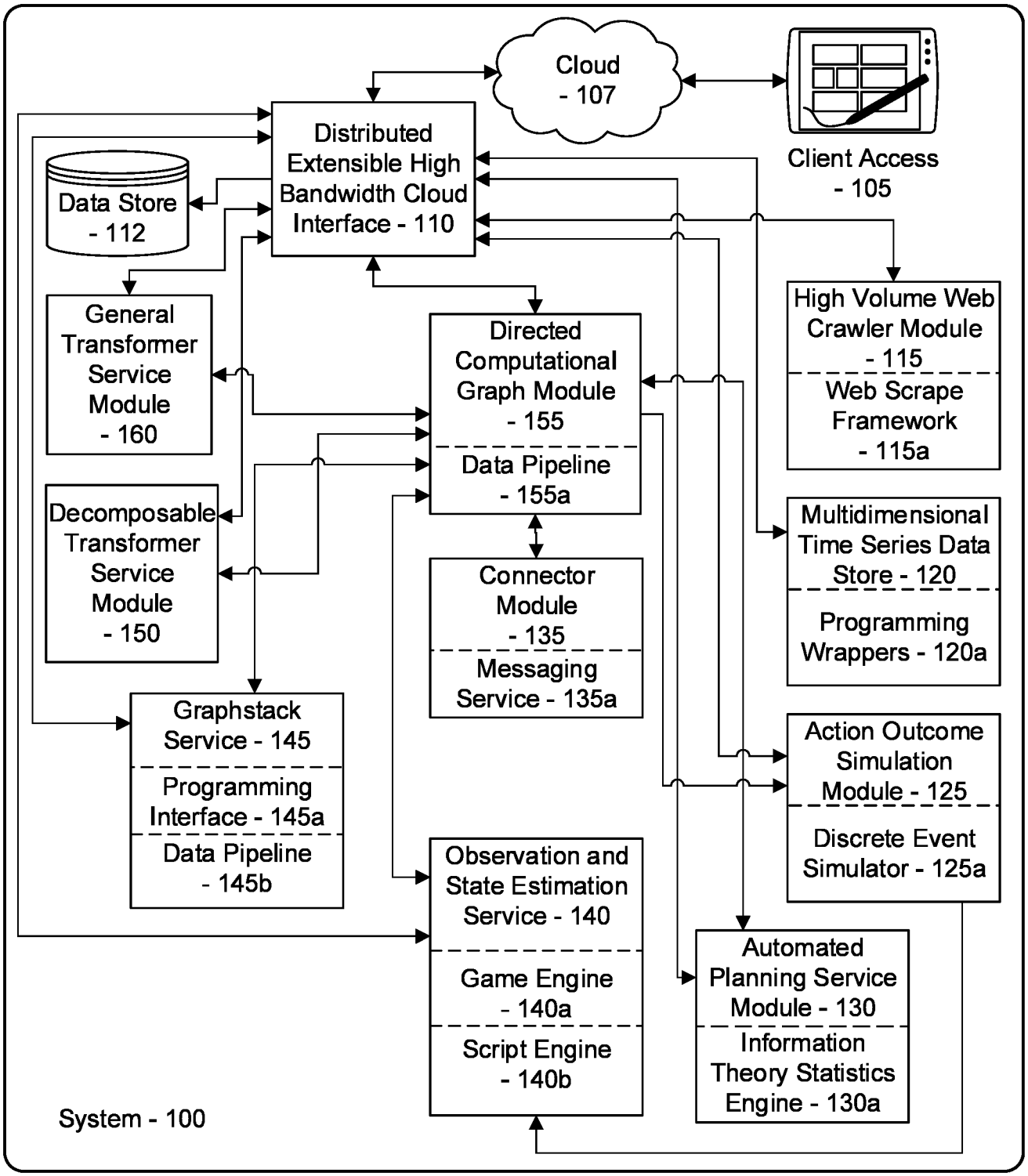

Cloud
- 107
Client Access
- 105
Distributed
Extensible High
Bandwidth Cloud
Interface - 110
Data Store
- 112
General
Transformer
Service
Module
- 160
Directed
Computational
Graph Module
- 155
Data Pipeline
- 155a
High Volume Web
Crawler Module
- 115
Web Scrape
Framework
- 115a
Decomposable
Transformer
Service
Module
- 150
Connector
Module
- 135
Messaging
Service - 135a
Multidimensional
Time Series Data
Store - 120
Programming
Wrappers - 120a
Graphstack
Service - 145
Programming
Interface - 145a
Data Pipeline
- 145b
Action Outcome
Simulation
Module - 125
Discrete Event
Simulator - 125a
Observation and
State Estimation
Service - 140
Game Engine
- 140a
Script Engine
- 140b
Automated
Planning Service
Module - 130
Information
Theory Statistics
Engine - 130a
System - 100

Fig. 1

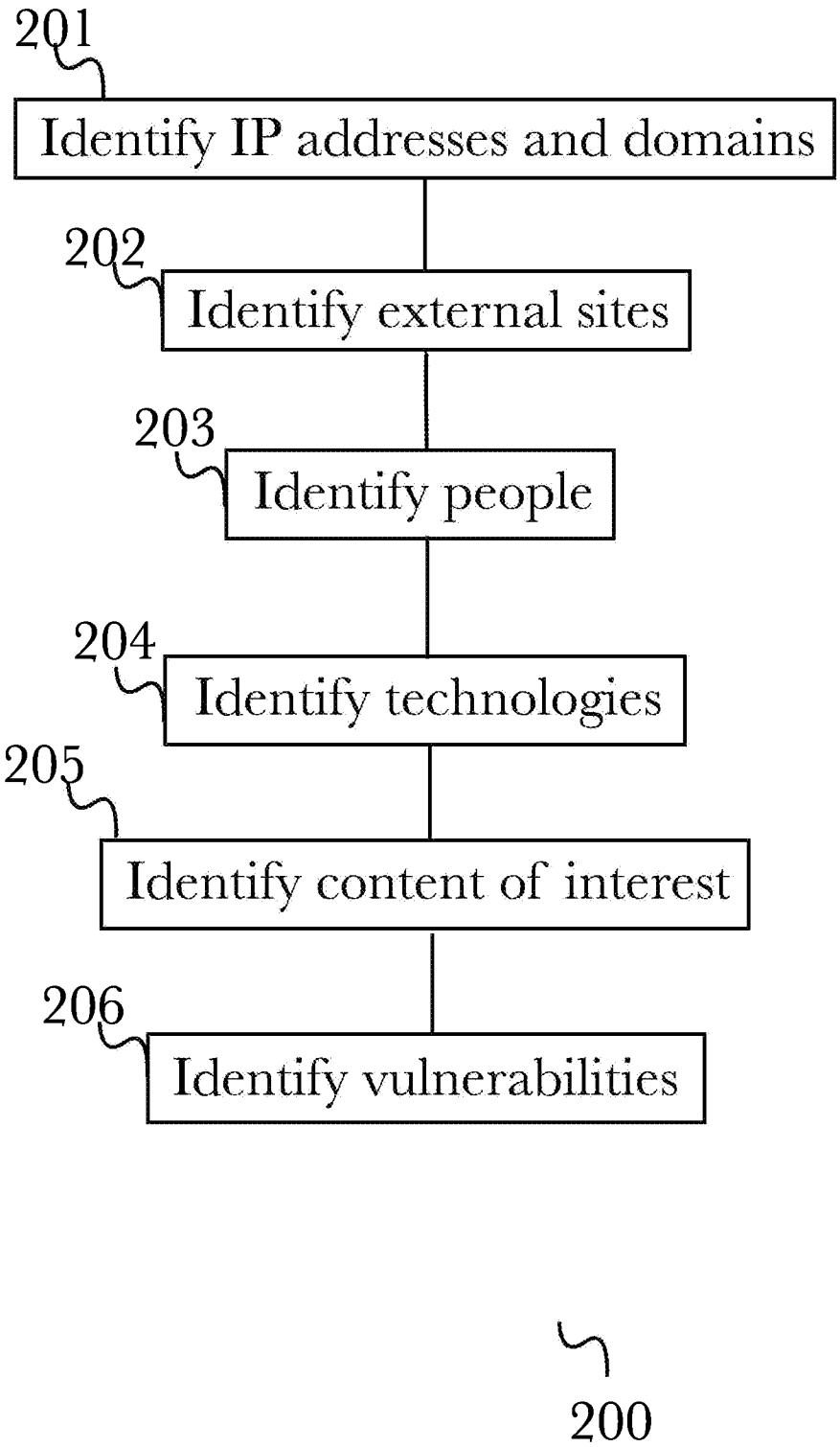

201
Identify IP addresses and domains
202
Identify external sites
203
Identify people
204
Identify technologies
205
Identify content of interest
206
Identify vulnerabilities
200

Fig. 2A

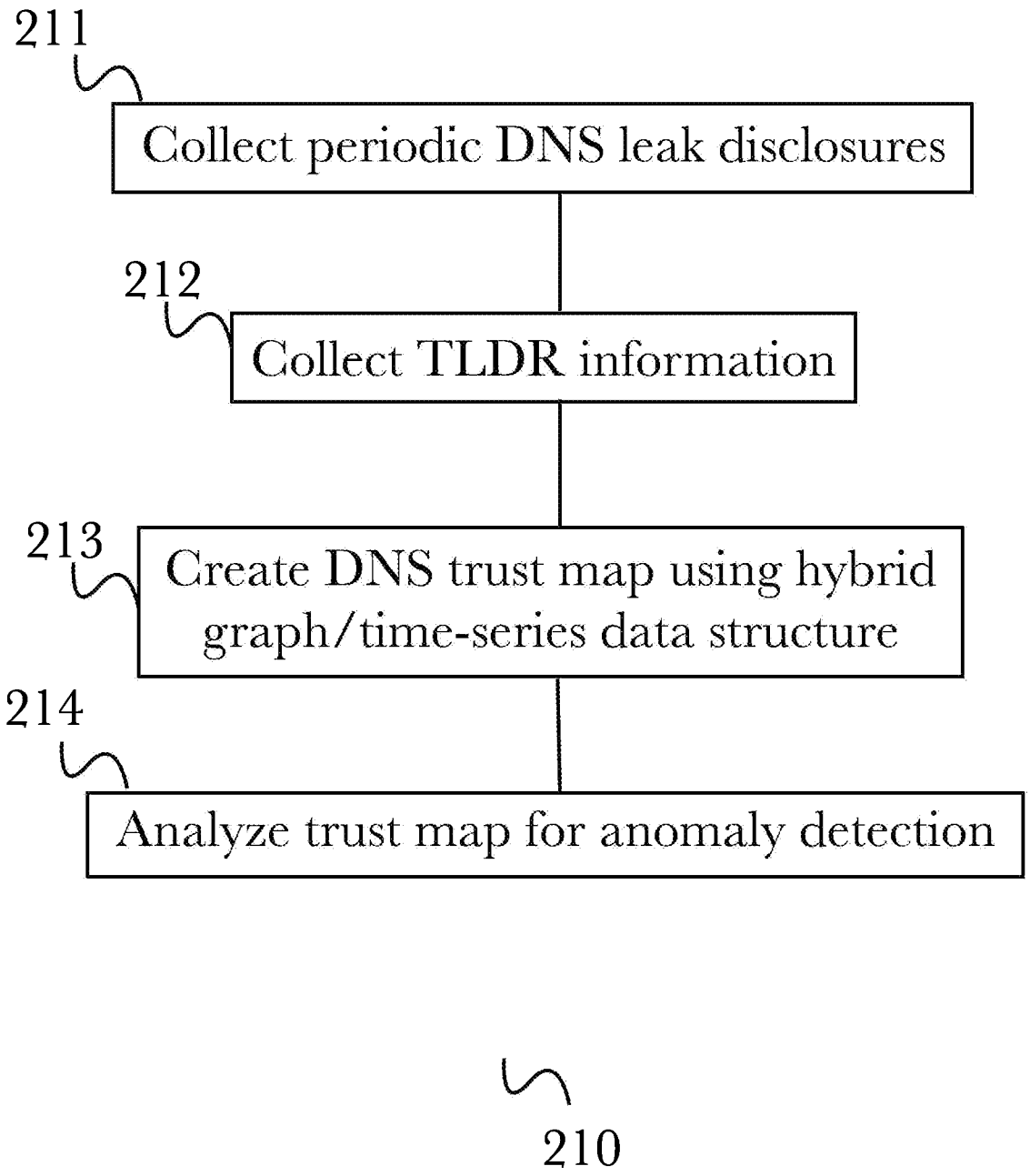

211
Collect periodic DNS leak disclosures
212
Collect TLDR information
213
Create DNS trust map using hybrid graph/time-series data structure
214
Analyze trust map for anomaly detection
210

Fig. 2B

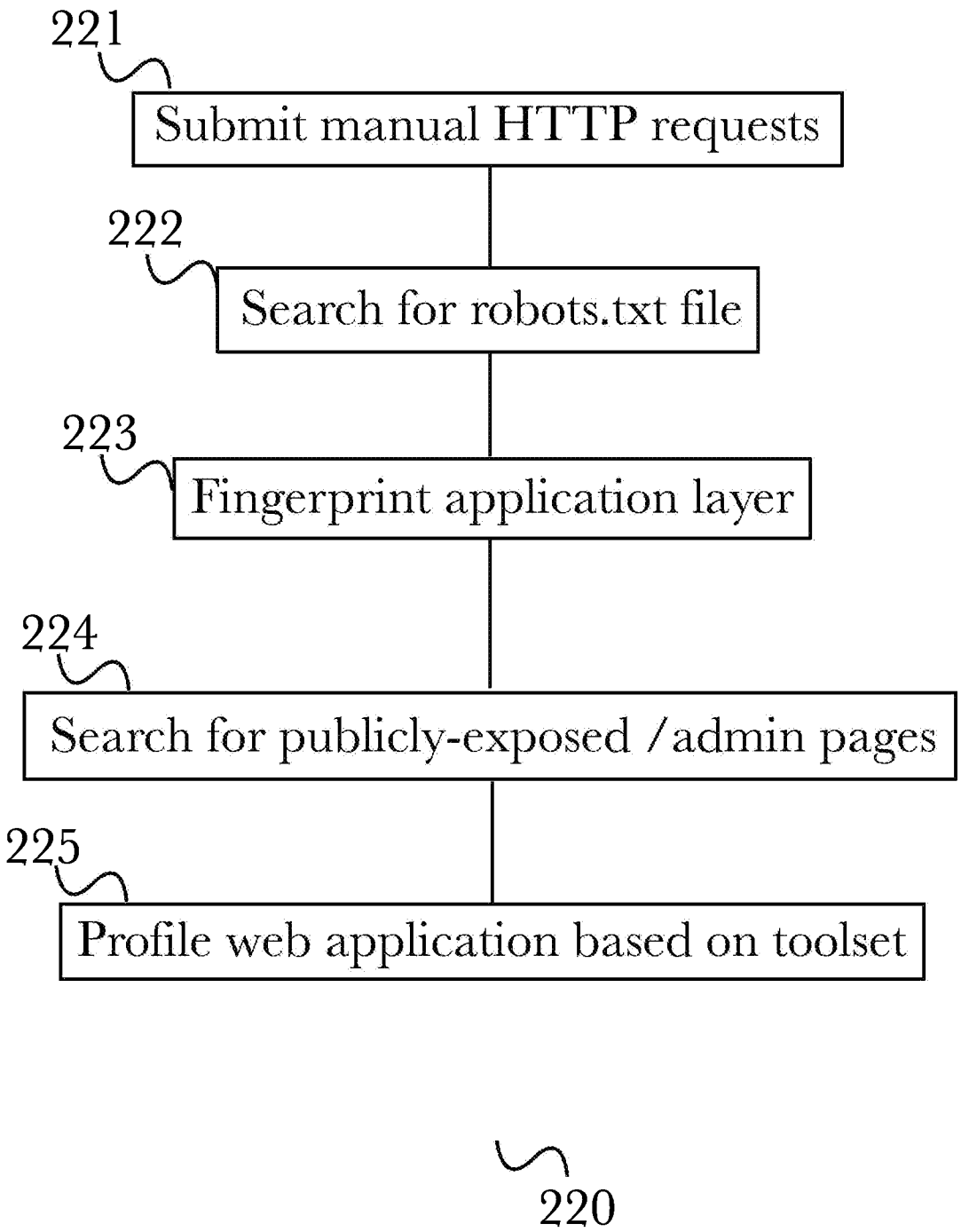

221
Submit manual HTTP requests
222
Search for robots.txt file
223
Fingerprint application layer
224
Search for publicly-exposed /admin pages
225
Profile web application based on toolset
220

Fig. 2C

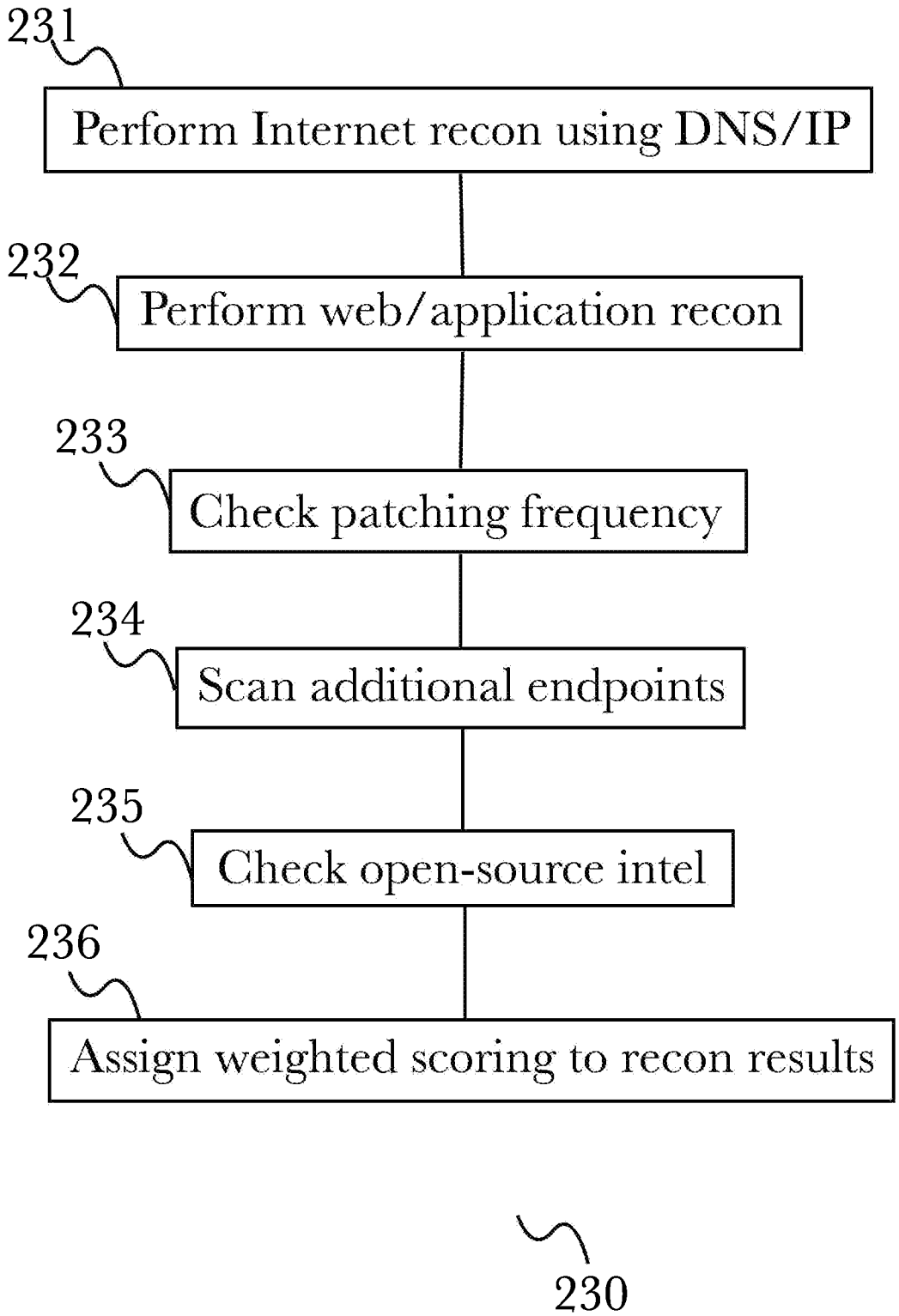

231
Perform Internet recon using DNS/IP
232
Perform web/application recon
233
Check patching frequency
234
Scan additional endpoints
235
Check open-source intel
236
Assign weighted scoring to recon results
230

Fig. 2D

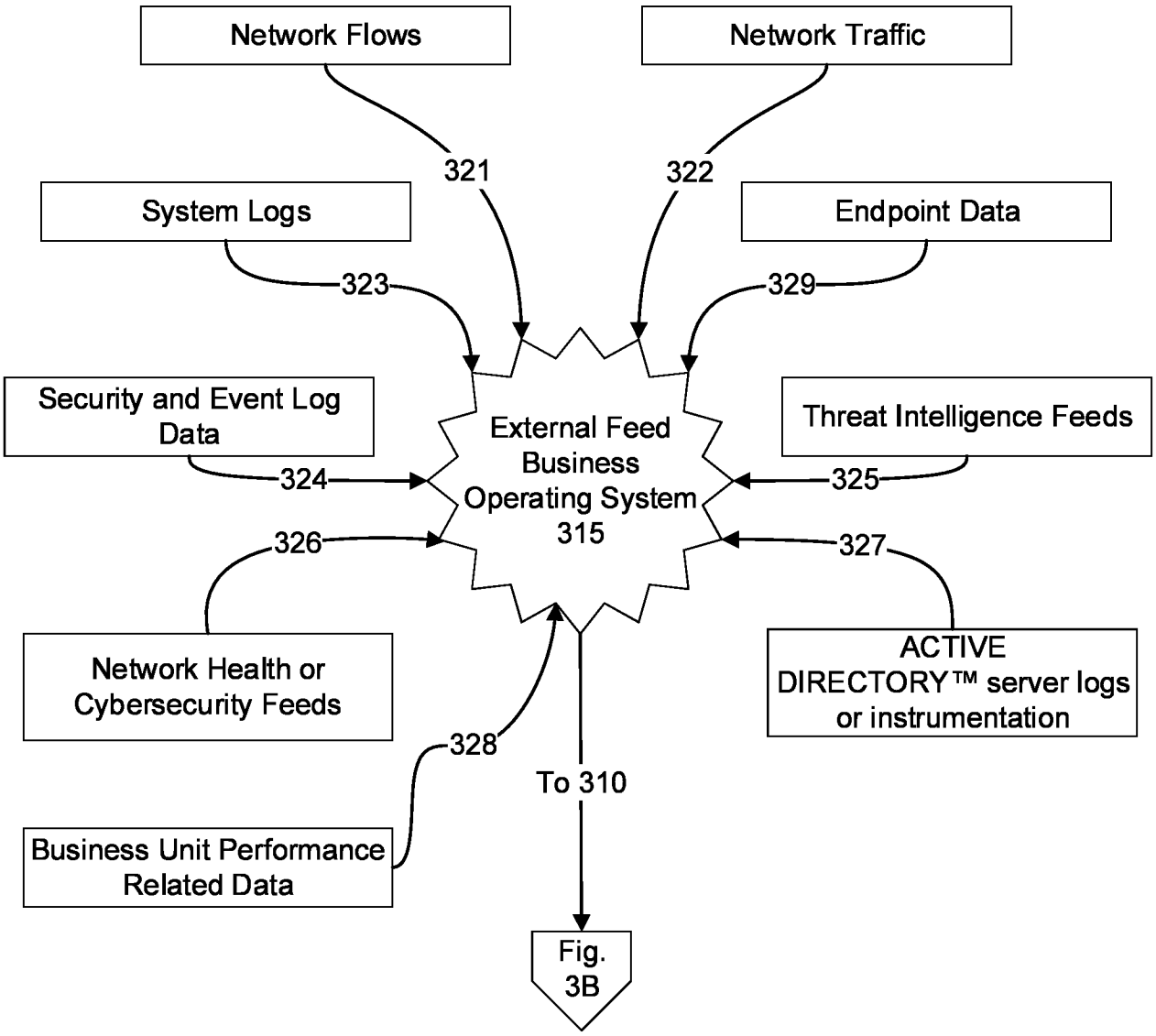

Network Flows
Network Traffic
321
322
System Logs
Endpoint Data
323
329
Security and Event Log Data
External Feed Business Operating System 315
Threat Intelligence Feeds
324
325
326
327
Network Health or Cybersecurity Feeds
ACTIVE DIRECTORY™ server logs or instrumentation
328
To 310
Business Unit Performance Related Data
Fig. 3B

Fig. 3A

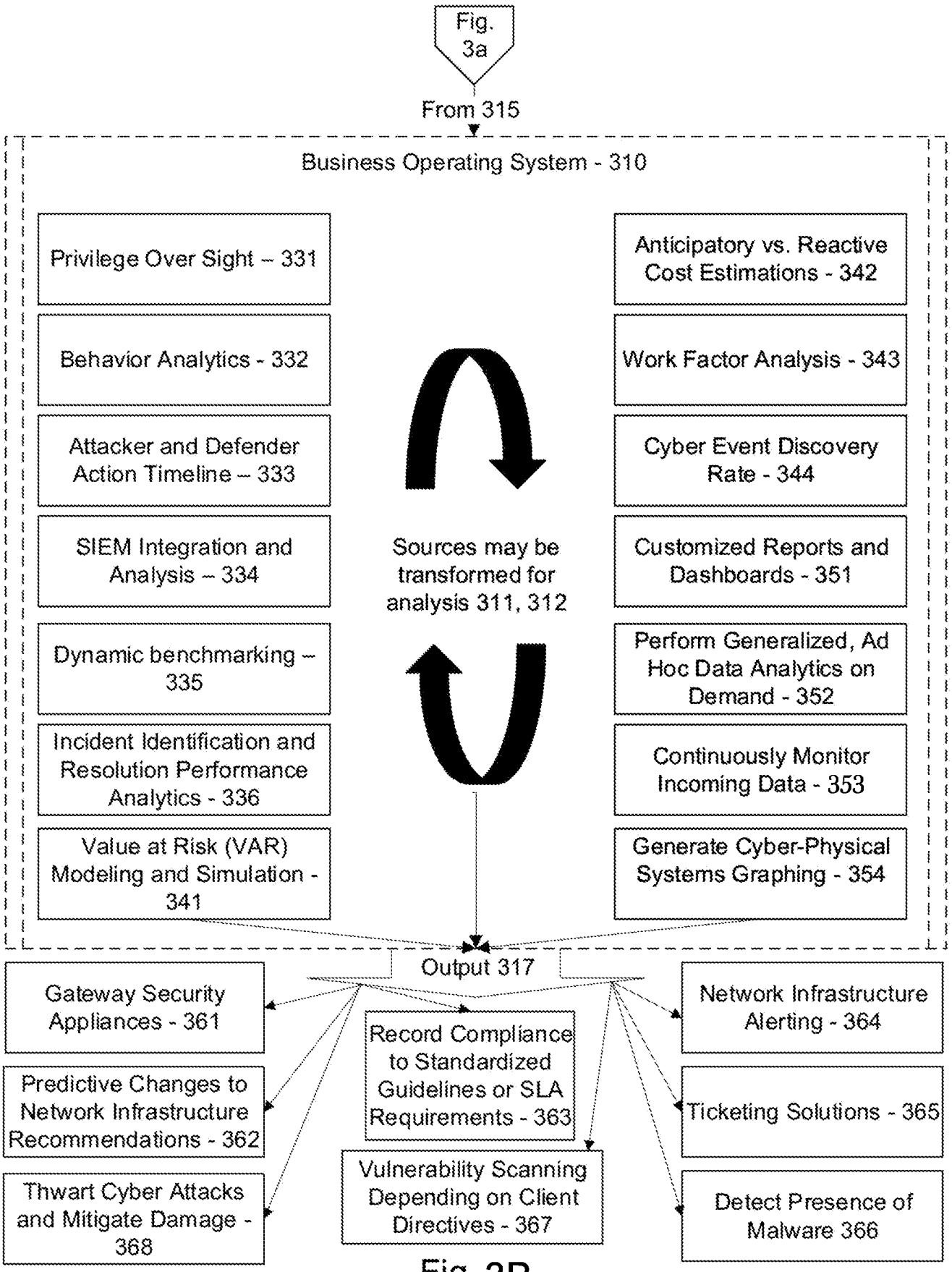
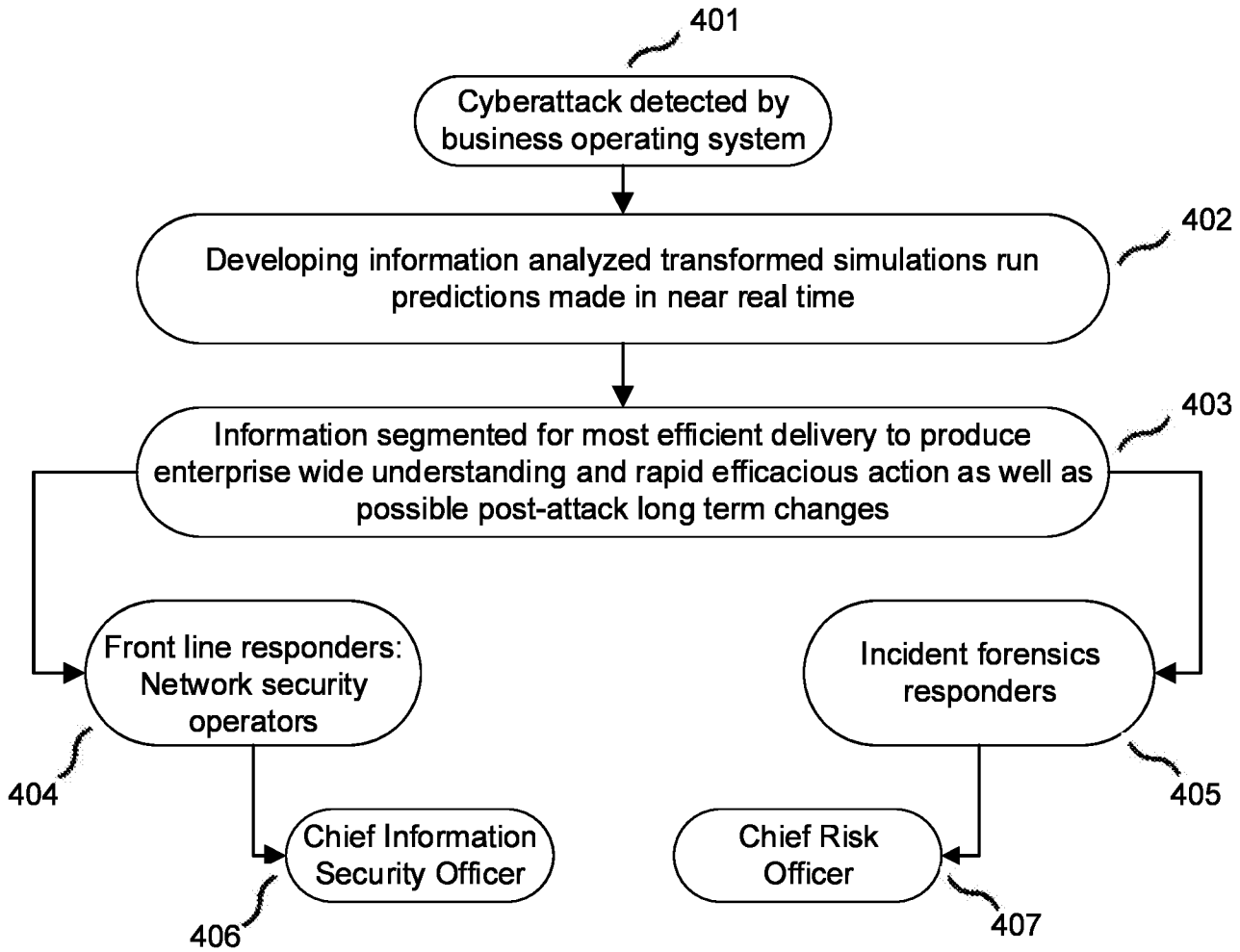


Fig. 3a
From 315
Business Operating System - 310
Privilege Over Sight – 331
Behavior Analytics - 332
Attacker and Defender Action Timeline – 333
SIEM Integration and Analysis – 334
Dynamic benchmarking – 335
Incident Identification and Resolution Performance Analytics - 336
Value at Risk (VAR) Modeling and Simulation - 341
Sources may be transformed for analysis 311, 312
Anticipatory vs. Reactive Cost Estimations - 342
Work Factor Analysis - 343
Cyber Event Discovery Rate - 344
Customized Reports and Dashboards - 351
Perform Generalized, Ad Hoc Data Analytics on Demand - 352
Continuously Monitor Incoming Data - 353
Generate Cyber-Physical Systems Graphing - 354
Output 317
Gateway Security Appliances - 361
Predictive Changes to Network Infrastructure Recommendations - 362
Thwart Cyber Attacks and Mitigate Damage - 368
Record Compliance to Standardized Guidelines or SLA Requirements - 363
Vulnerability Scanning Depending on Client Directives - 367
Network Infrastructure Alerting - 364
Ticketing Solutions - 365
Detect Presence of Malware 366

Fig. 3B


401
Cyberattack detected by business operating system
402
Developing information analyzed transformed simulations run predictions made in near real time
403
Information segmented for most efficient delivery to produce enterprise wide understanding and rapid efficacious action as well as possible post-attack long term changes
Front line responders: Network security operators
Incident forensics responders
404
405
Chief Information Security Officer
Chief Risk Officer
406
407

400

Fig. 4

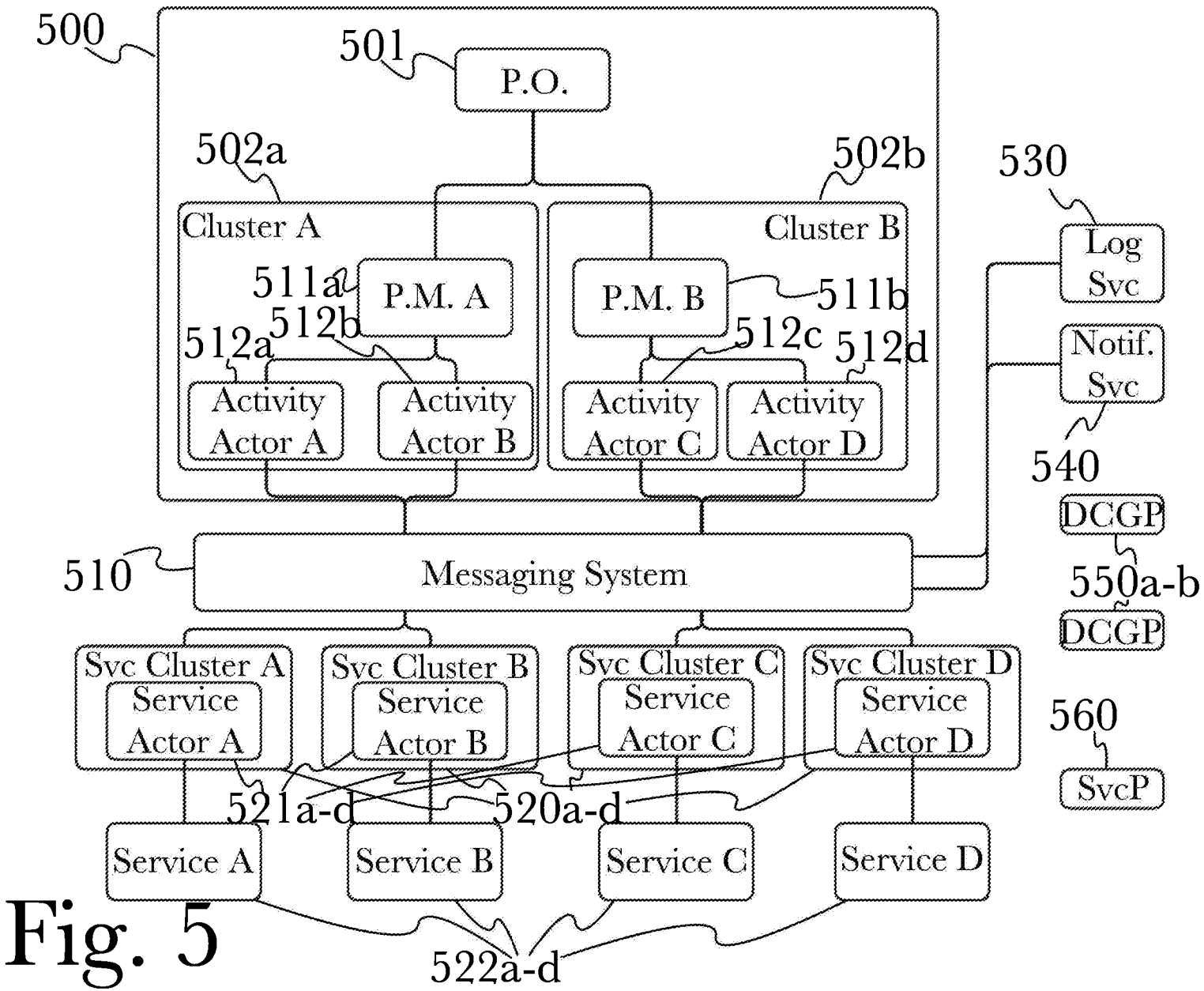

500
501
P.O.
502a
502b
530
Cluster A
Cluster B
Log Svc
511a
P.M. A
P.M. B
511b
512b
512c
512a
512d
Notif. Svc
Activity Actor A
Activity Actor B
Activity Actor C
Activity Actor D
540
DCGP
510
Messaging System
550a-b
DCGP
Svc Cluster A
Svc Cluster B
Svc Cluster C
Svc Cluster D
Service Actor A
Service Actor B
Service Actor C
Service Actor D
560
SvcP
521a-d
520a-d
Service A
Service B
Service C
Service D
522a-d

Fig. 5

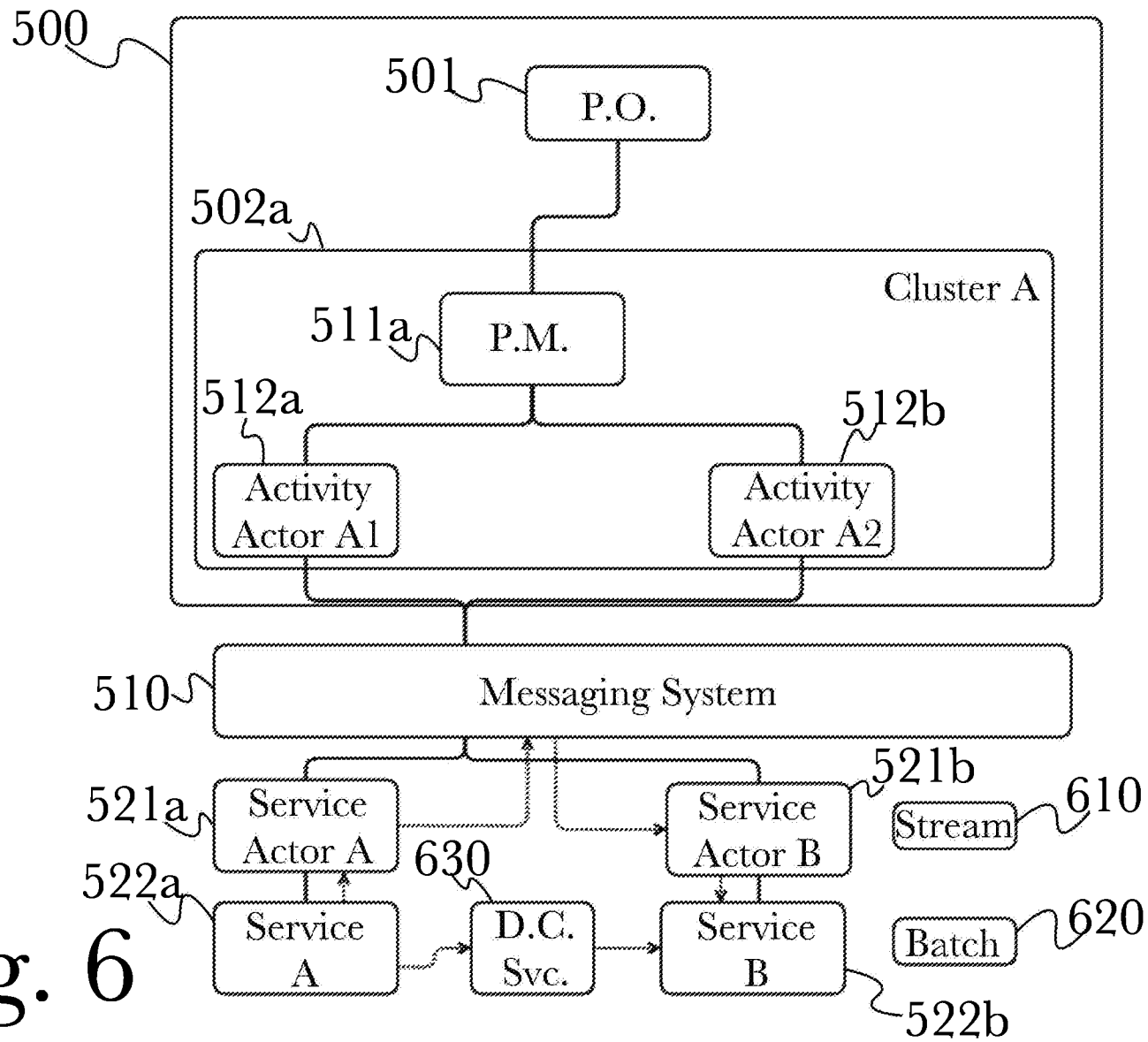

500
501
P.O.
502a
Cluster A
511a
P.M.
512a
512b
Activity Actor A1
Activity Actor A2
510
Messaging System
521a
Service Actor A
521b
Service Actor B
Stream
610
630
522a
Service A
D.C. Svc.
Service B
Batch
620
522b

Fig. 6

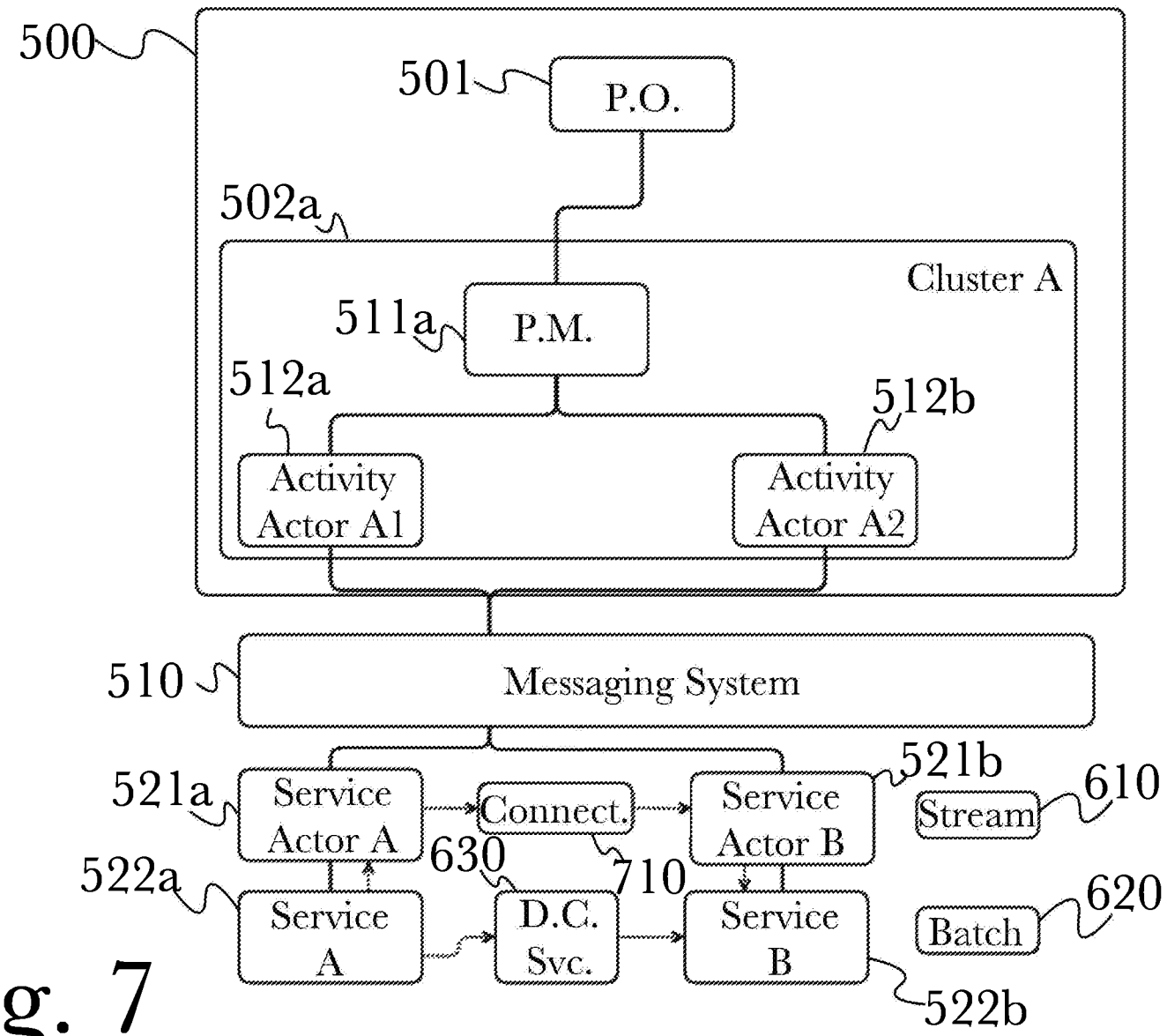

500
501
P.O.
502a
Cluster A
511a
P.M.
512a
512b
Activity Actor A1
Activity Actor A2
510
Messaging System
521a
Service Actor A
Connect.
Service Actor B
521b
Stream
610
630
710
522a
Service A
D.C. Svc.
Service B
Batch
620
522b

Fig. 7

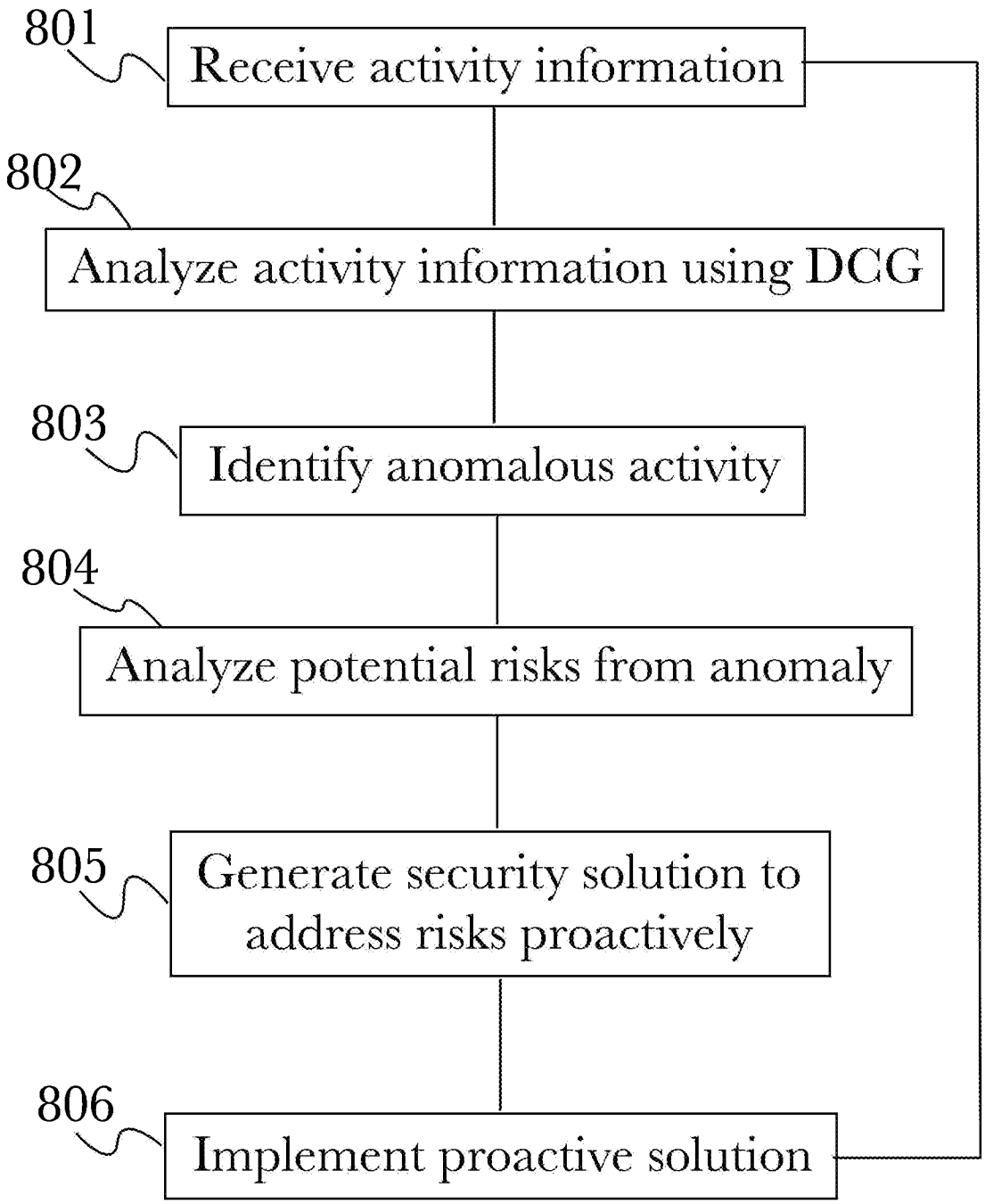

801
Receive activity information
802
Analyze activity information using DCG
803
Identify anomalous activity
804
Analyze potential risks from anomaly
805
Generate security solution to address risks proactively
806
Implement proactive solution

