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
63/150,664	02/18/2021	Gal Engelberg	12587-0887P01

CONFIRMATION NO. 2805

198326
POLSINELLI PC / Accenture Global Services Limited
PO Box 140310
KANSAS CITY, MO 64114-0310

POA ACCEPTANCE LETTER

OC000000073722477

Date Mailed: 06/11/2024

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 05/30/2024.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

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**.

/zabraha/

WIZ, Inc. EXHIBIT - 1007
WIZ, Inc. v. Orca Security LTD.

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82A (07-13)
Approved for use through 03/31/2021. OMB 0651-0035
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.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	63/150,664
Filing Date	2021-02-18
First Named Inventor	Gal Engelberg
Title	AUTOMATED PRIORITIZATION OF PROCESS-AWARE CYBER RISK MITIGATION
Art Unit	N/A
Examiner Name	N/A
Attorney Docket Number	12587-0887PO1

SIGNATURE of Applicant or Patent Practitioner

Signature	/Andrew Z. Weaver/	Date (Optional)	
Name	Andrew Z. Weaver	Registration Number	56,468
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			

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

☐ *Total of _____ 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.

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82B (07-13)
Approved for use through 09/30/2025. OMB 0651-0035
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: 198326

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):

ACCENTURE GLOBAL SOLUTIONS LIMITED

☐ 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	Renju	Date (Optional)	
Name	Renju Harikumar		
Title	Director Intellectual Property, Accenture		

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 forms are submitted.

A Federal agency may not conduct or sponsor, and a person is not required to respond to, nor shall a person be subject to a penalty for failure to comply with an information collection subject to the requirements of the Paperwork Reduction Act of 1995, unless the information collection has a currently valid OMB Control Number. The OMB Control Number for this information collection is 0651-0035. Public burden for this form is estimated to average 3 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the information collection. Send comments regarding this burden estimate or any other aspect of this information collection, including suggestions for reducing this burden to the Chief Administrative Officer, United States Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450 or email InformationCollection@uspto.gov. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.** If filing this completed form by mail, 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 ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
63/150,664	**05/30/2024 08:21:37 PM Z ET**	**12587-0887P01**

Title of Invention

AUTOMATED PRIORITIZATION OF PROCESS-AWARE CYBER RISK MITIGATION

Application Information

APPLICATION TYPE	Utility - Provisional Application under 35 USC 111(b)	PATENT #	-
CONFIRMATION #	2805	FILED BY	SUSAN BREWER
PATENT CENTER #	65743590	FILING DATE	02/18/2021
CUSTOMER #	26212	FIRST NAMED INVENTOR	Gal Engelberg
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Andrew Weaver

Documents

TOTAL DOCUMENTS: 2

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
12587-0887PO1 ACCENTURE GLOBAL SOLUTIONS LIMITED - POA signed.pdf	2	Power of Attorney	682 KB
12587-0887PO1 3.73c Statement - ACCENTURE GLOBAL SOLUTIONS LIMITED.pdf	3	Assignee showing of ownership per 37 CFR 3.73	110 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)

12587-0887PO1 ACCENTURE GLOBAL SOLUTIONS LIMITED - POA signed.pdf	87A06E9A28157673 0A792A579487C12BF672E70D618A086B3BE9BF84F2B11F7990C0B590D3C99F1B3C34370E1339F9D4952218FC07DDE1E5A4A2AF21E1628201
12587-0887PO1 3.73c Statement - ACCENTURE GLOBAL SOLUTIONS LIMITED.pdf	109C211A1509F6C1F1C4B6234C88A2F07CA5B3338D1AADF1BA92930A8367B5F4FB9BBB18C198BB0DD71093CE8123789F80E67CA920B4C7A33B69DF5B5D66A846

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.