Fig. 8

800

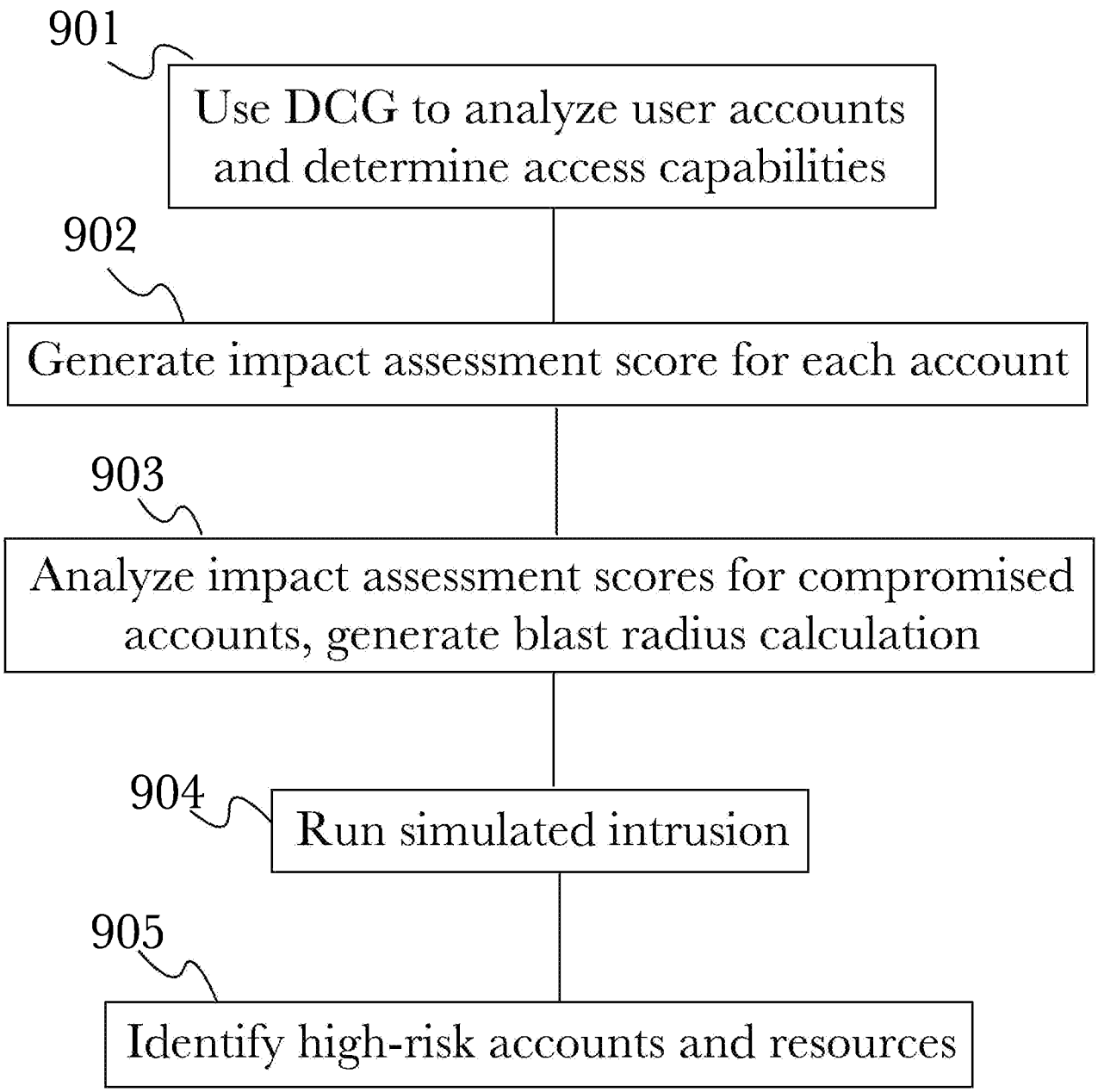

901
Use DCG to analyze user accounts and determine access capabilities
902
Generate impact assessment score for each account
903
Analyze impact assessment scores for compromised accounts, generate blast radius calculation
904
Run simulated intrusion
905
Identify high-risk accounts and resources

Fig. 9

900

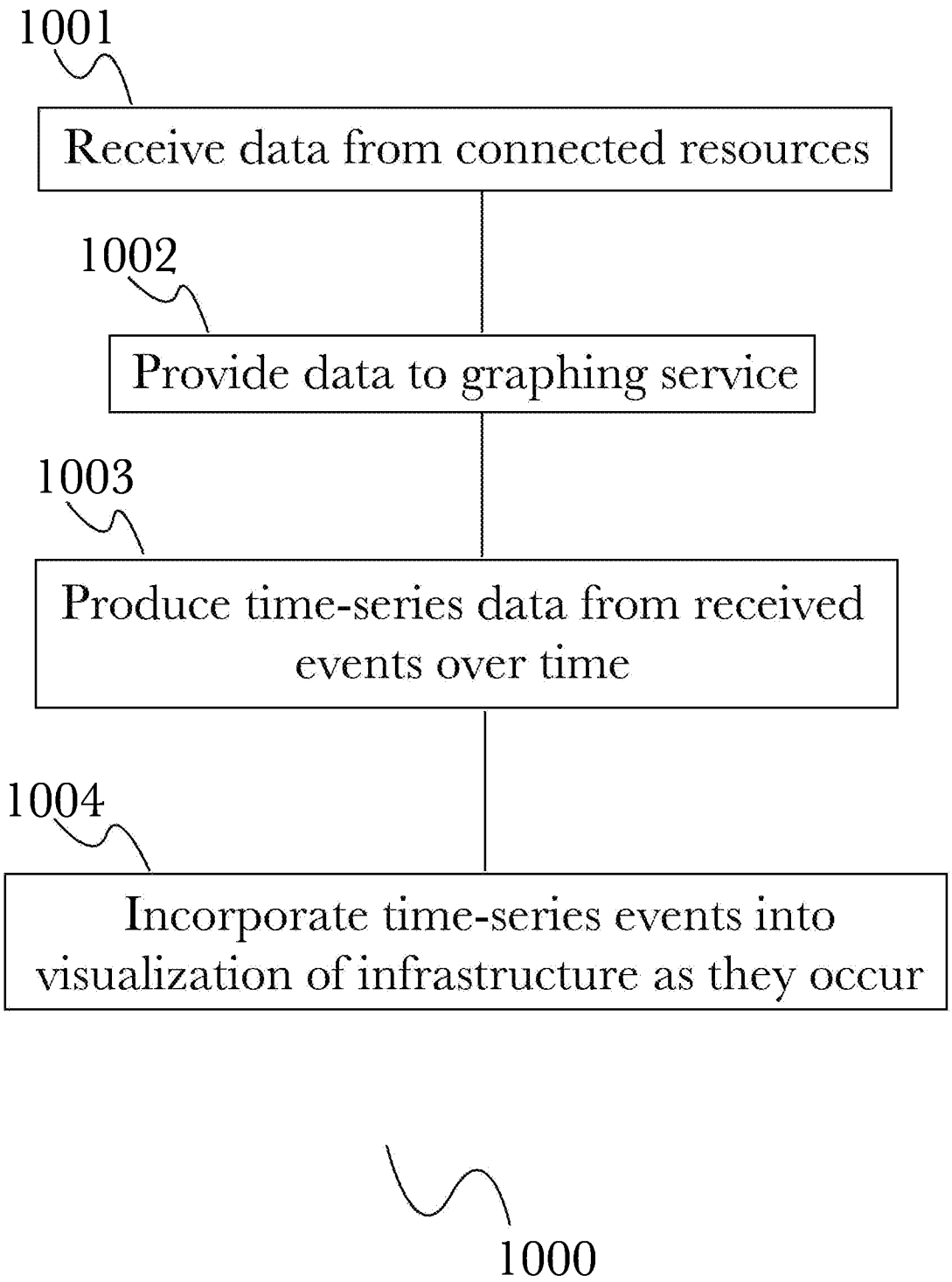
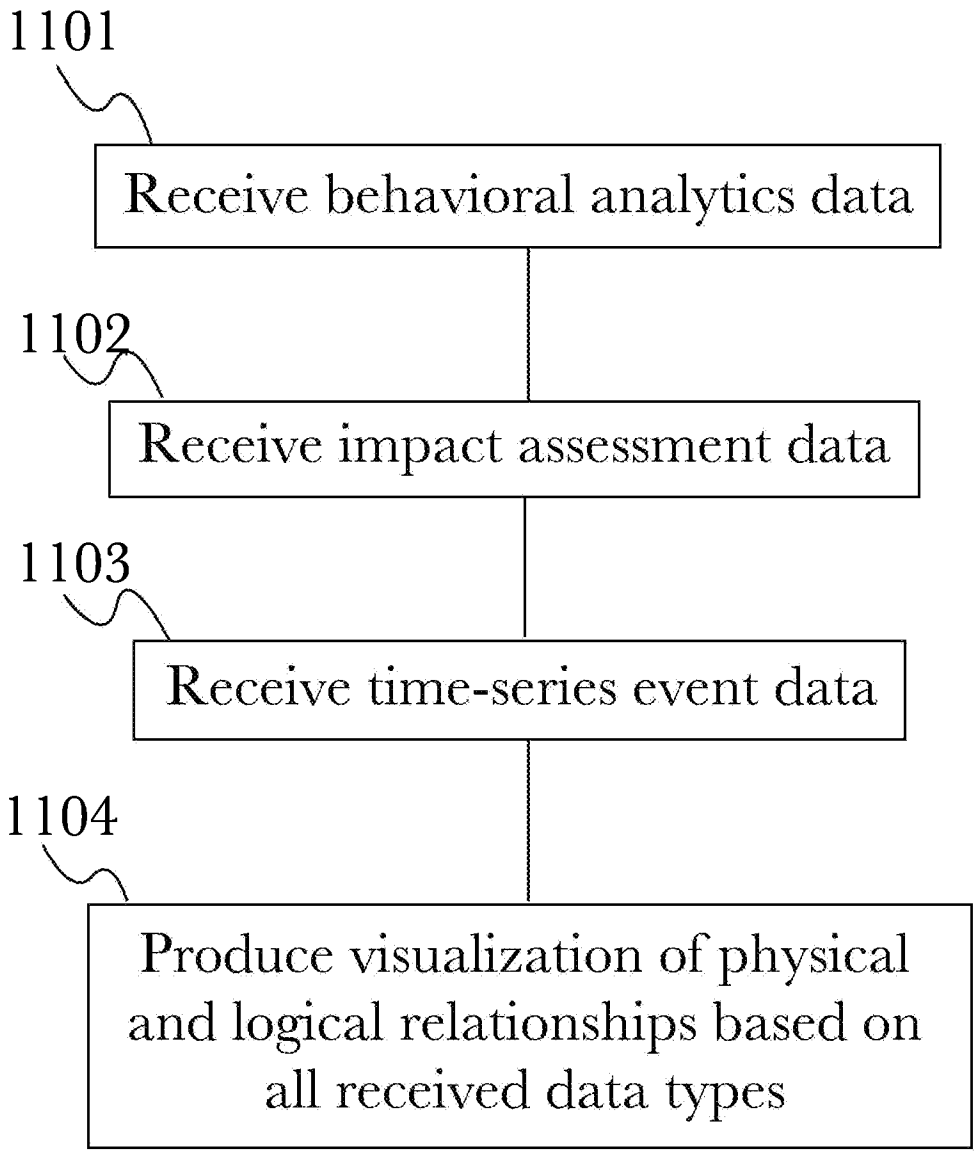

1001
Receive data from connected resources
1002
Provide data to graphing service
1003
Produce time-series data from received events over time
1004
Incorporate time-series events into visualization of infrastructure as they occur
1000

Fig. 10


1101
Receive behavioral analytics data
1102
Receive impact assessment data
1103
Receive time-series event data
1104
Produce visualization of physical and logical relationships based on all received data types

1100

Fig. 11

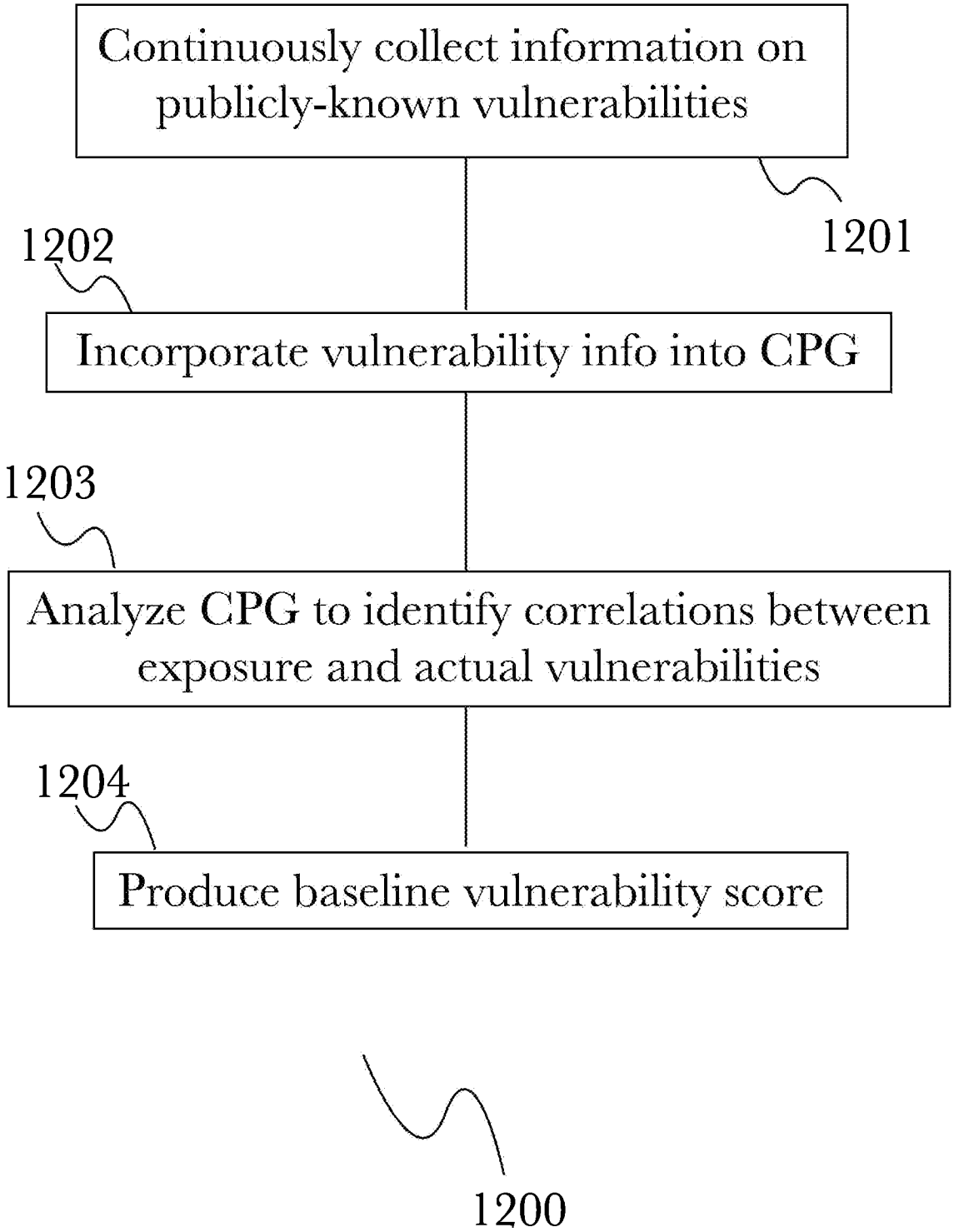

Continuously collect information on publicly-known vulnerabilities
1201
1202
Incorporate vulnerability info into CPG
1203
Analyze CPG to identify correlations between exposure and actual vulnerabilities
1204
Produce baseline vulnerability score
1200

Fig. 12

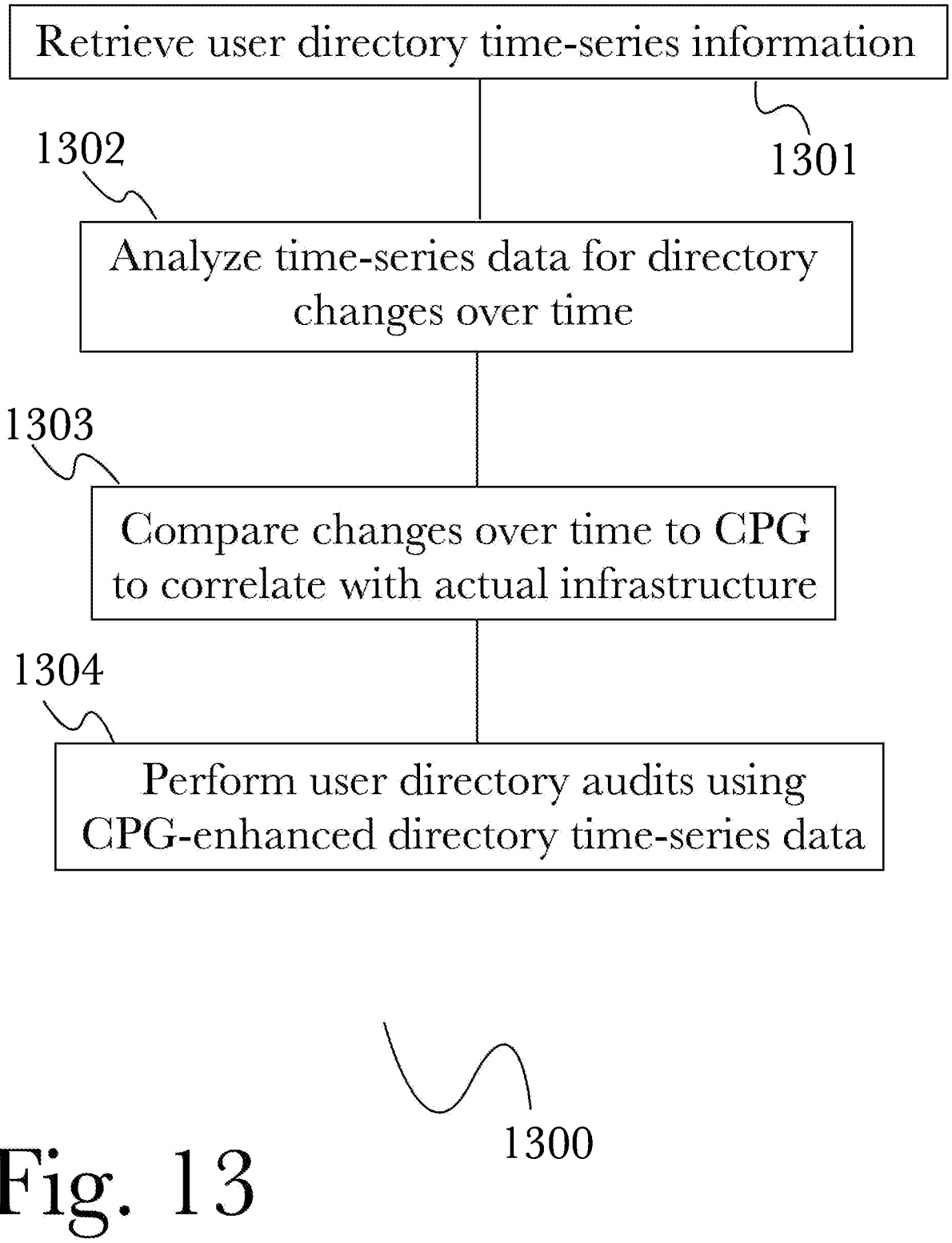

Retrieve user directory time-series information
1301
1302
Analyze time-series data for directory changes over time
1303
Compare changes over time to CPG to correlate with actual infrastructure
1304
Perform user directory audits using CPG-enhanced directory time-series data
1300

Fig. 13

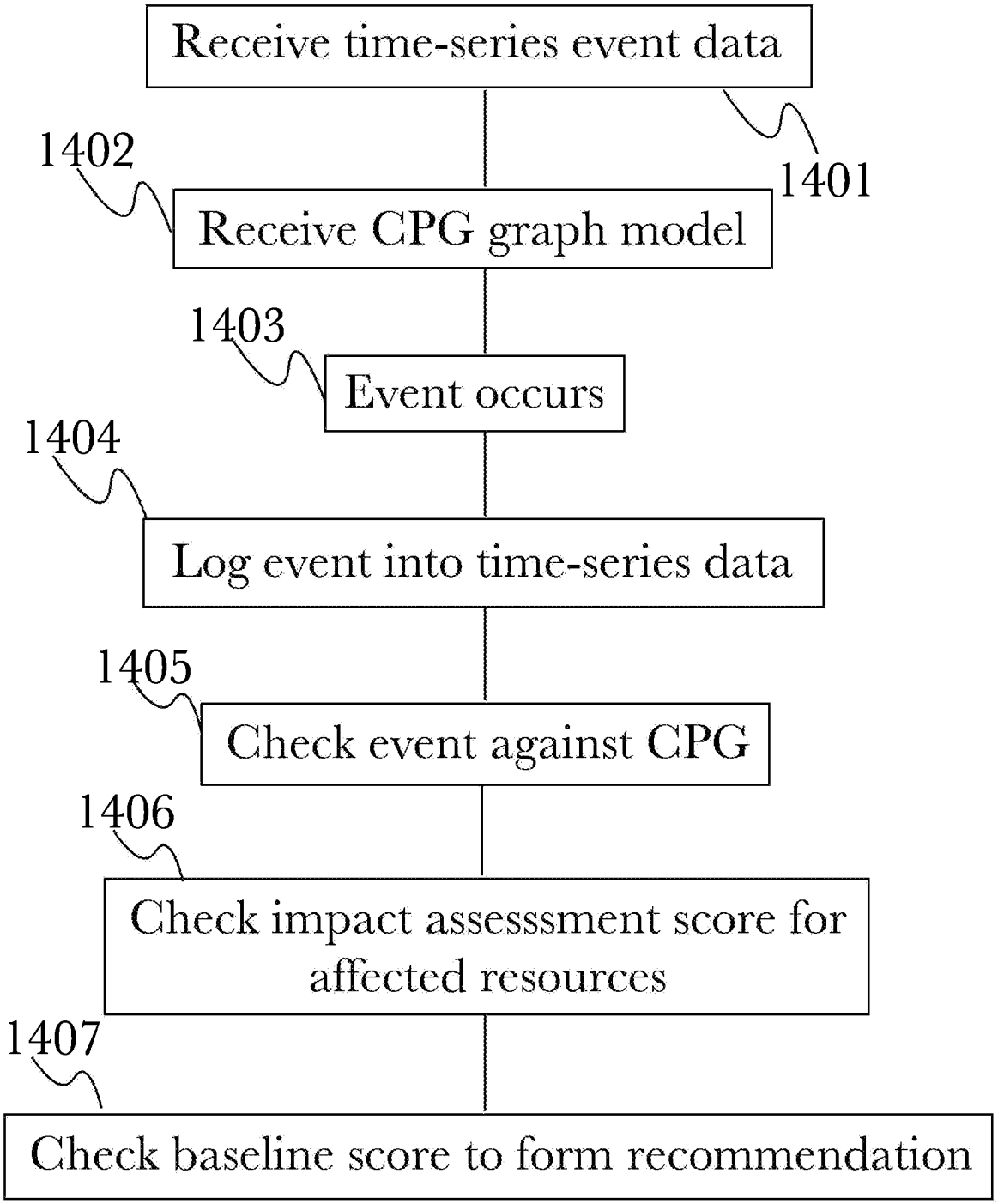

Receive time-series event data
1401
1402
Receive CPG graph model
1403
Event occurs
1404
Log event into time-series data
1405
Check event against CPG
1406
Check impact assesssment score for affected resources
1407
Check baseline score to form recommendation

Fig. 14

1400

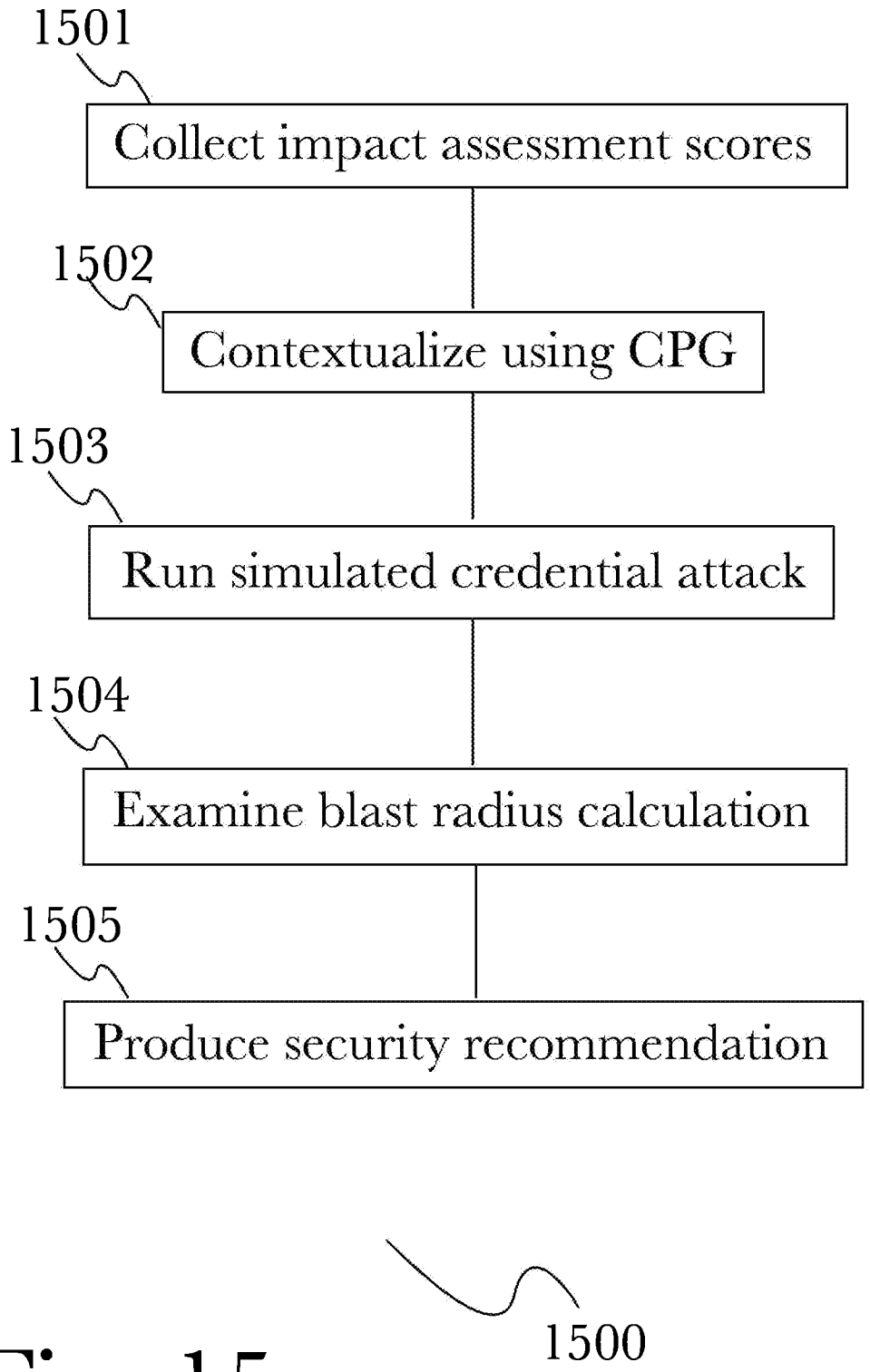

1501
Collect impact assessment scores
1502
Contextualize using CPG
1503
Run simulated credential attack
1504
Examine blast radius calculation
1505
Produce security recommendation
1500

Fig. 15

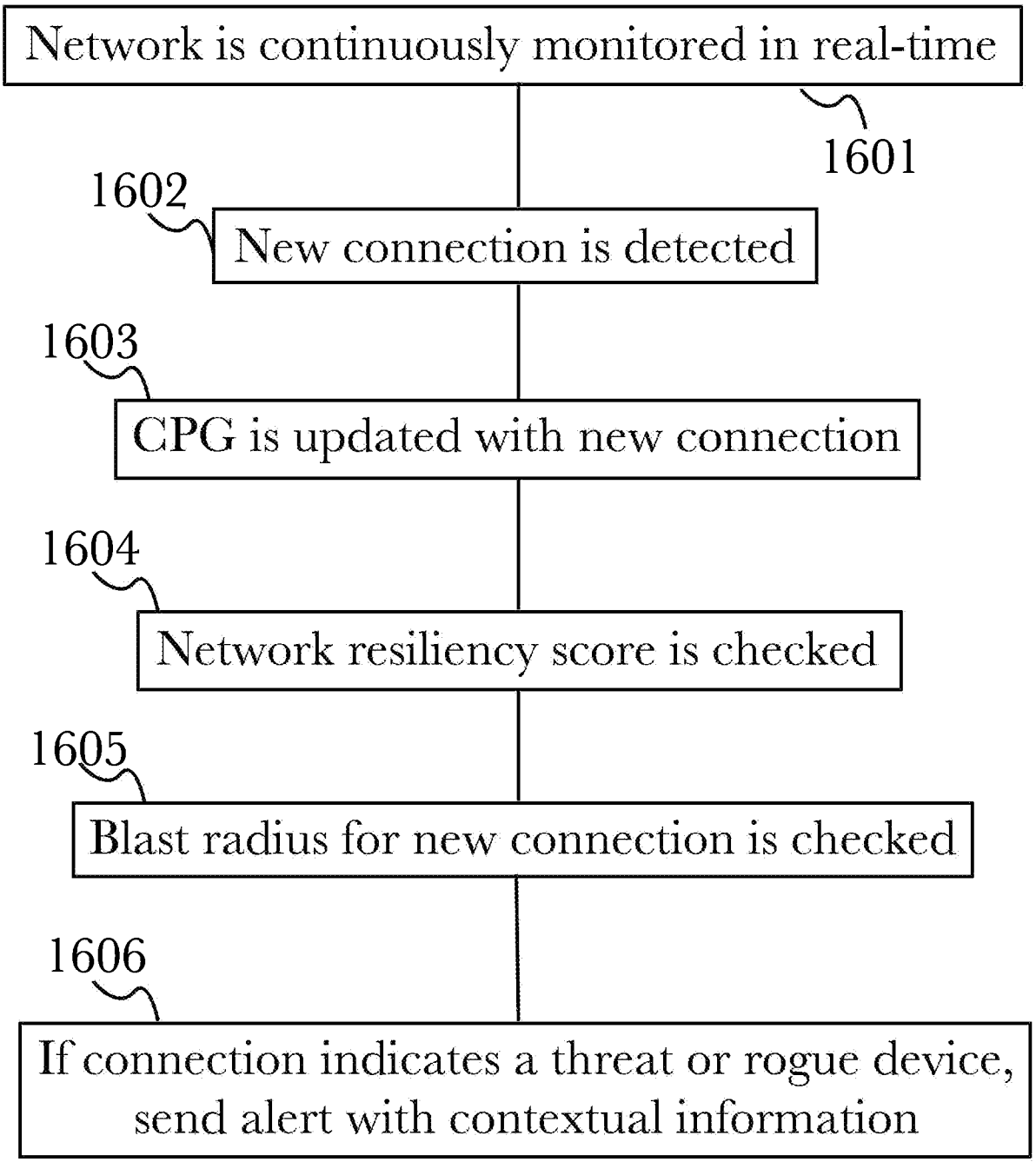

Network is continuously monitored in real-time
1601
1602
New connection is detected
1603
CPG is updated with new connection
1604
Network resiliency score is checked
1605
Blast radius for new connection is checked
1606
If connection indicates a threat or rogue device, send alert with contextual information

Fig. 16

1600

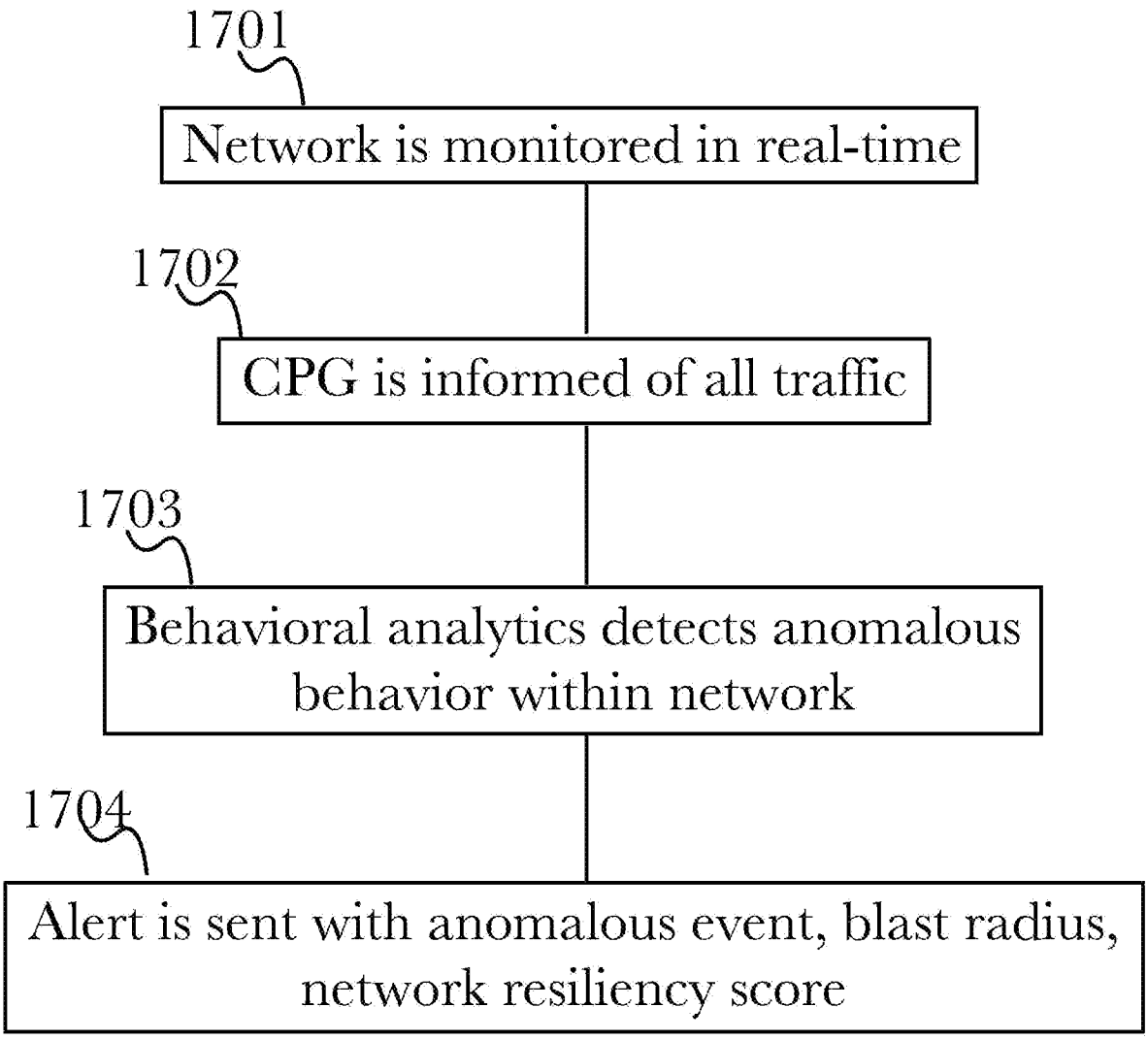

1701
Network is monitored in real-time
1702
CPG is informed of all traffic
1703
Behavioral analytics detects anomalous behavior within network
1704
Alert is sent with anomalous event, blast radius, network resiliency score

Fig. 17

1700

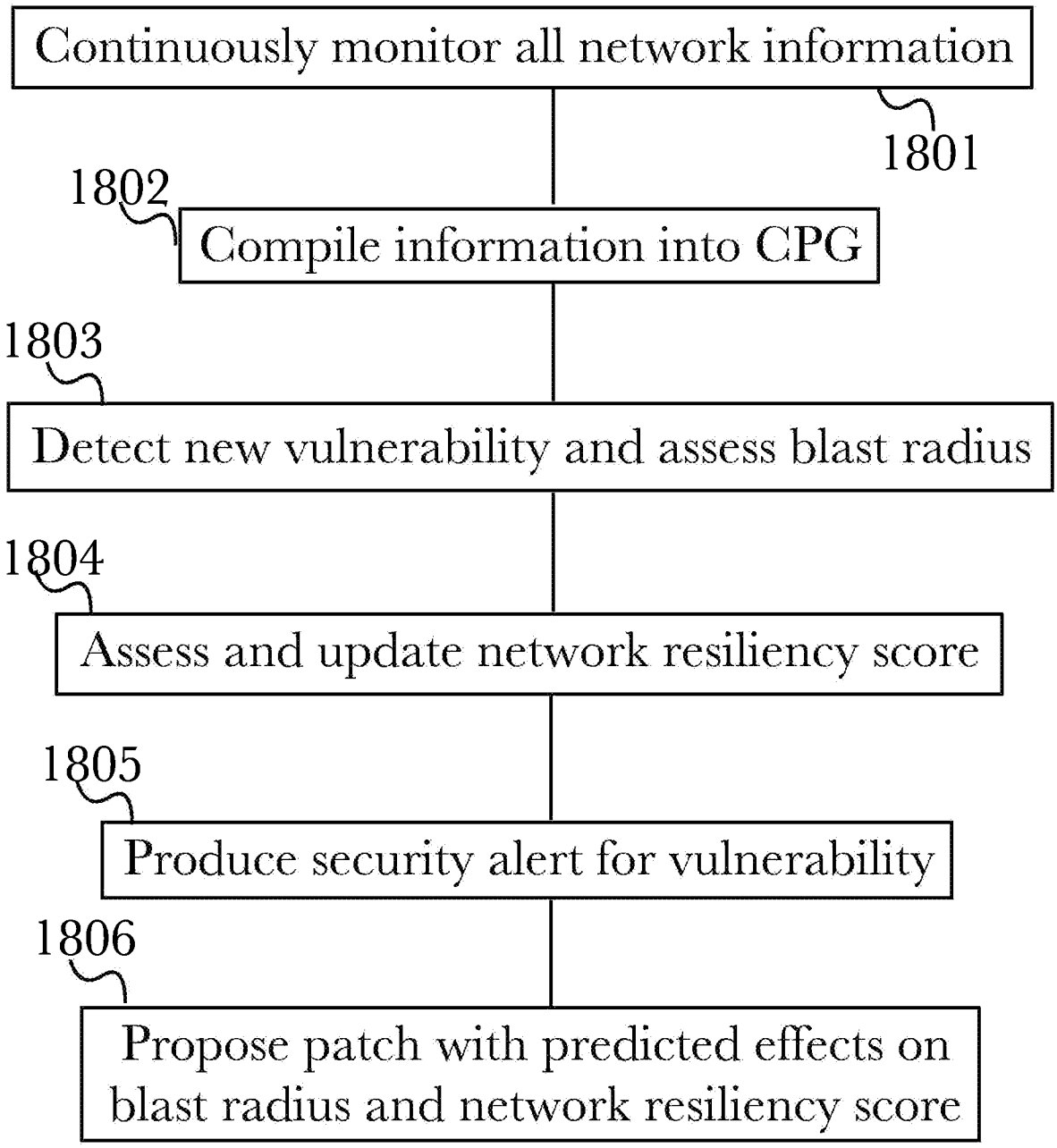

Continuously monitor all network information
1801
1802
Compile information into CPG
1803
Detect new vulnerability and assess blast radius
1804
Assess and update network resiliency score
1805
Produce security alert for vulnerability
1806
Propose patch with predicted effects on blast radius and network resiliency score

Fig. 18

1800

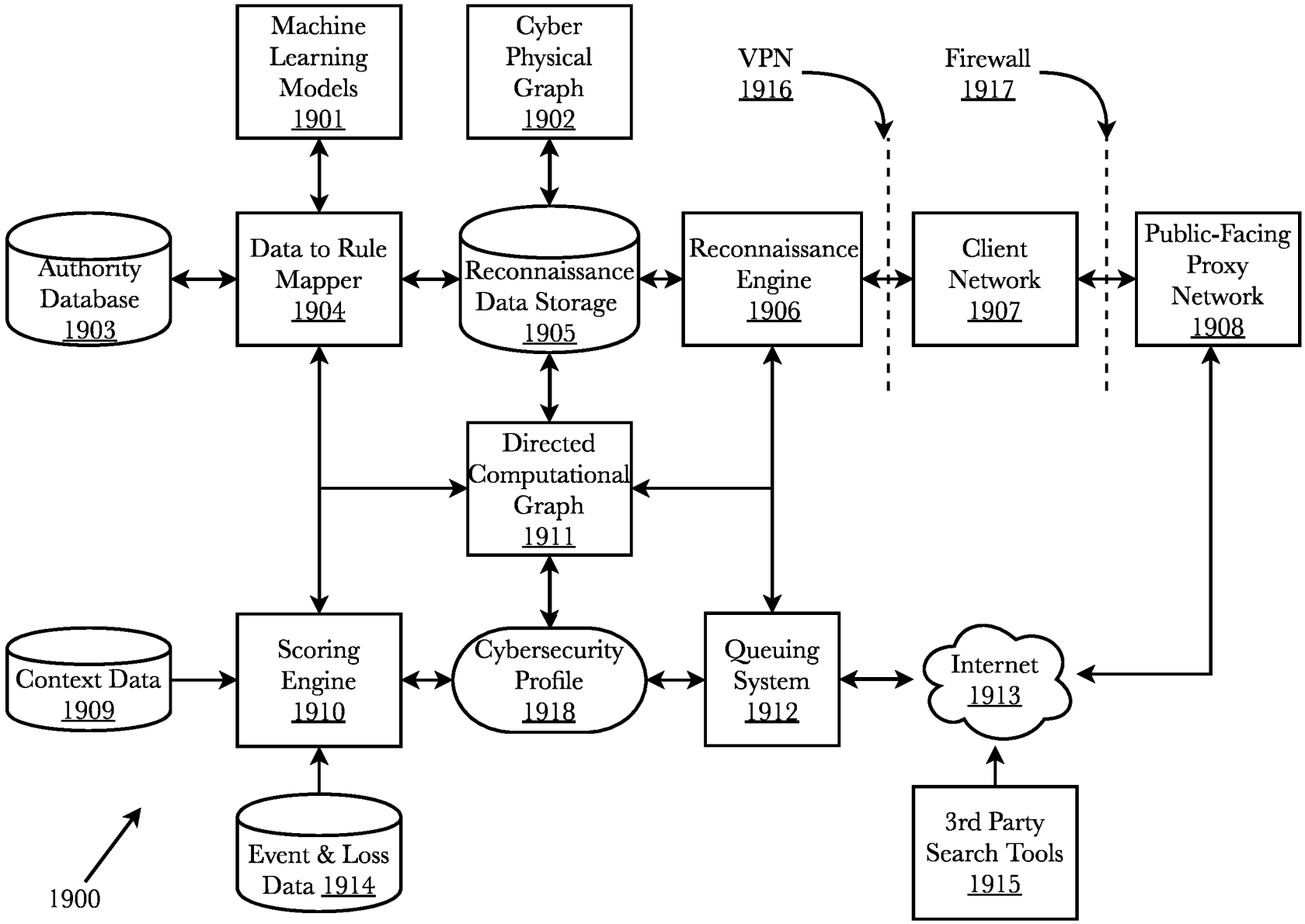

Machine Learning Models 1901
Cyber Physical Graph 1902
VPN 1916
Firewall 1917
Authority Database 1903
Data to Rule Mapper 1904
Reconnaissance Data Storage 1905
Reconnaissance Engine 1906
Client Network 1907
Public-Facing Proxy Network 1908
Directed Computational Graph 1911
Context Data 1909
Scoring Engine 1910
Cybersecurity Profile 1918
Queuing System 1912
Internet 1913
Event & Loss Data 1914
3rd Party Search Tools 1915
1900

Fig. 19

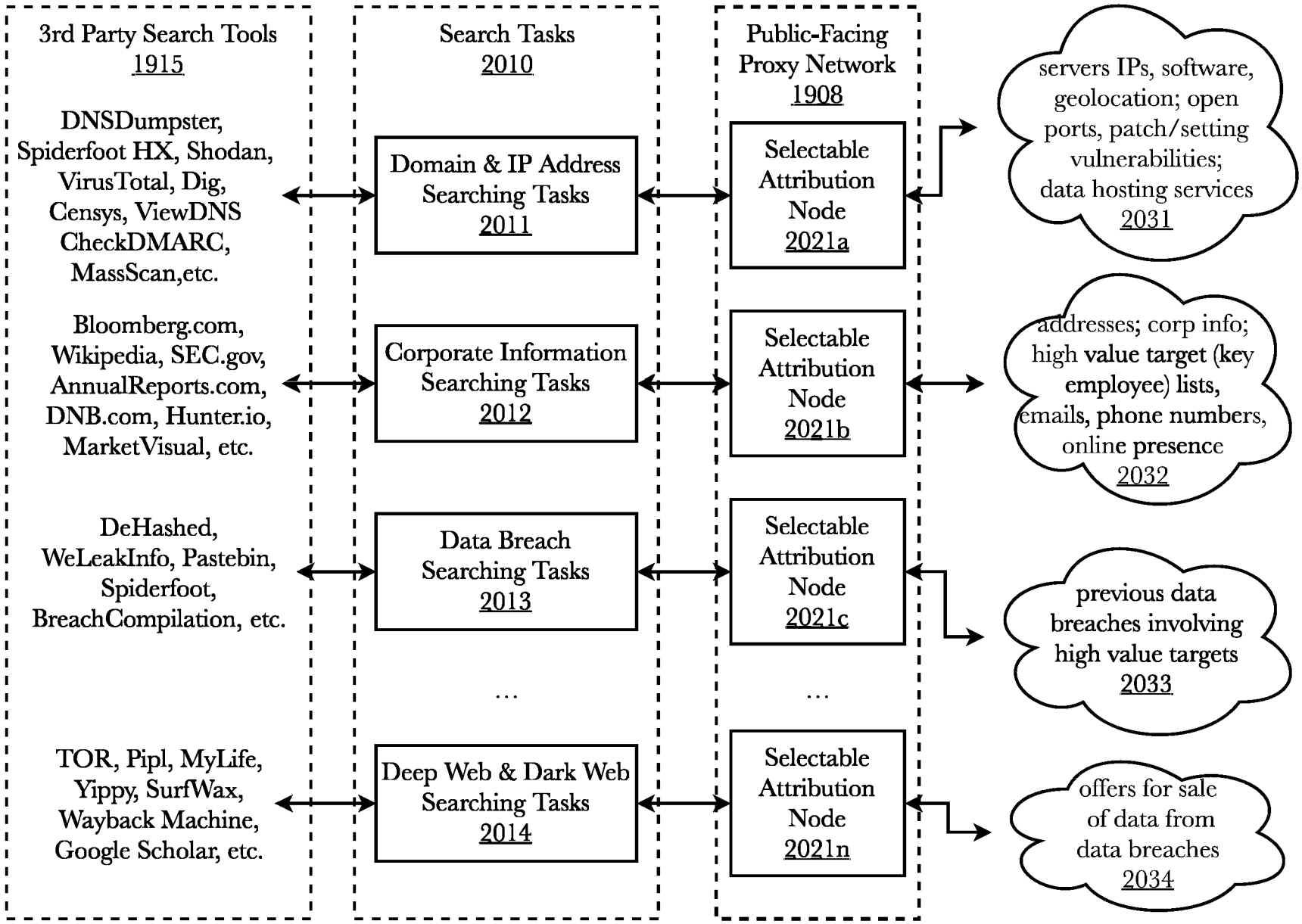

3rd Party Search Tools
1915
DNSDumpster, Spiderfoot HX, Shodan, VirusTotal, Dig, Censys, ViewDNS CheckDMARC, MassScan,etc.
Bloomberg.com, Wikipedia, SEC.gov, AnnualReports.com, DNB.com, Hunter.io, MarketVisual, etc.
DeHashed, WeLeakInfo, Pastebin, Spiderfoot, BreachCompilation, etc.
TOR, Pipl, MyLife, Yippy, SurfWax, Wayback Machine, Google Scholar, etc.
Search Tasks
2010
Domain & IP Address Searching Tasks
2011
Corporate Information Searching Tasks
2012
Data Breach Searching Tasks
2013
...
Deep Web & Dark Web Searching Tasks
2014
Public-Facing Proxy Network
1908
Selectable Attribution Node
2021a
Selectable Attribution Node
2021b
Selectable Attribution Node
2021c
...
Selectable Attribution Node
2021n
servers IPs, software, geolocation; open ports, patch/setting vulnerabilities; data hosting services
2031
addresses; corp info; high value target (key employee) lists, emails, phone numbers, online presence
2032
previous data breaches involving high value targets
2033
offers for sale of data from data breaches
2034

Fig. 20

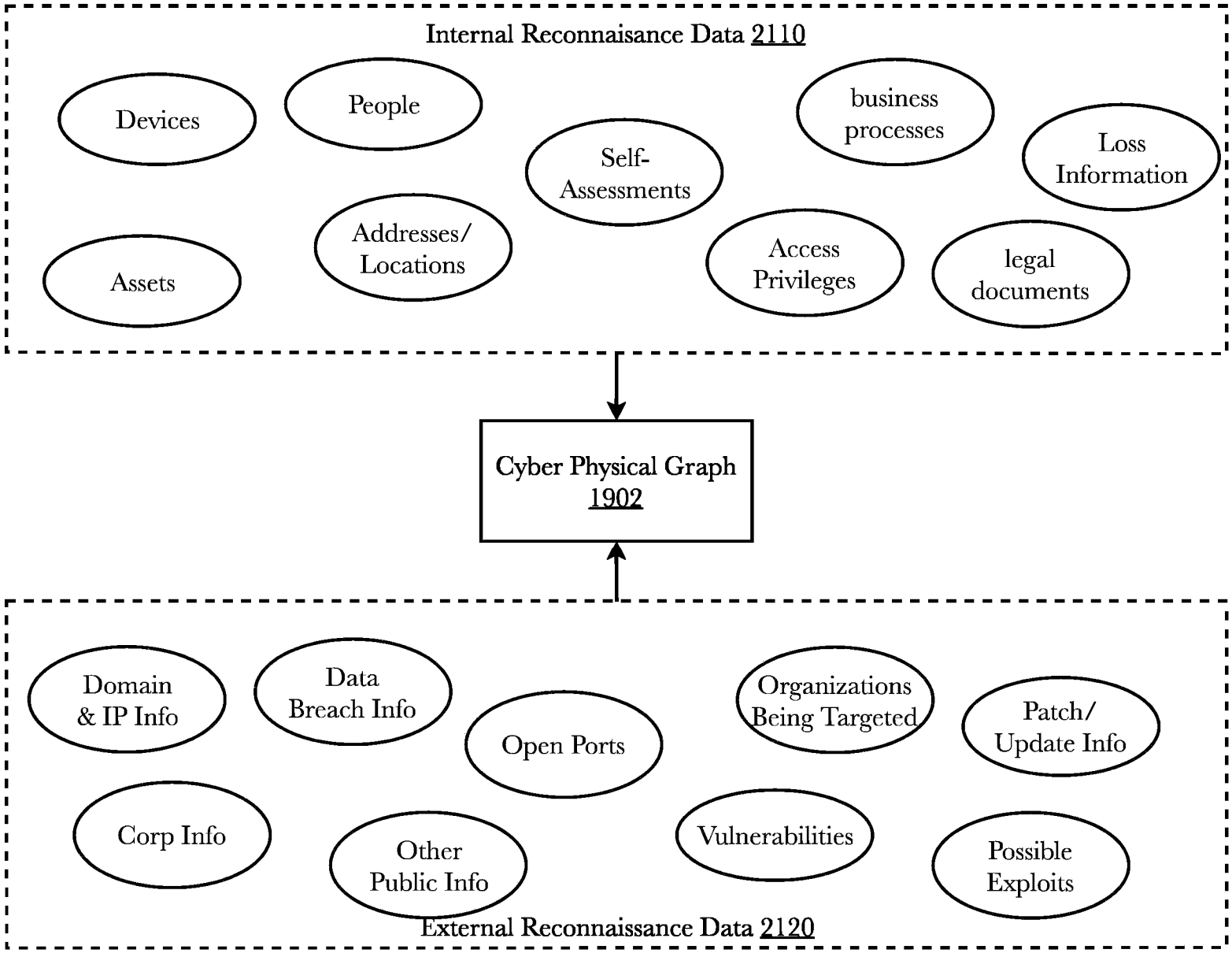

Internal Reconnaisance Data 2110
Devices
People
Self-Assessments
business processes
Loss Information
Assets
Addresses/ Locations
Access Privileges
legal documents
Cyber Physical Graph 1902
Domain & IP Info
Data Breach Info
Open Ports
Organizations Being Targeted
Patch/ Update Info
Corp Info
Other Public Info
Vulnerabilities
Possible Exploits
External Reconnaissance Data 2120

Fig. 21

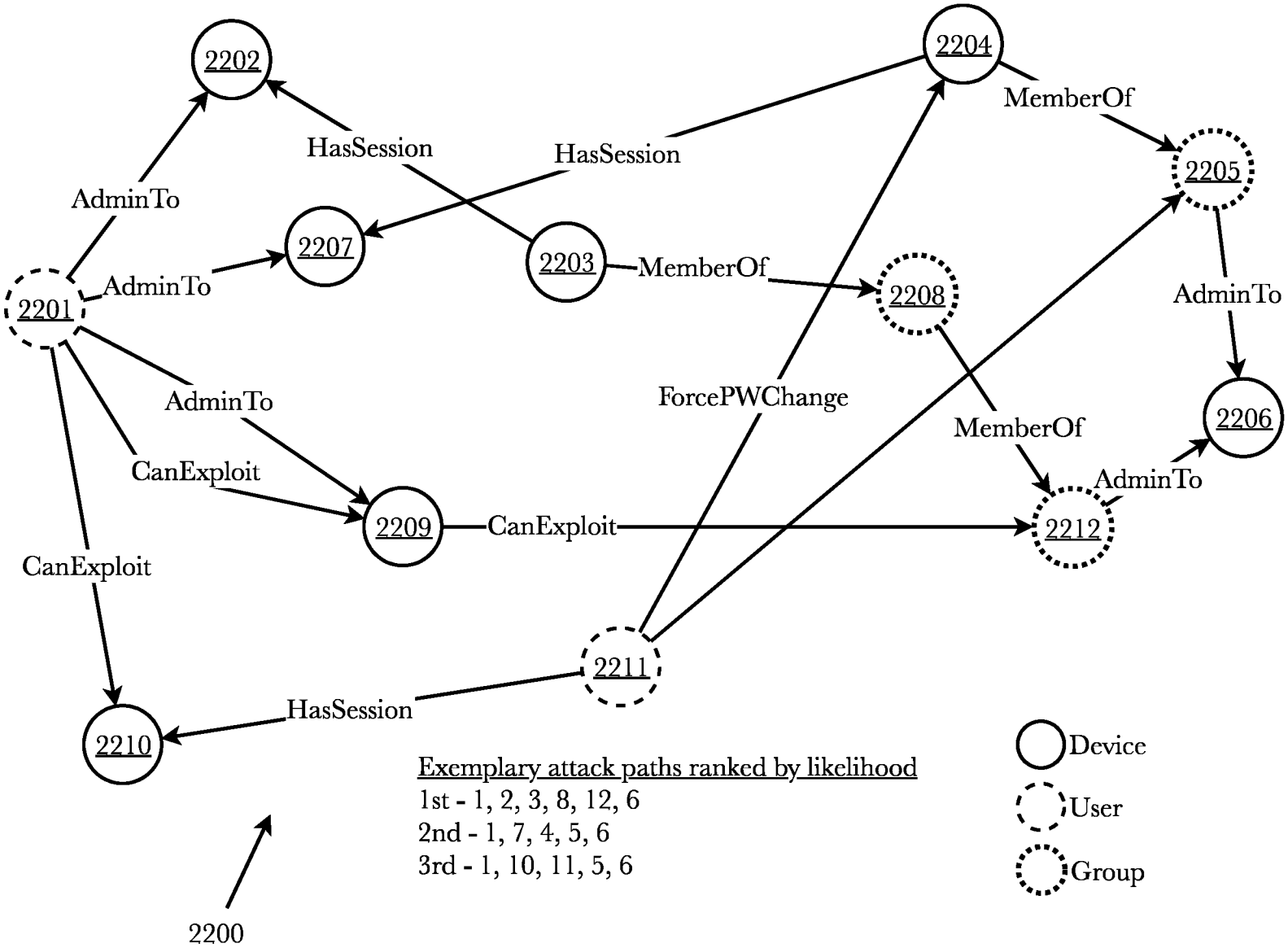
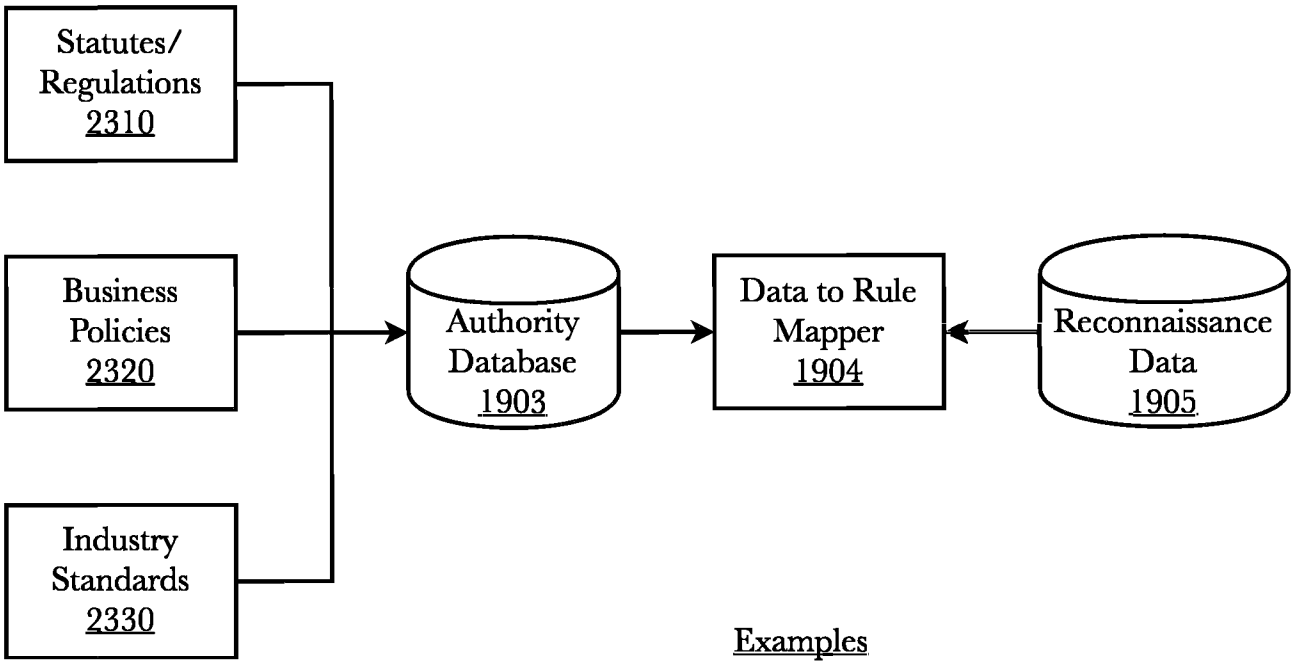

2202
2204
MemberOf
HasSession
HasSession
2205
AdminTo
2207
2203
MemberOf
2208
AdminTo
2201
AdminTo
AdminTo
ForcePWChange
2206
MemberOf
CanExploit
AdminTo
2209
CanExploit
2212
CanExploit
2211
HasSession
2210
Exemplary attack paths ranked by likelihood
1st - 1, 2, 3, 8, 12, 6
2nd - 1, 7, 4, 5, 6
3rd - 1, 10, 11, 5, 6
Device
User
Group
2200

Fig. 22



Examples

Authority	Rule	Data Point Received	Tagged with Impact
2311 GDPR Article 33, paragraph 1	Notify cognizant authority within 72 hours breach	Data breach reported online	Possible fines
2321 Corporate Policy	Do not access corp systems using personal computers	Employee account accessed using non-business computer	Possible data theft; security breach
2331 Industry Standards	No open ports accessible outside of network perimeter	Open ports detected	Possible data loss

Fig. 23

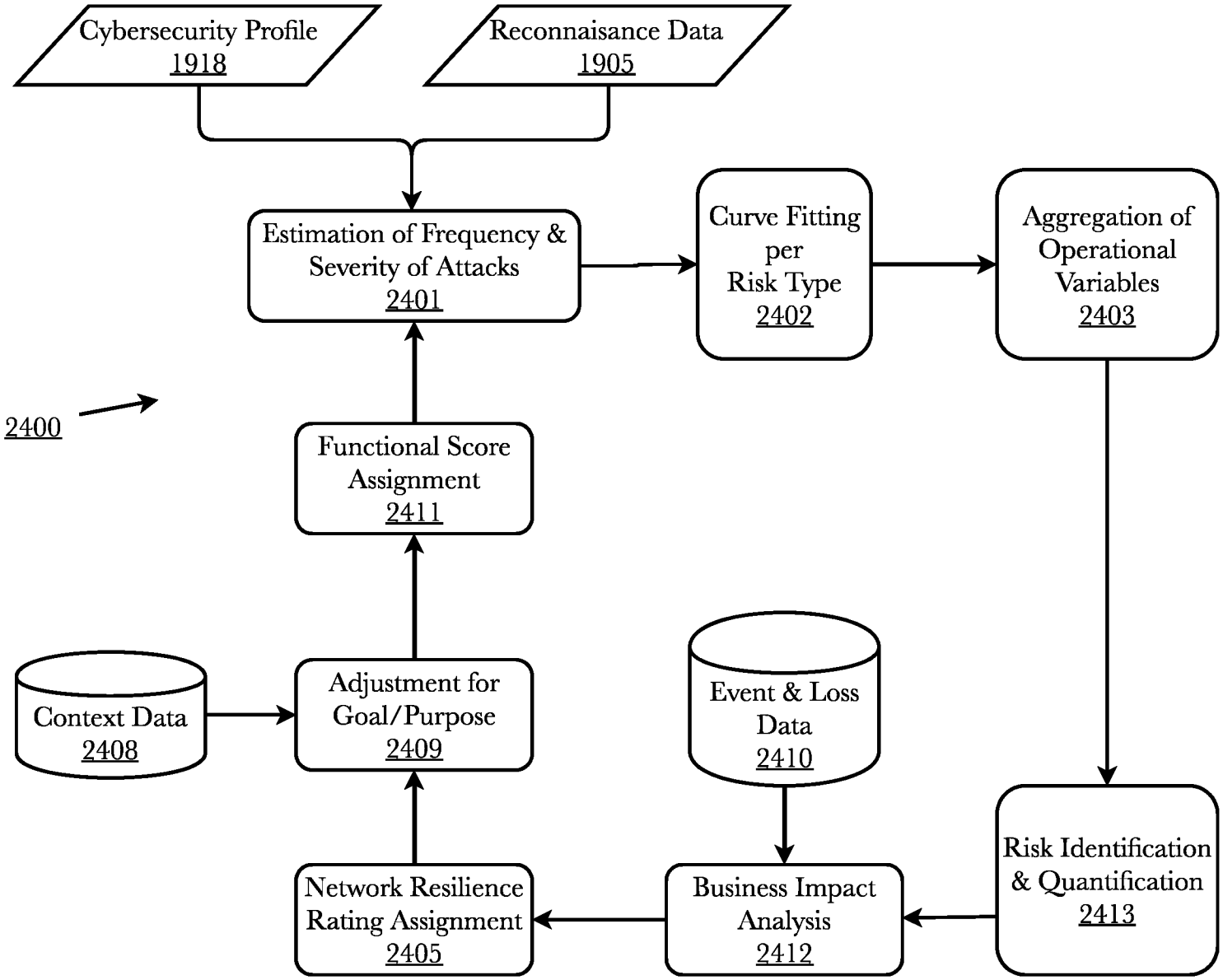

Cybersecurity Profile
1918
Reconnaisance Data
1905
Estimation of Frequency & Severity of Attacks
2401
Curve Fitting per Risk Type
2402
Aggregation of Operational Variables
2403
2400
Functional Score Assignment
2411
Context Data
2408
Adjustment for Goal/Purpose
2409
Event & Loss Data
2410
Network Resilience Rating Assignment
2405
Business Impact Analysis
2412
Risk Identification & Quantification
2413

Fig. 24

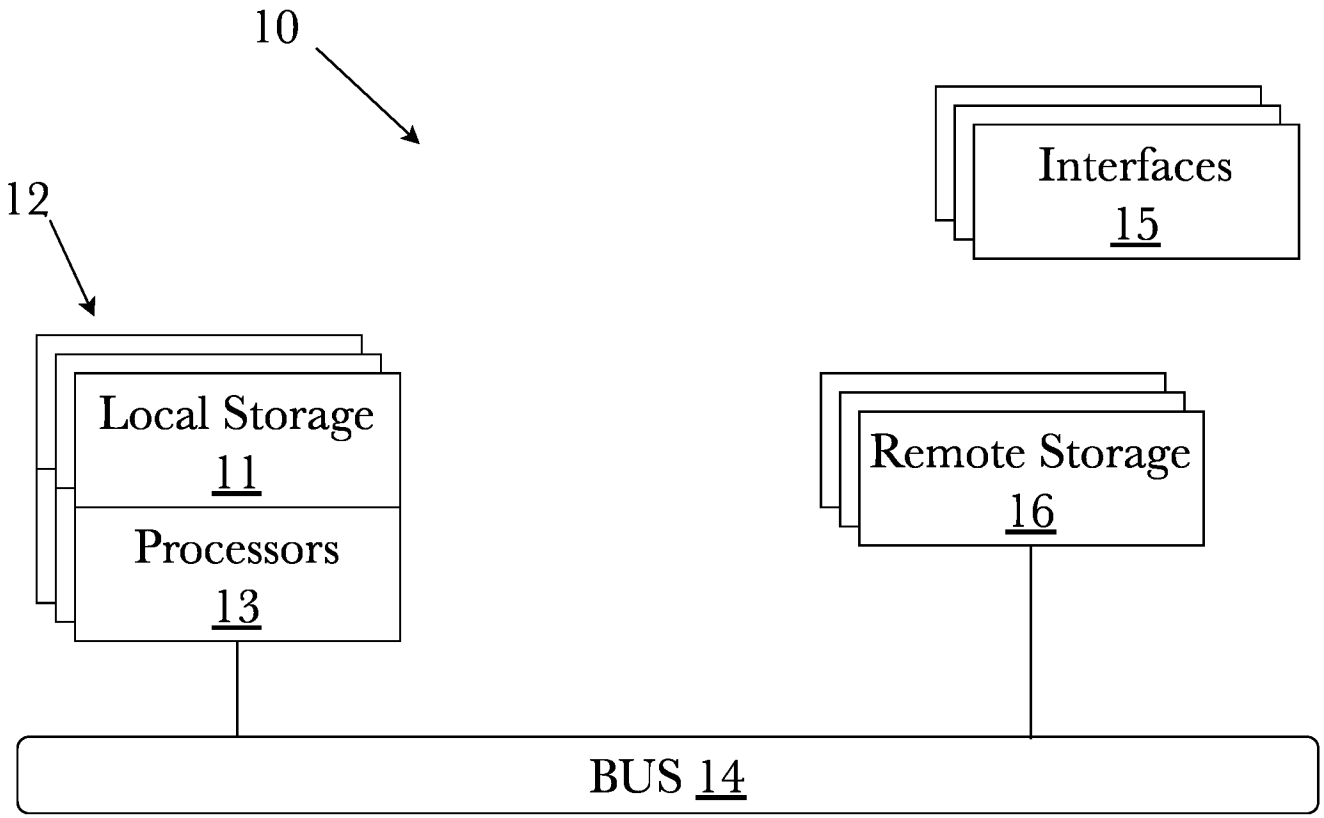

10
12
Local Storage
11
Processors
13
Interfaces
15
Remote Storage
16
BUS 14

Fig. 25

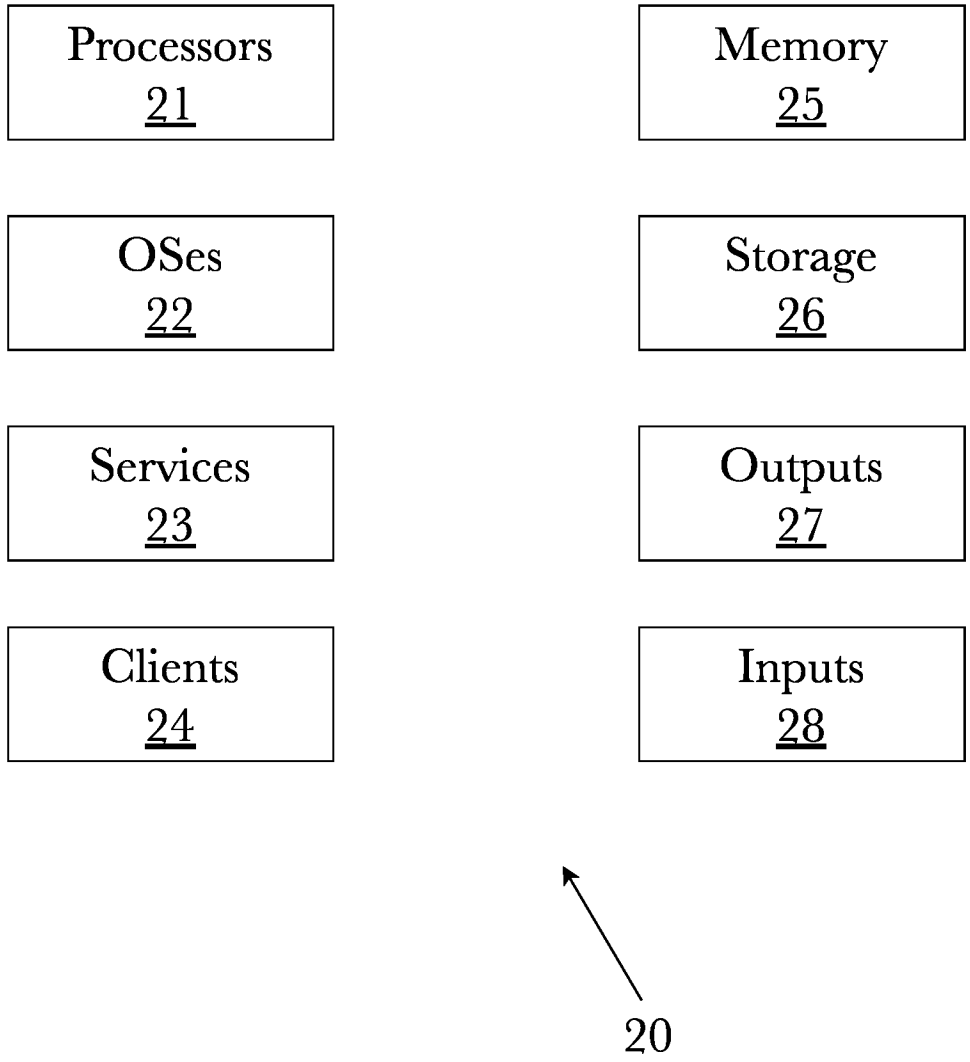

Processors
21
Memory
25
OSes
22
Storage
26
Services
23
Outputs
27
Clients
24
Inputs
28
20

Fig. 26

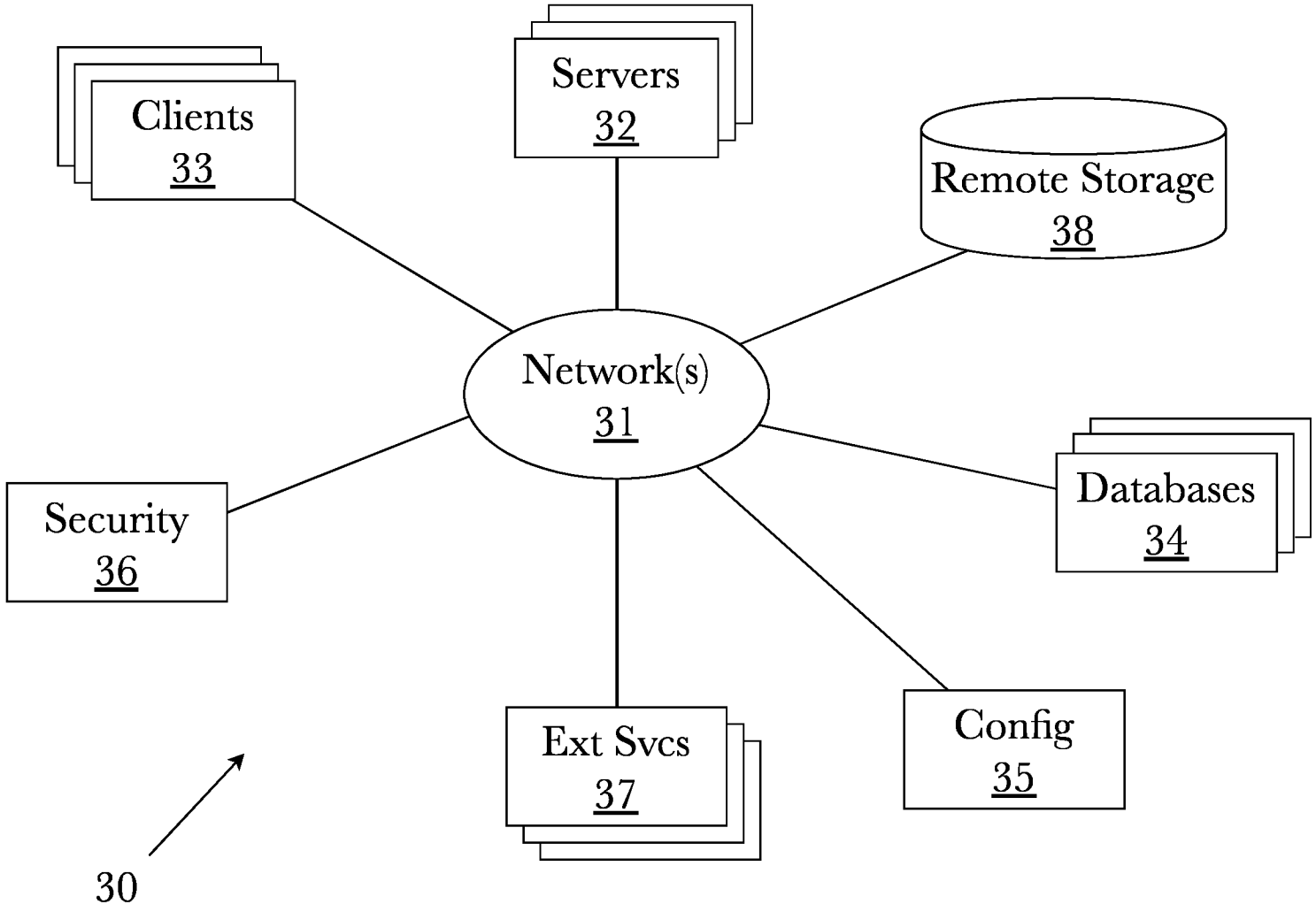

Clients
33
Servers
32
Remote Storage
38
Network(s)
31
Security
36
Databases
34
Ext Svcs
37
Config
35
30

Fig. 27

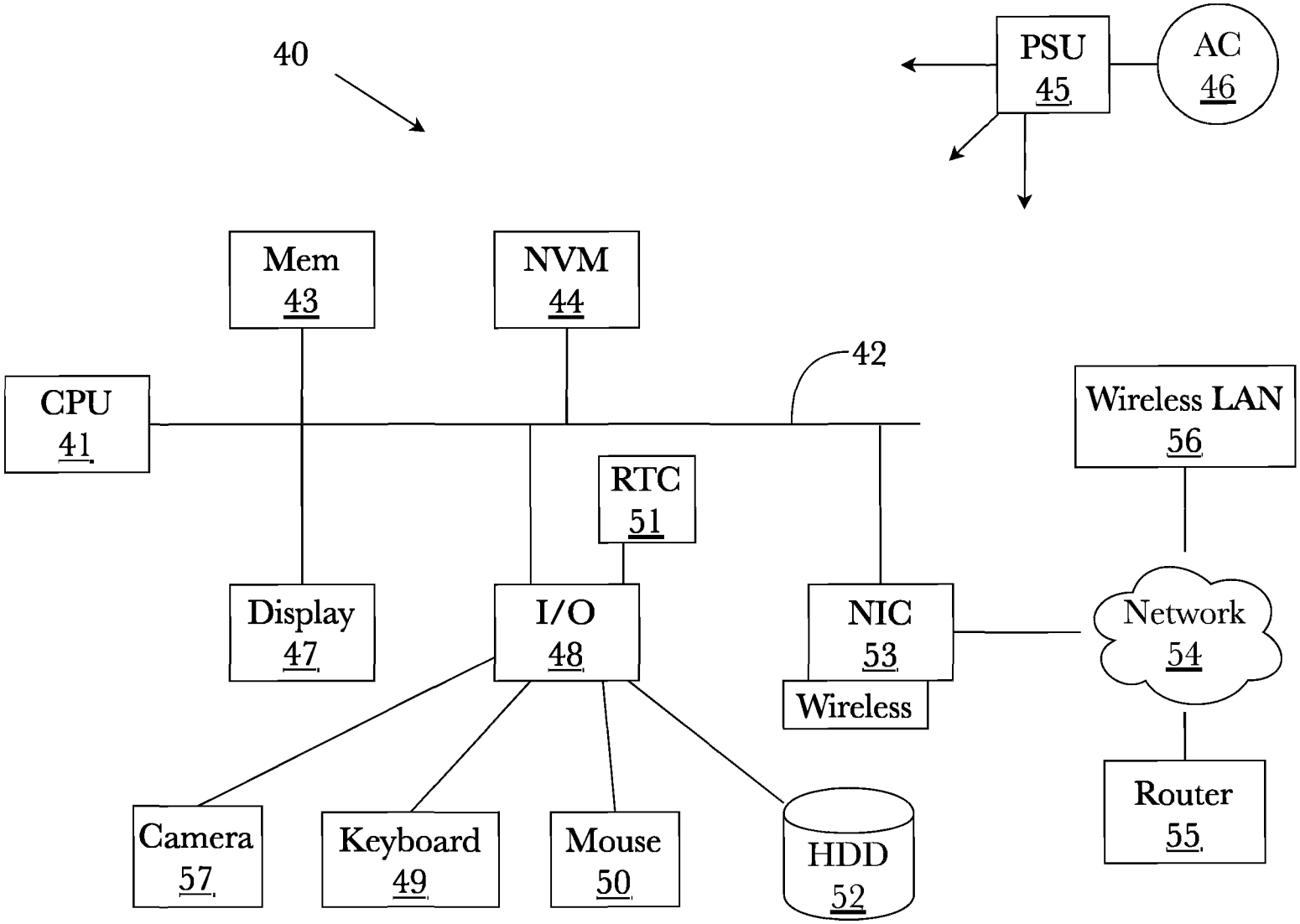

40
PSU
45
AC
46
Mem
43
NVM
44
42
CPU
41
Wireless LAN
56
RTC
51
Display
47
I/O
48
NIC
53
Wireless
Network
54
Router
55
Camera
57
Keyboard
49
Mouse
50
HDD
52

Fig. 28

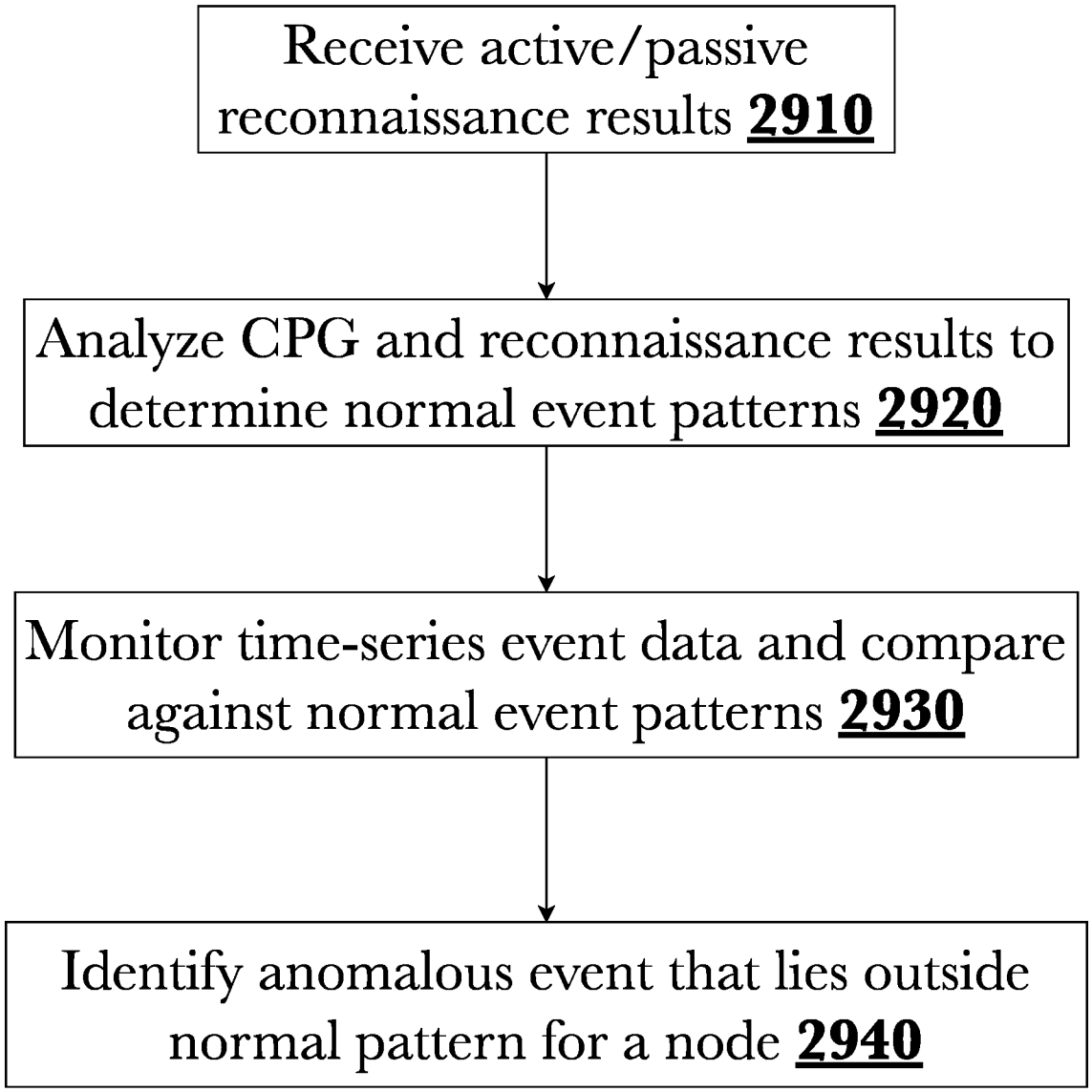

Receive active/passive reconnaissance results 2910
Analyze CPG and reconnaissance results to determine normal event patterns 2920
Monitor time-series event data and compare against normal event patterns 2930
Identify anomalous event that lies outside normal pattern for a node 2940

Fig. 29

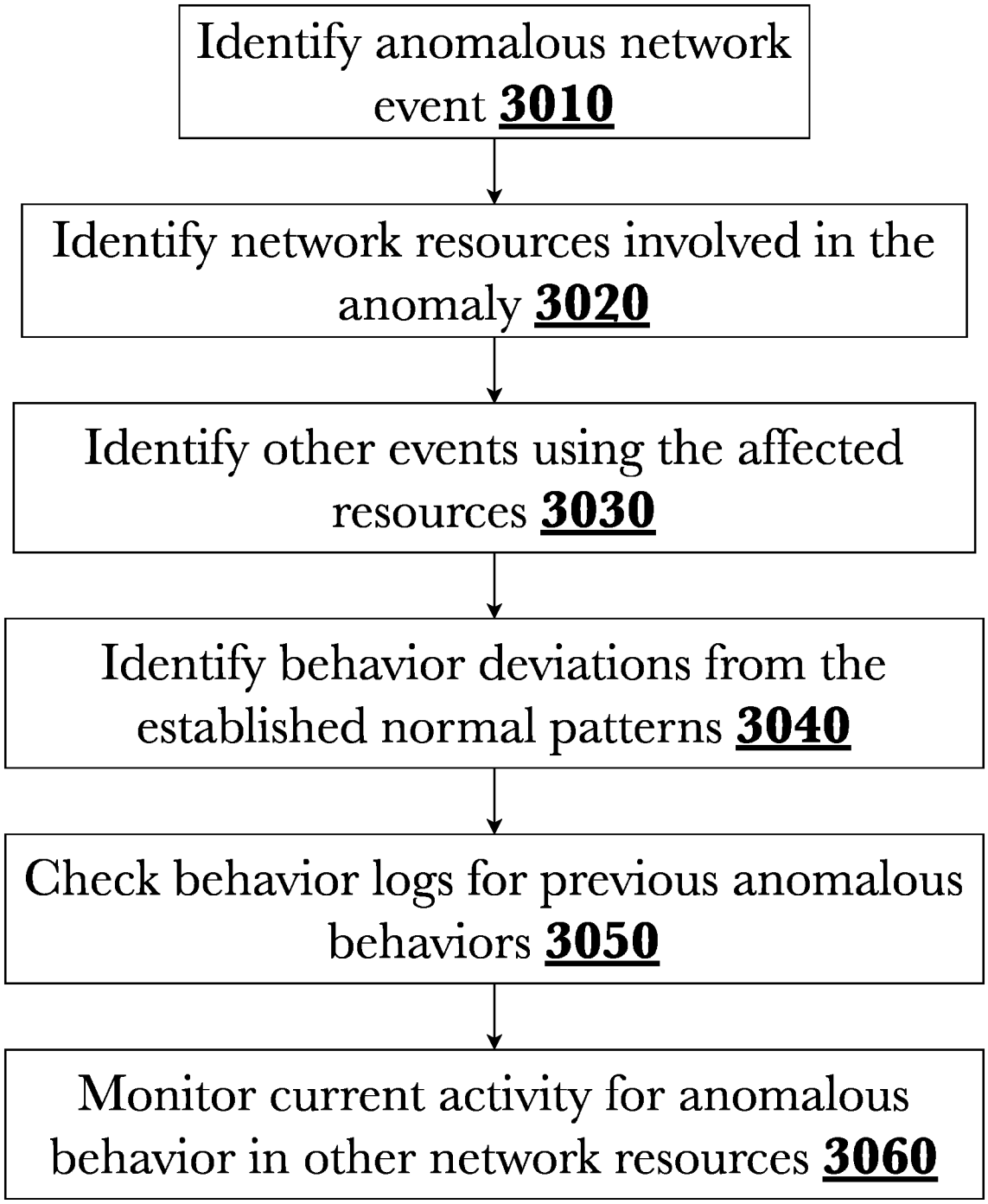

Identify anomalous network event 3010
Identify network resources involved in the anomaly 3020
Identify other events using the affected resources 3030
Identify behavior deviations from the established normal patterns 3040
Check behavior logs for previous anomalous behaviors 3050
Monitor current activity for anomalous behavior in other network resources 3060

Fig. 30

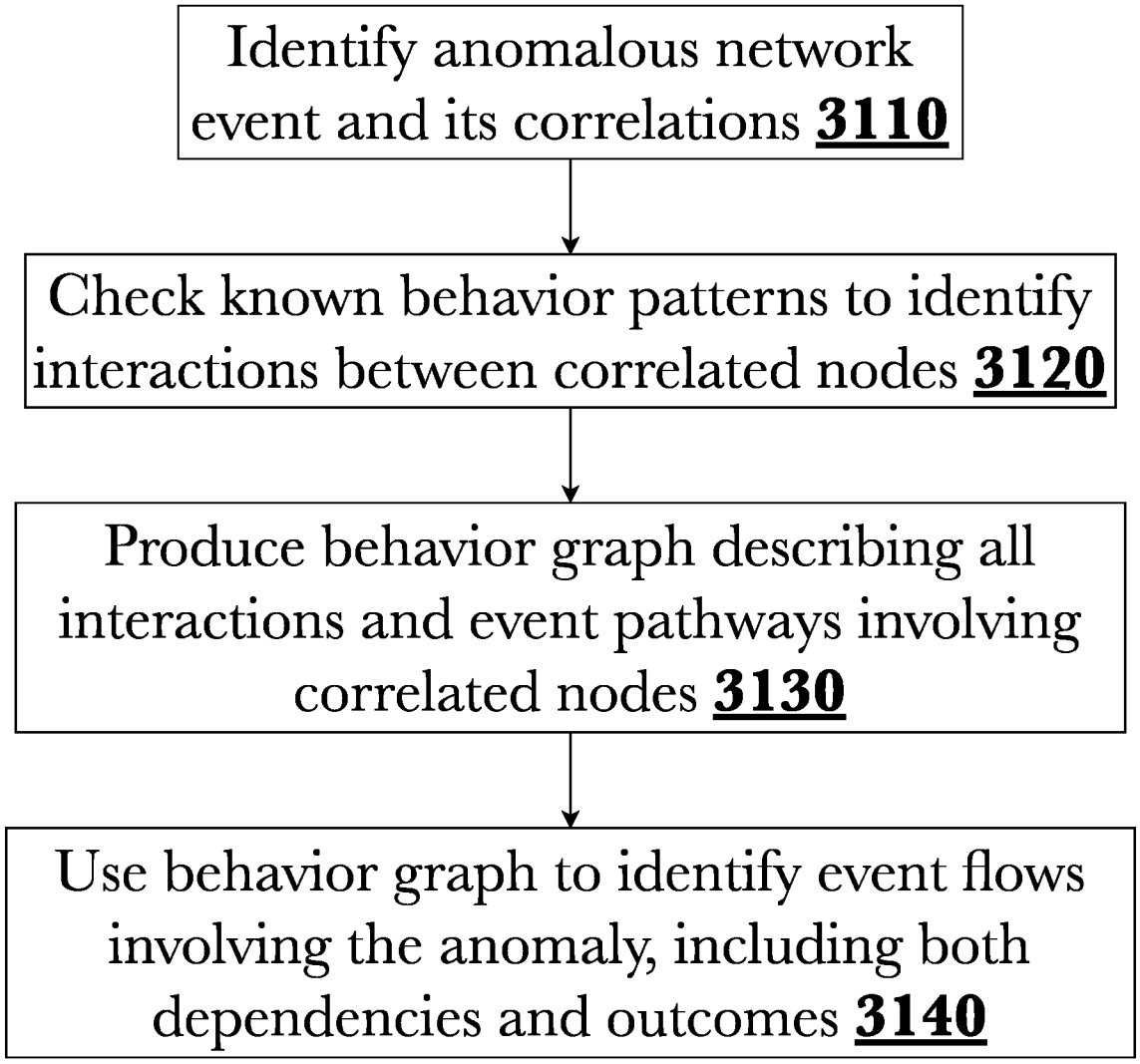

Identify anomalous network event and its correlations 3110
Check known behavior patterns to identify interactions between correlated nodes 3120
Produce behavior graph describing all interactions and event pathways involving correlated nodes 3130
Use behavior graph to identify event flows involving the anomaly, including both dependencies and outcomes 3140

Fig. 31

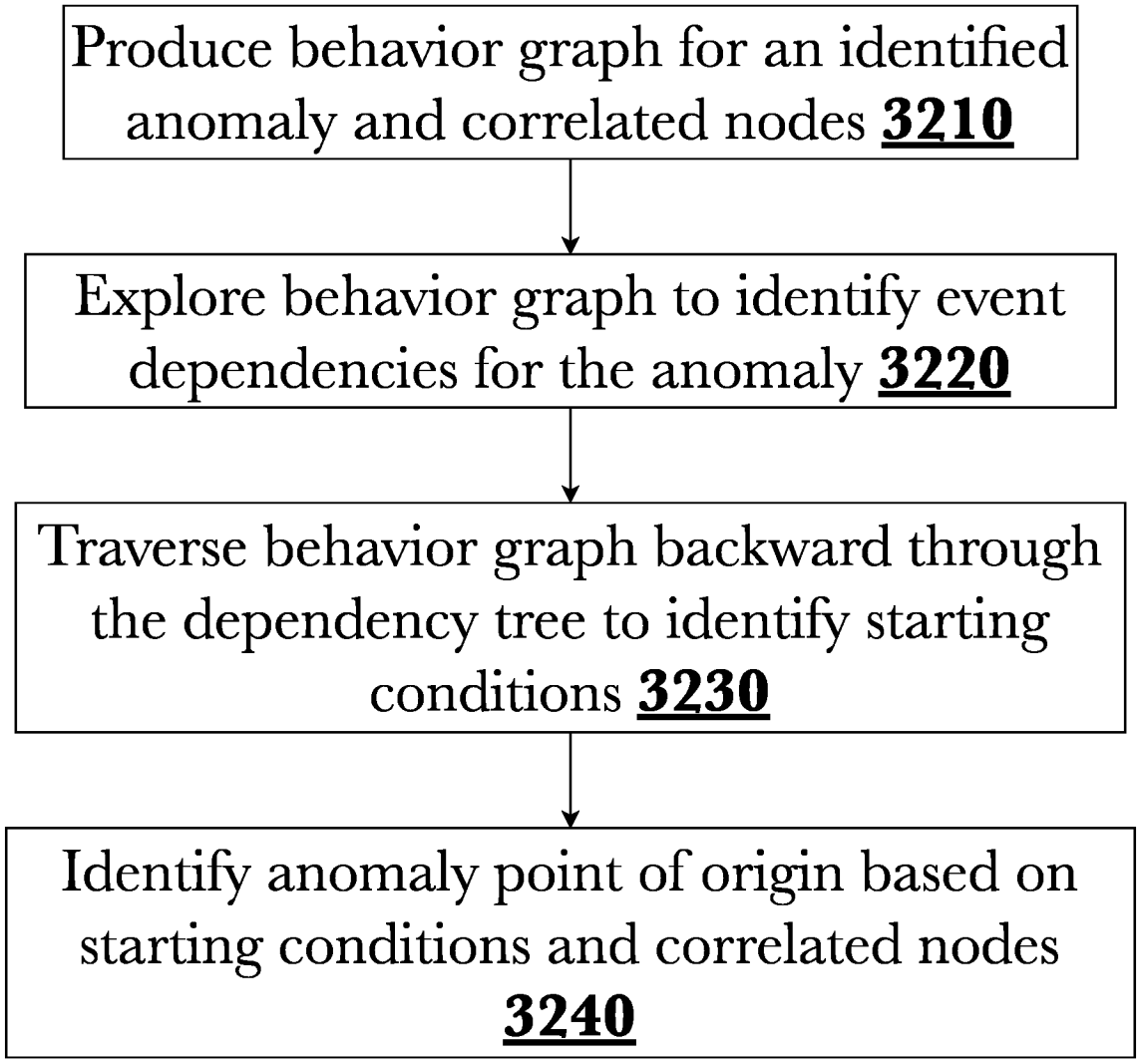

Produce behavior graph for an identified anomaly and correlated nodes 3210
Explore behavior graph to identify event dependencies for the anomaly 3220
Traverse behavior graph backward through the dependency tree to identify starting conditions 3230
Identify anomaly point of origin based on starting conditions and correlated nodes 3240

Fig. 32

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. 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	
Filing Date	2024-09-20
First Named Inventor	Jason Crabtree
Art Unit	
Examiner Name	
Attorney Docket Number	15388FT

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	6477572	B1	2002-11-05	Elderton et al.	Entire Document
	2	6906709	B1	2005-06-14	Larkin et al.	Entire Document
	3	7139747	B1	2006-11-21	Najork	Entire Document
	4	7227948	B2	2007-06-05	Ohkuma et al.	Entire Document
	5	7310632	B2	2007-12-18	Meek et al.	Entire Document
	6	7409721	B2	2008-08-05	Hernacki et al.	Entire Document
	7	7530105	B2	2009-05-05	Gilbert et al.	Entire Document
	8	7546333	B2	2009-06-09	Alon et al.	Entire Document

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	
	Filing Date	2024-09-20
	First Named Inventor	Jason Crabtree
	Art Unit	
	Examiner Name	
	Attorney Docket Number	15388FT

	9	7685296	B2	2010-03-23	Brill et al.	Entire Document
	10	7818224	B2	2010-10-19	Boerner	Entire Document
	11	7818417	B2	2010-10-19	Ginis et al.	Entire Document
	12	7925561	B2	2011-04-12	Xu	Entire Document
	13	7971252	B2	2011-06-28	Lippmann et al.	Entire Document
	14	8069190	B2	2011-11-29	McColl et al.	Entire Document
	15	8281121	B2	2012-10-02	Nath et al.	Entire Document
	16	8346753	B2	2013-01-01	Hayes	Entire Document
	17	8457996	B2	2013-06-04	Winkler et al.	Entire Document
	18	8464346	B2	2013-06-11	Barai et al.	Entire Document
	19	8516596	B2	2013-08-20	Sandoval et al.	Entire Document

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	
	Filing Date	2024-09-20
	First Named Inventor	Jason Crabtree
	Art Unit	
	Examiner Name	
	Attorney Docket Number	15388FT

	20	8751867	B2	2014-06-10	Marvasti et al.	Entire Document
	21	8752178	B2	2014-06-10	Coates et al.	Entire Document
	22	8782080	B2	2014-07-15	Lee et al.	Entire Document
	23	8881288	B1	2014-11-04	Levy et al.	Entire Document
	24	8914878	B2	2014-12-16	Burns et al.	Entire Document
	25	9100430	B1	2015-08-04	Seiver et al.	Entire Document
	26	9110706	B2	2015-08-18	Yu et al.	Entire Document
	27	9152727	B1	2015-10-06	Balducci et al.	Entire Document
	28	9231962	B1	2016-01-05	Yen et al.	Entire Document
	29	9235732	B2	2016-01-12	Eynon et al.	Entire Document
	30	9325732	B1	2016-04-26	Stickle et al.	Entire Document

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	
	Filing Date	2024-09-20
	First Named Inventor	Jason Crabtree
	Art Unit	
	Examiner Name	
	Attorney Docket Number	15388FT

	31	9344444	B2	2016-05-17	Lippmann et al.	Entire Document
	32	9400962	B2	2016-07-26	Prasad	Entire Document
	33	9466041	B2	2016-10-11	Simitsis et al.	Entire Document
	34	9507944	B2	2016-11-29	Lotem et al.	Entire Document
	35	9602530	B2	2017-03-21	Ellis et al.	Entire Document
	36	9628501	B2	2017-04-18	Datta Ray et al.	Entire Document
	37	9652538	B2	2017-05-16	Shivaswamy et al.	Entire Document
	38	9654495	B2	2017-05-16	Hubbard et al.	Entire Document
	39	9679125	B2	2017-06-13	Bailor et al.	Entire Document
	40	9686308	B1	2017-06-20	Srivastava	Entire Document
	41	9699205	B2	2017-07-04	Muddu et al.	Entire Document

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	
	Filing Date	2024-09-20
	First Named Inventor	Jason Crabtree
	Art Unit	
	Examiner Name	
	Attorney Docket Number	15388FT

	42	9712553	B2	2017-07-18	Nguyen et al.	Entire Document
	43	9736173	B2	2017-08-15	Li et al.	Entire Document
	44	9762443	B2	2017-09-12	Dickey	Entire Document
	45	9774522	B2	2017-09-26	Vasseur et al.	Entire Document
	46	9911088	B2	2018-03-06	Nath et al.	Entire Document
	47	9954884	B2	2018-04-24	Hassell et al.	Entire Document
	48	9967265	B1	2018-05-08	Peer et al.	Entire Document
	49	10021116	B2	2018-07-10	Bassett	Entire Document
	50	10044726	B2	2018-08-07	Dulkin et al.	Entire Document
	51	10083236	B2	2018-09-25	Crosby	Entire Document
	52	10191768	B2	2019-01-29	Bishop et al.	Entire Document

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	
	Filing Date	2024-09-20
	First Named Inventor	Jason Crabtree
	Art Unit	
	Examiner Name	
	Attorney Docket Number	15388FT

	53	10210246	B2	2019-02-19	Stojanovic et al.	Entire Document
	54	10210470	B2	2019-02-19	Datta Ray	Entire Document
	55	10212176	B2	2019-02-19	Wang	Entire Document
	56	10216485	B2	2019-02-26	Misra et al.	Entire Document
	57	10643144	B2	2020-05-05	Bowers et al.	Entire Document
	58	10846391	B1	2020-11-24	Bonney et al.	Entire Document
	59	11392875	B2	2022-07-19	Carstens et al.	Entire Document
	60	11836664	B2	2023-12-05	Ackerman et al.	Entire Document

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	20050165822	A1	2005-07-28	Yeung, Simon D. et al.	Entire Document

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	
	Filing Date	2024-09-20
	First Named Inventor	Jason Crabtree
	Art Unit	
	Examiner Name	
	Attorney Docket Number	15388FT

	2	20100299651	A1	2010-11-25	FAINEKOS et al.	Entire Document
	3	20110307467	A1	2011-12-15	Severance	Entire Document
	4	20120215575	A1	2012-08-23	Deb et al.	Entire Document
	5	20140244612	A1	2014-08-28	Bhasin et al.	Entire Document
	6	20140324521	A1	2014-10-30	Mun	Entire Document
	7	20150347414	A1	2015-12-03	Xiao et al.	Entire Document
	8	20160006629	A1	2016-01-07	Ianakiev et al.	Entire Document
	9	20160012235	A1	2016-01-14	Lee et al.	Entire Document
	10	20160057159	A1	2016-02-25	Yin et al.	Entire Document
	11	20170090893	A1	2017-03-30	Aditya et al.	Entire Document
	12	20180082304	A1	2018-03-22	Summerlin et al.	Entire Document

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	
	Filing Date	2024-09-20
	First Named Inventor	Jason Crabtree
	Art Unit	
	Examiner Name	
	Attorney Docket Number	15388FT

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] ¡	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]
	1	EBERLE, WILLIAM, HOLDER, LAWRENCE; Incremental Anomaly Detection in Graphs, 2013 IEEE 13th International Conference on Data Mining Workshops	☐
	2	HUANG, ALEX, A Comparison of Value at Risk Approaches and a New Method with Extreme Value Theory and Kernel Estimator	☐
	3	MAROZZO, Fabrizio; TALIA, Domenico; TRUNFIO, Paolo; P2P-MapReduce - Parallel Data Processing in Dynamic Cloud Environments, Journal of Computer and System Sciences, 78 (2012) 1382–1402	☐
	4	SIMONIAN, Joseph, DAVIS, Josh., Robust Value-At-Risk: An Information Theoretic Approach, Applied Economic Letters, 2010, 17, 1551-1553.	☐

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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	
	Filing Date	2024-09-20
	First Named Inventor	Jason Crabtree
	Art Unit	
	Examiner Name	
	Attorney Docket Number	15388FT

[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	
	Filing Date	2024-09-20
	First Named Inventor	Jason Crabtree
	Art Unit	
	Examiner Name	
	Attorney Docket Number	15388FT

CERTIFICATION STATEMENT

Please see 37 CFR 1.97(e) 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.