PTO/AIA/96 (08-12)
Approved for use through 11/30/2020. 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 displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: ACCENTURE GLOBAL SOLUTIONS LIMITED

Application No./Patent No.: 63/150,664 Filed/Issue Date: 2021-02-18

Titled: AUTOMATED PRIORITIZATION OF PROCESS-AWARE CYBER RISK MITIGATION

ACCENTURE GLOBAL SOLUTIONS LIMITED, a Corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☑ The assignee of the entire right, title, and interest.

2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):

   ☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

   ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (*e.g.*, bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

A. ☐ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: _____ To: _____

   The document was recorded in the United States Patent and Trademark Office at

   Reel _____, Frame _____, or for which a copy thereof is attached.

2. From: _____ To: _____

   The document was recorded in the United States Patent and Trademark Office at

   Reel _____, Frame _____, or for which a copy thereof is attached.

This collectionof information is required by 37CFR 3.73(b). The informationis required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application.Confidentiality isgoverned by 35U.S.C. 122 and37 CFR 1.11and 1.14.This collection is estimated to take 12 minutes to complete, including gathering,preparing, and submitting the completed applicationform 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 besent 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 COMPLETEDFORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA22313-1450** .

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

PTO/AIA/96 (08-12)
Approved for use through 11/30/2020. 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 displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☑ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Andrew Z. Weaver/	2024-05-30
Signature	Date
Andrew Z. Weaver	56,468
Printed or Typed Name	Title or Registration Number

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requiresthat you begiven certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirementsof the Act, please be advised that: (1)the general authority for the collectionof this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary;and (3) the principalpurpose for whichthe informationis used by the U.S. Patent and Trademark Office is to process and/or examine your submission related toa patent application or patent. If you do not furnishthe requested information, the U.S. Patent and Trademark Officemay not be able to process and/or examine yoursubmission, which may result in termination of proceedings orabandonment of the application or expiration of the patent.

Theinformation 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 forthe 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 recordrelated 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 recordfrom 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

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
63/150,664	02/18/2021		300	12587-0887P01		

CONFIRMATION NO. 2805

FILING RECEIPT

26212
FISH & RICHARDSON P.C. (ACCENTURE)
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

OC000000124146192

Date Mailed: 03/17/2021

Receipt is acknowledged of this provisional patent application. It will not be examined for patentability and will become abandoned not later than twelve months after its filing date. 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 identifying the requested changes, preferably by 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)

Gal Engelberg, Pardes-hana, ISRAEL;
Dan Klein, Rosh Ha'ayin, ISRAEL;
Tomer Ram, Netanya, ISRAEL;

Applicant(s)

Accenture Global Solutions Limited, DUBLIN, IRELAND

Power of Attorney:
Ryan McCarthy--50636

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: 03/16/2021

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 63/150,664**

Projected Publication Date: None, application is not eligible for pre-grant publication

Non-Publication Request: No

Early Publication Request: No
Title

AUTOMATED PRIORITIZATION OF PROCESS-AWARE CYBER RISK MITIGATION

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.

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

Express Mail Label No. _____

INVENTOR(S)		
Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
Gal Dan Tomer	Engelberg Klein Ram	Pardes-hana, ISRAEL Rosh Ha'ayin, ISRAEL Netanya, ISRAEL

Additional inventors are being named on the _____ *separately numbered sheets attached hereto*

TITLE OF THE INVENTION (500 characters max):

AUTOMATED PRIORITIZATION OF PROCESS-AWARE CYBER RISK MITIGATION

Direct all correspondence to: **CORRESPONDENCE ADDRESS**

☒ The address corresponding to Customer Number: 26212

OR

☐ Firm or Individual Name

Address

City	State	Zip
Country	Telephone	Email

ENCLOSED APPLICATION PARTS *(check all that apply)*

☒ Application Data Sheet. See 37 CFR 1.76

☐ CD(s), Number of CDs _____

☒ Drawing(s) *Number of Sheets* 7

☐ Other (specify) _____

☒ Specification (e.g. description of the invention) *Number of Pages* 36

Fees Due: Filing Fee of $300 ($150 for small entity) ($75 for micro entity). If the specification and drawings exceed 100 sheets of paper, an application size fee is also due, which is $420 ($210 for small entity) ($105 for micro entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

METHOD OF PAYMENT OF THE FILING FEE AND APPLICATION SIZE FEE FOR THIS PROVISIONAL APPLICATION FOR PATENT

☐ Applicant claims small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.