☒ A certification statement is not submitted herewith.

FEE

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

COPIES

☐ An identification of an earlier application pursuant to 37 CFR 1.98 (d) (1) is attached.

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	/BRIAN R. GALVIN/	Date (YYYY-MM-DD)	2024-09-20
Name/Print	Brian R. Galvin	Registration Number	50966

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.

PTO/AIA/01 (06-12)
Approved for use through 11/30/2020. 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.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [x] The attached application, or
- [ ] United States application or PCT international application number _____

filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Jason Crabtree Date (Optional) :_____

Signature: _____

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. 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 1 minute 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.

Doc ID: d7052b2b838a3b7fac6e89cc3ed044442f1f4022

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/892,283	**09/20/2024 09:26:06 PM Z ET**	**15388FT**

Title of Invention

CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	7526	FILED BY	Aura Morrey
PATENT CENTER #	67266989	AUTHORIZED BY	Brian Galvin
CUSTOMER #	82318	FILING DATE	-
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	Jason Crabtree

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 1009	**E20249JL27129906**	**Aura Morrey**

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
1830	PROCESSING FEE, EXCEPT IN PROVISIONAL APPLICATIONS	140.00	1	140.00
1817	REQUEST FOR PRIORITIZED EXAMINATION	4200.00	1	4200.00
1111	UTILITY PATENT APPL. SEARCH FEE	700.00	1	700.00
1011	BASIC FILING FEE - UTILITY (PAPER FILING ALSO REQUIRES NON-ELECTRONIC FILING FEE UNDER 1.16(T))	320.00	1	320.00
1311	PATENT APPL. EXAMINATION FEE	800.00	1	800.00
			TOTAL	**$6,160.00**

AMOUNT:

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 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.

CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation of U.S. patent application Ser. No. 17/237,346, titled "CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION", filed on April 22, 2021, which is a continuation-in-part of U.S. patent application Ser. No. 16/777,270, titled "CYBERSECURITY PROFILING AND RATING USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE", filed on Jan. 30, 2020, now issued as U.S. Patent No. 11,025,674 on Jun. 1, 2021, which is a continuation-in-part of U.S. patent application Ser. No. 16/720,383, titled "RATING ORGANIZATION CYBERSECURITY USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE", filed on Dec. 19, 2019, now issued as U.S. Patent No. 10,944,795 on Mar. 9, 2021, which is a continuation of U.S. patent application Ser. No. 15/823,363, filed on Nov. 27, 2017, now issued as U.S. Patent No. 10,560,483 on Feb. 11, 2020, which is a continuation-in-part of U.S. patent application Ser. No. 15/725,274, titled "APPLICATION OF ADVANCED CYBERSECURITY THREAT MITIGATION TO ROGUE DEVICES, PRIVILEGE ESCALATION, AND RISK-BASED VULNERABILITY AND PATCH MANAGEMENT", filed on Oct. 4, 2017, now issued as 10,609,079 on Mar. 31, 2020, which is a continuation-in-part of U.S. patent application Ser. No. 15/655,113, titled "ADVANCED CYBERSECURITY THREAT MITIGATION USING BEHAVIORAL AND DEEP ANALYTICS", filed on Jul. 20, 2017, now issued as U.S. Patent No. 10,735,456 on Aug. 4, 2020, which is a continuation-in-part of U.S. patent application Ser. No. 15/616,427, titled "RAPID PREDICTIVE ANALYSIS OF VERY LARGE DATA SETS USING AN ACTOR-DRIVEN DISTRIBUTED COMPUTATIONAL GRAPH", filed on Jun. 7, 2017, which is a continuation-in-part of U.S. patent application Ser. No. 14/925,974, titled "RAPID PREDICTIVE ANALYSIS OF VERY LARGE DATA SETS USING THE DISTRIBUTED COMPUTATIONAL GRAPH", filed on Oct. 28, 2015; said application Ser. No. 15/655,113 is also a continuation-in-part of U.S. patent application Ser. No. 15/237,625, titled "DETECTION MITIGATION AND REMEDIATION OF CYBERATTACKS EMPLOYING AN

ADVANCED CYBER-DECISION PLATFORM", filed on Aug. 15, 2016, now issued as U.S. Patent No. 10,248,910 on Apr. 2, 2019, which is a continuation-in-part of U.S. patent application Ser. No. 15/206,195, titled "ACCURATE AND DETAILED MODELING OF SYSTEMS WITH LARGE COMPLEX DATA SETS USING A DISTRIBUTED SIMULATION ENGINE", filed on Jul. 8, 2016, which is a continuation-in-part of U.S. patent application Ser. No. 15/186,453, titled "SYSTEM FOR AUTOMATED CAPTURE AND ANALYSIS OF BUSINESS INFORMATION FOR RELIABLE BUSINESS VENTURE OUTCOME PREDICTION", filed on Jun. 18, 2016, which is a continuation-in-part of U.S. patent application Ser. No. 15/166,158, titled "SYSTEM FOR AUTOMATED CAPTURE AND ANALYSIS OF BUSINESS INFORMATION FOR SECURITY AND CLIENT-FACING INFRASTRUCTURE RELIABILITY", filed on May 26, 2016, which is a continuation-in-part of U.S. patent application Ser. No. 15/141,752, titled "SYSTEM FOR FULLY INTEGRATED CAPTURE, AND ANALYSIS OF BUSINESS INFORMATION RESULTING IN PREDICTIVE DECISION MAKING AND SIMULATION", filed on Apr. 28, 2016, now issued as 10,860,962 on Dec. 8, 2020, which is a continuation-in-part of U.S. patent application Ser. No. 15/091,563, titled "SYSTEM FOR CAPTURE, ANALYSIS AND STORAGE OF TIME SERIES DATA FROM SENSORS WITH HETEROGENEOUS REPORT INTERVAL PROFILES", filed on Apr. 5, 2016, now issued as U.S. Patent No. 10,204,147 on Feb. 12, 2019, and is also a continuation-in-part of U.S. patent application Ser. No. 14/986,536, titled "DISTRIBUTED SYSTEM FOR LARGE VOLUME DEEP WEB DATA EXTRACTION", filed on Dec. 31, 2015, now issued as U.S. Patent No. 10,210,255 on Feb. 19, 2019, and is also a continuation-in-part of U.S. patent application Ser. No. 14/925,974, titled "RAPID PREDICTIVE ANALYSIS OF VERY LARGE DATA SETS USING THE DISTRIBUTED COMPUTATIONAL GRAPH", filed on Oct. 28, 2015, the entire contents of all of which are incorporated herein by reference in their entirety.

BACKGROUND OF THE INVENTION

Field of the Invention

[0002] The disclosure relates to the field of computer management, and more particularly to the field of cybersecurity and threat analytics.

Discussion of the State of the Art

[0003] Understanding the cybersecurity profile of an organization is a complex endeavor, and the larger the organization, the more difficult the task is. In fact, the complexity of the task increases exponentially with the size of the organization, not linearly, because each component of the organization's network connects to multiple other components. Existing cybersecurity rating methods (for example, the Common Vulnerability Scoring Systems, or CVSS) fail to adequately profile and rate the cybersecurity profiles of organizations because they do not incorporate sufficient information.

[0004] What is needed is a system and method for monitoring critical infrastructure entities within a network, identifying anomalous network events, and correlating those anomalous events to identify attack paths and points of origin.

SUMMARY OF THE INVENTION

[0005] Accordingly, the inventor has developed a system and method for correlating network event anomalies using active and passive reconnaissance to identify attack information, that can identify attack patterns and points of origin based on observed anomalies and their relationships to other observed network events. The system and method may further comprise gathering data about the totality of the organization's infrastructure and operations, particularly including the organization's network infrastructure, but also including such information as physical locations, data assets, corporate legal structure, etc., and gathering data about the organization's operations, including such information as business processes and policies, business process dependencies, prior data loss information and security breaches, and behavioral data for both devices and their users. The system and method may further comprise generating a cybersecurity profile using active and passive internal and external reconnaissance of the organization to determine cybersecurity vulnerabilities and potential impacts to the business in light of the information gathered about the organization's infrastructure and operations. The system and method may further comprise generating cybersecurity scores and ratings that take into account all of the above information, plus the context and purpose of the score or rating to be generated based on the cybersecurity profile.

[0006] According to a preferred embodiment, a system for correlating network event anomalies to identify attack information, comprising: a cyber-physical graph module comprising a first plurality of programming instructions stored in a memory of, and operating on a processor of, a

computing device, wherein the first plurality of programming instructions, when operating on the processor, cause the computing device to create a cyber-physical graph of the organization using the information, the cyber-physical graph comprising nodes representing entities associated with the organization and edges representing relationships between entities associated with the organization; a reconnaissance engine comprising a second plurality of programming instructions stored in the memory of, and operating on the processor of, the computing device, wherein the second plurality of programming instructions, when operating on the processor, cause the computing device to: perform a reconnaissance search using the cyber-physical graph; and apply some or all of the results of the reconnaissance search to the cyber-physical graph to create a normal behavior model for a plurality of nodes in the cyber-physical graph; and a directed computational graph engine comprising a third plurality of programming instructions stored in the memory of, and operating on the processor of, the computing device, wherein the third plurality of programming instructions, when operating on the processor, cause the computing device to: receive the cybersecurity profile and the normal behavior model; using the cyber-physical graph and the normal behavior model: identify an anomalous event based on analysis of cyber-physical graph and the normal behavior model; analyze the cyber-physical graph and the normal behavior model to identify correlations between affected nodes, the affected nodes being based on the anomalous event; generate a behavior graph based on the identified correlations; analyze the behavior graph to produce a dependency tree comprising causative relationships between events; and traverse the behavior tree backward in a temporal dimension to identify a plurality of starting conditions for the anomalous event, is disclosed.

[0007] According to another preferred embodiment, a method for correlating network event anomalies to identify attack information, comprising the steps of: creating a cyber-physical graph of an organization using entities associated with the organization and relationships between the entities associated with the organization, the cyber-physical graph comprising nodes representing the entities associated with the organization and edges representing the relationships between entities associated with the organization; performing a reconnaissance search using the cyber-physical graph; applying some or all of the results of the reconnaissance search to the cyber-physical graph to create a normal behavior model for a plurality of nodes in the cyber-physical graph; and using the cyber-physical graph and the normal behavior model: identifying an anomalous event based on analysis of cyber-physical graph and the normal behavior model;

analyzing the cyber-physical graph and the normal behavior model to identify correlations between affected nodes, the affected nodes being based on the anomalous event; generating a behavior graph based on the identified correlations; analyzing the behavior graph to produce a dependency tree comprising causative relationships between events; and traversing the behavior tree backward in a temporal dimension to identify a plurality of starting conditions for the anomalous event, is disclosed.

[0008] According to an aspect of an embodiment, a directed computational graph is used, comprising nodes representing data transformations and edges representing communications between the nodes; wherein a plurality of nodes represents a data transformation pipeline; and wherein the directed computational graph is used to direct a workflow in the system.

BRIEF DESCRIPTION OF THE DRAWING FIGURES

[0009] The accompanying drawings illustrate several aspects and, together with the description, serve to explain the principles of the invention according to the aspects. It will be appreciated by one skilled in the art that the particular arrangements illustrated in the drawings are merely exemplary, and are not to be considered as limiting of the scope of the invention or the claims herein in any way.

[0010] Fig. 1 is a block diagram of an exemplary system architecture for an advanced cyber decision platform for external network reconnaissance and cybersecurity rating.

[0011] Fig. 2A is a block diagram showing general steps for performing passive network reconnaissance.

[0012] Fig. 2B is a process diagram showing a general flow of a process for performing active reconnaissance using DNS leak information collection.

[0013] Fig. 2C is a process diagram showing a general flow of a process for performing active reconnaissance using web application and technology reconnaissance.

[0014] Fig. 2D is a process diagram showing a general flow of a process for producing a cybersecurity rating using reconnaissance data.

[0015] Figs. 3A and **3B** are process diagrams showing business operating system functions in use to mitigate cyberattacks.

[0016] Fig. 4 is a process flow diagram of a method for segmenting cyberattack information to appropriate corporation parties.

[0017] Fig. 5 is a diagram of an exemplary architecture for a system for rapid predictive analysis of very large data sets using an actor-driven distributed computational graph, according to one aspect.

[0018] Fig. 6 is a diagram of an exemplary architecture for a system for rapid predictive analysis of very large data sets using an actor-driven distributed computational graph, according to one aspect.

[0019] Fig. 7 is a diagram of an exemplary architecture for a system for rapid predictive analysis of very large data sets using an actor-driven distributed computational graph, according to one aspect.

[0020] Fig. 8 is a flow diagram of an exemplary method for cybersecurity behavioral analytics, according to one aspect.

[0021] Fig. 9 is a flow diagram of an exemplary method for measuring the effects of cybersecurity attacks, according to one aspect.

[0022] Fig. 10 is a flow diagram of an exemplary method for continuous cybersecurity monitoring and exploration, according to one aspect.

[0023] Fig. 11 is a flow diagram of an exemplary method for mapping a cyber-physical system graph, according to one aspect.

[0024] Fig. 12 is a flow diagram of an exemplary method for continuous network resilience rating, according to one aspect.

[0025] Fig. 13 is a flow diagram of an exemplary method for cybersecurity privilege oversight, according to one aspect.

[0026] Fig. 14 is a flow diagram of an exemplary method for cybersecurity risk management, according to one aspect.

[0027] Fig. 15 is a flow diagram of an exemplary method for mitigating compromised credential threats, according to one aspect.

[0028] Fig. 16 is a flow diagram of an exemplary method for dynamic network and rogue device discovery, according to one aspect.

[0029] Fig. 17 is a flow diagram of an exemplary method for Kerberos “golden ticket” attack detection, according to one aspect.

[0030] Fig. 18 is a flow diagram of an exemplary method for risk-based vulnerability and patch management, according to one aspect.

[0031] Fig. 19 is a block diagram showing an exemplary system architecture for a system for cybersecurity profiling and rating.

[0032] Fig. 20 is a relational diagram showing the relationships between exemplary 3rd party search tools, search tasks that can be generated using such tools, and the types of information that may be gathered with those tasks.

[0033] Fig. 21 is a relational diagram showing the exemplary types and classifications of information that may be used in constructing a cyber-physical graph of an organization's infrastructure and operations.

[0034] Fig. 22 is a directed graph diagram showing an exemplary cyber-physical graph and its possible use in analyzing cybersecurity threats.

[0035] Fig. 23 is a block diagram showing exemplary operation of a data to rule mapper.

[0036] Fig. 24 is a block diagram showing an exemplary architecture diagram for a scoring engine.

[0037] Fig. 25 is a block diagram illustrating an exemplary hardware architecture of a computing device.

[0038] Fig. 26 is a block diagram illustrating an exemplary logical architecture for a client device.

[0039] Fig. 27 is a block diagram illustrating an exemplary architectural arrangement of clients, servers, and external services.

[0040] Fig. 28 is another block diagram illustrating an exemplary hardware architecture of a computing device.

[0041] Fig. 29 is a flow diagram illustrating an exemplary method for identifying an anomalous network event.

[0042] Fig. 30 is a flow diagram illustrating an exemplary method for identifying correlations between an anomaly and other network events and resources.

[0043] Fig. 31 is a flow diagram illustrating an exemplary method for generating a behavior graph based on an identified anomaly and its correlations.

[0044] Fig. 32 is a flow diagram illustrating an exemplary method for determining an attack's point of origin using a behavior graph.

DETAILED DESCRIPTION OF THE INVENTION

[0045] The inventor has conceived, and reduced to practice, a system and method for correlating network event anomalies using active and passive reconnaissance to identify attack information, that can identify attack patterns and points of origin based on observed anomalies and their relationships to other observed network events. The system and method may further comprise gathering data about the totality of the organization's infrastructure and operations, particularly including the organization's network infrastructure, but also including such information as physical locations, data assets, corporate legal structure, etc., and gathering data about the organization's operations, including such information as business processes and policies, business process dependencies, prior data loss information and security breaches, and behavioral data for both devices and their users. The system and method may further comprise generating a cybersecurity profile using active and passive internal and external reconnaissance of the organization to determine cybersecurity vulnerabilities and potential impacts to the business in light of the information gathered about the organization's infrastructure and operations. The system and method may further comprise generating cybersecurity scores and ratings that take into account all of the above information, plus the context and purpose of the score or rating to be generated based on the cybersecurity profile.

[0046] One or more different aspects may be described in the present application. Further, for one or more of the aspects described herein, numerous alternative arrangements may be described; it should be appreciated that these are presented for illustrative purposes only and are not limiting of the aspects contained herein or the claims presented herein in any way. One or more of the arrangements may be widely applicable to numerous aspects, as may be readily apparent from the disclosure. In general, arrangements are described in sufficient detail to enable those skilled in the art to practice one or more of the aspects, and it should be appreciated that other arrangements may be utilized and that structural, logical, software, electrical and other changes may be made without departing from the scope of the particular aspects. Particular features of one or more of the aspects described herein may be described with reference to one or more particular aspects or figures that form a part of the present disclosure, and in which are shown, by way of illustration, specific arrangements of one or more of the aspects. It should be appreciated, however, that such features are not limited to usage in the one or more particular aspects or figures with reference to which they are described. The present disclosure is neither a

literal description of all arrangements of one or more of the aspects nor a listing of features of one or more of the aspects that must be present in all arrangements.

[0047] Headings of sections provided in this patent application and the title of this patent application are for convenience only, and are not to be taken as limiting the disclosure in any way.

[0048] Devices that are in communication with each other need not be in continuous communication with each other, unless expressly specified otherwise. In addition, devices that are in communication with each other may communicate directly or indirectly through one or more communication means or intermediaries, logical or physical.

[0049] A description of an aspect with several components in communication with each other does not imply that all such components are required. To the contrary, a variety of optional components may be described to illustrate a wide variety of possible aspects and in order to more fully illustrate one or more aspects. Similarly, although process steps, method steps, algorithms or the like may be described in a sequential order, such processes, methods and algorithms may generally be configured to work in alternate orders, unless specifically stated to the contrary. In other words, any sequence or order of steps that may be described in this patent application does not, in and of itself, indicate a requirement that the steps be performed in that order. The steps of described processes may be performed in any order practical. Further, some steps may be performed simultaneously despite being described or implied as occurring non-simultaneously (e.g., because one step is described after the other step). Moreover, the illustration of a process by its depiction in a drawing does not imply that the illustrated process is exclusive of other variations and modifications thereto, does not imply that the illustrated process or any of its steps are necessary to one or more of the aspects, and does not imply that the illustrated process is preferred. Also, steps are generally described once per aspect, but this does not mean they must occur once, or that they may only occur once each time a process, method, or algorithm is carried out or executed. Some steps may be omitted in some aspects or some occurrences, or some steps may be executed more than once in a given aspect or occurrence.

[0050] When a single device or article is described herein, it will be readily apparent that more than one device or article may be used in place of a single device or article. Similarly, where more than one device or article is described herein, it will be readily apparent that a single device or article may be used in place of the more than one device or article.

[0051] The functionality or the features of a device may be alternatively embodied by one or more other devices that are not explicitly described as having such functionality or features. Thus, other aspects need not include the device itself.

[0052] Techniques and mechanisms described or referenced herein will sometimes be described in singular form for clarity. However, it should be appreciated that particular aspects may include multiple iterations of a technique or multiple instantiations of a mechanism unless noted otherwise. Process descriptions or blocks in figures should be understood as representing modules, segments, or portions of code which include one or more executable instructions for implementing specific logical functions or steps in the process. Alternate implementations are included within the scope of various aspects in which, for example, functions may be executed out of order from that shown or discussed, including substantially concurrently or in reverse order, depending on the functionality involved, as would be understood by those having ordinary skill in the art.

Definitions

[0053] As used herein, "graph" is a representation of information and relationships, where each primary unit of information makes up a "node" or "vertex" of the graph and the relationship between two nodes makes up an edge of the graph. Nodes can be further qualified by the connection of one or more descriptors or "properties" to that node. For example, given the node "James R," name information for a person, qualifying properties might be "183 cm tall", "DOB 08/13/1965" and "speaks English". Similar to the use of properties to further describe the information in a node, a relationship between two nodes that forms an edge can be qualified using a "label". Thus, given a second node "Thomas G," an edge between "James R" and "Thomas G" that indicates that the two people know each other might be labeled "knows." When graph theory notation (Graph = (Vertices, Edges)) is applied this situation, the set of nodes are used as one parameter of the ordered pair,V and the set of 2 element edge endpoints are used as the second parameter of the ordered pair, E. When the order of the edge endpoints within the pairs of E is not significant, for example, the edge James R, Thomas G is equivalent to Thomas G, James R, the graph is designated as "undirected." Under circumstances when a relationship flows from one node to another in one direction, for example James R is "taller" than Thomas G, the order of the endpoints is significant. Graphs with such edges are designated as "directed." In the distributed computational graph system, transformations within transformation pipeline are

represented as directed graph with each transformation comprising a node and the output messages between transformations comprising edges. Distributed computational graph stipulates the potential use of non-linear transformation pipelines which are programmatically linearized. Such linearization can result in exponential growth of resource consumption. The most sensible approach to overcome possibility is to introduce new transformation pipelines just as they are needed, creating only those that are ready to compute. Such method results in transformation graphs which are highly variable in size and node, edge composition as the system processes data streams. Those familiar with the art will realize that transformation graph may assume many shapes and sizes with a vast topography of edge relationships. The examples given were chosen for illustrative purposes only and represent a small number of the simplest of possibilities. These examples should not be taken to define the possible graphs expected as part of operation of the invention

[0054] As used herein, "transformation" is a function performed on zero or more streams of input data which results in a single stream of output which may or may not then be used as input for another transformation. Transformations may comprise any combination of machine, human or machine-human interactions Transformations need not change data that enters them, one example of this type of transformation would be a storage transformation which would receive input and then act as a queue for that data for subsequent transformations. As implied above, a specific transformation may generate output data in the absence of input data. A time stamp serves as a example. In the invention, transformations are placed into pipelines such that the output of one transformation may serve as an input for another. These pipelines can consist of two or more transformations with the number of transformations limited only by the resources of the system. Historically, transformation pipelines have been linear with each transformation in the pipeline receiving input from one antecedent and providing output to one subsequent with no branching or iteration. Other pipeline configurations are possible. The invention is designed to permit several of these configurations including, but not limited to: linear, afferent branch, efferent branch and cyclical.

[0055] A "database" or "data storage subsystem" (these terms may be considered substantially synonymous), as used herein, is a system adapted for the long-term storage, indexing, and retrieval of data, the retrieval typically being via some sort of querying interface or language. "Database" may be used to refer to relational database management systems known in the art,

but should not be considered to be limited to such systems. Many alternative database or data storage system technologies have been, and indeed are being, introduced in the art, including but not limited to distributed non-relational data storage systems such as Hadoop, column-oriented databases, in-memory databases, and the like. While various aspects may preferentially employ one or another of the various data storage subsystems available in the art (or available in the future), the invention should not be construed to be so limited, as any data storage architecture may be used according to the aspects. Similarly, while in some cases one or more particular data storage needs are described as being satisfied by separate components (for example, an expanded private capital markets database and a configuration database), these descriptions refer to functional uses of data storage systems and do not refer to their physical architecture. For instance, any group of data storage systems of databases referred to herein may be included together in a single database management system operating on a single machine, or they may be included in a single database management system operating on a cluster of machines as is known in the art. Similarly, any single database (such as an expanded private capital markets database) may be implemented on a single machine, on a set of machines using clustering technology, on several machines connected by one or more messaging systems known in the art, or in a master/slave arrangement common in the art. These examples should make clear that no particular architectural approaches to database management is preferred according to the invention, and choice of data storage technology is at the discretion of each implementer, without departing from the scope of the invention as claimed.

[0056] A “data context”, as used herein, refers to a set of arguments identifying the location of data. This could be a Rabbit queue, a .csv file in cloud-based storage, or any other such location reference except a single event or record. Activities may pass either events or data contexts to each other for processing. The nature of a pipeline allows for direct information passing between activities, and data locations or files do not need to be predetermined at pipeline start.

[0057] A “pipeline”, as used herein and interchangeably referred to as a “data pipeline” or a “processing pipeline”, refers to a set of data streaming activities and batch activities. Streaming and batch activities can be connected indiscriminately within a pipeline. Events will flow through the streaming activity actors in a reactive way. At the junction of a streaming activity to batch activity, there will exist a *StreamBatchProtocol* data object. This object is responsible for determining when and if the batch process is run. One or more of three possibilities can be used

for processing triggers: regular timing interval, every N events, or optionally an external trigger. The events are held in a queue or similar until processing. Each batch activity may contain a "source" data context (this may be a streaming context if the upstream activities are streaming), and a "destination" data context (which is passed to the next activity). Streaming activities may have an optional "destination" streaming data context (optional meaning: caching/persistence of events vs. ephemeral), though this should not be part of the initial implementation.

Conceptual Architecture

[0058] Fig. 1 is a block diagram of an advanced cyber decision platform for external network reconnaissance and cybersecurity rating. Client access to the system **105** for specific data entry, system control and for interaction with system output such as automated predictive decision making and planning and alternate pathway simulations, occurs through the system's distributed, extensible high bandwidth cloud interface **110** which uses a versatile, robust web application driven interface for both input and display of client-facing information via network **107** and operates a data store **112** such as, but not limited to MONGODB™, COUCHDB™, CASSANDRA™ or REDIS™ according to various arrangements. Much of the business data analyzed by the system both from sources within the confines of the client business, and from cloud based sources, also enter the system through the cloud interface **110**, data being passed to the connector module **135** which may possess the API routines **135a** needed to accept and convert the external data and then pass the normalized information to other analysis and transformation components of the system, the directed computational graph module **155**, high volume web crawler module **115**, multidimensional time series database (MDTSDB) **120** and the graph stack service **145**. The directed computational graph module **155** retrieves one or more streams of data from a plurality of sources, which includes, but is in no way not limited to, a plurality of physical sensors, network service providers, web based questionnaires and surveys, monitoring of electronic infrastructure, crowd sourcing campaigns, and human input device information. Within the directed computational graph module **155**, data may be split into two identical streams in a specialized pre-programmed data pipeline **155a**, wherein one sub-stream may be sent for batch processing and storage while the other sub-stream may be reformatted for transformation pipeline analysis. The data is then transferred to the general transformer service module **160** for linear data transformation as part of analysis or the decomposable transformer service module **150** for branching or iterative transformations that are part of analysis. The

directed computational graph module **155** represents all data as directed graphs where the transformations are nodes and the result messages between transformations edges of the graph. The high volume web crawling module **115** uses multiple server hosted preprogrammed web spiders, which while autonomously configured are deployed within a web scraping framework **115a** of which SCRAPY™ is an example, to identify and retrieve data of interest from web based sources that are not well tagged by conventional web crawling technology. The multiple dimension time series data store module **120** may receive streaming data from a large plurality of sensors that may be of several different types. The multiple dimension time series data store module may also store any time series data encountered by the system such as but not limited to enterprise network usage data, component and system logs, performance data, network service information captures such as, but not limited to news and financial feeds, and sales and service related customer data. The module is designed to accommodate irregular and high volume surges by dynamically allotting network bandwidth and server processing channels to process the incoming data. Inclusion of programming wrappers **120a** for languages examples of which are, but not limited to C++, PERL, PYTHON, and ERLANG™ allows sophisticated programming logic to be added to the default function of the multidimensional time series database **120** without intimate knowledge of the core programming, greatly extending breadth of function. Data retrieved by the multidimensional time series database (MDTSDB) **120** and the high volume web crawling module **115** may be further analyzed and transformed into task optimized results by the directed computational graph **155** and associated general transformer service **150** and decomposable transformer service **160** modules. Alternately, data from the multidimensional time series database and high volume web crawling modules may be sent, often with scripted cuing information determining important vertexes **145a**, to the graph stack service module **145** which, employing standardized protocols for converting streams of information into graph representations of that data, for example, open graph internet technology although the invention is not reliant on any one standard. Through the steps, the graph stack service module **145** represents data in graphical form influenced by any pre-determined scripted modifications **145a** and stores it in a graph-based data store **145b** such as GIRAPH™ or a key value pair type data store REDIS™, or RIAK™, among others, all of which are suitable for storing graph-based information.

[0059] Results of the transformative analysis process may then be combined with further client directives, additional business rules and practices relevant to the analysis and situational information external to the already available data in the automated planning service module **130** which also runs powerful information theory **130a** based predictive statistics functions and machine learning algorithms to allow future trends and outcomes to be rapidly forecast based upon the current system derived results and choosing each a plurality of possible business decisions. The using all available data, the automated planning service module **130** may propose business decisions most likely to result is the most favorable business outcome with a usably high level of certainty. Closely related to the automated planning service module in the use of system derived results in conjunction with possible externally supplied additional information in the assistance of end user business decision making, the action outcome simulation module **125** with its discrete event simulator programming module **125a** coupled with the end user facing observation and state estimation service **140** which is highly scriptable **140b** as circumstances require and has a game engine **140a** to more realistically stage possible outcomes of business decisions under consideration, allows business decision makers to investigate the probable outcomes of choosing one pending course of action over another based upon analysis of the current available data.

[0060] When performing external reconnaissance via a network **107**, web crawler **115** may be used to perform a variety of port and service scanning operations on a plurality of hosts. This may be used to target individual network hosts (for example, to examine a specific server or client device) or to broadly scan any number of hosts (such as all hosts within a particular domain, or any number of hosts up to the complete IPv4 address space). Port scanning is primarily used for gathering information about hosts and services connected to a network, using probe messages sent to hosts that prompt a response from that host. Port scanning is generally centered around the transmission control protocol (TCP), and using the information provided in a prompted response a port scan can provide information about network and application layers on the targeted host.

[0061] Port scan results can yield information on open, closed, or undetermined ports on a target host. An open port indicated that an application or service is accepting connections on this port (such as ports used for receiving customer web traffic on a web server), and these ports generally disclose the greatest quantity of useful information about the host. A closed port indicates that no

application or service is listening for connections on that port, and still provides information about the host such as revealing the operating system of the host, which may discovered by fingerprinting the TCP/IP stack in a response. Different operating systems exhibit identifiable behaviors when populating TCP fields, and collecting multiple responses and matching the fields against a database of known fingerprints makes it possible to determine the OS of the host even when no ports are open. An undetermined port is one that does not produce a requested response, generally because the port is being filtered by a firewall on the host or between the host and the network (for example, a corporate firewall behind which all internal servers operate).

[0062] Scanning may be defined by scope to limit the scan according to two dimensions, hosts and ports. A horizontal scan checks the same port on multiple hosts, often used by attackers to check for an open port on any available hosts to select a target for an attack that exploits a vulnerability using that port. This type of scan is also useful for security audits, to ensure that vulnerabilities are not exposed on any of the target hosts. A vertical scan defines multiple ports to examine on a single host, for example a "vanilla scan" which targets every port of a single host, or a "strobe scan" that targets a small subset of ports on the host. This type of scan is usually performed for vulnerability detection on single systems, and due to the single-host nature is impractical for large network scans. A block scan combines elements of both horizontal and vertical scanning, to scan multiple ports on multiple hosts. This type of scan is useful for a variety of service discovery and data collection tasks, as it allows a broad scan of many hosts (up to the entire Internet, using the complete IPv4 address space) for a number of desired ports in a single sweep.

[0063] Large port scans involve quantitative research, and as such may be treated as experimental scientific measurement and are subject to measurement and quality standards to ensure the usefulness of results. To avoid observational errors during measurement, results must be precise (describing a degree of relative proximity between individual measured values), accurate (describing relative proximity of measured values to a reference value), preserve any metadata that accompanies the measured data, avoid misinterpretation of data due to faulty measurement execution, and must be well-calibrated to efficiently expose and address issues of inaccuracy or misinterpretation. In addition to these basic requirements, large volumes of data may lead to unexpected behavior of analysis tools, and extracting a subset to perform initial analysis may help to provide an initial overview before working with the complete data set.

Analysis should also be reproducible, as with all experimental science, and should incorporate publicly-available data to add value to the comprehensibility of the research as well as contributing to a "common framework" that may be used to confirm results.

[0064] When performing a port scan, web crawler **115** may employ a variety of software suitable for the task, such as Nmap, ZMap, or masscan. Nmap is suitable for large scans as well as scanning individual hosts, and excels in offering a variety of diverse scanning techniques. ZMap is a newer application and unlike Nmap (which is more general-purpose), ZMap is designed specifically with Internet-wide scans as the intent. As a result, ZMap is far less customizable and relies on horizontal port scans for functionality, achieving fast scan times using techniques of probe randomization (randomizing the order in which probes are sent to hosts, minimizing network saturation) and asynchronous design (utilizing stateless operation to send and receive packets in separate processing threads). Masscan uses the same asynchronous operation model of ZMap, as well as probe randomization. In masscan however, a certain degree of statistical randomness is sacrificed to improve computation time for large scans (such as when scanning the entire IPv4 address space), using the *BlackRock* algorithm. This is a modified implementation of symmetric encryption algorithm DES, with fewer rounds and modulo operations in place of binary ones to allow for arbitrary ranges and achieve faster computation time for large data sets.

[0065] Received scan responses may be collected and processed through a plurality of data pipelines **155a** to analyze the collected information. MDTSDB **120** and graph stack **145** may be used to produce a hybrid graph/time-series database using the analyzed data, forming a graph of Internet-accessible organization resources and their evolving state information over time. Customer-specific profiling and scanning information may be linked to CPG graphs (as described below in detail, referring to **Fig. 11**) for a particular customer, but this information may be further linked to the base-level graph of internet-accessible resources and information. Depending on customer authorizations and legal or regulatory restrictions and authorizations, techniques used may involve both passive, semi-passive and active scanning and reconnaissance.

[0066] **Fig. 2A** is a block diagram showing general steps **200** for performing passive network reconnaissance. It should be appreciated that the steps illustrated and described may be performed in any order, and that steps may be added or omitted as needed for any particular reconnaissance operation. In a step **201**, network address ranges and domains or sub-domains associated with a plurality of targets may be identified, for example to collect information for

defining the scope of further scanning operations. In another step **202**, external sites may be identified to understand relationships between targets and other third-party content providers, such as trust relationships or authoritative domain name service (DNS) resolution records. In another step **203**, individual people or groups may be identified using names, email addresses, phone numbers, or other identifying information that may be useful for a variety of social engineering activities. In another step **204**, technologies used may be identified, such as types or versions of hardware or software used by an organization, and this may include collecting and extracting information from job descriptions (for example) to identify technologies in use by an organization (for example, a job description for an administrator familiar with specific database software indicates that said software is in use within the organization). In another step **205**, content of interest may be identified, for example including web and email portals, log files, backup or archive files, and other forms of sensitive information that may be contained within HTML comments or client-side scripts, as may be useful for vulnerability discovery and penetration testing activities. In another step **206**, publicly-available information may be used to identify vulnerabilities that may be exploited with further active penetration testing.

[0067] Fig. 2B is a process diagram showing a general flow of a process **210** for performing active reconnaissance using DNS leak information collection. In an initial step **211**, publicly-available DNS leak disclosure information may be collected to maintain current information regarding known leaks and vulnerabilities. In a next step **212**, third-level domain (TLDR) information may be collected and used to report domain risk factors, such as domains that do not resolve properly (due to malformed DNS records, for example). In a next step **213**, a DNS trust map may be created using a hybrid graph/time-series data structure, using a graph stack service **145** and MDTSDB **120**. This trust map may be produced as the output of an extraction process performed by a DCG **155** through a plurality of data pipelines **155a**, analyzing collected data and mapping data points to produce hybrid structured output representing each data point over time. In a final step **214**, the trust map may then be analyzed to identify anomalies, for example using community detection algorithms that may discover when new references are being created, and this may be used to identify vulnerabilities that may arise as a byproduct of the referential nature of a DNS hierarchy. In this manner, DCG pipeline processing and time-series data graphing may be used to identify vulnerabilities that would otherwise be obscured within a large dataset.

[0068] Fig. 2C is a process diagram showing a general flow of a process **220** for performing active reconnaissance using web application and technology reconnaissance. In an initial step **221**, a plurality of manual HTTP requests may be transmitted to a host, for example to determine if a web server is announcing itself, or to obtain an application version number from an HTTP response message. In a next step **222**, a *robots.txt*, used to identify and communicate with web crawlers and other automated "bots", may be searched for to identify portions of an application or site that robots are requested to ignore. In a next step **223**, the host application layer may be fingerprinted, for example using file extensions and response message fields to identify characteristic patterns or markers that may be used to identify host or application details. In a next step **224**, publicly-exposed */admin* pages may be checked, to determine if any administrative portals are exposed and therefore potentially-vulnerable, as well as to potentially determine administration policies or capabilities based on exposed information. In a final step **225**, an application may be profiled according to a particular toolset in use, such as WORDPRESS™ (for example) or other specific tools or plugins.

[0069] Fig. 2D is a process diagram showing a general flow of a process **230** for producing a cybersecurity rating using reconnaissance data. In an initial step **231**, external reconnaissance may be performed using DNS and IP information as described above (referring to **Fig. 2B**), collecting information from DNS records, leak announcements, and publicly-available records to produce a DNS trust map from collected information and the DCG-driven analysis thereof. In a next step **232**, web and application recon may be performed (as described in **Fig. 2C**), collecting information on applications, sites, and publicly-available records. In a next step **233**, collected information over time may be analyzed for software version numbers, revealing the patching frequency of target hosts and their respective applications and services. Using a hybrid time-series graph, timestamps may be associated with ongoing changes to reveal these updates over time. In a next step **234**, a plurality of additional endpoints may be scanned, such as (for example, including but not limited to) internet-of-things (IoT) devices that may be scanned and fingerprinted, end-user devices such as personal smartphones, tablets, or computers, or social network endpoints such as scraping content from user social media pages or feeds. User devices may be fingerprinted and analyzed similar to organization hosts, and social media content may be retrieved such as collecting sentiment from services like TWITTER™ or LINKEDIN™, or analyzing job description listings and other publicly-available information. In a next step **235**,

open-source intelligence feeds may be checked, such as company IP address blacklists, search domains, or information leaks (for example, posted to public records such as PASTEBIN™). In a final step **236**, collected information from all sources may be scored according to a weighted system, producing an overall cybersecurity rating score based on the information collected and the analysis of that information to reveal additional insights, relationships, and vulnerabilities.

[0070] For example, in an exemplary scoring system similar to a credit rating, information from initial Internet recon operations may be assigned a score up to 400 points, along with up to 200 additional points for web/application recon results, 100 points for patch frequency, and 50 points each for additional endpoints and open-source intel results. This yields a weighted score incorporating all available information from all scanned sources, allowing a meaningful and readily-appreciable representation of an organization's overall cybersecurity strength. Additionally, as scanning may be performed repeatedly and results collected into a time-series hybrid data structure, this cybersecurity rating may evolve over time to continuously reflect the current state of the organization, reflecting any recent changes, newly-discovered or announced vulnerabilities, software or hardware updates, newly-added or removed devices or services, and any other changes that may occur.

[0071] Figs. 3A and **3B** are process diagrams showing business operating system functions in use to mitigate cyberattacks. Input network data which may include network flow patterns **321**, the origin and destination of each piece of measurable network traffic **322**, system logs from servers and workstations on the network **323**, endpoint data **329**, any security event log data from servers or available security information and event (SIEM) systems **324**, external threat intelligence feeds **324**, identity or assessment context **325**, external network health or cybersecurity feeds **326**, Kerberos domain controller or ACTIVE DIRECTORY™ server logs or instrumentation **327**, business unit performance related data **328**, endpoint data **329**, among many other possible data types for which the invention was designed to analyze and integrate, may pass into **315** the business operating system **310** for analysis as part of its cyber security function. These multiple types of data from a plurality of sources may be transformed for analysis **311**, **312** using at least one of the specialized cybersecurity, risk assessment or common functions of the business operating system in the role of cybersecurity system, such as, but not limited to network and system user privilege oversight **331**, network and system user behavior analytics **332**, attacker and defender action timeline **333**, SIEM integration and analysis **334**,

dynamic benchmarking **335**, and incident identification and resolution performance analytics **336** among other possible cybersecurity functions; value at risk (VAR) modeling and simulation **341**, anticipatory vs. reactive cost estimations of different types of data breaches to establish priorities **342**, work factor analysis **343** and cyber event discovery rate **344** as part of the system's risk analytics capabilities; and the ability to format and deliver customized reports and dashboards **351**, perform generalized, ad hoc data analytics on demand **352**, continuously monitor, process and explore incoming data for subtle changes or diffuse informational threads **353** and generate cyber-physical systems graphing **354** as part of the business operating system's common capabilities. Output **317** can be used to configure network gateway security appliances **361**, to assist in preventing network intrusion through predictive change to infrastructure recommendations **362**, to alert an enterprise of ongoing cyberattack early in the attack cycle, possibly thwarting it but at least mitigating the damage **362**, to record compliance to standardized guidelines or SLA requirements **363**, to continuously probe existing network infrastructure and issue alerts to any changes which may make a breach more likely **364**, suggest solutions to any domain controller ticketing weaknesses detected **365**, detect presence of malware **366**, perform one time or continuous vulnerability scanning depending on client directives **367**, and thwart or mitigate damage from cyber attacks **368**. These examples are, of course, only a subset of the possible uses of the system, they are exemplary in nature and do not reflect any boundaries in the capabilities of the invention.

[0072] Fig. 4 is a process flow diagram of a method for segmenting cyberattack information to appropriate corporation parties **400**. As previously disclosed **200**, **351**, one of the strengths of the advanced cyber-decision platform is the ability to finely customize reports and dashboards to specific audiences, concurrently is appropriate. This customization is possible due to the devotion of a portion of the business operating system's programming specifically to outcome presentation by modules which include the observation and state estimation service **140** with its game engine **140a** and script interpreter **140b**. In the setting of cybersecurity, issuance of specialized alerts, updates and reports may significantly assist in getting the correct mitigating actions done in the most timely fashion while keeping all participants informed at predesignated, appropriate granularity. Upon the detection of a cyberattack by the system **401** all available information about the ongoing attack and existing cybersecurity knowledge are analyzed, including through predictive simulation in near real time **402** to develop both the most accurate

appraisal of current events and actionable recommendations concerning where the attack may progress and how it may be mitigated. The information generated in totality is often more than any one group needs to perform their mitigation tasks. At this point, during a cyberattack, providing a single expansive and all inclusive alert, dashboard image, or report may make identification and action upon the crucial information by each participant more difficult, therefore the cybersecurity focused arrangement may create multiple targeted information streams each concurrently designed to produce most rapid and efficacious action throughout the enterprise during the attack and issue follow-up reports with and recommendations or information that may lead to long term changes afterward **403**. Examples of groups that may receive specialized information streams include but may not be limited to front line responders during the attack **404**, incident forensics support both during and after the attack **405**, chief information security officer **406** and chief risk officer **407** the information sent to the latter two focused to appraise overall damage and to implement both mitigating strategy and preventive changes after the attack. Front line responders may use the cyber-decision platform's analyzed, transformed and correlated information specifically sent to them **404** to probe the extent of the attack, isolate such things as: the predictive attacker's entry point onto the enterprise's network, the systems involved or the predictive ultimate targets of the attack and may use the simulation capabilities of the system to investigate alternate methods of successfully ending the attack and repelling the attackers in the most efficient manner, although many other queries known to those skilled in the art are also answerable by the invention. Simulations run may also include the predictive effects of any attack mitigating actions on normal and critical operation of the enterprise's IT systems and corporate users. Similarly, a chief information security officer may use the cyber-decision platform to predictively analyze **406** what corporate information has already been compromised, predictively simulate the ultimate information targets of the attack that may or may not have been compromised and the total impact of the attack what can be done now and in the near future to safeguard that information. Further, during retrospective forensic inspection of the attack, the forensic responder may use the cyber-decision platform **405a** to clearly and completely map the extent of network infrastructure through predictive simulation and large volume data analysis. The forensic analyst may also use the platform's capabilities to perform a time series and infrastructural spatial analysis of the attack's progression with methods used to infiltrate the enterprise's subnets and servers. Again, the chief risk officer would perform

analyses of what information **407a** was stolen and predictive simulations on what the theft means to the enterprise as time progresses. Additionally, the system's predictive capabilities may be employed to assist in creation of a plan for changes of the IT infrastructural that should be made that are optimal for remediation of cybersecurity risk under possibly limited enterprise budgetary constraints in place at the company so as to maximize financial outcome.

[0073] Fig. 5 is a diagram of an exemplary architecture for a system for rapid predictive analysis of very large data sets using an actor-driven distributed computational graph **500**, according to one aspect. According to the aspect, a DCG **500** may comprise a pipeline orchestrator **501** that may be used to perform a variety of data transformation functions on data within a processing pipeline, and may be used with a messaging system **510** that enables communication with any number of various services and protocols, relaying messages and translating them as needed into protocol-specific API system calls for interoperability with external systems (rather than requiring a particular protocol or service to be integrated into a DCG **500**).

[0074] Pipeline orchestrator **501** may spawn a plurality of child pipeline clusters **502a-b**, which may be used as dedicated workers for streamlining parallel processing. In some arrangements, an entire data processing pipeline may be passed to a child cluster **502a** for handling, rather than individual processing tasks, enabling each child cluster **502a-b** to handle an entire data pipeline in a dedicated fashion to maintain isolated processing of different pipelines using different cluster nodes **502a-b**. Pipeline orchestrator **501** may provide a software API for starting, stopping, submitting, or saving pipelines. When a pipeline is started, pipeline orchestrator **501** may send the pipeline information to an available worker node **502a-b**, for example using AKKA™ clustering. For each pipeline initialized by pipeline orchestrator **501**, a reporting object with status information may be maintained. Streaming activities may report the last time an event was processed, and the number of events processed. Batch activities may report status messages as they occur. Pipeline orchestrator **501** may perform batch caching using, for example, an IGFS™ caching filesystem. This allows activities **512a-d** within a pipeline **502a-b** to pass data contexts to one another, with any necessary parameter configurations.

[0075] A pipeline manager **511a-b** may be spawned for every new running pipeline, and may be used to send activity, status, lifecycle, and event count information to the pipeline orchestrator **501**. Within a particular pipeline, a plurality of activity actors **512a-d** may be created by a pipeline manager **511a-b** to handle individual tasks, and provide output to data services **522a-d**.

Data models used in a given pipeline may be determined by the specific pipeline and activities, as directed by a pipeline manager **511a-b**. Each pipeline manager **511a-b** controls and directs the operation of any activity actors **512a-d** spawned by it. A pipeline process may need to coordinate streaming data between tasks. For this, a pipeline manager **511a-b** may spawn service connectors to dynamically create TCP connections between activity instances **512a-d**. Data contexts may be maintained for each individual activity **512a-d**, and may be cached for provision to other activities **512a-d** as needed. A data context defines how an activity accesses information, and an activity **512a-d** may process data or simply forward it to a next step. Forwarding data between pipeline steps may route data through a streaming context or batch context.

[0076] A client service cluster **530** may operate a plurality of service actors **521a-d** to serve the requests of activity actors **512a-d**, ideally maintaining enough service actors **521a-d** to support each activity per the service type. These may also be arranged within service clusters **520a-d**, in a manner similar to the logical organization of activity actors **512a-d** within clusters **502a-b** in a data pipeline. A logging service **530** may be used to log and sample DCG requests and messages during operation while notification service **540** may be used to receive alerts and other notifications during operation (for example to alert on errors, which may then be diagnosed by reviewing records from logging service **530**), and by being connected externally to messaging system **510**, logging and notification services can be added, removed, or modified during operation without impacting DCG **500**. A plurality of DCG protocols **550a-b** may be used to provide structured messaging between a DCG **500** and messaging system **510**, or to enable messaging system **510** to distribute DCG messages across service clusters **520a-d** as shown. A service protocol **560** may be used to define service interactions so that a DCG **500** may be modified without impacting service implementations. In this manner it can be appreciated that the overall structure of a system using an actor-driven DCG **500** operates in a modular fashion, enabling modification and substitution of various components without impacting other operations or requiring additional reconfiguration.

[0077] **Fig. 6** is a diagram of an exemplary architecture for a system for rapid predictive analysis of very large data sets using an actor-driven distributed computational graph **500**, according to one aspect. According to the aspect, a variant messaging arrangement may utilize messaging system **510** as a messaging broker using a streaming protocol **610**, transmitting and receiving messages immediately using messaging system **510** as a message broker to bridge

communication between service actors **521a-b** as needed. Alternately, individual services **522a-b** may communicate directly in a batch context **620**, using a data context service **630** as a broker to batch-process and relay messages between services **522a-b**.

[0078] Fig. 7 is a diagram of an exemplary architecture for a system for rapid predictive analysis of very large data sets using an actor-driven distributed computational graph **500**, according to one aspect. According to the aspect, a variant messaging arrangement may utilize a service connector **710** as a central message broker between a plurality of service actors **521a-b**, bridging messages in a streaming context **610** while a data context service **630** continues to provide direct peer-to-peer messaging between individual services **522a-b** in a batch context **620**.

[0079] It should be appreciated that various combinations and arrangements of the system variants described above (referring to **Figs. 1-7**) may be possible, for example using one particular messaging arrangement for one data pipeline directed by a pipeline manager **511a-b**, while another pipeline may utilize a different messaging arrangement (or may not utilize messaging at all). In this manner, a single DCG **500** and pipeline orchestrator **501** may operate individual pipelines in the manner that is most suited to their particular needs, with dynamic arrangements being made possible through design modularity as described above in **Fig. 5**.

[0080] Fig. 19 is block diagram showing an exemplary system architecture **1900** for a system for cybersecurity profiling and rating. The system in this example contains a cyber-physical graph **1902** which is used to represent a complete picture of an organization's infrastructure and operations including, importantly, the organization's computer network infrastructure particularly around system configurations that influence cybersecurity protections and resiliency. The system further contains a directed computational graph **1911**, which contains representations of complex processing pipelines and is used to control workflows through the system such as determining which 3rd party search tools **1915** to use, assigning search tasks, and analyzing the cyber-physical graph **1902** and comparing results of the analysis against reconnaissance data received from the reconnaissance engine **1906** and stored in the reconnaissance data storage **1905**. In some embodiments, the determination of which 3rd party search tools **1915** to use and assignment of search tasks may be implemented by a reconnaissance engine **1906**. The cyber-physical graph **1902** plus the analyses of data directed by the directed computational graph on the reconnaissance data received from the reconnaissance engine **1906** are combined to represent the cyber-security profile of the client organization whose network **1907** is being evaluated. A

queuing system **1912** is used to organize and schedule the search tasks requested by the reconnaissance engine **1906**. A data to rule mapper **1904** is used to retrieve laws, policies, and other rules from an authority database **1903** and compare reconnaissance data received from the reconnaissance engine **1906** and stored in the reconnaissance data storage **1905** against the rules in order to determine whether and to what extent the data received indicates a violation of the rules. Machine learning models **1901** may be used to identify patterns and trends in any aspect of the system, but in this case are being used to identify patterns and trends in the data which would help the data to rule mapper **1904** determine whether and to what extent certain data indicate a violation of certain rules. A scoring engine **1910** receives the data analyses performed by the directed computational graph **1911**, the output of the data to rule mapper **1904**, plus event and loss data **1914** and contextual data **1909** which defines a context in which the other data are to be scored and/or rated. A public-facing proxy network **1908** is established outside of a firewall **1917** around the client network **1907** both to control access to the client network from the Internet **1913**, and to provide the ability to change the outward presentation of the client network **1907** to the Internet **1913**, which may affect the data obtained by the reconnaissance engine **1906**. In some embodiments, certain components of the system may operate outside the client network **1907** and may access the client network through a secure, encrypted virtual private network (VPN) **1916**, as in a cloud-based or platform-as-a-service implementation, but in other embodiments some or all of these components may be installed and operated from within the client network **1907**.

[0081] As a brief overview of operation, information is obtained about the client network **1907** and the client organization's operations, which is used to construct a cyber-physical graph **1902** representing the relationships between devices, users, resources, and processes in the organization, and contextualizing cybersecurity information with physical and logical relationships that represent the flow of data and access to data within the organization including, in particular, network security protocols and procedures. The directed computational graph **1911** containing workflows and analysis processes, selects one or more analyses to be performed on the cyber-physical graph **1902**. Some analyses may be performed on the information contained in the cyber-physical graph, and some analyses may be performed on or against the cyber-physical graph using information obtained from the Internet **1913** from reconnaissance engine **1906**. The workflows contained in the directed computational graph **1911** select one or more search tools to

obtain information about the organization from the Internet **1915**, and may comprise one or more third party search tools **1915** available on the Internet. As data are collected, they are fed into a reconnaissance data storage **1905**, from which they may be retrieved and further analyzed. Comparisons are made between the data obtained from the reconnaissance engine **1906**, the cyber-physical graph **1902**, the data to rule mapper, from which comparisons a cybersecurity profile of the organization is developed. The cybersecurity profile is sent to the scoring engine **1910** along with event and loss data **1914** and context data **1909** for the scoring engine **1910** to develop a score and/or rating for the organization that takes into consideration both the cybersecurity profile, context, and other information.

[0082] Fig. 24 is a block diagram showing an exemplary architecture **2400** for a scoring engine. Data fed into the scoring engine comprise the cybersecurity profile **1918** and reconnaissance data **1905** developed at earlier stages of system operation. Based on these data, a frequency and severity of attack is estimated **2408**. For each risk type, curve fitting **2402** may be performed on the data points to assign a "best fit" function along the range of data points, which captures trends in the data and allows for predictions of how similar data will behave in the future. Aggregations of operational variables **2403** may be applied to identify maxima, minima, counts, sums, and standard deviations of the data. Risk identification and quantification is then performed **2413**, and a business impact analysis is performed **2412** based on a totality of the predicted risks, their severity, business dependencies reflected in the cyber-physical graph, and prior event and loss data **2410**, among other variables. From this analysis of business impact **2412**, a network resilience rating is assigned **2405**, representing a weighted and adjusted total of relative exposure the organization has to various types of risks, each of which may be assigned a sub-rating. The network resilience rating **2405** may be a single score for all factors, a combination of scores, or a score for a particular risk or area of concern. The network resilience rating **2411** may then be adjusted or filtered depending on the context in which it is to be used **2409**. For example, context data received **2408** may indicate that the scores are to be used for compliance with internal theft policies, but the factors associated with the network resilience rating indicate that the highest risks are associated with cyber-attacks from external systems, which may cause the adjustment for goal/purpose **2409** to filter out the factors of the network resilience rating associated with risks from external cyber-attacks or reduce their contribution to a functional score. Finally, a functional cybersecurity score **2411** is assigned which takes into

account the adjusted factors of the network resilience score and the context in which the functional score is to be applied. The process may be iterative, in that the network resilience rating **2405** from previous analyses may be fed back into the start of the process at estimation of frequency and severity of attacks **2401**.

Detailed Description of Exemplary Aspects

[0083] Fig. 29 is a flow diagram illustrating an exemplary method for identifying an anomalous event. In an initial step **2910**, active and passive reconnaissance results may be received at a scoring engine **2400**. This data may then be analyzed **2920** along with a cyber-physical graph to determine patterns of normal event behavior for various nodes within the CPG, based on observed events over time. Event logs, reconnaissance data, and other time-series data may then be monitored **2930** to track event patterns over time, comparing against normal patterns to identify anomalies as well as enabling refinement of the normal pattern records by incorporating additional data as it is produced. When an event occurs that is recognized to be outside the normal patterns, for example if the event exceeds a configured threshold for aberrance or involves a known-compromised node or external address or resource (such as a deliberate "honeypot" node for intrusion detection), it may then be identified as an anomaly **2940** that may indicate a compromised node or an intrusion attempt. These anomalous events may be used to identify correlations in network behavior and identify attack patterns, as described below in **Figs. 30-32**.

[0084] Fig. 30 is a flow diagram illustrating an exemplary method for identifying correlations between an anomaly and other network events and resources. According to this method, when an anomaly is identified **3010** (as described above, with reference to **Fig. 29**), it may be correlated with other events, network resources, behavior patterns, or any other available information that may be contextually linked to the anomaly. Using a CPG for the network, correlations may be identified by first comparing resources involved in the anomaly **3020**, for example any machines that participated in the anomalous event or any databases or other resources that were accessed. This information may then be used to further correlate with other events involving those resources **3030**, such as events taking place at the same (or nearly the same) time, or events with a recognizable causative relationship such as non-anomalous events that may have been triggered by the anomaly (for example, as would occur if an attacker accessed a resource and used it to perform routine functions that are not anomalous in themselves, but were clearly related to the

anomalous event as they occurred immediately following it during a time when they would normally be unlikely to happen). An established normal behavior pattern (as described above, with reference to **Fig. 29**) may also be used to identify additional anomalies **3040** that may not comprise anomalous events (that is, discrete network events that do not correspond to established normal event behavior) but rather deviations from normal behavior that occur around the same time or involving the same resources as an anomalous event. For example, if an anomalous event occurs involving a particular computer on the network, behavior logs may be reviewed **3050** to identify any recent anomalous behavior that may have gone unnoticed, and current behavior **3060** may be checked for any deviations from established normal patterns. These deviations may be determined using preconfigured thresholds, or ad-hoc thresholds that may be established on the fly based on the anomalous event and other available information pertaining to the incident as it unfolds. For example, an event involving a large number of resources or particularly sensitive data stores may cause a threshold for behavior deviation to be set lower than a comparatively minor anomaly involving only a small number of nonessential network resources. In this manner, anomalous events may be rapidly correlated with any unusual behavior or activity on the network in order to gain a more-complete picture of the extent of any potential attack and reveal additional information that may be used in mitigating the attack, as described below in **Figs. 31-32**.

[0085] Fig. 31 is a flow diagram illustrating an exemplary method for generating a behavior graph based on an identified anomaly and its correlations. When an anomaly is detected and correlated **3110** as described above (with reference to **Figs. 29-30**), a DCG may be used to formulate a behavior graph representing the various behavioral connections and interactions between involved resources or processes pertaining to the anomaly, in order to identify possible event flows between affected nodes and gain further insight into the anomaly and any possible effects or outcomes it may produce. Initially **3120**, the DCG may be used to identify all behavior interactions between affected processes and resources, using established known behavior patterns and event correlations to iterate over the affected nodes in a CPG until all relationships have been identified. These behavioral relationships may then be used **3130** to produce an initial behavioral graph that describes the interconnectedness between nodes and the various event pathways that can occur, including potential (or actual) attach paths that an intruder may take advantage of when attempting to compromise the network or any particular nodes. These

pathways indicate what dependencies must be satisfied for any given event or node behavior, what the effects of the event or behavior are, what nodes are in turn affected by those outcomes, and other such directed flow information. The graph may then be used to identify **3140** any possible event flows and interactions between the affected nodes, indicating causative effect pathways that are triggered by events and node behaviors, which in the case of an anomaly allows insight into what effects the anomaly may have or what may have led up to the event in question as is described below, in **Fig. 32**.

[0086] Fig. 32 is a flow diagram illustrating an exemplary method for determining an attack's point of origin using a behavior graph. When a behavior graph is produced for an identified event anomaly **3210**, it may be used to determine event dependencies **3220** based on the identified behavioral patterns and causative relationships in the graph. Using these dependencies, a dependency tree may be produced that comprises the chain of causative events, behaviors, and conditions that led up to the anomaly. This dependency tree comprises the potential event flows and interaction pathways within and between the nodes, and causative relationships can be followed through time as branching paths through the tree. By traversing this dependency tree backward **3230** (that is, following the path of event flows back in time), it then becomes possible to determine a point of origin for the anomaly and the starting conditions that were in place **3240**. This enables more effective mitigation of attacks and resolution of flaws in a network, by identifying the precise causes of vulnerabilities and deficiencies so they may be addressed directly rather than traditional approaches that are inherently limited to mitigating the outcomes of an unknown attack; in other words, traditional approaches focus on current symptoms of an attack whereas this method is able to directly identify and address the root cause of the issue.

[0087] Fig. 8 is a flow diagram of an exemplary method **800** for cybersecurity behavioral analytics, according to one aspect. According to the aspect, behavior analytics may utilize passive information feeds from a plurality of existing endpoints (for example, including but not limited to user activity on a network, network performance, or device behavior) to generate security solutions. In an initial step **801**, a web crawler **115** may passively collect activity information, which may then be processed **802** using a DCG **155** to analyze behavior patterns. Based on this initial analysis, anomalous behavior may be recognized **803** (for example, based on a threshold of variance from an established pattern or trend) such as high-risk users or malicious software operators such as bots. These anomalous behaviors may then be used **804** to analyze

potential angles of attack and then produce **805** security suggestions based on this second-level analysis and predictions generated by an action outcome simulation module **125** to determine the likely effects of the change. The suggested behaviors may then be automatically implemented **806** as needed. Passive monitoring **801** then continues, collecting information after new security solutions are implemented **806**, enabling machine learning to improve operation over time as the relationship between security changes and observed behaviors and threats are observed and analyzed.

[0088] This method **800** for behavioral analytics enables proactive and high-speed reactive defense capabilities against a variety of cyberattack threats, including anomalous human behaviors as well as nonhuman "bad actors" such as automated software bots that may probe for, and then exploit, existing vulnerabilities. Using automated behavioral learning in this manner provides a much more responsive solution than manual intervention, enabling rapid response to threats to mitigate any potential impact. Utilizing machine learning behavior further enhances this approach, providing additional proactive behavior that is not possible in simple automated approaches that merely react to threats as they occur.

[0089] Fig. 9 is a flow diagram of an exemplary method **900** for measuring the effects of cybersecurity attacks, according to one aspect. According to the aspect, impact assessment of an attack may be measured using a DCG **155** to analyze a user account and identify its access capabilities **901** (for example, what files, directories, devices or domains an account may have access to). This may then be used to generate **902** an impact assessment score for the account, representing the potential risk should that account be compromised. In the event of an incident, the impact assessment score for any compromised accounts may be used to produce a "blast radius" calculation **903**, identifying exactly what resources are at risk as a result of the intrusion and where security personnel should focus their attention. To provide proactive security recommendations through a simulation module **125**, simulated intrusions may be run **904** to identify potential blast radius calculations for a variety of attacks and to determine **905** high risk accounts or resources so that security may be improved in those key areas rather than focusing on reactive solutions.

[0090] Fig. 10 is a flow diagram of an exemplary method **1000** for continuous cybersecurity monitoring and exploration, according to one aspect. According to the aspect, a state observation service **140** may receive data from a variety of connected systems **1001** such as (for example,

including but not limited to) servers, domains, databases, or user directories. This information may be received continuously, passively collecting events and monitoring activity over time while feeding **1002** collected information into a graphing service **145** for use in producing time-series graphs **1003** of states and changes over time. This collated time-series data may then be used to produce a visualization **1004** of changes over time, quantifying collected data into a meaningful and understandable format. As new events are recorded, such as changing user roles or permissions, modifying servers or data structures, or other changes within a security infrastructure, these events are automatically incorporated into the time-series data and visualizations are updated accordingly, providing live monitoring of a wealth of information in a way that highlights meaningful data without losing detail due to the quantity of data points under examination.

[0091] Fig. 11 is a flow diagram of an exemplary method **1100** for mapping a cyber-physical system graph (CPG), according to one aspect. According to the aspect, a cyber-physical system graph may comprise a visualization of hierarchies and relationships between devices and resources in a security infrastructure, contextualizing security information with physical device relationships that are easily understandable for security personnel and users. In an initial step **1101**, behavior analytics information (as described previously, referring to **Fig. 8**) may be received at a graphing service **145** for inclusion in a CPG. In a next step **1102**, impact assessment scores (as described previously, referring to **Fig. 9**) may be received and incorporated in the CPG information, adding risk assessment context to the behavior information. In a next step **1103**, time-series information (as described previously, referring to **Fig. 10**) may be received and incorporated, updating CPG information as changes occur and events are logged. This information may then be used to produce **1104** a graph visualization of users, servers, devices, and other resources correlating physical relationships (such as a user's personal computer or smartphone, or physical connections between servers) with logical relationships (such as access privileges or database connections), to produce a meaningful and contextualized visualization of a security infrastructure that reflects the current state of the internal relationships present in the infrastructure.

[0092] Fig. 12 is a flow diagram of an exemplary method **1200** for continuous network resilience rating, according to one aspect. According to the aspect, a baseline score can be used to measure an overall level of risk for a network infrastructure, and may be compiled by first

collecting **1201** information on publicly-disclosed vulnerabilities, such as (for example) using the Internet or common vulnerabilities and exploits (CVE) process. This information may then **1202** be incorporated into a CPG as described previously in **Fig. 11**, and the combined data of the CPG and the known vulnerabilities may then be analyzed **1203** to identify the relationships between known vulnerabilities and risks exposed by components of the infrastructure. This produces a combined CPG **1204** that incorporates both the internal risk level of network resources, user accounts, and devices as well as the actual risk level based on the analysis of known vulnerabilities and security risks.

[0093] Fig. 13 is a flow diagram of an exemplary method **1300** for cybersecurity privilege oversight, according to one aspect. According to the aspect, time-series data (as described above, referring to **Fig. 10**) may be collected **1301** for user accounts, credentials, directories, and other user-based privilege and access information. This data may then **1302** be analyzed to identify changes over time that may affect security, such as modifying user access privileges or adding new users. The results of analysis may be checked **1303** against a CPG (as described previously in **Fig. 11**), to compare and correlate user directory changes with the actual infrastructure state. This comparison may be used to perform accurate and context-enhanced user directory audits **1304** that identify not only current user credentials and other user-specific information, but changes to this information over time and how the user information relates to the actual infrastructure (for example, credentials that grant access to devices and may therefore implicitly grant additional access due to device relationships that were not immediately apparent from the user directory alone).

[0094] Fig. 14 is a flow diagram of an exemplary method **1400** for cybersecurity risk management, according to one aspect. According to the aspect, multiple methods described previously may be combined to provide live assessment of attacks as they occur, by first receiving **1401** time-series data for an infrastructure (as described previously, in **Fig. 10**) to provide live monitoring of network events. This data is then enhanced **1402** with a CPG (as described above in **Fig. 11**) to correlate events with actual infrastructure elements, such as servers or accounts. When an event (for example, an attempted attack against a vulnerable system or resource) occurs **1403**, the event is logged in the time-series data **1404**, and compared against the CPG **1405** to determine the impact. This is enhanced with the inclusion of impact assessment information **1406** for any affected resources, and the attack is then checked against a

baseline score **1407** to determine the full extent of the impact of the attack and any necessary modifications to the infrastructure or policies.

[0095] Fig. 15 is a flow diagram of an exemplary method **1500** for mitigating compromised credential threats, according to one aspect. According to the aspect, impact assessment scores (as described previously, referring to **Fig. 9**) may be collected **1501** for user accounts in a directory, so that the potential impact of any given credential attack is known in advance of an actual attack event. This information may be combined with a CPG **1502** as described previously in **Fig. 11**, to contextualize impact assessment scores within the infrastructure (for example, so that it may be predicted what systems or resources might be at risk for any given credential attack). A simulated attack may then be performed **1503** to use machine learning to improve security without waiting for actual attacks to trigger a reactive response. A blast radius assessment (as described above in **Fig. 9**) may be used in response **1504** to determine the effects of the simulated attack and identify points of weakness, and produce a recommendation report **1505** for improving and hardening the infrastructure against future attacks.

[0096] Fig. 16 is a flow diagram of an exemplary method **1600** for dynamic network and rogue device discovery, according to one aspect. According to the aspect, an advanced cyber decision platform may continuously monitor a network in real-time **1601**, detecting any changes as they occur. When a new connection is detected **1602**, a CPG may be updated **1603** with the new connection information, which may then be compared against the network's resiliency score **1604** to examine for potential risk. The blast radius metric for any other devices involved in the connection may also be checked **1605**, to examine the context of the connection for risk potential (for example, an unknown connection to an internal data server with sensitive information may be considered a much higher risk than an unknown connection to an externally-facing web server). If the connection is a risk, an alert may be sent to an administrator **1606** with the contextual information for the connection to provide a concise notification of relevant details for quick handling.

[0097] Fig. 17 is a flow diagram of an exemplary method **1700** for Kerberos "golden ticket" attack detection, according to one aspect. Kerberos is a network authentication protocol employed across many enterprise networks to enable single sign-on and authentication for enterprise services. This makes it an attractive target for attacks, which can result in persistent, undetected access to services within a network in what is known as a "golden ticket" attack. To

detect this form of attack, behavioral analytics may be employed to detect forged authentication tickets resulting from an attack. According to the aspect, an advanced cyber decision platform may continuously monitor a network **1701**, informing a CPG in real-time of all traffic associated with entities in an organization, for example, people, places, devices, or services **1702**. Machine learning algorithms detect behavioral anomalies as they occur in real-time **1703**, notifying administrators with an assessment of the anomalous event **1704** as well as a blast radius score for the particular event and a network resiliency score to advise of the overall health of the network. By automatically detecting unusual behavior and informing an administrator of the anomaly along with contextual information for the event and network, a compromised ticket is immediately detected when a new authentication connection is made.

[0098] Fig. 18 is a flow diagram of an exemplary method **1800** for risk-based vulnerability and patch management, according to one aspect. According to the aspect, an advanced cyber decision platform may monitor all information about a network **1801**, including (but not limited to) device telemetry data, log files, connections and network events, deployed software versions, or contextual user activity information. This information is incorporated into a CPG **1802** to maintain an up-to-date model of the network in real-time. When a new vulnerability is discovered, a blast radius score may be assessed **1803** and the network's resiliency score may be updated **1804** as needed. A security alert may then be produced **1805** to notify an administrator of the vulnerability and its impact, and a proposed patch may be presented **1806** along with the predicted effects of the patch on the vulnerability's blast radius and the overall network resiliency score. This determines both the total impact risk of any particular vulnerability, as well as the overall effect of each vulnerability on the network as a whole. This continuous network assessment may be used to collect information about new vulnerabilities and exploits to provide proactive solutions with clear result predictions, before attacks occur.

[0099] Fig. 20 is a relational diagram showing the relationships between exemplary 3rd party search tools **1915**, search tasks **2010** that can be generated using such tools, and the types of information that may be gathered with those tasks **2011-2014**, and how a public-facing proxy network **1908** may be used to influence the search task results. While the use of 3rd party search tools **1915** is in no way required, and proprietary or other self-developed search tools may be used, there are numerous 3rd party search tools **1915** available on the Internet, many of them available for use free of charge, that are convenient for purposes of performing external and

internal reconnaissance of an organization's infrastructure. Because they are well-known, they are included here as examples of the types of search tools that may be used and the reconnaissance data that may be gathered using such tools. The search tasks **2010** that may be generated may be classified into several categories. While this category list is by no means exhaustive, several important categories of reconnaissance data are domain and internet protocol (IP) address searching tasks **2011**, corporate information searching tasks **2012**, data breach searching tasks **2013**, and dark web searching tasks **2014**. Third party search tools **1915** for domain and IP address searching tasks **2011** include, for example, DNSDumpster, Spiderfoot HX, Shodan, VirusTotal, Dig, Censys, ViewDNS, and CheckDMARC, among others. These tools may be used to obtain reconnaissance data about an organization's server IPs, software, geolocation; open ports, patch/setting vulnerabilities; data hosting services, among other data **2031**. Third party search tools **1915** for corporate information searching tasks **2012** include, for example, Bloomberg.com, Wikipedia, SEC.gov, AnnualReports.com, DNB.com, Hunter.io, and MarketVisual, among others. These tools may be used to obtain reconnaissance data about an organization's addresses; corp info; high value target (key employee or key data assets) lists, emails, phone numbers, online presence **2032**. Third party search tools **1915** for data breach searching tasks **2013** include, for example, DeHashed, WeLeakInfo, Pastebin, Spiderfoot, and BreachCompilation, among others. These tools may be used to obtain reconnaissance data about an organization's previous data breaches, especially those involving high value targets, and similar data loss information **2033**. Third party search tools **1915** for deep web (reports, records, and other documents linked to in web pages, but not indexed in search results… estimated to be 90% of available web content) and dark web (websites accessible only through anonymizers such as TOR… estimated to be about 6% of available web content) searching tasks **2014** include, for example, Pipl, MyLife, Yippy, SurfWax, Wayback machine, Google Scholar, DuckDuckGo, Fazzle, Not Evil, and Start Page, among others. These tools may be used to obtain reconnaissance data about an organization's lost and stolen data such as customer credit card numbers, stolen subscription credentials, hacked accounts, software tools designed for certain exploits, which organizations are being targeted for certain attacks, and similar information **2034**. A public-facing proxy network **1908** may be used to change the outward presentation of the organization's network by conducting the searches through selectable attribution nodes **2021a-n**, which are configurable to present the network to the Internet in different ways such as,

but not limited to, presenting the organization network as a commercial IP address, a residential IP address, or as an IP address from a particular country, all of which may influence the reconnaissance data received using certain search tools.

[0100] Fig. 21 is a relational diagram showing the exemplary types and classifications of information that may be used in constructing a cyber-physical graph **1902** of an organization's infrastructure and operations. The cyber-physical graph **1902** is a directed graph that represents a comprehensive picture of an organization's infrastructure and operations. A cyber-physical graph **1902** represents the relationships between entities associated with an organization, for example, devices, users, resources, groups, and computing services, the relationships between the entities defining relationships and processes in an organization's infrastructure, thereby contextualizing security information with physical and logical relationships that represent the flow of data and access to data within the organization including, in particular, network security protocols and procedures. Data that may be incorporated into a cyber-physical graph may be any data relating to an organization's infrastructure and operations, and two primary categories of data that may be incorporated are internal reconnaissance data **2110** and external reconnaissance data **2120**. Non-limiting examples of internal reconnaissance data **2110** include computers and devices, physical and intangible (data) assets, people (employees, contractors, etc.), addresses and locations of buildings, servers, etc., business processes, access privileges, loss information, legal documents, and self-assessments of cybersecurity. Non-limiting examples of external reconnaissance data **2120** include domains and IP information, data breach information, organization information such as corporate structures, key employees, etc., open port information, information regarding which organizations are current targets of cyber-attacks, network vulnerability information, system version and patch/update information, known and possible exploits, and publicly available information.

[0101] In an initial step **1101**, behavior analytics information (as described previously, referring to **Fig. 8**) may be received at a graphing service **145** for inclusion in a CPG. In a next step **1102**, impact assessment scores (as described previously, referring to **Fig. 9**) may be received and incorporated in the CPG information, adding risk assessment context to the behavior information. In a next step **1103**, time-series information (as described previously, referring to **Fig. 10**) may be received and incorporated, updating CPG information as changes occur and events are logged. This information may then be used to produce **1104** a graph visualization of

users, servers, devices, and other resources correlating physical relationships (such as a user's personal computer or smartphone, or physical connections between servers) with logical relationships (such as access privileges or database connections), to produce a meaningful and contextualized visualization of a security infrastructure that reflects the current state of the internal relationships present in the infrastructure.

[0102] Fig. 22 is a directed graph diagram showing an exemplary cyber-physical graph **2200** and its possible use in creating cybersecurity profiles and ratings. A cyber-physical graph **1902** represents the relationships between entities associated with an organization, for example, devices, users, resources, groups, and computing services, the relationships between the entities defining relationships and processes in an organization's infrastructure, thereby contextualizing security information with physical and logical relationships that represent the flow of data and access to data within the organization including, in particular, network security protocols and procedures. A cyber-physical graph, in its most basic form, represents the network devices comprising an organization's network infrastructure as nodes (also called vertices) in the graph and the physical or logical connections between them as edges between the nodes. The cyber-physical graph may be expanded to include network information and processes such as data flow, security protocols and procedures, and software versions and patch information. Further, human users and their access privileges to devices and assets may be included. A cyber-security graph may be further expanded to include internal process information such as business processes, loss information, and legal requirements and documents; external information such as domain and IP information, data breach information; and generated information such as open port information from external network scans, and vulnerabilities and avenues of attack. Thus, a cyber-physical graph may be used to represent a complete picture of an organization's infrastructure and operations.

[0103] In this example, which is necessarily simplified for clarity, the cyber-physical graph **2200** contains 12 nodes (vertices) comprising: seven computers and devices designated by solid circles **2202, 2203, 2204, 2206, 2207, 2209, 2210**, two users designated by dashed-line circles **2201, 2211**, and three functional groups designated by dotted-line circles **2205, 2208, and 2212**. The edges (lines) between the nodes indicate relationships between the nodes, and have a direction and relationship indicator such as "AdminTo," "MemberOf," etc. While not shown here, the edges may also be assigned numerical weights or probabilities, indicating, for example, the

likelihood of a successful attack gaining access from one node to another. Possible attack paths may be analyzed using the cyber-physical graph by running graph analysis algorithms such as shortest path algorithms, minimum cost/maximum flow algorithms, strongly connected node algorithms, etc. In this example, several exemplary attack paths are ranked by likelihood. In the most likely attack path, user **2201** is an administrator to device **2202** to which device **2203** has connected. Device **2203** is a member of functional group **2208**, which has a member of group **2212**. Functional group **2212** is an administrator to the target **2206**. In a second most likely attack path, user **2201** is an administrator to device **2207** to which device **2204** has connected. Device **2204** is a member of functional group **2205**, which is an administrator to the target device **2206**. In a third most likely attack path, a flaw in the security protocols allow the credentials of user **2201** to be used to gain access to device **2210**. User **2211** who is working on device **2210** may be tricked into providing access to functional group **2205**, which is an administrator to the target device **2206**.

[0104] Fig. 23 is a block diagram showing exemplary operation of a data to rule mapper. Laws, policies, standards, and other rules are gathered and stored in an authority database **1903**. Non-limiting examples of such rules include federal, state, and local statutes, regulations, case law interpretations, and other laws **2310**, business policies and procedures **2320**, and industry standards (as one example, cybersecurity industry standards for network security) **2330**. Reconnaissance data are stored in a database **1905**. A data to rule mapper **1904** retrieves the reconnaissance data **1905** and matches it to rules from the authority database **1903**. An example of this operation for statues/regulations **2310** is shown in **2311**, where Article 33, paragraph 1 of the European Union's General Data Protection Regulation (GDPR) requires that an organization notify a cognizant authority of a data breach within 72 hours of knowledge of the breach. If a data point indicates that a data breach has been discovered because data of the organization is found online, the data point is associated with that rule, and tagged with the possible impact of fines if the rule is not followed. An example of this operation for business policies **2320** is shown in **2321**, where a corporate policy prohibits access of the organization's systems using personal computers. If a data point indicates that an employee account is accessed using a non-business-owned computer, the data point is associated with the rule, and tagged with possible data theft and/or security breach. An example of this operation for industry standards **2330** is shown in **2331**, where an industry standard prohibits open ports accessible from outside the network

perimeter. If a data point indicates an open port, the data point is associated with the rule, and tagged with possible data loss and/or security breach.

Hardware Architecture

[0105] Generally, the techniques disclosed herein may be implemented on hardware or a combination of software and hardware. For example, they may be implemented in an operating system kernel, in a separate user process, in a library package bound into network applications, on a specially constructed machine, on an application-specific integrated circuit (ASIC), or on a network interface card.

[0106] Software/hardware hybrid implementations of at least some of the aspects disclosed herein may be implemented on a programmable network-resident machine (which should be understood to include intermittently connected network-aware machines) selectively activated or reconfigured by a computer program stored in memory. Such network devices may have multiple network interfaces that may be configured or designed to utilize different types of network communication protocols. A general architecture for some of these machines may be described herein in order to illustrate one or more exemplary means by which a given unit of functionality may be implemented. According to specific aspects, at least some of the features or functionalities of the various aspects disclosed herein may be implemented on one or more general-purpose computers associated with one or more networks, such as for example an end-user computer system, a client computer, a network server or other server system, a mobile computing device (e.g., tablet computing device, mobile phone, smartphone, laptop, or other appropriate computing device), a consumer electronic device, a music player, or any other suitable electronic device, router, switch, or other suitable device, or any combination thereof. In at least some aspects, at least some of the features or functionalities of the various aspects disclosed herein may be implemented in one or more virtualized computing environments (e.g., network computing clouds, virtual machines hosted on one or more physical computing machines, or other appropriate virtual environments).

[0107] Referring now to **Fig. 25**, there is shown a block diagram depicting an exemplary computing device **10** suitable for implementing at least a portion of the features or functionalities disclosed herein. Computing device **10** may be, for example, any one of the computing machines listed in the previous paragraph, or indeed any other electronic device capable of executing software- or hardware-based instructions according to one or more programs stored in memory.

Computing device **10** may be configured to communicate with a plurality of other computing devices, such as clients or servers, over communications networks such as a wide area network a metropolitan area network, a local area network, a wireless network, the Internet, or any other network, using known protocols for such communication, whether wireless or wired.

[0108] In one aspect, computing device **10** includes one or more central processing units (CPU) **12**, one or more interfaces **15**, and one or more busses **14** (such as a peripheral component interconnect (PCI) bus). When acting under the control of appropriate software or firmware, CPU **12** may be responsible for implementing specific functions associated with the functions of a specifically configured computing device or machine. For example, in at least one aspect, a computing device **10** may be configured or designed to function as a server system utilizing CPU **12**, local memory **11** and/or remote memory **16**, and interface(s) **15**. In at least one aspect, CPU **12** may be caused to perform one or more of the different types of functions and/or operations under the control of software modules or components, which for example, may include an operating system and any appropriate applications software, drivers, and the like.

[0109] CPU **12** may include one or more processors **13** such as, for example, a processor from one of the Intel, ARM, Qualcomm, and AMD families of microprocessors. In some aspects, processors **13** may include specially designed hardware such as application-specific integrated circuits (ASICs), electrically erasable programmable read-only memories (EEPROMs), field-programmable gate arrays (FPGAs), and so forth, for controlling operations of computing device **10**. In a particular aspect, a local memory **11** (such as non-volatile random access memory (RAM) and/or read-only memory (ROM), including for example one or more levels of cached memory) may also form part of CPU **12**. However, there are many different ways in which memory may be coupled to system **10**. Memory **11** may be used for a variety of purposes such as, for example, caching and/or storing data, programming instructions, and the like. It should be further appreciated that CPU **12** may be one of a variety of system-on-a-chip (SOC) type hardware that may include additional hardware such as memory or graphics processing chips, such as a QUALCOMM SNAPDRAGON™ or SAMSUNG EXYNOS™ CPU as are becoming increasingly common in the art, such as for use in mobile devices or integrated devices.

[0110] As used herein, the term "processor" is not limited merely to those integrated circuits referred to in the art as a processor, a mobile processor, or a microprocessor, but broadly refers to

a microcontroller, a microcomputer, a programmable logic controller, an application-specific integrated circuit, and any other programmable circuit.

[0111] In one aspect, interfaces **15** are provided as network interface cards (NICs). Generally, NICs control the sending and receiving of data packets over a computer network; other types of interfaces **15** may for example support other peripherals used with computing device **10**. Among the interfaces that may be provided are Ethernet interfaces, frame relay interfaces, cable interfaces, DSL interfaces, token ring interfaces, graphics interfaces, and the like. In addition, various types of interfaces may be provided such as, for example, universal serial bus (USB), Serial, Ethernet, FIREWIRE™, THUNDERBOLT™, PCI, parallel, radio frequency (RF), BLUETOOTH™, near-field communications (e.g., using near-field magnetics), 802.11 (WiFi), frame relay, TCP/IP, ISDN, fast Ethernet interfaces, Gigabit Ethernet interfaces, Serial ATA (SATA) or external SATA (ESATA) interfaces, high-definition multimedia interface (HDMI), digital visual interface (DVI), analog or digital audio interfaces, asynchronous transfer mode (ATM) interfaces, high-speed serial interface (HSSI) interfaces, Point of Sale (POS) interfaces, fiber data distributed interfaces (FDDIs), and the like. Generally, such interfaces **15** may include physical ports appropriate for communication with appropriate media. In some cases, they may also include an independent processor (such as a dedicated audio or video processor, as is common in the art for high-fidelity A/V hardware interfaces) and, in some instances, volatile and/or non-volatile memory (e.g., RAM).

[0112] Although the system shown in **Fig. 25** illustrates one specific architecture for a computing device **10** for implementing one or more of the aspects described herein, it is by no means the only device architecture on which at least a portion of the features and techniques described herein may be implemented. For example, architectures having one or any number of processors **13** may be used, and such processors **13** may be present in a single device or distributed among any number of devices. In one aspect, a single processor **13** handles communications as well as routing computations, while in other aspects a separate dedicated communications processor may be provided. In various aspects, different types of features or functionalities may be implemented in a system according to the aspect that includes a client device (such as a tablet device or smartphone running client software) and server systems (such as a server system described in more detail below).

[0113] Regardless of network device configuration, the system of an aspect may employ one or more memories or memory modules (such as, for example, remote memory block **16** and local memory **11**) configured to store data, program instructions for the general-purpose network operations, or other information relating to the functionality of the aspects described herein (or any combinations of the above). Program instructions may control execution of or comprise an operating system and/or one or more applications, for example. Memory **16** or memories **11, 16** may also be configured to store data structures, configuration data, encryption data, historical system operations information, or any other specific or generic non-program information described herein.

[0114] Because such information and program instructions may be employed to implement one or more systems or methods described herein, at least some network device aspects may include nontransitory machine-readable storage media, which, for example, may be configured or designed to store program instructions, state information, and the like for performing various operations described herein. Examples of such nontransitory machine- readable storage media include, but are not limited to, magnetic media such as hard disks, floppy disks, and magnetic tape; optical media such as CD-ROM disks; magneto-optical media such as optical disks, and hardware devices that are specially configured to store and perform program instructions, such as read-only memory devices (ROM), flash memory (as is common in mobile devices and integrated systems), solid state drives (SSD) and "hybrid SSD" storage drives that may combine physical components of solid state and hard disk drives in a single hardware device (as are becoming increasingly common in the art with regard to personal computers), memristor memory, random access memory (RAM), and the like. It should be appreciated that such storage means may be integral and non-removable (such as RAM hardware modules that may be soldered onto a motherboard or otherwise integrated into an electronic device), or they may be removable such as swappable flash memory modules (such as "thumb drives" or other removable media designed for rapidly exchanging physical storage devices), "hot-swappable" hard disk drives or solid state drives, removable optical storage discs, or other such removable media, and that such integral and removable storage media may be utilized interchangeably. Examples of program instructions include both object code, such as may be produced by a compiler, machine code, such as may be produced by an assembler or a linker, byte code, such as may be generated by for example a JAVA™ compiler and may be executed using a Java virtual

machine or equivalent, or files containing higher level code that may be executed by the computer using an interpreter (for example, scripts written in Python, Perl, Ruby, Groovy, or any other scripting language).

[0115] In some aspects, systems may be implemented on a standalone computing system. Referring now to **Fig. 26**, there is shown a block diagram depicting a typical exemplary architecture of one or more aspects or components thereof on a standalone computing system. Computing device **20** includes processors **21** that may run software that carry out one or more functions or applications of aspects, such as for example a client application **24**. Processors **21** may carry out computing instructions under control of an operating system **22** such as, for example, a version of MICROSOFT WINDOWS™ operating system, APPLE macOS™ or iOS™ operating systems, some variety of the Linux operating system, ANDROID™ operating system, or the like. In many cases, one or more shared services **23** may be operable in system **20**, and may be useful for providing common services to client applications **24**. Services **23** may for example be WINDOWS™ services, user-space common services in a Linux environment, or any other type of common service architecture used with operating system **21**. Input devices **28** may be of any type suitable for receiving user input, including for example a keyboard, touchscreen, microphone (for example, for voice input), mouse, touchpad, trackball, or any combination thereof. Output devices **27** may be of any type suitable for providing output to one or more users, whether remote or local to system **20**, and may include for example one or more screens for visual output, speakers, printers, or any combination thereof. Memory **25** may be random-access memory having any structure and architecture known in the art, for use by processors **21**, for example to run software. Storage devices **26** may be any magnetic, optical, mechanical, memristor, or electrical storage device for storage of data in digital form (such as those described above, referring to **Fig. 25**). Examples of storage devices **26** include flash memory, magnetic hard drive, CD-ROM, and/or the like.

[0116] In some aspects, systems may be implemented on a distributed computing network, such as one having any number of clients and/or servers. Referring now to **Fig. 27**, there is shown a block diagram depicting an exemplary architecture **30** for implementing at least a portion of a system according to one aspect on a distributed computing network. According to the aspect, any number of clients **33** may be provided. Each client **33** may run software for implementing client-side portions of a system; clients may comprise a system **20** such as that illustrated in **Fig. 26**. In

addition, any number of servers **32** may be provided for handling requests received from one or more clients **33**. Clients **33** and servers **32** may communicate with one another via one or more electronic networks **31**, which may be in various aspects any of the Internet, a wide area network, a mobile telephony network (such as CDMA or GSM cellular networks), a wireless network (such as WiFi, WiMAX, LTE, and so forth), or a local area network (or indeed any network topology known in the art; the aspect does not prefer any one network topology over any other). Networks **31** may be implemented using any known network protocols, including for example wired and/or wireless protocols.

[0117] In addition, in some aspects, servers **32** may call external services **37** when needed to obtain additional information, or to refer to additional data concerning a particular call. Communications with external services **37** may take place, for example, via one or more networks **31**. In various aspects, external services **37** may comprise web-enabled services or functionality related to or installed on the hardware device itself. For example, in one aspect where client applications **24** are implemented on a smartphone or other electronic device, client applications **24** may obtain information stored in a server system **32** in the cloud or on an external service **37** deployed on one or more of a particular enterprise's or user's premises. In addition to local storage on servers **32**, remote storage **38** may be accessible through the network(s) **31**.

[0118] In some aspects, clients **33** or servers **32** (or both) may make use of one or more specialized services or appliances that may be deployed locally or remotely across one or more networks **31**. For example, one or more databases **34** in either local or remote storage **38** may be used or referred to by one or more aspects. It should be understood by one having ordinary skill in the art that databases in storage **34** may be arranged in a wide variety of architectures and using a wide variety of data access and manipulation means. For example, in various aspects one or more databases in storage **34** may comprise a relational database system using a structured query language (SQL), while others may comprise an alternative data storage technology such as those referred to in the art as "NoSQL" (for example, HADOOP CASSANDRA™, GOOGLE BIGTABLE™, and so forth). In some aspects, variant database architectures such as column-oriented databases, in-memory databases, clustered databases, distributed databases, or even flat file data repositories may be used according to the aspect. It will be appreciated by one having ordinary skill in the art that any combination of known or future database technologies may be

used as appropriate, unless a specific database technology or a specific arrangement of components is specified for a particular aspect described herein. Moreover, it should be appreciated that the term "database" as used herein may refer to a physical database machine, a cluster of machines acting as a single database system, or a logical database within an overall database management system. Unless a specific meaning is specified for a given use of the term "database", it should be construed to mean any of these senses of the word, all of which are understood as a plain meaning of the term "database" by those having ordinary skill in the art.

[0119] Similarly, some aspects may make use of one or more security systems **36** and configuration systems **35**. Security and configuration management are common information technology (IT) and web functions, and some amount of each are generally associated with any IT or web systems. It should be understood by one having ordinary skill in the art that any configuration or security subsystems known in the art now or in the future may be used in conjunction with aspects without limitation, unless a specific security **36** or configuration system **35** or approach is specifically required by the description of any specific aspect.

[0120] Fig. 28 shows an exemplary overview of a computer system **40** as may be used in any of the various locations throughout the system. It is exemplary of any computer that may execute code to process data. Various modifications and changes may be made to computer system **40** without departing from the broader scope of the system and method disclosed herein. Central processor unit (CPU) **41** is connected to bus **42**, to which bus is also connected memory **43**, nonvolatile memory **44**, display **47**, input/output (I/O) unit **48**, and network interface card (NIC) **53**. I/O unit **48** may, typically, be connected to peripherals such as a keyboard **49**, pointing device **50**, hard disk **52**, real-time clock **51,** a camera **57**, and other peripheral devices. NIC **53** connects to network **54**, which may be the Internet or a local network, which local network may or may not have connections to the Internet. The system may be connected to other computing devices through the network via a router **55**, wireless local area network **56**, or any other network connection. Also shown as part of system **40** is power supply unit **45** connected, in this example, to a main alternating current (AC) supply **46**. Not shown are batteries that could be present, and many other devices and modifications that are well known but are not applicable to the specific novel functions of the current system and method disclosed herein. It should be appreciated that some or all components illustrated may be combined, such as in various integrated applications, for example Qualcomm or Samsung system-on-a-chip (SOC) devices, or whenever it may be

appropriate to combine multiple capabilities or functions into a single hardware device (for instance, in mobile devices such as smartphones, video game consoles, in-vehicle computer systems such as navigation or multimedia systems in automobiles, or other integrated hardware devices).

[0121] In various aspects, functionality for implementing systems or methods of various aspects may be distributed among any number of client and/or server components. For example, various software modules may be implemented for performing various functions in connection with the system of any particular aspect, and such modules may be variously implemented to run on server and/or client components.

[0122] The skilled person will be aware of a range of possible modifications of the various aspects described above. Accordingly, the present invention is defined by the claims and their equivalents.

[0123] Where a method is claimed below, the steps of the method are intended to be construed without any order unless it is impossible to perform a given step before another.

What is claimed is:

1. A computer system comprising a memory, wherein the computer system is configured to execute software instructions stored on nontransitory machine-readable storage media that:

store in the memory a representation of a first graph, wherein the representation of the first graph comprises representations of a first plurality of nodes and a first plurality of edges,

wherein the first graph is a directed graph,

wherein each node of the first plurality of nodes corresponds to a respective entity of a plurality of entities, and

wherein the first plurality of edges includes at least one edge corresponding to a physical connection between entities and at least one edge corresponding to a logical connection between entities;

process, substantially in real time, streaming data received from a plurality of devices,

wherein the streaming data comprises information about events relating to the plurality of entities;

process the representation of the first graph to add, subtract, or modify a node of the first graph based on the streaming data,

process the representation of the first graph to add, subtract, or modify an edge of the first graph based on the streaming data,

use the representation of the first graph to determine whether an event, of the events relating to the plurality of entities, is anomalous, and,

if the event is anomalous, identify the event as a first anomalous event.

2. The computer system of claim 1, further configured to execute software instructions stored on nontransitory machine-readable storage media that:

identify a first plurality of possible event flows,

wherein the first plurality of possible event flows comprises a possible event flow relating to an entity of the plurality of entities,

wherein the entity relates to the first anomalous event;

identify a first plurality of dependencies,

wherein each dependency of the first plurality of dependencies is associated with a respective possible event flow of the first plurality of possible event flows; and,

a second plurality of nodes of the first graph,

wherein each node of the second plurality of nodes corresponds to a respective entity relating to a respective possible event flow of the first plurality of possible event flows.

3. The system of claim 2, further configured to execute software instructions stored on nontransitory machine-readable storage media that:

store in the memory a representation of a second graph,

wherein the representation of the second graph comprises a representation of a third plurality of nodes,

wherein each node of the third plurality of nodes corresponds to a respective node of the second plurality of nodes; and

wherein the representation of the second graph comprises a representation of a second plurality of edges,

wherein at least a portion of at least one of the first plurality of dependencies or the first plurality of possible event flows is used to generate the second plurality of edges; and,

traverse the second graph to identify a point of origin for the first anomalous event.

4. The computer system of claim 3, wherein the representation of the first graph comprises a representation of a node corresponding to an entity identified based on active reconnaissance results.

5. The computer system of claim 3, wherein the representation of the first graph comprises a representation of a node corresponding to an entity identified based on passive reconnaissance results.

6. The computer system of claim 3, wherein the representation of the second graph is generated at least in part by processing at least a portion of the representation of the first graph using at least one transformation pipeline.

7. The computer system of claim 3, further configured to execute software instructions stored on nontransitory machine-readable storage media that:

identify a fourth plurality of nodes of the first graph,

wherein each node of the fourth plurality of nodes corresponds to a respective entity of the plurality of entities,

wherein the respective entity of the plurality of entities relates to a second anomalous event;

identify a second plurality of possible event flows, and

identify a second plurality of dependencies,

wherein each dependency of the second plurality of dependencies is associated with a respective possible event flow of the second plurality of possible event flows.

8. The computer system of claim 7, wherein the representation of the second graph further comprises:

a representation of a fifth plurality of nodes,

wherein each node of the fifth plurality of nodes corresponds to a respective node of the fourth plurality of nodes; and,

a representation of a third plurality of edges,

wherein at least a portion of at least one of the second plurality of dependencies or the second plurality of possible event flows is used to generate the third plurality of edges.

9. The computer system of claim 8, wherein the second anomalous event is correlated in time to the first anomalous event.

10. The computer system of claim 1, wherein determining whether an event, of the events relating to the plurality of entities, is anomalous comprises:

determining that the event relates to a first entity of the plurality of entities,

determining at least one behavior pattern associated with the first entity, and

comparing the event to the at least one behavior pattern.

11. The computer system of claim 10, wherein comparing the event to the at least one behavior pattern comprises using a threshold.