Applicant must attach form PTO/SB/15A or B or equivalent.

$300

TOTAL FEE AMOUNT ($)

☐ A check or money order made payable to the *Director of the United States Patent and Trademark Office* is enclosed to cover the filing fee and application size fee (if applicable).

☐ Payment by credit card. Form PTO-2038 is attached

☒ The Director is hereby authorized to charge the filing fee and application size fee (if applicable) or credit any overpayment to Deposit Account Number: 06-1050.

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. 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 10 hours 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.

PROVISIONAL APPLICATION FOR PATENT COVER SHEET – Page 2 of 2

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government. (NOTE: Providing this information on a provisional cover sheet, such as this Provisional Application for Patent Cover Sheet (Form PTO/SB/16), does not satisfy the requirement of 35 U.S.C. 202(c)(6), which requires that the specification contain a statement specifying that the invention was made with Government support and that the Government has certain rights in the invention.)

☒ No.

☐ Yes, the invention was made by an agency of the U.S. Government. The U.S. Government agency name is: _____

☐ Yes, the invention was made under a contract with an agency of the U.S. Government.

_____

The contract number is: _____

The U.S. Government agency name is: _____

In accordance with 35 U.S.C. 2020(c)(6) and 37 CFR 401.14(f)(4), the specifications of any United States patent applications and any patent issuing thereon covering the invention, including the enclosed provisional application, must state the following:

"This invention was made with government support under [IDENTIFY THE CONTRACT] awarded by [IDENTIFY THE FEDERAL AGENCY]. The government has certain rights in the invention."

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.

SIGNATURE /Ryan McCarthy/ Date February 18, 2021

TYPED or PRINTED NAME Ryan McCarthy REGISTRATION NO. 50,636 *(if appropriate)*

TELEPHONE (512) 472-5070 Docket Number: 12587-0887P01

91435063.doc

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	12587-0887P01
	Application Number	
Title of Invention	AUTOMATED PRIORITIZATION OF PROCESS-AWARE CYBER RISK MITIGATION	

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
	Gal		Engelberg	

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

City	Country of Residence [i]
Pardes-hana	IL

Mailing Address of Inventor:

Address 1	Etrog 7, Apartment 13
Address 2	
City	Pardes-hana
State/Province	
Postal Code	
Country [i]	IL

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Dan		Klein	

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

City	Country of Residence [i]
Rosh Ha'ayin	IL

Mailing Address of Inventor:

Address 1	11 Lakhish Street
Address 2	
City	Rosh Ha'ayin
State/Province	
Postal Code	4856111
Country [i]	IL

Inventor 3 Remove

Legal Name

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	12587-0887P01
	Application Number	
Title of Invention	AUTOMATED PRIORITIZATION OF PROCESS-AWARE CYBER RISK MITIGATION	

Prefix	Given Name	Middle Name	Family Name	Suffix
	Tomer		Ram	

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

City	Netanya	Country of Residence [i]	IL

Mailing Address of Inventor:

Address 1	Dganya Road 79/17		
Address 2			
City	Netanya	State/Province	
Postal Code		Country [i]	IL

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	26212		
Email Address		Add Email	Remove Email

Application Information:

Title of the Invention	AUTOMATED PRIORITIZATION OF PROCESS-AWARE CYBER RISK MITIGATION		
Attorney Docket Number	12587-0887P01	Small Entity Status Claimed	☐
Application Type	Provisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	7	Suggested Figure for Publication (if any)	

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]

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	12587-0887P01
	Application Number	
Title of Invention	AUTOMATED PRIORITIZATION OF PROCESS-AWARE CYBER RISK MITIGATION	

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.

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	26212		

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			Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)

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).