12. The computer system of claim 10, further configured to execute software instructions stored on nontransitory machine-readable storage media that:

identify a first plurality of possible event flows,

wherein the first plurality of possible event flows comprises a possible event flow relating to a second entity of the plurality of entities,

wherein the second entity relates to the first anomalous event;

identify a first plurality of dependencies,

wherein each dependency of the first plurality of dependencies is associated with a respective possible event flow of the first plurality of possible event flows; and,

identify a second plurality of nodes of the first graph,

wherein each node of the second plurality of nodes corresponds to a respective entity relating to a respective possible event flow of the first plurality of possible event flows.

13. The computer system of claim 12, further configured to execute software instructions stored on nontransitory machine-readable storage media that:

store in the memory a representation of a second graph,

wherein the representation of the second graph comprises a representation of a third plurality of nodes,

wherein each node of the third plurality of nodes corresponds to a respective node of the second plurality of nodes; and,

wherein the representation of the second graph comprises a representation of a second plurality of edges,

wherein at least a portion of at least one of the first plurality of dependencies or the first plurality of possible event flows is used to generate the second plurality of edges; and,

traverse the second graph to identify a point of origin for the first anomalous event.

14. The system of claim 10, wherein comparing the event to the at least one behavior pattern further comprises:

determining that the first entity is associated with a resource,

wherein the resource is a sensitive resource.

15. The computer system of claim 14, further configured to execute software instructions stored on nontransitory machine-readable storage media that:

identify a first plurality of possible event flows,

wherein the first plurality of possible event flows comprises a possible event flow relating to a second entity of the plurality of entities,

wherein the second entity relates to the first anomalous event;

identify a first plurality of dependencies,

wherein each dependency of the first plurality of dependencies is associated with a respective possible event flow of the first plurality of possible event flows; and,

identify a second plurality of nodes of the first graph,

wherein each node of the second plurality of nodes corresponds to a respective entity relating to a respective possible event flow of the first plurality of possible event flows.

16. The computer system of claim 15, further configured to execute software instructions stored on nontransitory machine-readable storage media that:

store in the memory a representation of a second graph,

wherein the representation of the second graph comprises a representation of a third plurality of nodes,

wherein each node of the third plurality of nodes corresponds to a respective node of the second plurality of nodes; and,

wherein the representation of the second graph comprises a representation of a second plurality of edges,

wherein at least a portion of at least one of the first plurality of dependencies or the first plurality of possible event flows is used to generate the second plurality of edges; and,

traverse the second graph to identify a point of origin for the first anomalous event.

17. The computer system of claim 1, wherein the computer system comprises a plurality of physical computing machines.

18. The computer system of claim 1, wherein the computer system comprises a plurality of virtual computing machines.

19. The computer system of claim 1, wherein at least one entity of the first plurality of entities is at least one of a user, a place, a device, a resource, a group, or a service.

20. The computer system of claim 3, wherein the representation of the second graph further comprises a representation of at least one node that does not correspond to any node of the second plurality of nodes.

21. The computer system of claim 13, wherein the representation of the second graph further comprises a representation of at least one node that does not correspond to any node of the second plurality of nodes.

22. The computer system of claim 16, wherein the representation of the second graph further comprises a representation of at least one node that does not correspond to any node of the second plurality of nodes.

23. The computer system of claim 3,

wherein traversing the second graph to identify a point of origin for the first anomalous event comprises, in the following order:

processing a representation of a first node of the third plurality of nodes,

wherein the first node corresponds to a second node of the second plurality of nodes;

identifying an edge of the second plurality of edges, wherein the edge connects a third node of the third plurality of nodes with the first node, and

processing a representation of the third node.

24. The computer system of claim 13,

wherein traversing the second graph to identify a point of origin for the first anomalous event comprises, in the following order:

processing a representation of a first node of the third plurality of nodes,

wherein the first node corresponds to a second node of the second plurality of nodes;

identifying an edge of the second plurality of edges, wherein the edge connects a third node of the third plurality of nodes with the first node, and

processing a representation of the third node.

25. The computer system of claim 16,

wherein traversing the second graph to identify a point of origin for the first anomalous event comprises, in the following order:

processing a representation of a first node of the third plurality of nodes,

wherein the first node corresponds to a second node of the second plurality of nodes;

identifying an edge of the second plurality of edges, wherein the edge connects a third node of the third plurality of nodes with the first node, and

processing a representation of the third node.

26. The computer system of claim 1, wherein the representation of the first graph comprises a representation of at least one node that does not correspond to an entity.

ABSTRACT

A system and method for correlating network event anomalies to identify attack information, that identifies anomalous events within the network, identifies correlations between anomalies and other network events and resources, generates a behavior graph describing an attack pathway derived from the correlations, and determines an attack point of origin using the behavior graph.

Doc Code: ECOMM.AUTH/ECOMM.WTDW
Doc Description: Internet Communications Authorized/Internet Communications Authorization Withdrawn

PTO/SB/439 (11-15)

AUTHORIZATION FOR INTERNET COMMUNICATIONS IN A PATENT APPLICATION OR REQUEST TO WITHDRAW AUTHORIZATION FOR INTERNET COMMUNICATIONS		
	Application No.	
	Filing Date	2024-09-20
	First Named Inventor	Jason Crabtree
	Art Unit	
	Examiner Name	
	Practitioner Docket No.	15388FT

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

I. To authorize permission for Internet Communications.

☑ Recognizing that Internet communications are not secure, I hereby authorize the USPTO to communicate with the undersigned and practitioners in accordance with 37 CFR 1.33 and 37 CFR 1.34 concerning any subject matter of this application via video conferencing, instant messaging, or electronic mail. I understand that a copy of these communications will be made of record in the application file. (MPEP 502.03)

II. To withdraw authorization for Internet Communications.

☐ The authorization given on _____, to the USPTO to communicate with the undersigned and any practitioner in accordance with 37 CFR 1.33 and 37 CFR 1.34 concerning any subject matter of this application via Internet communications such as video conferencing, instant messaging, or electronic mail is hereby withdrawn. I understand that the withdrawal is effective when approved rather than when received.

I am the

☐ applicant.

☑ attorney or agent of record. Registration number 50966.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/BRIAN R. GALVIN/ — Signature

September 20, 2024 — Date

Brian R. Galvin — Typed or printed name

(360) 674-6233 — Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Juristic entities must be represented by a patent practitioner (see 37 CFR 1.31, which is applicable to any paper filed on or after September 16, 2012, that is presented on behalf of a juristic entity, regardless of application filing date). Submit multiple forms if more than one signature is required, see below*.

☑ * Total of 1 forms are submitted.

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.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/892,283	**09/20/2024 09:40:02 PM Z ET**	**15388FT**

Title of Invention

CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	7526	FILED BY	Aura Morrey
PATENT CENTER #	67267157	FILING DATE	-
CUSTOMER #	82318	FIRST NAMED INVENTOR	Jason Crabtree
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Brian Galvin

Documents

TOTAL DOCUMENTS: 0

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)

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 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

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/892,283	**09/20/2024 10:03:04 PM Z ET**	**15388FT**

Title of Invention

CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	7526	FILED BY	Aura Morrey
PATENT CENTER #	67267232	FILING DATE	-
CUSTOMER #	82318	FIRST NAMED INVENTOR	Jason Crabtree
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Brian Galvin

Documents

TOTAL DOCUMENTS: 0

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)

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 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

Office of the Chief Financial Officer

Document Code:WFEE

User :Saada Yousuf

Sale Accounting Date:09/23/2024

Sale Item Reference Number	Effective Date
18892283	09/20/2024

Document Number	Fee Code	Fee Code Description	Amount Paid	Payment Method
I20249M911166238	1202	CLAIMS IN EXCESS OF 20	$500.00	Credit Card

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
18/892,283	09/20/2024		2320	15388FT	26	1

CONFIRMATION NO. 7526

FILING RECEIPT

82318
Brian Galvin
Galvin Patent Law LLC
2916 NW Bucklin Hill Road
Suite 485
Silverdale, WA 98383

Date Mailed: 10/02/2024

Receipt is acknowledged of this non-provisional utility 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 FIRST INVENTOR, 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 corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction 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 provided that the request is grantable.

Inventor(s)

Jason Crabtree, Vienna, VA;
Andrew Sellers, Monument, CO;
Richard Kelley, Woodbridge, VA;

Applicant(s)

QOMPLX LLC, Reston, VA;

Power of Attorney: The patent practitioners associated with Customer Number 82318

Domestic Priority data as claimed by applicant

This application is a CON of 17/237,346 04/22/2021
which is a CIP of 16/777,270 01/30/2020 PAT 11,025,674
which is a CIP of 16/720,383 12/19/2019 PAT 10,944,795
which is a CON of 15/823,363 11/27/2017 PAT 10,560,483
which is a CIP of 15/725,274 10/04/2017 PAT 10,609,079
which is a CIP of 15/655,113 07/20/2017 PAT 10,735,456
which is a CIP of 15/616,427 06/07/2017 ABN
which is a CIP of 14/925,974 10/28/2015 ABN
and said 15/655,113 07/20/2017 is a CIP of 15/237,625 08/15/2016 PAT 10,248,910
which is a CIP of 15/206,195 07/08/2016 ABN
which is a CIP of 15/186,453 06/18/2016 ABN
which is a CIP of 15/166,158 05/26/2016 ABN
which is a CIP of 15/141,752 04/28/2016 PAT 10,860,962
which is a CIP of 15/091,563 04/05/2016 PAT 10,204,147

and is a CIP of 14/986,536 12/31/2015 PAT 10,210,255
and is a CIP of 14/925,974 10/28/2015 ABN

Foreign Applications for which priority is claimed (You may be eligible to benefit from the Patent Prosecution Highway program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 09/30/2024

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 18/892,283**

Projected Publication Date: 01/09/2025

Non-Publication Request: No

Early Publication Request: No
Title

CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION

Preliminary Class

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

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 (1-866-999-4258).

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 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 U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number
18/892,283

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	320
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	700
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	800
TOTAL CLAIMS (37 CFR 1.16(i))	26 minus 20 =	* 6			OR	x 100 =	600
INDEPENDENT CLAIMS (37 CFR 1.16(h))	1 minus 3 =	*				x =	0
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
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	2420

APPLICATION AS AMENDED - PART II

		(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($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
AMENDMENT A	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
AMENDMENT A	Application Size Fee (37 CFR 1.16(s))									
AMENDMENT A	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)	OR	RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
AMENDMENT B	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
AMENDMENT B	Application Size Fee (37 CFR 1.16(s))									
AMENDMENT B	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	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
18/892,283	09/20/2024	Jason Crabtree	15388FT

CONFIRMATION NO. 7526

FORMALITIES LETTER

OC000000078754241

82318
Brian Galvin
Galvin Patent Law LLC
2916 NW Bucklin Hill Road
Suite 485
Silverdale, WA 98383

Date Mailed: 10/02/2024

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

An application number and filing date have been accorded to the above-identified nonprovisional application. The item(s) indicated below, however, are missing.

Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- Additional claim fees of $**100** as an undiscounted entity, including any required multiple dependent claim fee, are required. Applicant must submit the additional claim fees or cancel the additional claims for which fees are due.

SUMMARY OF FEES DUE:

The fee(s) required (including the fees noted above) are as follows. No entity status discount is in effect. If applicant is qualified for small entity status, a written assertion of small entity status must be submitted to establish small entity status. (See 37 CFR 1.27). If applicant is qualified for micro entity status, an acceptable Certification of Micro Entity Status must be submitted to establish micro entity status. (See 37 CFR 1.29 and forms PTO/SB/15A and 15B.)

- $**600** for 6 total claims over 20.
- $(**500**) previous unapplied payment amount.
- $**100** TOTAL FEE BALANCE DUE.

Replies must be received in the USPTO within the set time period or must include a proper Certificate of Mailing or Transmission under 37 CFR 1.8 with a mailing or transmission date within the set time period. For more information and a suggested format, see Form PTO/SB/92 and MPEP 512.

Replies should be addressed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

REPLY VIA ELECTRONIC FILING

A reply may be submitted via electronic filing only by registered users of the appropriate USPTO patent electronic filing system and must include:

- A separate document having the document description, "**Applicant response to Pre-Exam Formalities Notice**"; and
- the item(s) for which a reply period is set forth above.

For more information about electronic filing, contact the Patent Electronic Business Center (EBC) 1-866-217-9197 or visit https://www.uspto.gov/ebc

NOTE: If the reply is not being submitted electronically, a copy of this notice must be included.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/ldvan/

United States Patent and Trademark Office

Under Secretary of Commerce for Intellectual Property and
Director of the United States Patent and Trademark Office

WELCOME TO THE UNITED STATES PATENT AND TRADEMARK OFFICE (USPTO)

*Congratulations on taking the first step to protect your invention. You can now advertise or mark any products covered by this application for your invention as **"Patent Pending"** for as long as this application is pending!*

We are here to help you on the rest of your journey.

New to the process? The Patent Basics page will take you from "What is a patent?" to assistance with the application process.

- **www.uspto.gov/PatentBasics**

Consider cost savings. You might qualify for small entity or micro entity status, which means a discount on most USPTO patent fees.

- **www.uspto.gov/EntityStatus**

Become a registered electronic filer (eFiler). You'll gain access to the full capabilities of Patent Center. As a registered eFiler, you can electronically view your submission, track the progress of your application, and respond to USPTO correspondence.

- **www.uspto.gov/NewPatentFilers**

Learn how to identify which of your creative ideas might be intellectual property assets and how to protect them by using the USPTO Intellectual Property (IP) Identifier.

- **ipidentifier.uspto.gov**

We also provide Pro Se Assistance, support specifically geared for **independent inventors without an attorney or agent.** Follow the link below, call us at 866-767-3848, or email **proseassistancecenter@uspto.gov**.

- **www.uspto.gov/ProSePatents**

Need help near you? We have regional offices across the country, as well as Patent and Trademark Resource Centers in libraries in nearly every state, with specialists standing by to help you at no cost.

- **www.uspto.gov/locations**
- **www.uspto.gov/ptrc**

Contact us:

- **General information:** USPTO Contact Center
  - **www.uspto.gov/help**
- **Patent Center:**
  Patent Electronic Business Center
  - **www.uspto.gov/EBC**
- **Pre or post-examination:** Application Assistance Unit
  - **www.uspto.gov/PatentAssistance**

Want to learn more?

- **Access our free services** all in one spot. Find all of our contact centers, nationwide services, events, education, and training.
  - **www.uspto.gov/FreeServices**
- **Connect with us** on Instagram, LinkedIn, Twitter, Facebook, and YouTube.
- **Hear about resources for startups, inventors, and entrepreneurs,** as well as our initiatives engaging women, the military community, and others. These programs offer helpful tips and tricks on identifying and managing your IP, finding options for funding, and expanding your network to support your business.
  - **www.uspto.gov/startups**
  - **www.uspto.gov/inventors**
  - **www.uspto.gov/initiatives**
- We hope you connect with us by subscribing to receive important notifications by email.
  - **www.uspto.gov/subscribe**

Kathi Vidal

Kathi Vidal
Under Secretary of Commerce for Intellectual Property and
Director of the United States Patent and Trademark Office

Derrick Brent
Deputy Under Secretary of Commerce for Intellectual Property and
Deputy Director of the United States Patent and Trademark Office

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
18/892,283	09/20/2024	Jason Crabtree	15388FT

CONFIRMATION NO. 7526

FORMALITIES LETTER

OC000000078754241

82318
Brian Galvin
Galvin Patent Law LLC
2916 NW Bucklin Hill Road
Suite 485
Silverdale, WA 98383

Date Mailed: 10/02/2024

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

An application number and filing date have been accorded to the above-identified nonprovisional application. The item(s) indicated below, however, are missing.

Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- Additional claim fees of $**100** as an undiscounted entity, including any required multiple dependent claim fee, are required. Applicant must submit the additional claim fees or cancel the additional claims for which fees are due.

SUMMARY OF FEES DUE:

The fee(s) required (including the fees noted above) are as follows. No entity status discount is in effect. If applicant is qualified for small entity status, a written assertion of small entity status must be submitted to establish small entity status. (See 37 CFR 1.27). If applicant is qualified for micro entity status, an acceptable Certification of Micro Entity Status must be submitted to establish micro entity status. (See 37 CFR 1.29 and forms PTO/SB/15A and 15B.)

- $**600** for 6 total claims over 20.
- $(**500**) previous unapplied payment amount.
- $**100** TOTAL FEE BALANCE DUE.

Replies must be received in the USPTO within the set time period or must include a proper Certificate of Mailing or Transmission under 37 CFR 1.8 with a mailing or transmission date within the set time period. For more information and a suggested format, see Form PTO/SB/92 and MPEP 512.

Replies should be addressed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

REPLY VIA ELECTRONIC FILING

A reply may be submitted via electronic filing only by registered users of the appropriate USPTO patent electronic filing system and must include:

- A separate document having the document description, "**Applicant response to Pre-Exam Formalities Notice**"; and
- the item(s) for which a reply period is set forth above.

For more information about electronic filing, contact the Patent Electronic Business Center (EBC) 1-866-217-9197 or visit https://www.uspto.gov/ebc

NOTE: If the reply is not being submitted electronically, a copy of this notice must be included.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/ldvan/

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/892,283	**10/03/2024 05:36:35 PM Z ET**	**15388FT**

Title of Invention

CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	7526	FILED BY	Aura Morrey
PATENT CENTER #	67430666	FILING DATE	09/20/2024
CUSTOMER #	82318	FIRST NAMED INVENTOR	Jason Crabtree
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Brian Galvin

Documents

TOTAL DOCUMENTS: 1

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
241003_15388FT_Applicant Response to Pre-Exam Formalities Notice_AS_FILED.pdf	2	Applicant Response to Pre-Exam Formalities Notice	102 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
241003_15388FT_Applicant Response to Pre-Exam Formalities Notice_AS_FILED.pdf	7468636520F3E084090B2B53BB085C7289918CE450F94295F93952CD01D599701B8E606A32CD81E59251264096586489F18362727FDA27B7F2C134F9F4AA29E0

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 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

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/892,283	**10/03/2024 05:36:35 PM Z ET**	**15388FT**

Title of Invention

CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	7526	FILED BY	Aura Morrey
PATENT CENTER #	67430666	AUTHORIZED BY	Brian Galvin
CUSTOMER #	82318	FILING DATE	09/20/2024
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	Jason Crabtree

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 1009	**E202403H37047233**	**Aura Morrey**

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
1202	EACH CLAIM IN EXCESS OF 20	100.00	1	100.00
			TOTAL AMOUNT:	**$100.00**

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 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 NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
18/892,283	09/20/2024	2493	2420	15388FT	26	1

CONFIRMATION NO. 7526

UPDATED FILING RECEIPT

OC000000079260656

82318
Brian Galvin
Galvin Patent Law LLC
2916 NW Bucklin Hill Road
Suite 485
Silverdale, WA 98383

Date Mailed: 10/15/2024

Receipt is acknowledged of this non-provisional utility 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 FIRST INVENTOR, 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 corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction 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 provided that the request is grantable.

Inventor(s)

Jason Crabtree, Vienna, VA;
Andrew Sellers, Monument, CO;
Richard Kelley, Woodbridge, VA;

Applicant(s)

QOMPLX LLC, Reston, VA;

Power of Attorney: The patent practitioners associated with Customer Number 82318

Domestic Priority data as claimed by applicant

This application is a CON of 17/237,346 04/22/2021
which is a CIP of 16/777,270 01/30/2020 PAT 11,025,674
which is a CIP of 16/720,383 12/19/2019 PAT 10,944,795
which is a CON of 15/823,363 11/27/2017 PAT 10,560,483
which is a CIP of 15/725,274 10/04/2017 PAT 10,609,079
which is a CIP of 15/655,113 07/20/2017 PAT 10,735,456
which is a CIP of 15/616,427 06/07/2017 ABN
which is a CIP of 14/925,974 10/28/2015 ABN
and said 15/655,113 07/20/2017 is a CIP of 15/237,625 08/15/2016 PAT 10,248,910
which is a CIP of 15/206,195 07/08/2016 ABN
which is a CIP of 15/186,453 06/18/2016 ABN
which is a CIP of 15/166,158 05/26/2016 ABN
which is a CIP of 15/141,752 04/28/2016 PAT 10,860,962
which is a CIP of 15/091,563 04/05/2016 PAT 10,204,147

and is a CIP of 14/986,536 12/31/2015 PAT 10,210,255
and is a CIP of 14/925,974 10/28/2015 ABN

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 09/30/2024

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 18/892,283**

Projected Publication Date: 01/23/2025

Non-Publication Request: No

Early Publication Request: No

Title

CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION

Preliminary Class

726

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

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 (1-866-999-4258).

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 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 U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 18/892,283

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	320
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	700
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	800
TOTAL CLAIMS (37 CFR 1.16(i))	26 minus 20 =	* 6			OR	x 100 =	600
INDEPENDENT CLAIMS (37 CFR 1.16(h))	1 minus 3 =	*				x =	0
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
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	2420

APPLICATION AS AMENDED - PART II

		(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($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
AMENDMENT A	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
AMENDMENT A	Application Size Fee (37 CFR 1.16(s))									
AMENDMENT A	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)	OR	RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
AMENDMENT B	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
AMENDMENT B	Application Size Fee (37 CFR 1.16(s))									
AMENDMENT B	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 NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
18/892,283	09/20/2024	Jason Crabtree	15388FT	7526

82318 7590 10/30/2024
Brian Galvin
Galvin Patent Law LLC
2916 NW Bucklin Hill Road
Suite 485
Silverdale, WA 98383

EXAMINER
CENTRAL, DOCKET

ART UNIT	PAPER NUMBER
OPAP	

NOTIFICATION DATE	DELIVERY MODE
10/30/2024	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):

USPTO@GALVINPATENTLAW.COM
eofficeaction@appcoll.com

Decision Granting Request for Prioritized Examination (Track I)	**Application No.** 18/892,283	**Applicant(s)** Crabtree et al.	
	Examiner FIKIRTE A GEREMEW	**Art Unit** OMBL	**AIA (FITF) Status** Yes

1. THE REQUEST FILED 20 September 2024 IS **GRANTED** .

   The above-identified application has met the requirements for prioritized examination
   A. ☑ for an original nonprovisional application (Track I).
   B. ☐ for an application undergoing continued examination (RCE).

2. **The above-identified application will undergo prioritized examination**. The application will be accorded special status throughout its entire course of prosecution until one of the following occurs:

   A. filing a **petition for extension of time** to extend the time period for filing a reply;

   B. filing an **amendment to amend the application to contain more than four independent claims, more than thirty total claims** , or a multiple dependent claim;

   C. filing a **request for continued examination** ;

   D. filing a notice of appeal;

   E. filing a request for suspension of action;

   F. mailing of a notice of allowance;

   G. mailing of a final Office action;

   H. completion of examination as defined in 37 CFR 41.102; or

   I. abandonment of the application.

Telephone inquiries with regard to this decision should be directed to FIKIRTE GEREMEW at (703) 756-1930. In his/her absence, calls may be directed to Petition Help Desk at (571) 272-3282.

/FIKIRTE A GEREMEW/ PROGRAM SUPPORT SPECIALIST, OMBL	

U.S. Patent and Trademark Office
PTO-2298 (Rev. 02-2012)

Doc Code: P.AS.V
Document Description: Patents Assignment Verification request

PTO/SB/469 (08-24)

CERTIFICATION AND REQUEST TO PLACE THE PATENT ASSIGNMENT ABSTRACT OF TITLE INTO THE PATENT APPLICATION FILE		
Practitioner Docket No.: 15388FT	Application No.: 18/892,283	Filing Date: September 20, 2024
First Named Inventor: Jason Crabtree	Title: CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION	

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS THAT THE USPTO PLACE THE PATENT ASSIGNMENT ABSTRACT OF TITLE INTO THE ABOVE-IDENTIFIED PATENT APPLICATION FILE.

1. This form is being filed by a practitioner or the applicant for this application.

2. This form is being transmitted by electronic mail to RecordedAssignmentPlacement@uspto.gov.

3. This patent application is not open to the public.

4. Recognizing that Internet communications are not secure, I hereby authorize the USPTO to communicate with the undersigned and practitioners in accordance with 37 CFR 1.33 and 37 CFR 1.34 concerning any subject matter of this application by video conferencing, instant messaging, or electronic mail. I understand that a copy of these communications will be made of record in the application file.

5. The undersigned requests that the Patent Assignment Abstract of Title for this application be placed into the patent application file.

Signature	Date	Practitioner Registration No.
/BRIAN R. GALVIN/	November 1, 2024	50,966
Name (Print/Typed)	Telephone Number	
Brian R. Galvin	(360) 674-6233	

***Note**: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.*

☑ * Total of 1 forms are submitted.

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. The United States Patent and Trademark Office (USPTO) collects the information in this record under authority of 35 U.S.C. 2. The USPTO's system of records is used to manage all applicant and owner information including name, citizenship, residence, post office address, and other information with respect to inventors and their legal representatives pertaining to the applicant's/owner's activities in connection with the invention for which a patent is sought or has been granted. The applicable Privacy Act System of Records Notice for the information collected in this form is COMMERCE/PAT-TM-7 Patent Application Files, available in the Federal Register at 78 FR 19243 (March 29, 2013), https://www.govinfo.gov/content/pkg/FR-2013-03-29/pdf/2013-07341.pdf.

Routine uses of the information in this record may include disclosure to: 1) law enforcement, in the event that the system of records indicates a violation or potential violation of law; 2) a federal, state, local, or international agency, in response to its request; 3) a contractor of the USPTO having need for the information in order to perform a contract; 4) the Department of Justice for determination of whether the Freedom of Information Act (FOIA) requires disclosure of the record; 5) a Member of Congress submitting a request involving an individual to whom the record pertains, when the individual has requested the Member's assistance with respect to the subject matter of the record; 6) a court, magistrate, or administrative tribunal, in the course of presenting evidence, including disclosures to opposing counsel in the course of settlement negotiations; 7) the Administrator, General Services Administration (GSA), or their designee, during an inspection of records conducted by GSA under authority of 44 U.S.C. 2904 and 2906, in accordance with the GSA regulations and any other relevant (i.e., GSA or Commerce) directive, where such disclosure shall not be used to make determinations about individuals; 8) 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)); 9) the Office of Personnel Management (OPM) for personnel research purposes; and 10) the Office of Management and Budget (OMB) for legislative coordination and clearance.

If you do not furnish the information requested on this form, the USPTO may not be able to process and/or examine your submission, which may result in termination of proceedings, abandonment of the application, and/or expiration of the patent.

Patent Assignment Abstract of Title

Total Assignments: 3

Application #: 18692283 **Filing Dt:** 09/20/2024 **Patent #:** NONE **Issue Dt:**
PCT #: NONE **Intl Reg #:** **Publication #:** NONE **Pub Dt:**
Inventors: Jason Crabtree, Andrew Sellers, Richard Kelley
Title: CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION

Assignment: 1

Reel/Frame: 068680 / 0657 **Received:** 09/24/2024 **Recorded:** 09/24/2024 **Mailed:** 09/25/2024 **Pages:** 6
Conveyance: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).
Assignors: CRABTREE, JASON **Exec Dt:** 04/21/2021
SELLERS, ANDREW **Exec Dt:** 04/21/2021
KELLEY, RICHARD **Exec Dt:** 04/21/2021
Assignee: QOMPLX, INC.
1775 TYSONS BLVD.
SUITE 800
TYSONS, VIRGINIA 22102
Correspondent: BRIAN GALVIN
2916 NW BUCKLIN HILL RD
SUITE 485
SILVERDALE, WA 98383

Assignment: 2

Reel/Frame: 069053 / 0339 **Received:** 09/26/2024 **Recorded:** 09/26/2024 **Mailed:** 10/30/2024 **Pages:** 28
Conveyance: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).
Assignor: QOMPLX, INC. **Exec Dt:** 08/10/2023
Assignee: QPX LLC
111 8TH AVE
NEW YORK, NEW YORK 10011
Correspondent: BRIAN GALVIN
2916 NW BUCKLIN HILL RD
SUITE 485
SILVERDALE, WA 98383

Assignment: 3

Reel/Frame: 069070 / 0283 **Received:** 09/28/2024 **Recorded:** 09/28/2024 **Mailed:** 10/31/2024 **Pages:** 7
Conveyance: CHANGE OF NAME (SEE DOCUMENT FOR DETAILS).
Assignor: QPX LLC **Exec Dt:** 08/24/2023
Assignee: QOMPLX LLC
1900 RESTON METRO PLAZA
SUITE 600
RESTON, VIRGINIA 20190
Correspondent: BRIAN GALVINI
2916 NW BUCKLIN HILL RD
SUITE 485
SILVERDALE, WA 98383

Search Results as of: 11/07/2024 09:00 AM

If you have any comments or questions concerning the data displayed, contact PRD / Assignments at 571-272-3350. v.2.6
Web interface last modified: Jun 26, 2017 v.2.6

Notice of References Cited	Application/Control No. 18/892,283	Applicant(s)/Patent Under Reexamination Crabtree et al.	
	Examiner CHENG-FENG HUANG	Art Unit 2497	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date YYYY-MM-DD	Name	CPC Classification	US Classification
*	A	US-9183387-B1	2015-11-10	Altman; Alon	H04L63/1425	1/1
*	B	US-20150020199-A1	2015-01-15	Neil; Joshua Charles	H04L63/1408	726/23
*	C	US-20100037293-A1	2010-02-11	StJohns; Michael	H04L9/3263	726/2
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date YYYY-MM-DD	Country	Name	CPC 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 YYYY-MM-DD format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	18/892,283	Crabtree et al.
	Examiner	**Art Unit**
	CHENG-FENG HUANG	2497

CPC - Searched*		
Symbol	**Date**	**Examiner**
H04L63/20 or G06F16/2477 or G06F16/951 or H04L63/1425 or H04L63/1441	11/06/2024	C. H.

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	**Date**	**Examiner**
PE2E Searches (including inventor and assignee search)	11/06/2024	C. H.
PE2E classification search (keywords combined with CPC)	11/06/2024	C. H.

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**
	General interference and searches of claim (PGPUB,USPAT)	11/06/2024	C. H.

/CHENG-FENG HUANG/ Primary Examiner, Art Unit 2497	

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	18/892,283	Crabtree et al.
	Examiner	**Art Unit**
	CHENG-FENG HUANG	2497

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

CLAIMS

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

CLAIM		DATE								
Final	Original	11/06/2024								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								
	23	✓								
	24	✓								
	25	✓								
	26	✓								

Bibliographic Data

Application No: 18/892,283

Foreign Priority claimed: ○ Yes ◉ No

35 USC 119 (a-d) conditions met: ☐ Yes ☑ No ☐ Met After Allowance

Verified and Acknowledged: /CHENG-FENG HUANG/ [ ]

Examiner's Signature | Initials

Title: CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
09/20/2024	726	2497	15388FT
RULE			

APPLICANTS

QOMPLX LLC, Reston, VA, UNITED STATES

INVENTORS

Jason Crabtree, Vienna, VA, UNITED STATES

Andrew Sellers, Monument, CO, UNITED STATES

Richard Kelley, Woodbridge, VA, UNITED STATES

CONTINUING DATA

This application is a CON of 17237346 04/22/2021

17237346 is a CIP of 16777270 01/30/2020 PAT 11025674

16777270 is a CIP of 16720383 12/19/2019 PAT 10944795

16720383 is a CON of 15823363 11/27/2017 PAT 10560483

15823363 is a CIP of 15725274 10/04/2017 PAT 10609079

15725274 is a CIP of 15655113 07/20/2017 PAT 10735456

15655113 is a CIP of 15616427 06/07/2017ABN

15655113 is a CIP of 15237625 08/15/2016 PAT 10248910

15237625 is a CIP of 15206195 07/08/2016ABN

15206195 is a CIP of 15186453 06/18/2016ABN

15186453 is a CIP of 15166158 05/26/2016ABN

15166158 is a CIP of 15141752 04/28/2016 PAT 10860962

15141752 is a CIP of 15091563 04/05/2016 PAT 10204147

15141752 is a CIP of 14986536 12/31/2015 PAT 10210255

15141752 is a CIP of 14925974 10/28/2015ABN

15616427 is a CIP of 14925974 10/28/2015ABN

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

09/30/2024

STATE OR COUNTRY

UNITED STATES

ADDRESS

Brian Galvin
Galvin Patent Law LLC
2916 NW Bucklin Hill Road
Suite 485
Silverdale, WA 98383
UNITED STATES

FILING FEE RECEIVED

$6,160

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1	12	"18892283"	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/05 06:46 PM
L2	2	"17237346"	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/06 10:15 AM
L3	76	((("QOMPLX") near3 ("LLC"))).AS,AANM.	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/06 10:21 AM
L4	658	((("CRABTREE") near3 ("Jason")) OR (("SELLERS") near3 ("Andrew")) OR (("KELLEY") near3 ("Richard"))).INV.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2024/11/06 10:21 AM
L5	1355	3 4	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO,	OR	ON	ON	2024/11/06 10:21 AM

			RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L6	405	5 AND (directed near2 graph)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; IBM_TDB)	OR	ON	ON	2024/11/06 10:22 AM
L7	103	5 AND (directed near2 graph).clm.	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; IBM_TDB)	OR	ON	ON	2024/11/06 10:22 AM
L8	250	("10204147"|"10210255"|"10572828"|"10860951"|"10860962"|"10884999"|"11023284"|"11055451"|"20050005272"|"20170109678"|"20170322959"|"20180103088"|"20180300930"|"20190082305"|"20220012093"|"10061635"|"10242406"|"10248910"|"10367829"|"20030041254"|"20030145225"|"20070150744"|"20090089227"|"20090182672"|"20090222562"|"20090293128"|"20110087888"|"20120266244"|"20130073062"|"20130132149"|"20130191416"|"20130304623"|"20140156806"|"20140244612"|"20140279762"|"20150149979"|"20150163242"|"20150169294"|"20150195192"|"20150236935"|"20150281225"|"20150317481"|"20150339263"|"20150347414"|"20150379424"|"20160028758"|"20160072845"|"20160078361"|"20160105454"|"20160140519"|"20160275123"|"20160285732"|"20160350442"|"20160364307"|"20170019678"|"20170063896"|"20170126712"|"20170139763"|"20170149802"|"20170193110"|"20170322959"|"20170323089"|"20180197128"|"20180300930"|"20190082305"|"5669000"|"6256544"|"6477572"|"8281121"|"8615800"|"8793758"|"8914878"|"923	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/06 10:28 AM

		1962"|"9602530"|"9654495"|"9686308"|"9762443"|"9887933").PN.					
L9	10	8 AND (directed near2 graph).clm.	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; IBM_TDB)	OR	ON	ON	2024/11/06 10:30 AM
L10	1	9 AND @ad<"20151028"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; IBM_TDB)	OR	ON	ON	2024/11/06 10:30 AM
L11	13	"20110066590"	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/06 10:31 AM
L12	1	"20110066590"	(US-PGPUB)	OR	ON	ON	2024/11/06 10:32 AM
L13	50	("10204147"|"10210255"|"10572828"|"10860951"|"10860962"|"10884999"|"11023284"|"11055451"|"20050005272"|"20170109678"|"20170322959"|"20180103088"|"20180300930"|"20190082305"|"20220012093"|"10061635"|"10242406"|"10248910"|"10367829"|"20030041254"|"20030145225"|"20070150744"|"20090089227"|"20090182672"|"20090222562"|"20090293128"|"20110087888"|"20120266244"|"20130073062"|"20130132149"|"20130191416"|"20130304623"|"20140156806"|"20140244612"|"20140279762"|"20150149979"|"20150163242"|"20150169294"|"20150195192"|"20150236935"|"20150281225"|"20150317481"|"20150339263"|"20150347414"|"20150379424"|"20	(US-PGPUB)	OR	ON	ON	2024/11/06 10:37 AM

		160028758"|"20160072845"|"20160078361"|"20160105454"|"20160140519"|"20160275123"|"20160285732"|"20160350442"|"20160364307"|"20170019678"|"20170063896"|"20170126712"|"20170139763"|"20170149802"|"20170193110"|"20170322959"|"20170323089"|"20180197128"|"20180300930"|"20190082305"|"5669000"|"6256544"|"6477572"|"8281121"|"8615800"|"8793758"|"8914878"|"9231962"|"9602530"|"9654495"|"9686308"|"9762443"|"9887933").PN.					
L14	323751	(H04L63/20 or G06F16/2477 or G06F16/951 or H04L63/1425 or H04L63/1441).cpc.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/06 10:39 AM
L15	503	14 AND (directed near2 graph).clm.	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; IBM_TDB)	OR	ON	ON	2024/11/06 10:39 AM
L16	197	15 AND (anomalous malicious malevolent) AND stream$3 AND (node edge)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/06 10:46 AM
L17	17	16 AND	(US-PGPUB; USPAT;	OR	ON	ON	2024/11/06

		@ad<"20151028"	USOCR; FPRS; EPO; JPO; IBM_TDB)				10:46 AM
L18	13	17 AND (graph WITH (node edge)) AND graph AND memory	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; IBM_TDB)	OR	ON	ON	2024/11/06 03:22 PM
L19	10	"20150020199" AND memory WITH graph	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/06 03:31 PM
L20	10	"20150020199" AND memory WITH graph AND graph	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/06 03:37 PM
L21	6	17 AND ((add$3 subtract$3 modif$7) WITH (node edge)) AND graph	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; IBM_TDB)	OR	ON	ON	2024/11/07 07:59 AM
L22	1	1 AND (sensitive resource)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT;	OR	ON	ON	2024/11/07 09:17 AM

			IBM_TDB)				
L23	19	"20150020199" AND node	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/07 09:50 AM
L24	4	14 AND (bogus near2 node)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; IBM_TDB)	OR	ON	ON	2024/11/07 09:56 AM
L25	0	(travers$3 near3 graph WITH identif$7 near3 origin near3 (anomalous ADJ event))	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; IBM_TDB)	OR	ON	ON	2024/11/07 02:39 PM

PE2E SEARCH - Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
N1	0	(travers$3 near3 graph WITH identif$7 near3 origin near3 (anomalous ADJ event)).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/07 02:39 PM

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

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. 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	18/892,283
Filing Date	2024-09-20
First Named Inventor	Jason Crabtree
Art Unit	2497
Examiner Name	Cheng-Feng Huang
Attorney Docket Number	15388FT

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	6477572	B1	2002-11-05	Elderton et al.	Entire Document
	2	6906709	B1	2005-06-14	Larkin et al.	Entire Document
	3	7139747	B1	2006-11-21	Najork	Entire Document
	4	7227948	B2	2007-06-05	Ohkuma et al.	Entire Document
	5	7310632	B2	2007-12-18	Meek et al.	Entire Document
	6	7409721	B2	2008-08-05	Hernacki et al.	Entire Document
	7	7530105	B2	2009-05-05	Gilbert et al.	Entire Document
	8	7546333	B2	2009-06-09	Alon et al.	Entire Document

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18/892,283
	Filing Date	2024-09-20
	First Named Inventor	Jason Crabtree
	Art Unit	2497
	Examiner Name	Cheng-Feng Huang
	Attorney Docket Number	15388FT

	9	7685296	B2	2010-03-23	Brill et al.	Entire Document
	10	7818224	B2	2010-10-19	Boerner	Entire Document
	11	7818417	B2	2010-10-19	Ginis et al.	Entire Document
	12	7925561	B2	2011-04-12	Xu	Entire Document
	13	7971252	B2	2011-06-28	Lippmann et al.	Entire Document
	14	8069190	B2	2011-11-29	McColl et al.	Entire Document
	15	8281121	B2	2012-10-02	Nath et al.	Entire Document
	16	8346753	B2	2013-01-01	Hayes	Entire Document
	17	8457996	B2	2013-06-04	Winkler et al.	Entire Document
	18	8464346	B2	2013-06-11	Barai et al.	Entire Document
	19	8516596	B2	2013-08-20	Sandoval et al.	Entire Document

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18/892,283
	Filing Date	2024-09-20
	First Named Inventor	Jason Crabtree
	Art Unit	2497
	Examiner Name	Cheng-Feng Huang
	Attorney Docket Number	15388FT

	20	8751867	B2	2014-06-10	Marvasti et al.	Entire Document
	21	8752178	B2	2014-06-10	Coates et al.	Entire Document
	22	8782080	B2	2014-07-15	Lee et al.	Entire Document
	23	8881288	B1	2014-11-04	Levy et al.	Entire Document
	24	8914878	B2	2014-12-16	Burns et al.	Entire Document
	25	9100430	B1	2015-08-04	Seiver et al.	Entire Document
	26	9110706	B2	2015-08-18	Yu et al.	Entire Document
	27	9152727	B1	2015-10-06	Balducci et al.	Entire Document
	28	9231962	B1	2016-01-05	Yen et al.	Entire Document
	29	9235732	B2	2016-01-12	Eynon et al.	Entire Document
	30	9325732	B1	2016-04-26	Stickle et al.	Entire Document

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18/892,283
	Filing Date	2024-09-20
	First Named Inventor	Jason Crabtree
	Art Unit	2497
	Examiner Name	Cheng-Feng Huang
	Attorney Docket Number	15388FT

	31	9344444	B2	2016-05-17	Lippmann et al.	Entire Document
	32	9400962	B2	2016-07-26	Prasad	Entire Document
	33	9466041	B2	2016-10-11	Simitsis et al.	Entire Document
	34	9507944	B2	2016-11-29	Lotem et al.	Entire Document
	35	9602530	B2	2017-03-21	Ellis et al.	Entire Document
	36	9628501	B2	2017-04-18	Datta Ray et al.	Entire Document
	37	9652538	B2	2017-05-16	Shivaswamy et al.	Entire Document
	38	9654495	B2	2017-05-16	Hubbard et al.	Entire Document
	39	9679125	B2	2017-06-13	Bailor et al.	Entire Document
	40	9686308	B1	2017-06-20	Srivastava	Entire Document
	41	9699205	B2	2017-07-04	Muddu et al.	Entire Document

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18/892,283
	Filing Date	2024-09-20
	First Named Inventor	Jason Crabtree
	Art Unit	2497
	Examiner Name	Cheng-Feng Huang
	Attorney Docket Number	15388FT

	42	9712553	B2	2017-07-18	Nguyen et al.	Entire Document
	43	9736173	B2	2017-08-15	Li et al.	Entire Document
	44	9762443	B2	2017-09-12	Dickey	Entire Document
	45	9774522	B2	2017-09-26	Vasseur et al.	Entire Document
	46	9911088	B2	2018-03-06	Nath et al.	Entire Document
	47	9954884	B2	2018-04-24	Hassell et al.	Entire Document
	48	9967265	B1	2018-05-08	Peer et al.	Entire Document
	49	10021116	B2	2018-07-10	Bassett	Entire Document
	50	10044726	B2	2018-08-07	Dulkin et al.	Entire Document
	51	10083236	B2	2018-09-25	Crosby	Entire Document
	52	10191768	B2	2019-01-29	Bishop et al.	Entire Document

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18/892,283
	Filing Date	2024-09-20
	First Named Inventor	Jason Crabtree
	Art Unit	2497
	Examiner Name	Cheng-Feng Huang
	Attorney Docket Number	15388FT

	53	10210246	B2	2019-02-19	Stojanovic et al.	Entire Document
	54	10210470	B2	2019-02-19	Datta Ray	Entire Document
	55	10212176	B2	2019-02-19	Wang	Entire Document
	56	10216485	B2	2019-02-26	Misra et al.	Entire Document
	57	10643144	B2	2020-05-05	Bowers et al.	Entire Document
	58	10846391	B1	2020-11-24	Bonney et al.	Entire Document
	59	11392875	B2	2022-07-19	Carstens et al.	Entire Document
	60	11836664	B2	2023-12-05	Ackerman et al.	Entire Document

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	20050165822	A1	2005-07-28	Yeung, Simon D. et al.	Entire Document

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18/892,283
	Filing Date	2024-09-20
	First Named Inventor	Jason Crabtree
	Art Unit	2497
	Examiner Name	Cheng-Feng Huang
	Attorney Docket Number	15388FT

	2	20100299651	A1	2010-11-25	FAINEKOS et al.	Entire Document
	3	20110307467	A1	2011-12-15	Severance	Entire Document
	4	20120215575	A1	2012-08-23	Deb et al.	Entire Document
	5	20140244612	A1	2014-08-28	Bhasin et al.	Entire Document
	6	20140324521	A1	2014-10-30	Mun	Entire Document
	7	20150347414	A1	2015-12-03	Xiao et al.	Entire Document
	8	20160006629	A1	2016-01-07	Ianakiev et al.	Entire Document
	9	20160012235	A1	2016-01-14	Lee et al.	Entire Document
	10	20160057159	A1	2016-02-25	Yin et al.	Entire Document
	11	20170090893	A1	2017-03-30	Aditya et al.	Entire Document
	12	20180082304	A1	2018-03-22	Summerlin et al.	Entire Document

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18/892,283
Filing Date	2024-09-20
First Named Inventor	Jason Crabtree
Art Unit	2497
Examiner Name	Cheng-Feng Huang
Attorney Docket Number	15388FT

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] ¡	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]
	1	EBERLE, WILLIAM, HOLDER, LAWRENCE; Incremental Anomaly Detection in Graphs, 2013 IEEE 13th International Conference on Data Mining Workshops	☐
	2	HUANG, ALEX, A Comparison of Value at Risk Approaches and a New Method with Extreme Value Theory and Kernel Estimator	☐
	3	MAROZZO, Fabrizio; TALIA, Domenico; TRUNFIO, Paolo; P2P-MapReduce - Parallel Data Processing in Dynamic Cloud Environments, Journal of Computer and System Sciences, 78 (2012) 1382–1402	☐
	4	SIMONIAN, Joseph, DAVIS, Josh., Robust Value-At-Risk: An Information Theoretic Approach, Applied Economic Letters, 2010, 17, 1551-1553.	☐

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

EXAMINER SIGNATURE

Examiner Signature	/CHENG-FENG HUANG/	Date Considered	11/06/2024

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.H/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18/892,283
	Filing Date	2024-09-20
	First Named Inventor	Jason Crabtree
	Art Unit	2497
	Examiner Name	Cheng-Feng Huang
	Attorney Docket Number	15388FT

[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. /C.H/

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.
18/892,283	09/20/2024	Jason Crabtree	15388FT	7526

82318 7590 11/13/2024
Brian Galvin
Galvin Patent Law LLC
2916 NW Bucklin Hill Road
Suite 485
Silverdale, WA 98383

EXAMINER
HUANG, CHENG-FENG

ART UNIT	PAPER NUMBER
2497	

NOTIFICATION DATE	DELIVERY MODE
11/13/2024	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):

USPTO@GALVINPATENTLAW.COM
eofficeaction@appcoll.com

Office Action Summary	Application No. 18/892,283	Applicant(s) Crabtree et al.	
	Examiner CHENG-FENG HUANG	Art Unit 2497	AIA (FITF) Status Yes

-- 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 09/20/2024.

☐ 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) 1-26 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) 1-26 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 09/20/2024 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 _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

Notice of Pre-AIA or AIA Status

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

DETAILED ACTION

2. This is a reply to the application filed on 09/20/2024, in which, claim(s) 1-26 are pending. Claim(s) 1 is independent.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on 09/20/2024, has been reviewed. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statement.

Drawings

4. The drawings filed on 09/20/2024 are accepted by The Examiner.

Claim Objections

5. Claim 1 is objected to because of the following informalities:

- Claim 1 (Line 11) recites "***substantially*** *in real time*". It is not clear to what degree can be considered as substantially.
- Claim 1 (Line 20) recites "***if*** *the event is anomalous*". The limitation is confusing with the term "if".

Appropriate correction is required.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 1-26 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 1 recites "A computer system" in the preamble and "a memory", in the claim body. As recited in the body of the claim, the claimed system lacks a structural component because the memory can be implemented as software only. Therefore, **claim 1 is directed to non-statutory subject matter for lack of a hardware component**. The Examiner respectfully suggests that the claim be further amended to positively recite at least one hardware element within the body of the claim to make the claim statutory subject matter under 35 U.S.C. 101 such as "a hardware memory" or any variants supported by the specification.

8. Dependent claims 2-26 don't cure the deficiency of claim 1 and are rejected under 35 U.S.C. 101 for their dependency upon claim 1.

Double Patenting

9. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the claims at issue are not identical, but at least

one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the reference application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO internet Web site contains terminal disclaimer forms which may be used. Please visit http://www.uspto.gov/forms/. The filing date of the application will determine what form should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to http://www.uspto.gov/patents/process/file/efs/guidance/eTD-info-I.jsp.

10. Claims 1-26 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over:

Claims 1-8 of copending Application 17/237,346.

This is a provisional nonstatutory double patenting rejection because the patentably indistinct claims have not in fact been patented.

Copending Application No. (17/237,346)	Instant Application No. (18/892,283)
Claim 1. A system for correlating network event anomalies to identify attack information, comprising: a cyber-physical graph module comprising a first plurality of programming instructions stored in a memory of, and operating on a processor of, a computing device, wherein the first plurality of programming instructions, when operating on the processor, cause the computing device to create a cyber-physical graph of the organization using the information, the cyber-physical graph comprising nodes representing entities associated with the organization and edges representing relationships between entities associated with the organization; a reconnaissance engine comprising a second plurality of programming instructions stored in the memory of, and operating on the processor of, the computing device, wherein the second plurality of programming instructions, when operating on the processor, cause the computing device to: perform a reconnaissance search using the cyber-physical graph; and apply some or all of the results of the reconnaissance search to the cyber-physical graph to create a normal behavior model for a plurality of nodes in the cyber-physical graph; and a directed computational graph engine comprising a third plurality of	Claim 1. A computer system comprising a memory, wherein the computer system is configured to execute software instructions stored on nontransitory machine-readable storage media that: store in the memory a representation of a first graph, wherein the representation of the first graph comprises representations of a first plurality of nodes and a first plurality of edges, wherein the first graph is a directed graph, wherein each node of the first plurality of nodes corresponds to a respective entity of a plurality of entities, and wherein the first plurality of edges includes at least one edge corresponding to a physical connection between entities and at least one edge corresponding to a logical connection between entities; process, substantially in real time, streaming data received from a plurality of devices, wherein the streaming data comprises information about events relating to the plurality of entities; process the representation of the first graph to add, subtract, or modify a node of the first graph based on the streaming

programming instructions stored in the memory of, and operating on the processor of, the computing device, wherein the third plurality of programming instructions, when operating on the processor, cause the computing device to: receive the cybersecurity profile and the normal behavior model; using the cyber-physical graph and the normal behavior model: identify an anomalous event based on analysis of cyber-physical graph and the normal behavior model; analyze the cyber-physical graph and the normal behavior model to identify correlations between affected nodes, the affected nodes being based on the anomalous event; generate a behavior graph based on the identified correlations; analyze the behavior graph to produce a dependency tree comprising causative relationships between events; and traverse the behavior tree backward in a temporal dimension to identify a plurality of starting conditions for the anomalous event.	data, process the representation of the first graph to add, subtract, or modify an edge of the first graph based on the streaming data, use the representation of the first graph to determine whether an event, of the events relating to the plurality of entities, is anomalous, and, if the event is anomalous, identify the event as a first anomalous event.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

> A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102 of this title, if the differences

between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

12. Claims 1-2, 10-12, 14-15 and 17-19 are rejected under 35 U.S.C. 103 as being unpatentable over Neil et al. (US 2015/0020199 A1) in view of Altman et al. (US 9,183,387 B1).