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	12587-0887P01
	Application Number	
Title of Invention	AUTOMATED PRIORITIZATION OF PROCESS-AWARE CYBER RISK MITIGATION	

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.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	12587-0887P01
	Application Number	
Title of Invention	AUTOMATED PRIORITIZATION OF PROCESS-AWARE CYBER RISK MITIGATION	

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.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	12587-0887P01
	Application Number	
Title of Invention	AUTOMATED PRIORITIZATION OF PROCESS-AWARE CYBER RISK MITIGATION	

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. ☒

Organization Name	Accenture Global Solutions Limited		
Mailing Address Information For Applicant:			
Address 1	3 Grand Canal Plaza		
Address 2	Upper Grand Canal Street		
City	Dublin	**State/Province**	
Country	IE	Postal Code	4
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.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	12587-0887P01
	Application Number	
Title of Invention	AUTOMATED PRIORITIZATION OF PROCESS-AWARE CYBER RISK MITIGATION	

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 i		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	/Ryan McCarthy/			Date (YYYY-MM-DD)	2021-02-18
First Name	Ryan	Last Name	McCarthy	Registration Number	50636

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

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	12587-0887P01
	Application Number	
Title of Invention	AUTOMATED PRIORITIZATION OF PROCESS-AWARE CYBER RISK MITIGATION	

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.

ABSTRACT

Implementations are directed to receiving graph data representative of a process-aware AAG that is representative of potential lateral movement of adversaries within a computer network, receiving risk profile data representative of a risk profile of an enterprise with respect to two or more risk aspects, generating, by a process-aware risk assessment module, a risk assessment based on the process-aware AAG and the risk profile, and generating, by a mitigation simulator module, a mitigation list based on the process-aware AAG, the risk profile, and the risk assessment, the mitigation list comprising a prioritized list of two or more facts of the process-aware AAG. Other implementations of this aspect include corresponding systems, apparatus, and computer programs, configured to perform the actions of the methods, encoded on computer storage devices.

WHAT IS CLAIMED IS:

1. A computer-implemented method for prioritizing mitigation in enterprise networks, the method being executed by one or more processors and comprising:

receiving graph data representative of a process-aware analytical attack graph (AAG) that is representative of potential lateral movement of adversaries within a computer network;

receiving risk profile data representative of a risk profile of an enterprise with respect to two or more risk aspects;

generating, by a process-aware risk assessment module, a risk assessment based on the process-aware AAG and the risk profile; and

generating, by a mitigation simulator module, a mitigation list based on the process-aware AAG, the risk profile, and the risk assessment, the mitigation list comprising a prioritized list of two or more facts of the process-aware AAG.

2. The method of claim 1, further comprising:

providing a set of remediation actions based on the mitigation list; and

executing at least one remediation action in the set of remediation actions to mitigate risk to the computer network.

3. The method of claim 1, wherein nodes of the process-aware AAG are associated with process attributes, a process attribute maps a node to at least a portion of a process that is at least partially executed within the computer network.

4. The method of claim 1, wherein the risk profile comprises a set of risk acceptance scores, each risk acceptance score representing a tolerance of the enterprise to a respective risk aspect.

5. The method of claim 1, wherein a risk aspect comprises one of a safety, availability, integrity, and confidentiality.

6. The method of claim 1, the mitigation list is generated based on one of minimizing a risk aspect of the two or more risk aspects and minimizing a total score that is determined based on all of the two or more risk aspects.

7. One or more non-transitory computer-readable storage media coupled to one or more processors and having instructions stored thereon which, when executed by the one or more processors, cause the one or more processors to perform operations for prioritizing mitigation in enterprise networks in accordance with the method of one or more of claims 1-6.

8. A system, comprising:

one or more processors; and

a computer-readable storage device coupled to the one or more processors and having instructions stored thereon which, when executed by the one or more processors, cause the one or more processors to perform operations for prioritizing mitigation in enterprise networks in accordance with the method of one or more of claims 1-6.

AUTOMATED PRIORITIZATION OF PROCESS-AWARE CYBER RISK MITIGATION

BACKGROUND

[0001] Computer networks are susceptible to attack by malicious users (e.g., hackers). For example, hackers can infiltrate computer networks in an effort to obtain sensitive information (e.g., user credentials, payment information, address information, social security numbers) and/or to take over control of one or more systems. Computer networks are used to execute processes that support operations of enterprises and/or industrial infrastructures. Enterprises, in general, and industrial infrastructures, in particular, are increasingly connected to external networks such as the Internet. As such, processes that were once isolated from the open Internet network, are now vulnerable to external cyber-attacks. As the frequency and derived impact of these attacks increase, there is a need to prioritize and mitigate risks in order of importance to the operations.

[0002] To defend against such attacks, enterprises use security systems to monitor occurrences of potentially adverse events occurring within a network, and alert security personnel to such occurrences. For example, one or more dashboards can be provided, which provide lists of alerts that are to be addressed by the security personnel.

[0003] Modern computer networks are largely segregated and often deployed with diverse cyber defense mechanisms, which makes it challenging for an attacker (hacker) to gain direct access to a target (e.g., administrator credentials). This pattern is commonly seen in industrial control systems (ICSs) where a layered architecture ensures that targets are not in close proximity to the perimeter. Despite the presence of a layered architecture, the spate of attacks is increasing rapidly and span from large enterprises to critical infrastructure (CINF) networks. Due to the potential severe damage and cost experienced by a victim, CINFs have been intentionally targeted and have suffered from significant losses when successfully exploited.

[0004] In an effort to defend against cyber-attacks, so-called analytical attack graphs (AAGs) can be generated, which represent potential lateral movements of adversaries within computer networks. An AAG can be used to understand how a computer network can be hacked and undesirable consequences that can result. Accordingly, AAGs can be described as an important tool in developing anti-hacker defenses. For example, an AAG

can be used to identify the most vulnerable components within a computer network, and can be used to evaluate fixes of vulnerabilities that the AAG reveals (e.g., by fixing a limited number of issues, any adversary attack on the computer network, or on certain components in the computer network can be stopped).

SUMMARY

[0005] Implementations of the present disclosure are directed to mitigating cyber security risk in enterprise networks. More particularly, implementations of the present disclosure are directed to using process-aware analytical attack graphs (AAGs) and a mitigation simulator to prioritize mitigation efforts to mitigate risk in enterprise networks. In some examples, a mitigation list is provided, a set of remedial actions can be identified based on the mitigation list, and remedial actions can be executed to mitigate risk to enterprise networks.

[0006] In some examples, implementations of the present disclosure are provided within an agile security platform that determines asset vulnerability of enterprise-wide assets including cyber-intelligence and discovery aspects of enterprise information technology (IT) systems and operational technology (OT) systems, asset value, potential for asset breach and criticality of attack paths towards target(s) including hacking analytics of enterprise IT/OT systems.

[0007] In some implementations, actions include receiving graph data representative of a process-aware AAG that is representative of potential lateral movement of adversaries within a computer network, receiving risk profile data representative of a risk profile of an enterprise with respect to two or more risk aspects, generating, by a process-aware risk assessment module, a risk assessment based on the process-aware AAG and the risk profile, and generating, by a mitigation simulator module, a mitigation list based on the process-aware AAG, the risk profile, and the risk assessment, the mitigation list comprising a prioritized list of two or more facts of the process-aware AAG. Other implementations of this aspect include corresponding systems, apparatus, and computer programs, configured to perform the actions of the methods, encoded on computer storage devices.

[0008] These and other implementations can each optionally include one or more of the following features: actions further include providing a set of remediation actions based on the mitigation list, and executing at least one remediation action in the set of remediation actions to mitigate risk to the computer network; nodes of the process-aware AAG are associated with process attributes, a process attribute maps a node to at least a portion of a process that is at least partially executed within the computer network; the

risk profile includes a set of risk acceptance scores, each risk acceptance score representing a tolerance of the enterprise to a respective risk aspect; a risk aspect includes one of a safety, availability, integrity, and confidentiality; and the mitigation list is generated based on one of minimizing a risk aspect of the two or more risk aspects and minimizing a total score that is determined based on all of the two or more risk aspects.