13. Regarding Claim 1, Neil discloses

A computer system comprising a memory, wherein the computer system is configured to execute software instructions stored on nontransitory machine-readable storage media ([0012], "a system includes memory storing computer program instructions configured to detect anomalous behavior in a network and a plurality of processing cores configured to execute the stored computer program instructions", [0036], "Non-transitory computer-readable media") ***that***:

store in the memory a representation of a first graph ([0010], "The computer-implemented method also includes enumerating a plurality of paths in the network as part of a graph representing the network"),

wherein the representation of the first graph comprises representations of a first plurality of nodes and a first plurality of edges, wherein the first graph is a directed graph, wherein each node of the first plurality of nodes corresponds to a

respective entity of a plurality of entities, and wherein the first plurality of edges includes at least one edge corresponding to a physical connection between entities and at least one edge corresponding to a logical connection between entities ([0010], “where each computing system in the network may be a node in the graph and the sequence of connections between two computing systems may be a directed edge in the graph”, [0026], “In the graph, a "node" represents a computing system and an "edge" represents a sequence of connections between two computing systems”);

process, substantially in real time, streaming data received from a plurality of devices ([0060], “to handle larger graphs than the already sizable graphs that are currently being analyzed, all while keeping up with real-time data stream”),

wherein the streaming data comprises information about events relating to the plurality of entities ([0109-0110], “UDP streams may be encrypted so that network data is protected”, “While UDP may be used, some embodiments also have the ability to detect packet loss using sequence numbering of packets. The Media Access Control ("MAC") address plus a sequence number may be used to track packets on a per-machine basis”);

use the representation of the first graph to determine whether an event, of the events relating to the plurality of entities, is anomalous, and, if the event is anomalous, identify the event as a first anomalous event ([0102], “detecting anomalous activity using data defined over time on edges of an underlying graph structure”, [0110], “to track packets on a per-machine basis. This information can also be used independently of anomaly detection”).

Neil does not explicitly teach but Altman teaches

process the representation of the first graph to add, subtract, or modify a node of the first graph based on the streaming data (Col 8 Lines 11-14, "Propagation analysis of node 7 yields one new node, node 9, and one new edge pointing from node 7 to node 9"),

process the representation of the first graph to add, subtract, or modify an edge of the first graph based on the streaming data (Col 8 Lines 11-14, "Propagation analysis of node 7 yields one new node, node 9, and one new edge pointing from node 7 to node 9", "a directed edge from node 10 to node 7 may be added"),

Neil and Altman are analogous art as they are in the same field of endeavor of information security. It would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to combine the teachings of Altman with the disclosure of Neil. The motivation/suggestion would have been to detecting online attacks (Altman).

14. Regarding Claim 2, the combined teaching of Neil and Altman teaches

identify a first plurality of possible event flows, wherein the first plurality of possible event flows comprises a possible event flow relating to an entity of the plurality of entities, wherein the entity relates to the first anomalous event (Neil, [0107], "the data was collected from secondary server sources, instead of getting the data directly from the host. Some embodiments take this observed information into account to generate new events. Some embodiments also provide efficient aggregation

of the data. The server may have one-way communication with the hosts where it receives messages from a large number of host agents");

identify a first plurality of dependencies, wherein each dependency of the first plurality of dependencies is associated with a respective possible event flow of the first plurality of possible event flows; and, a second plurality of nodes of the first graph, wherein each node of the second plurality of nodes corresponds to a respective entity relating to a respective possible event flow of the first plurality of possible event flows (Neil, [0107], "the data was collected from secondary server sources, instead of getting the data directly from the host. Some embodiments take this observed information into account to generate new events. Some embodiments also provide efficient aggregation of the data. The server may have one-way communication with the hosts where it receives messages from a large number of host agents", [0113], "Collection capabilities of the agent may include process stop and start information with checksums of starting process images, network connection event logs, mapping of running processes to established network connections, and current network connection state").

15. Regarding Claim 10, the combined teaching of Neil and Altman teaches

determining that the event relates to a first entity of the plurality of entities, determining at least one behavior pattern associated with the first entity, and comparing the event to the at least one behavior pattern (Neil, [0028-0029], "To identify local anomalies, a scan statistic may be used for data extracted from the edges of a graph over time. Two shapes may be especially beneficial for capturing locality in a

graph: a star and the above-mentioned k-path. The use of the path as a scan window is novel. Both of these shapes are motivated by hacker behaviors observed in real network attacks", "To identify local anomalies, these shapes may be enumerated over the entire graph using a set of sliding time windows. Local statistics in each window may be compared with historic behavior to capture anomalies").

16. Regarding Claim 11, the combined teaching of Neil and Altman teaches

wherein comparing the event to the at least one behavior pattern comprises using a threshold (Neil, [0026], "Deviations by a certain threshold, which may be regulated according to a user-defined alarm rate, from historical parameters may indicate an anomalous path").

17. Regarding Claim 12, the combined teaching of Neil and Altman teaches

identify a first plurality of possible event flows, wherein the first plurality of possible event flows comprises a possible event flow relating to a second entity of the plurality of entities, wherein the second entity relates to the first anomalous event (Neil, [0107], "the data was collected from secondary server sources, instead of getting the data directly from the host. Some embodiments take this observed information into account to generate new events. Some embodiments also provide efficient aggregation of the data. The server may have one-way communication with the hosts where it receives messages from a large number of host agents");

identify a first plurality of dependencies, wherein each dependency of the first plurality of dependencies is associated with a respective possible event flow

of the first plurality of possible event flows (Neil, [0107], "the data was collected from secondary server sources, instead of getting the data directly from the host. Some embodiments take this observed information into account to generate new events. Some embodiments also provide efficient aggregation of the data. The server may have one-way communication with the hosts where it receives messages from a large number of host agents"); ***and***,

identify a second plurality of nodes of the first graph, wherein each node of the second plurality of nodes corresponds to a respective entity relating to a respective possible event flow of the first plurality of possible event flows (Neil, [0107], "the data was collected from secondary server sources, instead of getting the data directly from the host. Some embodiments take this observed information into account to generate new events. Some embodiments also provide efficient aggregation of the data. The server may have one-way communication with the hosts where it receives messages from a large number of host agents", [0113], "Collection capabilities of the agent may include process stop and start information with checksums of starting process images, network connection event logs, mapping of running processes to established network connections, and current network connection state").

18. Regarding Claim 14, the combined teaching of Neil and Altman teaches

determining that the first entity is associated with a resource, wherein the resource is a sensitive resource (Neil, [0006], "threat to companies, <u>governmental organizations</u>, and other entities").

19. Regarding Claim 15, the combined teaching of Neil and Altman teaches

identify a first plurality of possible event flows, wherein the first plurality of possible event flows comprises a possible event flow relating to a second entity of the plurality of entities, wherein the second entity relates to the first anomalous event (Neil, [0107], "the data was collected from secondary server sources, instead of getting the data directly from the host. Some embodiments take this observed information into account to generate new events. Some embodiments also provide efficient aggregation of the data. The server may have one-way communication with the hosts where it receives messages from a large number of host agents");

identify a first plurality of dependencies, wherein each dependency of the first plurality of dependencies is associated with a respective possible event flow of the first plurality of possible event flows (Neil, [0107], "the data was collected from secondary server sources, instead of getting the data directly from the host. Some embodiments take this observed information into account to generate new events. Some embodiments also provide efficient aggregation of the data. The server may have one-way communication with the hosts where it receives messages from a large number of host agents"); ***and***,

identify a second plurality of nodes of the first graph, wherein each node of the second plurality of nodes corresponds to a respective entity relating to a respective possible event flow of the first plurality of possible event flows (Neil, [0107], "the data was collected from secondary server sources, instead of getting the data directly from the host. Some embodiments take this observed information into account to generate new events. Some embodiments also provide efficient aggregation

of the data. The server may have one-way communication with the hosts where it receives messages from a large number of host agents", [0113], "Collection capabilities of the agent may include process stop and start information with checksums of starting process images, network connection event logs, mapping of running processes to established network connections, and current network connection state").

20. Regarding Claim 17, the combined teaching of Neil and Altman teaches ***wherein the computer system comprises a plurality of physical computing machines*** (Neil, [0041], "one or more physical or logical blocks of computer").

21. Regarding Claim 18, the combined teaching of Neil and Altman teaches ***wherein the computer system comprises a plurality of virtual computing machines*** (Neil, [0041], "one or more physical or logical blocks of computer").

22. Regarding Claim 19, the combined teaching of Neil and Altman teaches ***wherein at least one entity of the first plurality of entities is at least one of a user, a place, a device, a resource, a group, or a service*** (Neil, [0041], "a "system" could be embodied as a personal computer, a server, a console, a personal digital assistant ("PDA"), a cell phone, or any other suitable computing device, or combination of devices").

23. Claim 26 is rejected under 35 U.S.C. 103 as being unpatentable over Neil et al. (US 2015/0020199 A1) in view of Altman et al. (US 9,183,387 B1) further in view of

StJohns et al. (US 2010/0037293 A1).

24. Regarding Claim 26, the combined teaching of Neil and Altman does not explicitly teach but StJohns teaches

wherein the representation of the first graph comprises a representation of at least one node that does not correspond to an entity (Neil, [0017], "the other node is identified as bogus").

Neil, Altman and StJohns are analogous art as they are in the same field of endeavor of information security. It would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to combine the teachings of StJohns with the combined teaching of Neil and Altman. The motivation/suggestion would have been for security in a wireless utility network (StJohns, Abstract).

Allowable Subject Matter

25. Claims 3-9, 13, 16 and 20-25 are objected to as being dependent upon rejected base claim 1, but would be allowable if rewritten in independent form **including all of the limitations of the base claim and any intervening claims** since the prior arts taken individually or in combination fails to particular discloses, fairly suggest or render obvious the limitations of the claims.

Conclusion

26. Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHENG-FENG HUANG whose telephone number is (571)272-6186. The examiner can normally be reached Monday-Friday: 9 am - 5 pm.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Eleni A Shiferaw can be reached on (571) 272-3867. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: https://patentcenter.uspto.gov. Visit https://www.uspto.gov/patents/apply/patent-center for more information about Patent Center and https://www.uspto.gov/patents/docx for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/CHENG-FENG HUANG/
Primary Examiner, Art Unit 2497

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.
18/892,283	09/20/2024	Jason Crabtree	15388FT	7526

82318 7590 11/29/2024
Brian Galvin
Galvin Patent Law LLC
2916 NW Bucklin Hill Road
Suite 485
Silverdale, WA 98383

EXAMINER
HUANG, CHENG-FENG

ART UNIT	PAPER NUMBER
2497	

NOTIFICATION DATE	DELIVERY MODE
11/29/2024	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):

USPTO@GALVINPATENTLAW.COM
eofficeaction@appcoll.com

Applicant-Initiated Interview Summary	Application No. 18/892,283	Applicant(s) Crabtree et al.		
	Examiner CHENG-FENG HUANG	Art Unit 2497	AIA (First Inventor to File) Status Yes	Page 1 of 1

All Participants (applicant, applicants representative, PTO personnel)	Title	Type
CHENG-FENG HUANG	Primary Examiner	Telephonic
Brian Galvin	Attorney of Record	
Doug Meier	Attorney	

Date of Interview: 25 November 2024

Issues Discussed:

35 U.S.C. 101

Examiner suggested to include the non-transitory machine-readable storage media in the computer system to overcome the rejection.

35 U.S.C. 103

This is a preliminary, informal Interview for 18892283. Applicant's representatives discussed the invention with examiner. Examiner suggested to clarify some issues in the claims and further amend the claims with more details of the novelty of the invention.

/CHENG-FENG HUANG/ Primary Examiner, Art Unit 2497	

Applicant is reminded that a complete written statement as to the substance of the interview must be made of record in the application file. It is the applicants responsibility to provide the written statement, unless the interview was initiated by the Examiner and the Examiner has indicated that a written summary will be provided. See MPEP 713.04
Please further see:
MPEP 713.04
Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews, paragraph (b)
37 CFR § 1.2 Business to be transacted in writing

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.

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.
18/892,283	09/20/2024	Jason Crabtree	15388FT	7526

82318 7590 12/06/2024
Brian Galvin
Galvin Patent Law LLC
2916 NW Bucklin Hill Road
Suite 485
Silverdale, WA 98383

EXAMINER
HUANG, CHENG-FENG

ART UNIT	PAPER NUMBER
2497	

NOTIFICATION DATE	DELIVERY MODE
12/06/2024	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):

USPTO@GALVINPATENTLAW.COM
eofficeaction@appcoll.com

Applicant-Initiated Interview Summary	Application No. 18/892,283	Applicant(s) Crabtree et al.		
	Examiner CHENG-FENG HUANG	Art Unit 2497	AIA (First Inventor to File) Status Yes	Page 1 of 1

All Participants (applicant, applicants representative, PTO personnel)	**Title**	**Type**
CHENG-FENG HUANG	Primary Examiner	Telephonic
Brian Galvin	Attorney of Record	
Doug Meier	Attorney	

Date of Interview: 03 December 2024

Issues Discussed:

35 U.S.C. 103

Applicant's representatives apologized for the unexpected delay of proposed amendment. Applicant's representatives then explained the amendment in progress with the idea of a modified first graph and a subset as 2nd graph. Examiner thanked Applicant's representatives for the update.

/CHENG-FENG HUANG/ Primary Examiner, Art Unit 2497	

Applicant is reminded that a complete written statement as to the substance of the interview must be made of record in the application file. It is the applicants responsibility to provide the written statement, unless the interview was initiated by the Examiner and the Examiner has indicated that a written summary will be provided. See MPEP 713.04
Please further see:
MPEP 713.04
Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews, paragraph (b)
37 CFR § 1.2 Business to be transacted in writing

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.

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.
18/892,283	09/20/2024	Jason Crabtree	15388FT	7526

82318 7590 01/22/2025
Brian Galvin
Galvin Patent Law LLC
2916 NW Bucklin Hill Road
Suite 485
Silverdale, WA 98383

EXAMINER
HUANG, CHENG-FENG

ART UNIT	PAPER NUMBER
2497	

NOTIFICATION DATE	DELIVERY MODE
01/22/2025	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):

USPTO@GALVINPATENTLAW.COM
eofficeaction@appcoll.com

Applicant-Initiated Interview Summary	Application No. 18/892,283	Applicant(s) Crabtree et al.		
	Examiner CHENG-FENG HUANG	Art Unit 2497	AIA (First Inventor to File) Status Yes	Page 1 of 1

All Participants (applicant, applicants representative, PTO personnel)	Title	Type
CHENG-FENG HUANG	Primary Examiner	Telephonic
Brian Galvin	Attorney of Record	
Doug Meier	Attorney	

Date of Interview: 15 January 2025

Issues Discussed:

35 U.S.C. 103

Applicant's representatives first provided an overview of the invention and support of the proposed amendment by referring to [0085-0086], [0090-0091] and Fig. 31. Examiner then discussed the invention with Applicant's representatives. The proposed amendment could overcome the current 103 rejections and raise new issues that would require further consideration and/or search. Examiner also suggested to further amend the claims to clarify several issues to make the claims more detailed and distinguished from the prior arts to move the case forward. Examiner will hold final consideration until a formal amendment has been filed.

☑ Attachment

/CHENG-FENG HUANG/ Primary Examiner, Art Unit 2497	

Applicant is reminded that a complete written statement as to the substance of the interview must be made of record in the application file. It is the applicants responsibility to provide the written statement, unless the interview was initiated by the Examiner and the Examiner has indicated that a written summary will be provided. See MPEP 713.04
Please further see:
MPEP 713.04
Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews, paragraph (b)
37 CFR § 1.2 Business to be transacted in writing

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.

Proposed Claim Amendments – For Discussion Purposes Only

CLAIMS

What is claimed is:

1. (Proposed – Currently Amended) A computer system comprising ~~a memory, wherein the computer system is configured to execute software instructions stored on nontransitory machine-readable storage media that~~:

a hardware memory, wherein the computer system is configured to execute software instructions stored on nontransitory machine-readable storage media that:

store in the hardware memory a representation of a first graph~~, wherein the representation of the first graph~~ comprising[[es]] representations of a first plurality of nodes corresponding to a first plurality of entities and a first plurality of edges,

wherein the first graph is a directed graph,

wherein the first plurality of entities comprises a plurality of user accounts and a plurality of devices,

wherein each ~~node~~ edge of the first plurality of ~~nodes~~ edges corresponds to a respective ~~entity of a plurality~~ relationship between a respective pair of entities, and

wherein the representation of the first plurality of edges ~~includes at least one edge~~ comprises representations of relationship indicators corresponding to a plurality of relationship types ~~a physical connection between entities and at least one edge corresponding to a logical connection between entities~~;

~~process, substantially in real time, streaming data received from a plurality of devices,~~

~~wherein the~~ receive streaming data comprising[[es]] ~~information~~ time-stamped data about events relating to one or more entities of the first plurality of entities,[[;]]

~~process the representation of the first graph to add, subtract, or modify a node of the first graph based on the streaming data,~~

based on a first portion of the streaming data, identify a first entity that does not correspond to any node of the first plurality of nodes,

based on a second portion of the streaming data, identify a first relationship between a pair of entities of the first plurality of entities that does not correspond to any edge of the first plurality of edges,

based on a third portion of the streaming data, identify a first edge of the first plurality of edges that corresponds to a second relationship, the third portion of the streaming data indicating that the second relationship is not current,

~~process~~ modify in the hardware memory the representation of the first graph ~~to add, subtract, or modify an edge of the first graph based on the streaming data~~, wherein the modified ~~use the~~ representation ~~of the first graph to determine whether~~ comprises representations of a first node corresponding to the first entity and a second edge corresponding to the first relationship, and wherein the modified representation does not comprise any edge indicating that the second relationship is current ~~an event, of the events relating to the plurality of entities, is anomalous, and~~,

~~if the event is anomalous,~~ identify an attack path involving the ~~event as a~~ first ~~anomalous event~~ entity, wherein identifying the attack path comprises:

identifying a second entity corresponding to a device based on a potential for gaining access to the device using the first entity, wherein the second entity is related by a third edge to the first entity in the modified representation of the first graph; and,

generate an alert comprising a visual representation of:

the first entity and the second entity,

a relationship between the first entity and the second entity, and

a third entity, wherein the third entity is a target of the attack path.

27. (New) A computer system comprising a hardware memory, wherein the computer system is configured to execute software instructions stored on nontransitory machine-readable storage media that:

store in the hardware memory a representation of a first graph comprising representations of a first plurality of nodes corresponding to a first plurality of entities and a first plurality of edges, the first graph being a directed graph,

wherein the first plurality of entities comprises a plurality of user accounts and a plurality of devices,

wherein each edge of the first plurality of edges corresponds to a respective relationship between a respective pair of entities, and

wherein the representation of the first plurality of edges comprises representations of relationship indicators corresponding to a plurality of relationship types;

based on the representation of the first graph, identify a first plurality of attack paths comprising a first entity of the first plurality of entities, wherein each attack path of the first plurality of attack paths targets a second entity of the first plurality of entities,

receive streaming data comprising time-stamped data about events relating to one or more entities of the first plurality of entities,

based on a first portion of the streaming data, identify a third entity that does not correspond to any node of the first plurality of nodes,

based on a second portion of the streaming data, identify a first relationship between a pair of entities of the first plurality of entities that does not correspond to any edge of the first plurality of edges,

based on a third portion of the streaming data, identify a first edge of the first plurality of edges that corresponds to a second relationship, the third portion of the streaming data indicating that the second relationship is not current,

modify in the hardware memory the representation of the first graph, wherein the modified representation comprises representations of a node corresponding to the third entity and an edge corresponding to the first relationship, and wherein the modified representation does not comprise any edge indicating that the second relationship is current, and

based on the modified representation of the first graph, identify a second plurality of attack paths comprising the first entity, wherein each attack path of the second plurality of attack paths targets the second entity, and wherein an attack path of the second plurality of attack paths comprises the third entity.

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
18/892,283	09/20/2024	Jason Crabtree	15388FT

CONFIRMATION NO. 7526

PUBLICATION NOTICE

OC000000083414765

82318
Brian Galvin
Galvin Patent Law LLC
2916 NW Bucklin Hill Road
Suite 485
Silverdale, WA 98383

Date Mailed: 01/23/2025

Title:CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION

Publication No.US-2025-0030745-A1
Publication Date:01/23/2025

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 viewed using the USPTO's publicly available Searchable Databases via the Patent Public Search tool at www.uspto.gov. The direct link to access the Patent Public Search tool is currently https://ppubs.uspto.gov/pubwebapp/static/pages/ppubsbasic.html.

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 Public Records Division. The Public Records Division can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Public Records Division, 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 Patent Center, the USPTO's electronic patent application filing and management system. The direct link to access this status information is currently https://patentcenter.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of Patent Center.

Further assistance in electronically accessing the publication, or about Patent Center, 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

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 18/892,283	Filing Date 09/20/2024	☐ To be Mailed

ENTITY: ☑ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) 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 $100 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $480 =	
☐ 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	02/13/2025	(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))	* 29	Minus	** 26	= 3		x $200 =	600
	Independent (37 CFR 1.16(h))	* 2	Minus	*** 3	= 0		x $600 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	600

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 $0 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x $0 =	
	☐ 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.	PSS
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/LINDA A WISE/
*** 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.	

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

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/892,283	**02/13/2025 07:03:51 PM Z ET**	**15388FT**

Title of Invention

CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	7526	FILED BY	Aura Morrey
PATENT CENTER #	69180461	AUTHORIZED BY	Brian Galvin
CUSTOMER #	82318	FILING DATE	09/20/2024
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	Jason Crabtree

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 1009	**E20252CJ04286441**	**Brian Galvin**

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
1814	STATUTORY DISCLAIMER, INCLUDING TERMINAL DISCLAIMER	183.00	1	183.00
			TOTAL AMOUNT:	**$183.00**

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 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

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A PRIOR PATENT

APPLICATION #	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET #
18892283	**09/20/2024**	**Jason Crabtree**	**15388FT**

Title of Invention

CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION

- ✔ Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action
- ✔ This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.

Owner	Percent interest
QOMPLX LLC	100%
Total	**100%**

The owner(s) of percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending reference Application Number(s)

Application #	Filing Date

as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the reference application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.
In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term of any patent granted on said reference application, "as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application," in the event that any such patent granted on the pending reference application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

The owner(s) of percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of prior patent number(s)

Patent #
12206708

as the term of said prior patent is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the prior patent are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.
In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the prior patent, "as the term of said prior patent is presently shortened by any terminal disclaimer," in the event that said prior patent later:
• expires for failure to pay a maintenance fee;
• is held unenforceable;
• is found invalid by a court of competent jurisdiction;
• is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
• has all claims canceled by a reexamination certificate;
• is reissued; or
• is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Terminal disclaimer fee under 37 CFR 1.20(d) included with Electronic Terminal Disclaimer request.

Applicant claims the following entity status:
Regular Undiscounted

I hereby declare that all statements made herein of my own knowledge are true and that all statemnts 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.

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 is of record in this application

Signature	Name	Registration #
/BRIAN R. GALVIN/	Brian Galvin	50966

* Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner). Form PTO/SB/96 may be used for making this certification. See MPEP 324.

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

APPROVAL LETTER

APPLICATION #	FILING DATE	APPLICANT/PATENT UNDER REEXAMINATION
18/892,283	**09/20/2024**	**Jason Crabtree**

Title of Invention

CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION

Electronic terminal disclaimer filed on 02/13/2025

Approved

This patent is subject to a Terminal Disclaimer

Approved / Disapproved by: Electronic Terminal Disclaimer automatically approved

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/892,283	**02/13/2025 07:03:51 PM Z ET**	**15388FT**

Title of Invention

CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	7526	FILED BY	Aura Morrey
PATENT CENTER #	69180461	FILING DATE	09/20/2024
CUSTOMER #	82318	FIRST NAMED INVENTOR	Jason Crabtree
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Brian Galvin

Documents

TOTAL DOCUMENTS: 2

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
petition-request.pdf	3	Terminal Disclaimer-Filed (Electronic)	44 KB
grantLetter.pdf	1	Terminal Disclaimer-Electronic-Approved	18 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
petition-request.pdf	33A084833BABE45C504539F03EF9B37C587B17C6A37CA8C2F51B0D72345AF9DCA6EBA69E06CBABD22EF144FF2C0A161F8F5758B51C360262146AD7C290E9C5CF

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 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

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/892,283	**02/13/2025 07:21:03 PM Z ET**	**15388FT**

Title of Invention

CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	7526	FILED BY	Aura Morrey
PATENT CENTER #	69180576	FILING DATE	09/20/2024
CUSTOMER #	82318	FIRST NAMED INVENTOR	Jason Crabtree
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Brian Galvin

Documents

TOTAL DOCUMENTS: 1

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
250213_15388FT_OAR 1_AS_FILED.pdf	20	Amendment/Request for Reconsideration-After Non-Final Rejection	137 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
250213_15388FT_OAR 1_AS_FILED.pdf	195BB0457D6F2F7C4C43ED93739D07F23D0016894DB06DE9604D713EF9696D529DAFC38CD690142BD38490D31DC23338F6691974E7D2EDACBE3FB6542AF9A309

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 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

Art Unit: 2497 Examiner: Cheng-Feng Huang

In Re:	Jason Crabtree et al.
Case:	15388FT
Serial No.:	18/892,283
Filed:	September 20, 2024
Subject:	CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

Response A

In the Claims

All of the claims standing for examination are reproduced below with appropriate status indication.

1. (Currently Amended) A computer system comprising ~~a memory, wherein the computer system is configured to execute software instructions stored on nontransitory machine-readable storage media that~~:

a hardware memory, wherein the computer system is configured to execute software instructions stored on nontransitory machine-readable storage media comprising software instructions that:

store in the hardware memory a representation of a first graph, wherein the representation of the first graph comprises representations of a first plurality of nodes corresponding to a first plurality of entities and further comprises representations of a first plurality of edges, wherein the first graph is a directed graph,

wherein the first plurality of entities comprises a plurality of accounts and a plurality of resources, and

wherein each ~~node~~ edge of the first plurality of ~~nodes~~ edges corresponds to a respective ~~entity of a plurality~~ relationship between a respective pair of entities;~~, and~~

~~wherein the first plurality of edges includes at least one edge corresponding to a physical connection between entities and at least one edge corresponding to a logical connection between entities;~~

~~process, substantially in real time, streaming data received from a plurality of devices,~~

~~wherein the~~ receive streaming data comprising[[es]] ~~information~~ time-stamped data about events relating to one or more entities of the first plurality of entities,[[;]]

~~process the representation of the first graph to add, subtract, or modify a node of the first graph based on the streaming data,~~

based on a first portion of the streaming data, identify a first entity that does not correspond to any of the first plurality of nodes, wherein the first entity is not of the first plurality of entities,

based on a second portion of the streaming data, wherein the second portion is not identical to the first portion, identify a first relationship between a pair of entities of the first plurality of entities that does not correspond to any of the first plurality of edges,

~~process~~ modify, in the hardware memory, the representation of the first graph to generate a modified representation of the first graph ~~to add, subtract, or modify an edge of the first graph based on the streaming data~~, wherein the modified ~~use the~~ representation of the first graph ~~to determine whether~~ comprises a representation of a first node corresponding to the first entity and a representation of a first edge corresponding to the first relationship, wherein the first node is not of the first plurality of nodes and the first edge is not of the first plurality of edges ~~an event, of the events relating to the plurality of entities, is anomalous, and~~,

~~if the event is anomalous,~~ identify, based on the modified representation of the first graph, an attack path involving the ~~event as a~~ first ~~anomalous event~~ entity, wherein identifying the attack path comprises identifying a second entity that can potentially be accessed using the first entity, wherein the second entity corresponds to a second node, and the second node is related by one or more edges to the first node corresponding to the first entity in the modified representation of the first graph; and,

generate a report comprising an identification of at least one of the first entity and the second entity.

2. (Currently Amended) The computer system of claim 1, wherein identifying the attack path further comprises ~~configured to execute software instructions stored on nontransitory machine-readable storage media that~~:

identifying a first plurality of possible event flows for a first anomalous event associated with the first entity[[,]]

~~wherein the first plurality of possible event flows comprises a possible event flow relating to an entity of the plurality of entities,~~

~~wherein the entity relates to the first anomalous event;~~

~~identify a first plurality of dependencies,~~

~~wherein each dependency of the first plurality of dependencies is associated with a respective possible event flow of the first plurality of possible event flows; and,~~

~~a second plurality of nodes of the first graph,~~

~~wherein each node of the second plurality of nodes corresponds to a respective entity relating to a respective possible event flow of the first plurality of possible event flows~~.

3. (Currently Amended) The system of claim 2, wherein identifying the attack path further comprises ~~configured to execute software instructions stored on nontransitory machine-readable storage media that~~:

~~store in the memory a representation of a second graph,~~

~~wherein the representation of the second graph comprises a representation of a third plurality of nodes,~~

~~wherein each node of the third plurality of nodes corresponds to a respective node of the second plurality of nodes; and~~

~~wherein the representation of the second graph comprises a representation of a second plurality of edges,~~

~~wherein at least a portion of at least one of the first plurality of dependencies or the first plurality of possible event flows is used to generate the second plurality of edges; and,~~

~~traverse the second graph to~~ identifying a point of origin for the first anomalous event based on the first plurality of possible event flows.

4. (Currently Amended) The computer system of claim [[3]] 1, wherein the modified representation of the first graph comprises a representation of a node corresponding to [[an]] the first entity, wherein the first entity is identified based on active reconnaissance results.

5. (Currently Amended) The computer system of claim [[3]] 1, wherein the modified representation of the first graph comprises a representation of a node corresponding to [[an]] the first entity, wherein the first entity is identified based on passive reconnaissance results.

6. (Currently Amended) The computer system of claim [[3]] 1, wherein the ~~representation of the second graph~~ attack path is ~~generated~~ identified at least in part by processing at least a portion of the modified representation of the first graph using at least one transformation pipeline.

7. (Currently Amended) The computer system of claim [[3]] 1, wherein the computer system is further configured to execute software instructions stored on nontransitory machine-readable storage media comprising software instructions that:

~~identify~~ based on a third portion of the streaming data, detect a change in a relationship corresponding to an existing edge of the first ~~fourth~~ plurality of ~~nodes of the first graph~~ edges,

wherein ~~each node~~ the modified representation of the first graph further comprises a modified representation of the ~~fourth~~ first plurality of ~~nodes~~ edges that accounts for the detected change in the relationship, and ~~corresponds to a respective entity of the plurality of entities,~~

~~wherein the respective entity of the plurality of entities relates to a second anomalous event;~~

~~identify a second plurality of possible event flows, and~~

~~identify a second plurality of dependencies,~~

wherein ~~each dependency of~~ the report further comprises a visual representation of the detected change in the relationship ~~second plurality of dependencies is associated with a respective possible event flow of the second plurality of possible event flows~~.

8. (Currently Amended) The computer system of claim [[7]] 1, wherein the ~~representation of the second~~ first graph is a cyber-physical graph ~~further comprises:~~

~~a representation of a fifth plurality of nodes,~~

~~wherein each node of the fifth plurality of nodes corresponds to a respective node of the fourth plurality of nodes; and,~~

~~a representation of a third plurality of edges,~~

~~wherein at least a portion of at least one of the second plurality of dependencies or the second plurality of possible event flows is used to generate the third plurality of edges~~.

9. (Currently Amended) The computer system of claim 8, wherein the report is an alert ~~second anomalous event is correlated in time to the first anomalous event~~.

10. (Currently Amended) The computer system of claim 1, wherein the computer system is further configured to execute software instructions stored on nontransitory machine-readable storage media comprising software instructions that determine[[ing]] whether an event, of the events relating to one or more entities of the first plurality of entities, is anomalous, wherein determining whether the event is anomalous comprises:

determining that the event relates to [[a]] the first entity ~~of the plurality of entities~~,

determining at least one behavior pattern associated with the first entity, and

comparing the event to the at least one behavior pattern.

11. (Original) The computer system of claim 10, wherein comparing the event to the at least one behavior pattern comprises using a threshold.

12. (Canceled)

13. (Canceled)

14. (Original) The system of claim 10, wherein comparing the event to the at least one behavior pattern further comprises:

determining that the first entity is associated with a resource,

wherein the resource is a sensitive resource.

15. (Canceled)

16. (Canceled)

17. (Original) The computer system of claim 1, wherein the computer system comprises a plurality of physical computing machines.

18. (Original) The computer system of claim 1, wherein the computer system comprises a plurality of virtual computing machines.

19. (Original) The computer system of claim 1, wherein at least one entity of the first plurality of entities is at least one of a user, a place, a device, a resource, a group, or a service.

20. (Currently Amended) The computer system of claim [[3]] 1, wherein identifying the attack path further comprises identifying a third entity that can potentially be accessed using

~~representation of~~ the second ~~graph~~ entity, wherein the third entity corresponds to a third node, and the third node is related by one or more edges to the second node in the modified ~~further comprises a~~ representation of ~~at least one node that does not correspond to any node of the second plurality of nodes~~ the first graph.

21. (Canceled)

22. (Canceled)

23. (Currently Amended) The computer system of claim 3,

wherein ~~traversing the second graph to~~ identifying the [[a]] point of origin for the first anomalous event comprises[[,]] ~~in the following order~~:

traversing a second graph, wherein a representation of the second graph is stored in the hardware memory, wherein the representation of the second graph comprises a representation of a second plurality of nodes and a representation of a second plurality of edges, wherein each node of the second plurality of nodes corresponds to a respective node of the first plurality of nodes;

processing a representation of a first node of the ~~third~~ second plurality of nodes,

wherein the first node corresponds to a second node of the ~~second~~ first plurality of nodes;

identifying an edge of the second plurality of edges, wherein the edge connects a third node of the ~~third~~ first plurality of nodes with the first node, and

processing a representation of the third node.

24. (Canceled)

25. (Canceled)

26. (Original) The computer system of claim 1, wherein the representation of the first graph comprises a representation of at least one node that does not correspond to an entity.

27. (New) A computer system comprising:

a hardware memory, wherein the computer system is configured to execute software instructions stored on nontransitory machine-readable storage media comprising software instructions that:

store in the hardware memory a representation of a first graph, wherein the representation of the first graph comprises representations of a first plurality of nodes corresponding to a first plurality of entities and further comprises representations of a first plurality of edges, wherein the first graph is a directed graph,

wherein the first plurality of entities comprises a plurality of accounts and a plurality of resources, and

wherein each edge of the first plurality of edges corresponds to a respective relationship between a respective pair of entities;

identify, based on the representation of the first graph, a first plurality of attack paths comprising a first entity of the first plurality of entities, wherein each attack path of the first plurality of attack paths targets a second entity of the first plurality of entities,

receive streaming data comprising time-stamped data about events relating to one or more entities of the first plurality of entities,

based on a first portion of the streaming data, identify a third entity that does not correspond to any of the first plurality of nodes, wherein the third entity is not of the first plurality of entities,

based on a second portion of the streaming data, wherein the second portion is not identical to the first portion, identify a first relationship between a pair of entities of the first plurality of entities that does not correspond to any of the first plurality of edges,

modify, in the hardware memory, the representation of the first graph to generate a modified representation of the first graph, wherein the modified representation of the first graph comprises a representation of a node corresponding to the third entity and an edge corresponding to the first relationship, wherein the node is not of the first plurality of nodes and the edge is not of the first plurality of edges, and

identify, based on the modified representation of the first graph, a second plurality of attack paths comprising the first entity, wherein each attack path of the second plurality of

attack paths targets the second entity, and wherein an attack path of the second plurality of attack paths comprises the third entity.

28. (New) The computer system of claim 27, wherein the first graph is a cyber-physical graph.

29. (New) The computer system of claim 27, wherein identifying the second plurality of attack paths comprises:

identifying a first plurality of possible event flows involving the first entity, and

identifying a first plurality of dependencies associated with the first plurality of event flows.

30. (New) The computer system of claim 29, further configured to execute software instructions stored on nontransitory machine-readable storage media comprising software instructions that:

based on a third portion of the streaming data, identify an anomalous event,

store in the hardware memory a dependency tree for the anomalous event, and

based on the dependency tree, determine a point of origin for the anomalous event.

31. (New) The computer system of claim 27, wherein a portion of the representation of the first graph is derived from reconnaissance data received by the computer system from a plurality of computer systems,

wherein a first computer system of the plurality of computer systems performs passive reconnaissance, and

wherein a second computer system of the plurality of computer systems performs active reconnaissance.

32. (New) The computer system of claim 27, further configured to execute software instructions stored on nontransitory machine-readable storage media comprising software instructions that:

identify a third plurality of attack paths, comprising attack paths of the second plurality of attack paths that are not in the first plurality of attack paths, and

generate a report comprising information about the third plurality of attack paths.

33. (New) The computer system of claim 27, further configured to execute software instructions stored on nontransitory machine-readable storage media comprising software instructions that analyze an attack path of the plurality of attack paths using a graph analysis algorithm.

34. (New) The computer system of claim 33, wherein the graph analysis algorithm comprises a shortest-path algorithm.

35. (New) The computer system of claim 34, further configured to execute software instructions stored on nontransitory machine-readable storage media comprising software instructions that generate a report comprising information obtained from the graph analysis algorithm.

36. (New) The computer system of claim 27, wherein the representation of the first graph comprises an identification of the third entity as a sensitive resource, and wherein the computer system is further configured to execute software instructions stored on nontransitory machine-readable storage media comprising software instructions that generate a report that identifies the third entity as a sensitive resource.

37. (New) The computer system of claim 27, wherein the representation of the first graph comprises an identification of a security vulnerability associated with the third entity, and wherein an attack path of the second plurality of attack paths is based on the security vulnerability.

REMARKS

This communication is responsive to the office action pertaining to the instant invention that was mailed on November 13, 2024.

By this amendment, claims 1-10, 20, and 23 are amended, claims 12-13, 15-16, 21-22, and 24-25 are canceled, and new claims 27-37 are added. No new matter is added by these amendments. Upon entry of these amendments, claims 1-11, 14, 17-20, 23, and 26-37 will be pending.

1. *Summary of Examiner Interview*

Applicant wishes to thank Examiner Huang for the helpful interviews conducted by phone between Applicant's undersigned representative (Brian Galvin, Reg. No. 50,966), Doug Meier (Reg. No. 65,727), and Examiner Huang on December 3, 2024 and January 15, 2025. During the interviews, the pending claims and the cited references were discussed, along with some proposed claim amendments and their support. No agreement was reached.

2. *Support for Claim Amendments*

Support for the amendments to the claims are as follows (these citations are illustrative only, and they are not intended to be exhaustive):

Claim Element	Example Spec. Support
Claim 1: "receive streaming data comprising time-stamped data about events relating to one or more entities of the first plurality of entities"	At least at ¶¶ [93] and [94] of the as-filed specification.
Claim 1: "based on a first portion of the streaming data, identify a first entity that does not correspond to any of the first plurality of nodes, wherein the first entity is not of the first plurality of entities"	At least at ¶¶ [93], [94], and [96] of the as-filed specification.
Claim 1: "based on a second portion of the streaming data, wherein the second portion is not identical to the first portion, identify a first relationship between a pair of entities of the first plurality of entities that does not correspond to any of the first plurality of edges"	At least at ¶¶ [93], [94], and [96] of the as-filed specification.
Claim 1: "modify, in the hardware memory, the representation of the first graph to generate a modified representation of the first graph, wherein the modified representation of the first graph comprises a representation of a first node corresponding to the first entity and a representation of a first edge corresponding to the first relationship, wherein the first node is not of the first plurality of nodes and the first edge is not of the first plurality of edges"	At least at ¶¶ [93], [94], and [96] of the as-filed specification.
Claim 1: "identify, based on the modified representation of the first graph, an attack path involving the first entity, wherein identifying the attack path comprises identifying a second entity that can potentially be accessed using the first entity, wherein the second entity corresponds to a second node, and the second node is related by one or more edges to the first node corresponding to the first entity in the modified representation of the first graph"	At least at ¶¶ [85], [86], and [103], and FIG. 31 of the as-filed specification.
Claim 1: "generate a report comprising an identification of at least one of the first entity and the second entity"	At least at ¶¶ [91] and [96]-[98], and FIG. 11 of the as-filed specification.
Claim 2: "wherein identifying the attack path further comprises identifying a first plurality of possible event flows for a first anomalous event associated with the first entity"	At least at ¶ [85] and FIG. 31 of the as-filed specification.
Claim 3: "wherein identifying the attack path further comprises identifying a point of origin for the first anomalous event based on the first plurality of possible event flows"	At least at ¶ [86] and FIG. 32 of the as-filed specification.
Claim 7: "based on a third portion of the streaming data, detect a change in a relationship corresponding to an existing edge of the first plurality of edges, wherein the modified representation of the first graph further comprises a modified representation of the first plurality of edges that accounts for the detected change in the relationship; and wherein the report further comprises a visual representation of the detected change in the relationship"	At least at ¶ [86] and FIG. 32 of the as-filed specification.

Claim 8: "wherein the first graph is a cyber-physical graph"	At least at ¶¶ [81] and [102]-[103] of the as-filed specification.
Claim 9: "wherein the report is an alert"	At least at ¶ [96] of the as-filed specification.
Claim 10: "determine whether an event, of the events relating to one or more entities of the first plurality of entities, is anomalous, wherein determining whether the event is anomalous comprises: determining that the event relates to the first entity, determining at least one behavior pattern associated with the first entity, and comparing the event to the at least one behavior pattern"	At least at ¶¶ [84] and [85], and FIGS. 30 and 31 of the as-filed specification.
Claim 20: "wherein identifying the attack path further comprises identifying a third entity that can potentially be accessed using the second entity, wherein the third entity corresponds to a third node, and the third node is related by one or more edges to the second node in the modified representation of the first graph"	At least at ¶¶ [85], [86], and [103], and FIG. 31 of the as-filed specification.
Claim 23: "wherein identifying the point of origin for the first anomalous event comprises: traversing a second graph, wherein a representation of the second graph is stored in the hardware memory, wherein the representation of the second graph comprises a representation of a second plurality of nodes and a representation of a second plurality of edges, wherein each node of the second plurality of nodes corresponds to a respective node of the first plurality of nodes; processing a representation of a first node of the second plurality of nodes, wherein the first node corresponds to a second node of the first plurality of nodes; identifying an edge of the second plurality of edges, wherein the edge connects a third node of the first plurality of nodes with the first node, and processing a representation of the third node"	At least at ¶¶ [86], [93], [94], and [96], and FIGS. 22 and 32 of the as-filed specification.
Claim 27: "identify, based on the representation of the first graph, a first plurality of attack paths comprising a first entity of the first plurality of entities, wherein each attack path of the first plurality of attack paths targets a second entity of the first plurality of entities"	At least at ¶ [103] of the as-filed specification.
Claim 27: "receive streaming data comprising time-stamped data about events relating to one or more entities of the first plurality of entities"	At least at ¶¶ [93] and [94] of the as-filed specification.
Claim 27: "based on a first portion of the streaming data, identify a third entity that does not correspond to any node of the first plurality of nodes, wherein the third entity is not of the first plurality of entities"	At least at ¶¶ [93], [94], and [96] of the as-filed specification.

Claim 27: "based on a second portion of the streaming data, wherein the second portion is not identical to the first portion, identify a first relationship between a pair of entities of the first plurality of entities that does not correspond to any of the first plurality of edges"	At least at ¶¶ [93], [94], and [96] of the as-filed specification.
Claim 27: "modify, in the hardware memory, the representation of the first graph to generate a modified representation of the first graph, wherein the modified representation of the first graph comprises a representation of a node corresponding to the third entity and an edge corresponding to the first relationship, wherein the node is not of the first plurality of nodes and the edge is not of the first plurality of edges"	At least at ¶¶ [93], [94], and [96] of the as-filed specification.
Claim 27: "identify, based on the modified representation of the first graph, a second plurality of attack paths comprising the first entity, wherein each attack path of the second plurality of attack paths targets the second entity, and wherein an attack path of the second plurality of attack paths comprises the third entity"	At least at ¶¶ [85], [86], and [103], and FIG. 31 of the as-filed specification.
Claim 28: "wherein the first graph is a cyber-physical graph"	At least at ¶¶ [81] and [102]-[103] of the as-filed specification.
Claim 29: "wherein identifying the second plurality of attack paths comprises: identifying a first plurality of possible event flows involving the first entity, and identifying a first plurality of dependencies associated with the first plurality of event flows.	At least at ¶ [85] and FIG. 31 of the as-filed specification.
Claim 30: "based on a third portion of the streaming data, identify an anomalous event, store in the hardware memory a dependency tree for the anomalous event, and based on the dependency tree, determine a point of origin for the anomalous event"	At least at ¶ [86] and FIG. 32 of the as-filed specification.
Claim 31: "wherein a portion of the representation of the first graph is derived from reconnaissance data received by the computer system from a plurality of computer systems, wherein a first computer system of the plurality of computer systems performs passive reconnaissance, and wherein a second computer system of the plurality of computer systems performs active reconnaissance"	At least at ¶ [81] of the as-filed specification.
Claim 32: "identify a third plurality of attack paths, comprising attack paths of the second plurality of attack paths that are not in the first plurality of attack paths, and generate a report comprising information about the third plurality of attack paths"	At least at ¶¶ [85], [86], and [103], and FIG. 31 of the as-filed specification.
Claim 33: "analyze an attack path of the plurality of attack paths using a graph analysis algorithm"	At least at ¶ [103] of the as-filed specification.
Claim 34: "wherein the graph analysis algorithm comprises a shortest-path algorithm"	At least at ¶ [103] of the as-filed specification.

Claim 35: "generate a report comprising information obtained from the graph analysis algorithm"	At least at ¶¶ [91] and [96]-[98], and FIG. 11 of the as-filed specification.
Claim 36: "wherein the representation of the first graph comprises an identification of the third entity as a sensitive resource, and . . . generate a report that identifies the third entity as a sensitive resource"	At least at ¶ [103] of the as-filed specification.
Claim 37: "wherein the representation of the first graph comprises an identification of a security vulnerability associated with the third entity, and wherein an attack path of the second plurality of attack paths is based on the security vulnerability"	At least at ¶ [98] of the as-filed specification.

From the Action:

Claim 1 is objected to because of the following informalities:

Claim 1 (Line 11) recites "substantially in real time." It is not clear to what degree can be considered as substantially.

Claim 1 (Line 20) recites "if the event is anomalous." The limitation is confusing with the term "if."

Appropriate correction is required.

Applicant's Response

Without conceding the propriety of these objections, Applicant respectfully submits that the pending claims have been amended to no longer recite "substantially in real time" or "if the event is anomalous," thereby rendering these objections moot.

From the Action:

Claims 1-26 are rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter.

Applicant's Response

The Office Action rejected claims 1-26 under 35 U.S.C. § 101 as being directed to non-statutory subject matter. In particular, the Office Action states that "claim 1 is directed to non-statutory subject matter for lack of a hardware component," and suggests that the claim be further amended to positively recite at least one hardware element within the body of the claim to make

the claim statutory subject matter under 35 U.S.C. § 101. Applicant respectfully traverses these rejections. Nevertheless, in the interest of furthering prosecution, Applicant has amended the pending claims to incorporate the Office Action's suggestion. Accordingly, Applicant respectfully requests that the section §101 rejections be withdrawn.

From the Action:

Claims 1-26 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over: Claims 1-8 of copending Application 17/237,346.

A timely filed terminal disclaimer in compliance with 37 CFR §1.321(c) or §1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the reference application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. See MPEP §717.02 for applications subject to examination under the first inventor to file provisions of the AIA as explained in MPEP §2159. See MPEP §§706.02(l)(1)–706.02(l)(3) for applications not subject to examination under the first inventor to file provisions of the AIA. A terminal disclaimer must be signed in compliance with 37 CFR §1.321(b).

Applicant's Response

Without conceding the propriety of these rejections, and in the interest of furthering prosecution, Applicant is submitting herewith a Terminal Disclaimer listing U.S. Patent 12,206,708 (U.S. App. No. 17/237,346) and U.S. App. No. 18/892,295, thereby rendering these provisional rejections moot.

From the Action:

Claims 1-2, 10-12, 14-15 and 17-19 are rejected under 35 U.S.C. §103 as being unpatentable over Neil et al. (US 2015/0020199 A1) in view of Altman et al. (US 9,183,387 B1).

Applicant's Response

Applicant respectfully traverses these rejections. Without conceding the Office Action's interpretations of *Neil*, *Altman*, and/or *StJohns*, Applicant respectfully submits that the pending claims, as amended herein, are allowable over the cited references.