[0009] The present disclosure also provides a computer-readable storage medium coupled to one or more processors and having instructions stored thereon which, when executed by the one or more processors, cause the one or more processors to perform operations in accordance with implementations of the methods provided herein.

[0010] The present disclosure further provides a system for implementing the methods provided herein. The system includes one or more processors, and a computer-readable storage medium coupled to the one or more processors having instructions stored thereon which, when executed by the one or more processors, cause the one or more processors to perform operations in accordance with implementations of the methods provided herein.

[0011] It is appreciated that methods in accordance with the present disclosure can include any combination of the aspects and features described herein. That is, methods in accordance with the present disclosure are not limited to the combinations of aspects and features specifically described herein, but also include any combination of the aspects and features provided.

[0012] The details of one or more implementations of the present disclosure are set forth in the accompanying drawings and the description below. Other features and advantages of the present disclosure will be apparent from the description and drawings, and from the claims.

DESCRIPTION OF DRAWINGS

[0013] FIG. 1 depicts an example architecture that can be used to execute implementations of the present disclosure.

[0014] FIG. 2 depicts an example conceptual architecture of an agile security platform.

[0015] FIG. 3 depicts an example portion of an example analytical attack graph (AAG) to illustrate implementations of the present disclosure.

[0016] FIG. 4 depicts a conceptual architecture for prioritizing risk mitigation for cyber security in accordance with implementations of the present disclosure.

[0017] FIG. 5 depicts an example user interface (UI) depicting an example process-aware AAG.

[0018] FIG. 6 depicts an example UI displaying an example process-aware risk assessment in accordance with implementations of the present disclosure.

[0019] FIG. 7 depicts an example process that can be executed in accordance with implementations of the present disclosure.

[0020] Like reference symbols in the various drawings indicate like elements.

DETAILED DESCRIPTION

[0021] Implementations of the present disclosure are directed to mitigating cyber security risk in enterprise networks. More particularly, implementations of the present disclosure are directed to using process-aware analytical attack graphs (AAGs) and a mitigation simulator to prioritize mitigation efforts to mitigate risk in enterprise networks. In some examples, a mitigation list is provided, a set of remedial actions can be identified based on the mitigation list, and remedial actions can be executed to mitigate risk to enterprise networks.

[0022] In some examples, implementations of the present disclosure are provided within an agile security platform that determines asset vulnerability of enterprise-wide assets including cyber-intelligence and discovery aspects of enterprise information technology (IT) systems and operational technology (OT) systems, asset value, potential for asset breach and criticality of attack paths towards target(s) including hacking analytics of enterprise IT/OT systems.

[0023] In some implementations, actions include receiving graph data representative of a process-aware AAG that is representative of potential lateral movement of adversaries within a computer network, receiving risk profile data representative of a risk profile of an enterprise with respect to two or more risk aspects, generating, by a process-aware risk assessment module, a risk assessment based on the process-aware AAG and the risk profile, and generating, by a mitigation simulator module, a mitigation list based on the process-aware AAG, the risk profile, and the risk assessment, the mitigation list comprising a prioritized list of two or more facts of the process-aware AAG.

[0024] To provide context for implementations of the present disclosure, and as introduced above, computer networks are susceptible to attack by malicious users (e.g., hackers). For example, hackers can infiltrate computer networks in an effort to obtain sensitive information (e.g., user credentials, payment information, address information, social security numbers) and/or to take over control of one or more systems. Computer networks are used to execute processes that support operations of enterprises and/or industrial infrastructures. Enterprises, in general, and industrial infrastructures, in particular, are increasingly connected to external networks such as the Internet. As such, processes that were once isolated from the open Internet network, are now vulnerable to

external cyber-attacks. As the frequency and derived impact of these attacks increase, there is a need to prioritize and mitigate risks in order of importance to the operations.

[0025] Modern computer networks are largely segregated and often deployed with diverse cyber defense mechanisms, which makes it challenging for an attacker (hacker) to gain direct access to a target (e.g., administrator credentials). This pattern is commonly seen in industrial control system (ICSs) where a layered architecture ensures that targets are not in close proximity to the perimeter. Despite the presence of a layered architecture, the spate of attacks is increasing rapidly and span from large enterprises to the critical infrastructure (CINF) networks. Due to the potential severe damage and cost experienced by a victim nation, CINF networks have been intentionally targeted intentionally and have suffered from significant losses when successfully exploited.

[0026] In general, attacks on CINF networks occur in multiple stages. Consequently, detecting a single intrusion does not necessarily indicate the end of the attack as the attack could have progressed far deeper into the network. Accordingly, individual attack footprints are insignificant in an isolated manner, because each is usually part of a more complex multi-step attack. That is, it takes a sequence of steps to form an attack path toward a target in the network. Researchers have investigated several attack path analysis methods for identifying attacker's required effort (e.g., number of paths to a target and the cost and time required to compromise each path) to diligently estimate risk levels. However, traditional techniques fail to consider important features and provide incomplete solutions for addressing real attack scenarios. For example, some traditional techniques only consider the topological connection between stepping stones to measure the difficulty of reaching a target. As another example, some traditional techniques only assume some predefined attacker skill set to estimate the path complexity. In reality, an attacker's capabilities and knowledge of the enterprise network evolve along attack paths to the target.

[0027] In an effort to defend against cyber-attacks, AAGs can be generated, which represent potential lateral movements of adversaries within computer networks. An AAG can be used to understand how a computer network can be hacked and undesirable consequences that can result. Accordingly, AAGs can be described as an important tool in developing anti-hacker defenses. For example, an AAG can be used to identify the

most vulnerable components within a computer network, and can be used to evaluate fixes of vulnerabilities that the AAG reveals (e.g., by fixing a limited number of issues, any adversary attack on the computer network, or on certain components in the computer network can be stopped). While much research has been dedicated to the analysis of a single AAG, little focus has been given to the analysis and comparison of multiple AAGs. In comparing multiple AAGs, the difference between the AAGs is a target of interest, as differences can reveal vulnerabilities that were added, were removed or that persisted across all AAGs.

[0028] In view of the above context, implementations of the present disclosure are directed to recommending remedial actions for cyber security. More particularly, implementations of the present disclosure are directed to automated process-aware recommendation of remedial actions to mitigate cyber security. As described in further detail, prioritization of remedial actions can include determining a risk assessment based on a process-aware AAG, and generating a prioritized list of remedial actions based on the risk assessment and a risk tolerance profile, the prioritized list of remedial actions being generated by a mitigation simulator.

[0029] In some examples, automated prioritization of remedial actions of the present disclosure can be realized within an agile security platform that considers attack complexity within an interconnected cyber infrastructure with a variety of attack paths to comprehensively address real attack scenarios. It is contemplated, however, that implementations of the present disclosure of the present disclosure can be realized in any appropriate cyber security platform.

[0030] In general, the agile security platform provides a cyber-threat analysis framework based on characterizing adversarial behavior in a multi-stage cyber-attack process. As described in further detail herein, how a threat proceeds within a network is investigated using an AAG and all possible attack stages are identified. In some implementations, each stage can be associated with network attributes. Using a holistic view of threat exposure provided by AAGs, attack techniques and tactics are incorporated into stepping stones found in AAGs.

[0031] In further detail, the cyber-threat analysis framework adds context to each attack stage using a real-world knowledge base of adversary tactics and techniques to

more comprehensively characterize progression along the attack path. In some implementations, an attack path analysis model identifies a level of difficulty in taking a path by considering the complexity of the path, the skill set of the attacker, and the like. Implementations of the present disclosure provide a path hardness that is measured in terms of a capability of the attacker and challenges. The insight into the level of difficulty of an attack path in the network helps security administrators to pinpoint critical paths and prioritize path hardening actions.