For ease of reference, claim 1, as amended herein, is reproduced below:

1. A computer system comprising:

a hardware memory, wherein the computer system is configured to execute software instructions stored on nontransitory machine-readable storage media comprising software instructions that:

store in the hardware memory a representation of a first graph, wherein the representation of the first graph comprises representations of a first plurality of nodes corresponding to a first plurality of entities and further comprises representations of a first plurality of edges, wherein the first graph is a directed graph,

wherein the first plurality of entities comprises a plurality of accounts and a plurality of resources, and

wherein each edge of the first plurality of edges corresponds to a respective relationship between a respective pair of entities;

receive streaming data comprising time-stamped data about events relating to one or more entities of the first plurality of entities,

based on a first portion of the streaming data, identify a first entity that does not correspond to any of the first plurality of nodes, wherein the first entity is not of the first plurality of entities,

based on a second portion of the streaming data, wherein the second portion is not identical to the first portion, identify a first relationship between a pair of entities of the first plurality of entities that does not correspond to any of the first plurality of edges,

modify, in the hardware memory, the representation of the first graph to generate a modified representation of the first graph, wherein the modified representation of the first graph comprises a representation of a first node corresponding to the first entity and a representation of a first edge corresponding to the first relationship, wherein the first node is not of the first plurality of nodes and the first edge is not of the first plurality of edges,

identify, based on the modified representation of the first graph, an attack path involving the first entity, wherein identifying the attack path comprises identifying a second entity that can potentially be accessed using the first entity, wherein the second entity corresponds to a second node, and the second node is related by one or more edges to the first node corresponding to the first entity in the modified representation of the first graph; and,

generate a report comprising an identification of at least one of the first entity and the second entity.

In particular, pending claim 1, as amended herein, recites "receive streaming data comprising time-stamped data about events…;" "based on a first portion of the streaming data, identify a first entity that does not correspond to any node of the first plurality of nodes;" "modify…the representation of the first graph to generate a modified representation of the first graph, wherein the modified representation of the first graph comprises a representation of a first node corresponding to the first entity…;" and "identify, based on the modified representation of the first graph, an attack path involving the first entity, wherein identifying the attack path comprises identifying a second entity that can potentially be accessed using the first entity…."

Neil does not teach or suggest at least this combination of claim elements. In particular, *Neil* relates to detecting anomalous behavior in a network by applying, on a sliding window basis, a statistical model to paths in a graph that represents the network. *Neil* at Abstract. The *Neil* system relies on the fact that, "as the attacker traverses the network, he or she creates anomalous activity in time series of communications along each edge that he or she traverses" and performs its detection by looking for a, "union of these anomalous edges in some interval of time" that were created as the attacker traversed the network. *Neil* at ¶ [34]. Thus, *Neil* focuses on types of statistical models that are used to identify where the attacker has already been in the network, in contrast to pending claim 1.

Nor does *Altman* teach or suggest at least this combination of claim elements. In particular, *Altman* relates to detecting online attacks by identifying events associated with users on a social graph. *Altman* at Abstract. *Altman* focuses on message traversal within a social network. Referring to propagation analysis, *Altman* explains that "the temporal factor provides evidence of a movement or propagation of the events and the direction of the movement. The movement and

direction can be used to build a DAG to represent followership of attacks." *Altman* at 6:32-35. "The graph structure becomes a Directed Acyclic Graph (DAG) if formed with a temporal order." *Altman* at 6:41-42. Thus, *Altman*, like *Neil*, is based on message traversal through the network that has already happened, in contrast to pending claim 1.

For at least these reasons, neither *Neil* nor *Altman*, alone or in combination, teaches or suggests the elements of pending claim 1, as amended herein. Dependent claims 2-11, 14, 17-19, 23, and 26 depend from claim 1 and are therefore allowable for at least the same reasons by virtue of their dependence.

New claim 27 recites similar features as pending claim 1. Claim 27 differs from claim 1, at least in part, because it recites "identify, based on the representation of the first graph, a first plurality of attack paths comprising a first entity of the first plurality of entities, wherein each attack path of the first plurality of attack paths targets a second entity of the first plurality of entities" and "identify, based on the modified representation of the first graph, a second plurality of attack paths comprising the first entity, wherein each attack path of the second plurality of attack paths targets the second entity, and wherein an attack path of the second plurality of attack paths comprises the third entity." Claim 27 is allowable for similar reasons as claim 1, as explained in detail above. Dependent claims 28-37 depend from claim 27 and are therefore allowable at least by virtue of their dependence on claim 27.

Allowable Subject Matter

The Office Action objected to claims 3-9, 13, 16, and 20-25 as being dependent on rejected base claim 1 but would be allowable if rewritten in independent form including all the limitations of the base claim and any intervening claims. Applicant acknowledges with thanks the Office Action's acknowledgement that these claims recite allowable subject matter; however, Applicant has amended the pending claims and respectfully submits that the pending claims, as amended herein, are allowable for the reasons explained herein.

SUMMARY

As all of the claims are believed to be, and to have been shown to be, patentable over the references cited, applicant respectfully requests that the case be passed quickly to issue. If any

time extension is needed beyond any extension requested with this amendment, such extension is hereby requested.

Respectfully Submitted,

Jason Crabtree

By: */BRIAN R. GALVIN/*

Brian R. Galvin
Reg. No. 50,966

Galvin Patent Law LLC
2916 NW Bucklin Hill Road
Suite 485
Silverdale, WA 98383
(360) 674-6233
February 13, 2025

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.
18/892,283	09/20/2024	Jason Crabtree	15388FT	7526

82318 7590 02/26/2025
Brian Galvin
Galvin Patent Law LLC
2916 NW Bucklin Hill Road
Suite 485
Silverdale, WA 98383

EXAMINER
HUANG, CHENG-FENG

ART UNIT	PAPER NUMBER
2497	

NOTIFICATION DATE	DELIVERY MODE
02/26/2025	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):

USPTO@GALVINPATENTLAW.COM
eofficeaction@appcoll.com

NOTICE REQUIRING EXCESS CLAIMS FEES	Application No. 18/892,283	Applicant(s) Crabtree et al.
	Art Unit OED1	AIA (FITF) Status Yes

The excess claim(s) filed on 13 February 2025 is/are not accompanied by the appropriate payment of excess claims fees set forth in 37 CFR 1.16(h)-(j) or 1.492(d)-(f). Excess claims fees are required for each claim in independent form in excess of three (§ 1.16(h)), each claim (whether dependent or independent) in excess of twenty (note that § 1.75(c) indicates how multiple dependent claims are considered for fee calculation purposes) (§ 1.16(i)), and each application that contains a multiple dependent claim (§ 1.16(j)).

Since the application is not under a final rejection, applicant is given a time period of **TWO (2) MONTHS** from the mailing date of this notice to submit either: (1) the fee payment of $ 600.00 , or (2) an amendment in compliance with 37 CFR 1.121 that cancels the excess claim(s), in order to avoid ABANDONMENT. Extensions of this time period may be granted under 37 CFR 1.136, unless the excess claim(s) was/were presented in a preliminary amendment.

☐ 1. The funds in Deposit Account No. _____ are insufficient to cover the entire fee due. The balance is due within the time period set forth in this notice. See note below regarding the appropriate service charge.

☐ 2. The Credit Card payment to cover the entire fee due to Account _____ (**Card type + last 4 digits ONLY**) was refused. The balance is due within the time period set forth in this notice. See note below regarding the appropriate service charge.

☐ 3. The amendment that includes the excess claim(s) has not been entered, since applicant has failed to remit (or authorize charge to a Deposit Account or Credit Card) the fee as indicated on the attached Patent Application Fee Determination Record (PTO/SB/06). Remittance or authorization is due within the time period set forth in this notice .

☐ 4. The fee submitted in this application is insufficient. A balance of $ _____ is due for presentation of excess claims (37 CFR 1.16(h)-(j) or 1.492(d)-(f)).

☐ 5. Other.

Explanation (*Provide specific details of the required correction in order to assist the applicant. Indicate whether a service charge has been added to the fee due*): _____

THE AMOUNT OF THE FEE(S) DUE IS SUBJECT TO CHANGE, GENERALLY ON OCTOBER 1 OF EACH YEAR (37 CFR 1.16, 1.21 & 1.492). THE **AMOUNT OF THE FEE(S) DUE IS DETERMINED AS OF THE DATE A COMPLETE REPLY WITH THE APPROPRIATE FEE(S) IS RECEIVED BY THE OFFICE** (37 CFR 1.8 & 1.10). BECAUSE THE AMOUNT DUE IS SUBJECT TO CHANGE, IT IS RECOMMENDED THAT APPLICANT CHECK THE CURRENT FEE SCHEDULE WHICH IS AVAILABLE ON THE USPTOS WEBSITE AT: ***http://www.uspto.gov/web/offices/ac/qs/ope/fees.htm***

Service Charges: There is a $50 service charge for processing each payment refused (including a check returned unpaid) or charged back by a financial institution (37 CFR 1.21(m)). There is a $25.00 service charge for each month when the balance of a deposit account is below $1000 at the end of the month (37 CFR 1.21(b)(2)).

Technical Support Staff (TSS): /LINDA A WISE/ Phone Number: (571)272-1682

Note to TSS: Please do NOT use this notice if the application is under a final rejection.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/892,283	**02/26/2025 11:15:42 PM Z ET**	**15388FT**

Title of Invention

CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	7526	FILED BY	Aura Morrey
PATENT CENTER #	69356293	FILING DATE	09/20/2024
CUSTOMER #	82318	FIRST NAMED INVENTOR	Jason Crabtree
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Brian Galvin

Documents

TOTAL DOCUMENTS: 0

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)

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 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

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/892,283	**02/26/2025 11:15:42 PM Z ET**	**15388FT**

Title of Invention

CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	7526	FILED BY	Aura Morrey
PATENT CENTER #	69356293	AUTHORIZED BY	Brian Galvin
CUSTOMER #	82318	FILING DATE	09/20/2024
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	Jason Crabtree

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 1009	**E20252PN17139001**	**Aura Morrey**

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
1202	EACH CLAIM IN EXCESS OF 20	200.00	3	600.00
			TOTAL AMOUNT:	**$600.00**

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 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.

Examiner-Initiated Interview Summary	**Application No.** 18/892,283	**Applicant(s)** Crabtree et al.		
	Examiner CHENG-FENG HUANG	**Art Unit** 2497	**AIA (First Inventor to File) Status** Yes	**Page** 1 of 1

All Participants (applicant, applicants representative, PTO personnel)	**Title**	**Type**
CHENG-FENG HUANG	Primary Examiner	Telephonic
Brian Galvin	Attorney of Record	

Date of Interview: 18 March 2025

Issues Discussed:

35 U.S.C. 103

Examiner first thanked applicant's representative for taking this interview. Examiner then discussed the invention with applicant's representative and suggested to further amend the claims to put the application in the condition of allowance by 1) removing the word "potentially" in claim 1 to avoid ambiguity; 2) eliminating "possible" in claims 2, 3 and 29 and 3) incorporating dependent claim 20 into claim 1. Agreement was reached.

/CHENG-FENG HUANG/ Primary Examiner, Art Unit 2497	

Applicant is reminded that a complete written statement as to the substance of the interview must be made of record in the application file. It is the applicants responsibility to provide the written statement, unless the interview was initiated by the Examiner and the Examiner has indicated that a written summary will be provided. See MPEP 713.04
Please further see:
MPEP 713.04
Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews, paragraph (b)
37 CFR § 1.2 Business to be transacted in writing

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of 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.

Notice of References Cited	Application/Control No. 18/892,283	Applicant(s)/Patent Under Reexamination Crabtree et al.	
	Examiner CHENG-FENG HUANG	Art Unit 2497	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date YYYY-MM-DD	Name	CPC Classification	US Classification
*	A	US-9183387-B1	2015-11-10	Altman; Alon	H04L63/1425	1/1
*	B	US-20150020199-A1	2015-01-15	Neil; Joshua Charles	H04L63/1408	726/23
*	C	US-20100037293-A1	2010-02-11	StJohns; Michael	H04L9/3263	726/2
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date YYYY-MM-DD	Country	Name	CPC 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 YYYY-MM-DD format are publication dates. Classifications may be US or foreign.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	18/892,283	Crabtree et al.
	Examiner	**Art Unit**
	CHENG-FENG HUANG	2497

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

CLAIMS

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

CLAIM		DATE								
Final	Original	11/06/2024	03/24/2025							
1	1	✓	=							
2	2	✓	=							
3	3	✓	=							
5	4	✓	=							
6	5	✓	=							
7	6	✓	=							
8	7	✓	=							
9	8	✓	=							
10	9	✓	=							
11	10	✓	=							
12	11	✓	=							
	12	✓	-							
	13	✓	-							
13	14	✓	=							
	15	✓	-							
	16	✓	-							
14	17	✓	=							
15	18	✓	=							
16	19	✓	=							
	20	✓	-							
	21	✓	-							
	22	✓	-							
4	23	✓	=							
	24	✓	-							
	25	✓	-							
17	26	✓	=							
18	27		=							
19	28		=							
20	29		=							
21	30		=							
22	31		=							
23	32		=							
24	33		=							
25	34		=							
26	35		=							
27	36		=							
28	37		=							

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	18/892,283	Crabtree et al.
	Examiner	**Art Unit**
	CHENG-FENG HUANG	2497

CPC

Symbol					Type	Version
H04L	/	63	/	20	F	2013-01-01
H04L	/	63	/	1425	I	2013-01-01
G06F	/	16	/	951	I	2019-01-01
G06F	/	16	/	2477	I	2019-01-01
H04L	/	63	/	1441	I	2013-01-01
H04L	/	63	/	1433	I	2013-01-01
H04L	/	63	/	1466	A	2013-01-01
H04L	/	63	/	0807	A	2013-01-01

CPC Combination Sets

Symbol					Type	Set	Ranking	Version
	/		/					

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 28	
/CHENG-FENG HUANG/ Primary Examiner, Art Unit 2497 (Primary Examiner)	24 March 2025 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 1

U.S. Patent and Trademark Office

Part of Paper No.: 20250324

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	18/892,283	Crabtree et al.
	Examiner	**Art Unit**
	CHENG-FENG HUANG	2497

INTERNATIONAL CLASSIFICATION				
CLAIMED				
H04L	/	9	/	40

NON-CLAIMED				
	/		/	

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					

NONE (Assistant Examiner) (Date)		**Total Claims Allowed:** 28	
/CHENG-FENG HUANG/ Primary Examiner, Art Unit 2497 (Primary Examiner) (Date)	24 March 2025	O.G. Print Claim(s) 1	O.G. Print Figure 1

U.S. Patent and Trademark Office Part of Paper No.: 20250324

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	18/892,283	Crabtree et al.
	Examiner	**Art Unit**
	CHENG-FENG HUANG	2497

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

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	11	10	16	19	19	28	28	37						
2	2	12	11		20	20	29								
3	3		12		21	21	30								
5	4		13		22	22	31								
6	5	13	14	4	23	23	32								
7	6		15		24	24	33								
8	7		16		25	25	34								
9	8	14	17	17	26	26	35								
10	9	15	18	18	27	27	36								

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 28	
/CHENG-FENG HUANG/ Primary Examiner, Art Unit 2497 (Primary Examiner)	24 March 2025 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 1

U.S. Patent and Trademark Office Part of Paper No.: 20250324

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	18/892,283	Crabtree et al.
	Examiner	**Art Unit**
	CHENG-FENG HUANG	2497

CPC - Searched*		
Symbol	**Date**	**Examiner**
H04L63/20 or G06F16/2477 or G06F16/951 or H04L63/1425 or H04L63/1441	11/06/2024	C. H.
H04L63/20 or G06F16/2477 or G06F16/951 or H04L63/1425 or H04L63/1433 or H04L63/1441 or H04L63/0807 or H04L63/1466	03/24/2025	C. H.

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	**Date**	**Examiner**
PE2E Searches (including inventor and assignee search)	11/06/2024	C. H.
PE2E classification search (keywords combined with CPC)	11/06/2024	C. H.
PE2E Searches (including inventor and assignee search)	03/24/2025	C. H.
PE2E classification search (keywords combined with CPC)	03/24/2025	C. H.
NPL: correlating network event anomalies to identify attack information	03/24/2025	C. H.
NPL Searches with IP.com	03/24/2025	C. H.
NPL Searches with Google Patents	03/24/2025	C. H.

/CHENG-FENG HUANG/ Primary Examiner, Art Unit 2497	

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	18/892,283	Crabtree et al.
	Examiner	**Art Unit**
	CHENG-FENG HUANG	2497

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**
	General interference and searches of claim (PGPUB,USPAT)	11/06/2024	C. H.
	General interference and searches of claim (PGPUB,USPAT)	03/24/2025	C. H.

/CHENG-FENG HUANG/ Primary Examiner, Art Unit 2497	

Bibliographic Data

Application No: 18/892,283

Foreign Priority claimed: ○ Yes ◉ No

35 USC 119 (a-d) conditions met: ☐ Yes ☑ No | ☐ Met After Allowance

Verified and Acknowledged: /CHENG-FENG HUANG/ | Examiner's Signature | Initials

Title: CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
09/20/2024	726	2497	15388FT
RULE			

APPLICANTS

QOMPLX LLC, Reston, VA, UNITED STATES

INVENTORS

Jason Crabtree, Vienna, VA, UNITED STATES

Andrew Sellers, Monument, CO, UNITED STATES

Richard Kelley, Woodbridge, VA, UNITED STATES

CONTINUING DATA

This application is a CON of 17237346 04/22/2021 PAT 12206708

17237346 is a CIP of 16777270 01/30/2020 PAT 11025674

16777270 is a CIP of 16720383 12/19/2019 PAT 10944795

16720383 is a CON of 15823363 11/27/2017 PAT 10560483

15823363 is a CIP of 15725274 10/04/2017 PAT 10609079

15725274 is a CIP of 15655113 07/20/2017 PAT 10735456

15655113 is a CIP of 15616427 06/07/2017ABN

15655113 is a CIP of 15237625 08/15/2016 PAT 10248910

15237625 is a CIP of 15206195 07/08/2016ABN

15206195 is a CIP of 15186453 06/18/2016ABN

15186453 is a CIP of 15166158 05/26/2016ABN

15166158 is a CIP of 15141752 04/28/2016 PAT 10860962

15141752 is a CIP of 15091563 04/05/2016 PAT 10204147

15141752 is a CIP of 14986536 12/31/2015 PAT 10210255

15141752 is a CIP of 14925974 10/28/2015ABN

15616427 is a CIP of 14925974 10/28/2015ABN

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

09/30/2024

STATE OR COUNTRY

UNITED STATES

ADDRESS

Brian Galvin
Galvin Patent Law LLC
2916 NW Bucklin Hill Road
Suite 485
Silverdale, WA 98383
UNITED STATES

FILING FEE RECEIVED

$6,160

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1	12	"18892283"	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/05 06:46 PM
L2	2	"17237346"	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/06 10:15 AM
L3	76	((("QOMPLX") near3 ("LLC"))).AS,AANM.	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/06 10:21 AM
L4	658	((("CRABTREE") near3 ("Jason")) OR (("SELLERS") near3 ("Andrew")) OR (("KELLEY") near3 ("Richard"))).INV.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2024/11/06 10:21 AM
L5	1355	3 4	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO,	OR	ON	ON	2024/11/06 10:21 AM

			RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L6	405	5 AND (directed near2 graph)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; IBM_TDB)	OR	ON	ON	2024/11/06 10:22 AM
L7	103	5 AND (directed near2 graph).clm.	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; IBM_TDB)	OR	ON	ON	2024/11/06 10:22 AM
L8	250	("10204147"|"10210255"|"10572828"|"10860951"|"10860962"|"10884999"|"11023284"|"11055451"|"20050005272"|"20170109678"|"20170322959"|"20180103088"|"20180300930"|"20190082305"|"20220012093"|"10061635"|"10242406"|"10248910"|"10367829"|"20030041254"|"20030145225"|"20070150744"|"20090089227"|"20090182672"|"20090222562"|"20090293128"|"20110087888"|"20120266244"|"20130073062"|"20130132149"|"20130191416"|"20130304623"|"20140156806"|"20140244612"|"20140279762"|"20150149979"|"20150163242"|"20150169294"|"20150195192"|"20150236935"|"20150281225"|"20150317481"|"20150339263"|"20150347414"|"20150379424"|"20160028758"|"20160072845"|"20160078361"|"20160105454"|"20160140519"|"20160275123"|"20160285732"|"20160350442"|"20160364307"|"20170019678"|"20170063896"|"20170126712"|"20170139763"|"20170149802"|"20170193110"|"20170322959"|"20170323089"|"20180197128"|"20180300930"|"20190082305"|"5669000"|"6256544"|"6477572"|"8281121"|"8615800"|"8793758"|"8914878"|"923	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/06 10:28 AM

		1962"|"9602530"|"9654495"|"9686308"|"9762443"|"9887933").PN.					
L9	10	8 AND (directed near2 graph).clm.	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; IBM_TDB)	OR	ON	ON	2024/11/06 10:30 AM
L10	1	9 AND @ad<"20151028"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; IBM_TDB)	OR	ON	ON	2024/11/06 10:30 AM
L11	13	"20110066590"	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/06 10:31 AM
L12	1	"20110066590"	(US-PGPUB)	OR	ON	ON	2024/11/06 10:32 AM
L13	50	("10204147"|"10210255"|"10572828"|"10860951"|"10860962"|"10884999"|"11023284"|"11055451"|"20050005272"|"20170109678"|"20170322959"|"20180103088"|"20180300930"|"20190082305"|"20220012093"|"10061635"|"10242406"|"10248910"|"10367829"|"20030041254"|"20030145225"|"20070150744"|"20090089227"|"20090182672"|"20090222562"|"20090293128"|"20110087888"|"20120266244"|"20130073062"|"20130132149"|"20130191416"|"20130304623"|"20140156806"|"20140244612"|"20140279762"|"20150149979"|"20150163242"|"20150169294"|"20150195192"|"20150236935"|"20150281225"|"20150317481"|"20150339263"|"20150347414"|"20150379424"|"20	(US-PGPUB)	OR	ON	ON	2024/11/06 10:37 AM

		160028758"|"20160072845"|"20160078361"|"20160105454"|"20160140519"|"20160275123"|"20160285732"|"20160350442"|"20160364307"|"20170019678"|"20170063896"|"20170126712"|"20170139763"|"20170149802"|"20170193110"|"20170322959"|"20170323089"|"20180197128"|"20180300930"|"20190082305"|"5669000"|"6256544"|"6477572"|"8281121"|"8615800"|"8793758"|"8914878"|"9231962"|"9602530"|"9654495"|"9686308"|"9762443"|"9887933").PN.					
L14	323751	(H04L63/20 or G06F16/2477 or G06F16/951 or H04L63/1425 or H04L63/1441).cpc.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/06 10:39 AM
L15	503	14 AND (directed near2 graph).clm.	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; IBM_TDB)	OR	ON	ON	2024/11/06 10:39 AM
L16	197	15 AND (anomalous malicious malevolent) AND stream$3 AND (node edge)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/06 10:46 AM
L17	17	16 AND	(US-PGPUB; USPAT;	OR	ON	ON	2024/11/06

		@ad<"20151028"	USOCR; FPRS; EPO; JPO; IBM_TDB)				10:46 AM
L18	13	17 AND (graph WITH (node edge)) AND graph AND memory	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; IBM_TDB)	OR	ON	ON	2024/11/06 03:22 PM
L19	10	"20150020199" AND memory WITH graph	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/06 03:31 PM
L20	10	"20150020199" AND memory WITH graph AND graph	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/06 03:37 PM
L21	6	17 AND ((add$3 subtract$3 modif$7) WITH (node edge)) AND graph	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; IBM_TDB)	OR	ON	ON	2024/11/07 07:59 AM
L22	1	1 AND (sensitive resource)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT;	OR	ON	ON	2024/11/07 09:17 AM

			IBM_TDB)				
L23	19	"20150020199" AND node	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/07 09:50 AM
L24	4	14 AND (bogus near2 node)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; IBM_TDB)	OR	ON	ON	2024/11/07 09:56 AM
L25	0	(travers$3 near3 graph WITH identif$7 near3 origin near3 (anomalous ADJ event))	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; IBM_TDB)	OR	ON	ON	2024/11/07 02:39 PM
L26	7	1 AND (physical logical connect$3)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/11/25 12:12 PM
L27	114996	((add$3 subtract$3 modif$7) WITH (node edge)) AND graph	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; IBM_TDB)	OR	ON	ON	2024/11/25 12:47 PM
L28	12	"18892283"	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK,	OR	ON	ON	2025/01/15 04:00 PM

			TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L29	13	"18892283"	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2025/03/24 03:48 PM
L30	408348	(H04L63/20 or G06F16/2477 or G06F16/951 or H04L63/1425 or H04L63/1433 or H04L63/1441 or H04L63/0807 or H04L63/1466).cpc.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2025/03/24 05:20 PM
L31	0	((generat$3 near2 report) WITH (identification near2 (first ADJ entity) near4 ((second third) ADJ entity))).clm.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2025/03/24 05:32 PM
L32	0	30 AND ((generat$3 near2 report) WITH (identification WITH ((first second third) ADJ	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; IBM_TDB)	OR	ON	ON	2025/03/24 05:32 PM

		entity)))					
L33	60545	((add$3 subtract$3 modif$7) WITH (node edge)) AND (graph WITH (node edge)) AND graph	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; IBM_TDB)	OR	ON	ON	2025/03/24 06:15 PM
L34	3778	30 AND ((add$3 subtract$3 modif$7) WITH (node edge)) AND (graph WITH (node edge)) AND graph	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; IBM_TDB)	OR	ON	ON	2025/03/24 06:16 PM
L35	0	4 AND ((generat$3 near2 report) WITH (identification WITH ((first second third))))	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; IBM_TDB)	OR	ON	ON	2025/03/24 06:16 PM

PE2E SEARCH - Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
N1	0	(travers$3 near3 graph WITH identif$7 near3 origin near3 (anomalous ADJ event)).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2024/11/07 02:39 PM
N2	1	(travers$3 near3 graph WITH identif$7 near3 origin near3 (anomalous ADJ event)).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2025/03/24 05:28 PM
N3	0	((generat$3 near2 report) WITH (identification near2 (first ADJ entity) near4 ((second third) ADJ entity))).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2025/03/24 05:32 PM

Discover +IP Analysis correlating network event anomalies to ide... STIC

Visuals

1 - 50 5,712,868 results

1. Challenges in Identifying Network Attacks Using Netflow Data

Large networks often encounter attacks that can affect the network availability. While multiple techniques exist to detect network attacks, a comprehensive understanding of how an attack occurs considering the various layers and components of the network software stack, can be an important element...

IEEE Xplore | IEEE Conferences | 2021-11-23 | 4 | 2021 IEEE 20th International Symposium on Network Computing and Applications (NCA) (2021), Page(s): 1-10

2. **Correlation-Based Anomaly Detection in Industrial Control Systems**

Industrial Control Systems (ICSs) were initially designed to be operated in an isolated network. However, recently, ICSs have been increasingly connected to the Internet to expand their capability, such as remote management. This interconnectivity of ICSs exposes them to cyber-attacks. At the same...

PMC9926748 | PubMed Central | 2023-02-01 | 4 | Sensors (Basel, Switzerland), 23(3), 1561

3. **Anomaly detection in IP networks**

Network anomaly detection is a vibrant research area. Researchers have approached this problem using various techniques such as artificial intelligence, machine learning, and state machine modeling. In this paper, we first review these anomaly detection methods and then describe in detail a...

IEEE Xplore | IEEE Periodicals | 2003-08-01 | 4 | IEEE Transactions on Signal Processing

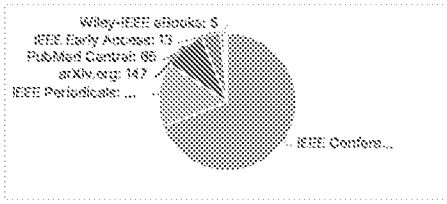
4. **Reducing false positives through fuzzy alert correlation in collaborative intelligent intrusion detection systems --- A review**

As complete prevention of computer attacks is not possible, Intrusion detection systems (IDS) play a very important role in minimizing the damage caused by different computer attacks. There are two intrusion detection methods: namely misuse- and anomaly-based. A collaborative intelligent intrusion...

IEEE Xplore | IEEE Conferences | 2010-07-01 | 4 | International Conference on Fuzzy Systems (2010), Page(s): 1-8

Relevance

Collections



Publication Date

More Visuals

Keyboard Shortcuts Result 1

Patents correlating network event anomalies to identify attack information

(correlating network event anomalies to identify attack information);

More than 100,000 results Download Side-by-si

Sort by · Relevance · Group by · None · Deduplicate by · Family · Results / page · 10 ·

CIDD: A cloud intrusion detection dataset for cloud computing and masquerade attacks

Google Scholar · www.academia.edu · Khalidy H · 2012 Ninth International Conference on Information Technology-New Generations

Published 2012

... The parser extracts from the security event log files the following parameters: type (audit ... of the outside network or outside the simulation network. Part 2 testing data has the same attack ...

Security situation analysis method and graph device using graph representation ...

KR · KR100609792B1 · 이수형 · 한국전자통신연구원

Priority 2004-11-10 · Filed 2004-11-10 · Granted 2006-08-09 · Published 2006-08-09

Security situation analysis method and apparatus using a graph representation of the network event according to the present invention comprises the steps of collecting network traffic information and security-related event information; Extracting security-related characteristic information from ...

Multi-step attack detection method based on multi-source anomalous event ...

CN · CN106790186A · 郭晓晓 · 中国人民解放军信息工程大学

Priority 2016-12-30 · Filed 2016-12-30 · Published 2017-05-31

Multi-step attack detection method based on correlation analysis of multi-source anomaly events technical field The invention belongs to the technical field of network security, in particular to a multi-step attack detection method based on correlation analysis of multi-source abnormal events.

Methods and systems for internet protocol (IP) packet header collection and ...

US · US9848004B2 · Stephen Knapp · The Boeing Company

Priority 2008-08-20 · Filed 2014-07-09 · Granted 2017-12-19 · Published 2017-12-19

A computer-based method for providing information about a potential security incident ascertained from received internet protocol (IP) packets is described. The method includes capturing IP packets from a network, stripping packet header data from the captured IP packets, calculating a cyclic ...

Network behavior data collection and analysis for anomaly detection

WO EP US CN · CN113766339B · 帕洛阿尔托网络公司 · 帕洛阿尔托公司

Priority 2015-06-04 · Filed 2016-05-16 · Granted 2021-08-13 · Published 2021-08-13

In one embodiment, a method comprises: receiving, at an analysis module running at a network device, network traffic data collected from a plurality of sensors distributed throughout a network and installed in a network component to obtain network traffic data from packets sent to and from the ...

Method and system for reviewing identified threats for performing computer ...

US · US10212174B2 · Sudhakar Muddu · Splunk Inc.

Priority 2015-08-31 · Filed 2015-10-30 · Granted 2019-02-19 · Published 2019-02-19

A security platform employs a variety techniques and mechanisms to detect security related anomalies and threats in a computer network environment. The security platform is "big data" driven and employs machine learning to perform security analytics. The security platform performs user/entity ...

Analysis of time series data

WO US AU · AU2013302297B2 · Michael Baker · Mts Consulting Pty Limited

Priority 2012-08-13 · Filed 2013-08-09 · Granted 2020-04-30 · Published 2020-04-30

A data model, methods, software, user interfaces and a computer system for the analysis of time series data, particularly, but not limited to, the analysis of the data packets sent on a computer network to identify security risks, which consist of a datastore (110) for network traffic, map/reduce ...

A method for detecting anomaly action within a computer network

WO EP US · EP2737404A1 · Glenn Engel · Light Cyber Ltd

Priority 2011-07-26 · Filed 2012-07-25 · Published 2014-06-04

A method and system for detecting anomalous action within a computer network is provided herein. The method starts with collecting raw data from at least one probe sensor that is associated with at least one router, switch or at least one server which are part of the computer network. Next, the ...

Methods and systems for anomaly detection using internet protocol (IP) traffic ...

US · US7930356B2 · Stephen Knapp · The Boeing Company

Priority 2008-08-20 · Filed 2008-08-20 · Granted 2011-03-08 · Published 2011-03-08

A computer-based method for detecting anomalies in the traffic passing through an internet protocol (IP) network is described. The method includes extracting, from a database, a single instance of each unique packet header associated with a plurality of IP-to-IP packets, the IP-to-IP packets ...

A survey of network anomaly detection techniques

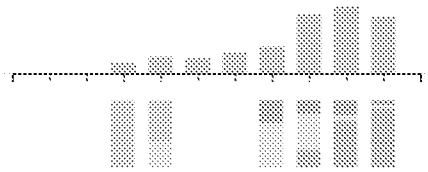
Google Scholar - www.sciencedirect.com - Ahmed M - Journal of Network and Computer Applications

Published 2016

... , in this section we identify the relationship among the attacks and anomalies. The DoS ... attack as collective anomaly. Probe attacks are based on specific intention to attain information ...

Next > >> More than 100,000 results

Top 1000 results by filing date



Relative count of top 5 values

Assignees	Inventors	CPCs
Gompix, Inc.		3
Darktrace Holdings Limited		2
Cisco Technology, Inc.		
Splunk Inc.		1
Riverbed Technology, Inc.		1

Expand

Related landscapes

Engineering & Computer Science

General Engineering & Computer Science

Computer Hardware Design

About Send Feedback Public Datasets Terms Privacy Policy Help

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

82318 7590 04/07/2025
Brian Galvin
Galvin Patent Law LLC
2916 NW Bucklin Hill Road
Suite 485
Silverdale, WA 98383

EXAMINER
HUANG, CHENG-FENG

ART UNIT	PAPER NUMBER
2497	

DATE MAILED: 04/07/2025

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
18/892,283	09/20/2024	Jason Crabtree	15388FT	7526

TITLE OF INVENTION: CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1290	$0.00	$0.00	$1290	07/07/2025

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 40% the amount of undiscounted fees, and micro entity fees are 20% the amount of undiscounted 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. 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: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via the USPTO patent electronic filing system.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (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 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. **Because electronic patent issuance may occur shortly after issue fee payment, any desired continuing application should preferably be filed prior to payment of this issue fee in order not to jeopardize copendency.**

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

82318 7590 04/07/2025

Brian Galvin
Galvin Patent Law LLC
2916 NW Bucklin Hill Road
Suite 485
Silverdale, WA 98383

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 transmitted to the USPTO via the USPTO patent electronic filing system or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
18/892,283	09/20/2024	Jason Crabtree	15388FT	7526

TITLE OF INVENTION: CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1290	$0.00	$0.00	$1290	07/07/2025

EXAMINER	ART UNIT	CLASS-SUBCLASS
HUANG, CHENG-FENG	2497	726-022000

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/AIA/122 or PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or 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 must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). 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. Fees submitted: ❑Issue Fee ❑Publication Fee (if required)

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

❑ Electronic Payment via the USPTO patent electronic filing system ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

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. _____

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.
18/892,283	09/20/2024	Jason Crabtree	15388FT	7526

82318 7590 04/07/2025

Brian Galvin
Galvin Patent Law LLC
2916 NW Bucklin Hill Road
Suite 485
Silverdale, WA 98383

EXAMINER
HUANG, CHENG-FENG

ART UNIT	PAPER NUMBER
2497	

DATE MAILED: 04/07/2025

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.

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 30 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. The United States Patent and Trademark Office (USPTO) collects the information in this record under authority of 35 U.S.C. 2. The USPTO's system of records is used to manage all applicant and owner information including name, citizenship, residence, post office address, and other information with respect to inventors and their legal representatives pertaining to the applicant's/owner's activities in connection with the invention for which a patent is sought or has been granted. The applicable Privacy Act System of Records Notice for the information collected in this form is COMMERCE/PAT-TM-7 Patent Application Files, available in the Federal Register at 78 FR 19243 (March 29, 2013).
https://www.govinfo.gov/content/pkg/FR-2013-03-29/pdf/2013-07341.pdf

Routine uses of the information in this record may include disclosure to:

1) law enforcement, in the event that the system of records indicates a violation or potential violation of law;
2) a federal, state, local, or international agency, in response to its request;
3) a contractor of the USPTO having need for the information in order to perform a contract;
4) the Department of Justice for determination of whether the Freedom of Information Act (FOIA) requires disclosure of the record;
5) a Member of Congress submitting a request involving an individual to whom the record pertains, when the individual has requested the Member's assistance with respect to the subject matter of the record;
6) a court, magistrate, or administrative tribunal, in the course of presenting evidence, including disclosures to opposing counsel in the course of settlement negotiations;
7) the Administrator, General Services Administration (GSA), or their designee, during an inspection of records conducted by GSA under authority of 44 U.S.C. 2904 and 2906, in accordance with the GSA regulations and any other relevant (i.e., GSA or Commerce) directive, where such disclosure shall not be used to make determinations about individuals;
8) 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));
9) the Office of Personnel Management (OPM) for personnel research purposes; and
10) the Office of Management and Budget (OMB) for legislative coordination and clearance.

If you do not furnish the information requested on this form, the USPTO may not be able to process and/or examine your submission, which may result in termination of proceedings, abandonment of the application, and/or expiration of the patent.

Notice of Allowability	Application No. 18/892,283	Applicant(s) Crabtree et al.	
	Examiner CHENG-FENG HUANG	Art Unit 2497	AIA (FITF) Status Yes

-- 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 02/13/2025.
   ☐ 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 See Continuation Sheet . 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 _____.
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 _____.

/CHENG-FENG HUANG/
Primary Examiner, Art Unit 2497

Continuation of 3. The allowed claim(s) is/are: 1-11,14,17-19,23 and 26-37

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Response to Amendment

2. This communication is in response to applicant's amendment filed on 02/13/2025. Claims 1-11, 14, 17-20, 23, and 26-37 are pending for examination. Claims 1-10, 20, and 23 have been amended. Claims 27-37 are newly added. Claims 12-13, 15-16, 21-22, and 24-25 are canceled

Response to Arguments

Claim Objection:

3. Applicant's arguments with respect to objection of claim(s) 1 have been considered. The objection of claim(s) 1 have been withdrawn in view of the amendment to claim.

Claim Rejections - 35 U.S.C. § 101:

4. Applicants' arguments with respect to claim(s) 1-26 have been fully considered and are persuasive. The rejection of 35 USC §101 regarding claim(s) 1-26 have been withdrawn in view of the amendment to claim.

Double Patenting (DP):

5. Applicant submitted an eTD on 02/13/2025 to overcome DP rejection issued in the previous office action. The eTD has been approved. The DP rejection issued in the previous action has been withdrawn.

Claim Rejections - 35 U.S.C. § 103:

6. Applicants' arguments with respect to claims rejected under prior art have been fully considered and the rejection of 35 U.S.C. § 103 have been withdrawn in view of the examiner's amendment to claim.

EXAMINER'S AMENDMENT

7. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

8. Authorization for this examiner's amendment was given in a telephone interview with Attorney Brian R. Galvin (Reg. No. 50,966) on 03/18/2025 and followed up on 03/21/2025.

The application has been amended as follows:

- ***Please replace claim 1 with:***

1. (Currently Amended) A computer system comprising:

a hardware memory, wherein the computer system is configured to execute

software instructions stored on nontransitory machine-readable storage media comprising software instructions that:

store in the hardware memory a representation of a first graph, wherein the representation of the first graph comprises representations of a first plurality of nodes corresponding to a first plurality of entities and further comprises representations of a first plurality of edges, wherein the first graph is a directed graph,

wherein the first plurality of entities comprises a plurality of accounts and a plurality of resources, and

wherein each edge of the first plurality of edges corresponds to a respective relationship between a respective pair of entities;

receive streaming data comprising time-stamped data about events relating to one or more entities of the first plurality of entities,

based on a first portion of the streaming data, identify a first entity that does not correspond to any of the first plurality of nodes, wherein the first entity is not of the first plurality of entities,

based on a second portion of the streaming data, wherein the second portion is not identical to the first portion, identify a first relationship between a pair of entities of the first plurality of entities that does not correspond to any of the first plurality of edges,

modify, in the hardware memory, the representation of the first graph to generate a modified representation of the first graph, wherein the modified representation of the first graph comprises a representation of a first node

corresponding to the first entity and a representation of a first edge corresponding to the first relationship, wherein the first node is not of the first plurality of nodes and the first edge is not of the first plurality of edges,

identify, based on the modified representation of the first graph, an attack path <u>that could be involved in an attack</u> involving the first entity, wherein identifying the attack path comprises<u>:</u>

identifying a second entity that can ~~potentially~~ be ~~accessed~~ <u>reached</u> using the first entity, wherein the second entity corresponds to a second node, and the second node is related by one or more edges to the first node corresponding to the first entity in the modified representation of the first graph; and,

<u>identifying a third entity that can be reached using the second entity, wherein the third entity corresponds to a third node, and the third node is related by one or more edges to the second node in the modified representation of the first graph; and</u>

generate a report comprising an identification of ~~at least one of~~ the first entity and <u>at least one of</u> the second entity <u>and the third entity</u>.

- ***Please replace claim 2 with:***

2. (Currently Amended) The computer system of claim 1, wherein identifying the attack path further comprises:

identifying a first plurality of ~~possible~~ event flows ~~for~~ <u>that include</u> a first anomalous event associated with the first entity.

- ***Please replace claim 3 with:***

3. (Currently Amended) The system of claim 2, wherein identifying the attack path further comprises:

identifying a point of origin for the first anomalous event based on the first plurality of ~~possible~~ event flows.

- ***Please cancel claim 20;***

- ***Please replace claim 29 with:***

29. (Currently Amended) The computer system of claim 27, wherein identifying the second plurality of attack paths comprises:

identifying a first plurality of ~~possible~~ event flows <u>that could</u> involve[[ing]] the first entity, and

identifying a first plurality of dependencies associated with the first plurality of event flows.

Allowable Subject Matter

9. Claims 1-11, 14, 17-19, 23, and 26-37 are allowed.

10. The following is an examiner's statement of reasons for allowance:

Independent Claim(s) and their respective dependent claims are allowable over prior arts since the prior arts taken individually or in combination fails to particular discloses, fairly suggest or render obvious the following italic limitations:

In regards to claim(s) 1, the prior art of record (Neil et al. (US 2015/0020199 A1; hereinafter Neil) in view of Altman et al. (US 9,183,387 B1; hereinafter Altman)) does not disclose:

"***identify, based on the modified representation of the first graph, an attack path that could be involved in an attack involving the first entity, wherein identifying the attack path comprises:***

identifying a second entity that can be reached using the first entity, wherein the second entity corresponds to a second node, and the second node is related by one or more edges to the first node corresponding to the first entity in the modified representation of the first graph; and,

identifying a third entity that can be reached using the second entity, wherein the third entity corresponds to a third node, and the third node is related by one or more edges to the second node in the modified representation of the first graph; and

generate a report comprising an identification of the first entity and at least one of the second entity and the third entity" in combination with other limitations recited as specified in the independent claim(s).

In regards to claim(s) 27, the prior art of record (Neil et al. (US 2015/0020199 A1; hereinafter Neil) in view of Altman et al. (US 9,183,387 B1; hereinafter Altman)) does not disclose:

"***based on a first portion of the streaming data, identify a third entity that does not correspond to any of the first plurality of nodes, wherein the third entity is not of the first plurality of entities,***

based on a second portion of the streaming data, wherein the second portion is not identical to the first portion, identify a first relationship between a pair of entities of the first plurality of entities that does not correspond to any of the first plurality of edges,

modify, in the hardware memory, the representation of the first graph to generate a modified representation of the first graph, wherein the modified representation of the first graph comprises a representation of a node corresponding to the third entity and an edge corresponding to the first relationship, wherein the node is not of the first plurality of nodes and the edge is not of the first plurality of edges, and

identify, based on the modified representation of the first graph, a second plurality of attack paths comprising the first entity, wherein each attack path of the second plurality of attack paths targets the second entity, and wherein an attack path of the second plurality of attack paths comprises the third entity" in combination with other limitations recited as specified in the independent claim(s).

Rather, Neil discloses "*detecting anomalous behavior in a network*" ([0010-0026], and [0036]). Similarly, Altman teaches "*detecting online attacks*" (Col 8 Lines 11-14). Accordingly, the claims are allowed.

11. 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

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHENG-FENG HUANG whose telephone number is (571)272-6186. The examiner can normally be reached Monday-Friday: 9 am - 5 pm.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Eleni A Shiferaw can be reached on (571) 272-3867. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: https://patentcenter.uspto.gov. Visit https://www.uspto.gov/patents/apply/patent-center for more information about Patent Center and https://www.uspto.gov/patents/docx for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197

(toll-free). If you would like assistance from a USPTO Customer Service

Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/CHENG-FENG HUANG/
Primary Examiner, Art Unit 2497

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via the USPTO patent electronic filing system.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (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 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. **Because electronic patent issuance may occur shortly after issue fee payment, any desired continuing application should preferably be filed prior to payment of this issue fee in order not to jeopardize copendency.**

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

82318 7590 04/07/2025

Brian Galvin
Galvin Patent Law LLC
2916 NW Bucklin Hill Road
Suite 485
Silverdale, WA 98383

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 transmitted to the USPTO via the USPTO patent electronic filing system or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)

(Signature)

(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
18/892,283	09/20/2024	Jason Crabtree	15388FT	7526

TITLE OF INVENTION: CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1290	$0.00	$0.00	$1290	07/07/2025

EXAMINER	ART UNIT	CLASS-SUBCLASS
HUANG, CHENG-FENG	2497	726-022000

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/AIA/122 or PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or 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 Galvin Patent Law LLC
2 Brian R. Galvin
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 must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: QOMPLX LLC

(B) RESIDENCE: (CITY and STATE OR COUNTRY): RESTON, VIRGINIA

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

4a. Fees submitted: ☒ Issue Fee ☐ Publication Fee (if required)

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

☒ Electronic Payment via the USPTO patent electronic filing system ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. .....

5. **Change in Entity Status** (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

☐ Applicant asserting small entity status. See 37 CFR 1.27

☐ Applicant changing to regular undiscounted fee status.

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.

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.

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 /BRIAN R. GALVIN/ Date April 7, 2025

Typed or printed name Brian R. Galvin Registration No. 50,966

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/892,283	**04/07/2025 07:40:27 PM Z ET**	**15388FT**

Title of Invention

CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	7526	FILED BY	Aura Morrey
PATENT CENTER #	69904132	FILING DATE	09/20/2024
CUSTOMER #	82318	FIRST NAMED INVENTOR	Jason Crabtree
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Brian Galvin

Documents

TOTAL DOCUMENTS: 1

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
250407_15388FT_Issue Fee Form_AS_FILED.pdf	1	Issue Fee Payment (PTO-85B)	847 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
250407_15388FT_Issue Fee Form_AS_FILED.pdf	03F38491D914D0188A6A1212C4528D2A581C3DFDA79FBACD9B47CFBDE71052C9B6BBDDD913338B6DB6EAA934F599764E26F0A88B9EFAB67B16D9E32A9D35DF1F

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 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

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/892,283	**04/07/2025 07:40:27 PM Z ET**	**15388FT**

Title of Invention

CORRELATING NETWORK EVENT ANOMALIES USING ACTIVE AND PASSIVE EXTERNAL RECONNAISSANCE TO IDENTIFY ATTACK INFORMATION

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	7526	FILED BY	Aura Morrey
PATENT CENTER #	69904132	AUTHORIZED BY	Brian Galvin
CUSTOMER #	82318	FILING DATE	09/20/2024
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	Jason Crabtree

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 1009	**E202547J41347605**	**Aura Morrey**

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
1501	UTILITY ISSUE FEE	1290.00	1	1290.00
			TOTAL AMOUNT:	**$1,290.00**

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 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.
18/892,283	05/13/2025	12301627	15388FT	7526

82318 7590 04/30/2025

Brian Galvin
Galvin Patent Law LLC
2916 NW Bucklin Hill Road
Suite 485
Silverdale, WA 98383

ISSUE NOTIFICATION

The projected patent number and issue date are specified above. The patent will issue electronically. The electronically issued patent is the official patent grant pursuant to 35 U.S.C. § 153. The patent may be accessed on or after the issue date through Patent Center at https://patentcenter.uspto.gov/. The patent will be available in both the public and the private sides of Patent Center. Further assistance in electronically accessing the patent, or about Patent Center, is available by calling the Patent Electronic Business Center at 1-888-217-9197.

The USPTO is implementing electronic patent issuance with a transition period, during which period the USPTO will mail a ceremonial paper copy of the electronic patent grant to the correspondence address of record. Additional copies of the patent (i.e., certified and presentation copies) may be ordered for a fee from the USPTO's Certified Copy Center at https://certifiedcopycenter.uspto.gov/index.html. The Certified Copy Center may be reached at (800)972-6382.

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 0 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 Center (https://patentcenter.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 Patents Stakeholder Experience (OPSE), Stakeholder Support Division (SSD) at (571)-272-4200.

INVENTOR(s) (Please see PATENT CENTER site https://patentcenter.uspto.gov for additional inventors):

Jason Crabtree, Vienna, VA;
Andrew Sellers, Monument, CO;
Richard Kelley, Woodbridge, VA;

APPLICANT(s) (Please see PATENT CENTER site https://patentcenter.uspto.gov for additional applicants):

QOMPLX LLC, Reston, VA;

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.

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.
18/892,283	09/20/2024	Jason Crabtree	15388FT	7526

82318 7590 05/13/2025
Brian Galvin
Galvin Patent Law LLC
2916 NW Bucklin Hill Road
Suite 485
Silverdale, WA 98383

EXAMINER
HUANG, CHENG-FENG

ART UNIT	PAPER NUMBER
2497	

NOTIFICATION DATE	DELIVERY MODE
05/13/2025	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):

USPTO@GALVINPATENTLAW.COM
eofficeaction@appcoll.com

APPLICATION NO.	ISSUE DATE	PATENT NO.
18/892,283	13-May-2025	12301627

Brian Galvin
Galvin Patent Law LLC
2916 NW Bucklin Hill Road
Silverdale, WA 98383

EGRANT NOTIFICATION

Your electronic patent grant (eGrant) is now available, which can be accessed via Patent Center at https://patentcenter.uspto.gov

The electronic patent grant is the official patent grant under 35 U.S.C. 153. For more information, please visit https://www.uspto.gov/electronicgrants