[0032] As described herein, the agile security platform enables continuous cyber and enterprise-operations alignment controlled by risk management. The agile security platform improves decision-making by helping enterprises to prioritize security actions that are most critical to their operations. In some examples, the agile security platform combines methodologies from agile software development lifecycle, IT management, development operations (DevOps), and analytics that use artificial intelligence (AI). In some examples, agile security automation bots continuously analyze attack probability, predict impact, and recommend prioritized actions for cyber risk reduction. In this manner, the agile security platform enables enterprises to increase operational efficiency and availability, maximize existing cyber security resources, reduce additional cyber security costs, and grow organizational cyber resilience.

[0033] As described in further detail herein, the agile security platform provides for discovery of IT/OT supporting elements within an enterprise, which elements can be referred to as configuration items (CI). Further, the agile security platform can determine how these CIs are connected to provide a CI network topology. In some examples, the CIs are mapped to processes and services of the enterprise, to determine which CIs support which services, and at what stage of an operations process. In this manner, a services CI topology is provided.

[0034] In some implementations, the specific vulnerabilities and improper configurations of each CI are determined and enable a list of risks to be mapped to the specific IT/OT network of the enterprise. Further, the agile security platform of the present disclosure can determine what a malicious user (hacker) could do within the enterprise network, and whether the malicious user can leverage additional elements in the network such as scripts, CI configurations, and the like. Accordingly, the agile

security platform enables analysis of the ability of a malicious user to move inside the network, namely, lateral movement within the network. This includes, for example, how a malicious user could move from one CI to another CI, what CI (logical or physical) can be damaged, and, consequently, damage to a respective service provided by the enterprise.

[0035] FIG. 1 depicts an example architecture 100 in accordance with implementations of the present disclosure. In the depicted example, the example architecture 100 includes a client device 102, a network 106, and a server system 108. The server system 108 includes one or more server devices and databases (e.g., processors, memory). In the depicted example, a user 112 interacts with the client device 102.

[0036] In some examples, the client device 102 can communicate with the server system 108 over the network 106. In some examples, the client device 102 includes any appropriate type of computing device such as a desktop computer, a laptop computer, a handheld computer, a tablet computer, a personal digital assistant (PDA), a cellular telephone, a network appliance, a camera, a smart phone, an enhanced general packet radio service (EGPRS) mobile phone, a media player, a navigation device, an email device, a game console, or an appropriate combination of any two or more of these devices or other data processing devices. In some implementations, the network 106 can include a large computer network, such as a local area network (LAN), a wide area network (WAN), the Internet, a cellular network, a telephone network (e.g., PSTN) or an appropriate combination thereof connecting any number of communication devices, mobile computing devices, fixed computing devices and server systems.

[0037] In some implementations, the server system 108 includes at least one server and at least one data store. In the example of FIG. 1, the server system 108 is intended to represent various forms of servers including, but not limited to a web server, an application server, a proxy server, a network server, and/or a server pool. In general, server systems accept requests for application services and provides such services to any number of client devices (e.g., the client device 102 over the network 106). In accordance with implementations of the present disclosure, and as noted above, the server system 108 can host an agile security platform.

[0038] In the example of FIG. 1, an enterprise network 120 is depicted. The enterprise network 120 represents a network implemented by an enterprise to perform its operations. In some examples, the enterprise network 120 represents on-premise systems (e.g., local and/or distributed), cloud-based systems, and/or combinations thereof. In some examples, the enterprise network 120 includes IT systems and OT systems. In general, IT systems include hardware (e.g., computing devices, servers, computers, mobile devices) and software used to store, retrieve, transmit, and/or manipulate data within the enterprise network 120. In general, OT systems include hardware and software used to monitor and detect or cause changes in processes within the enterprise network 120 as well as store, retrieve, transmit, and/or manipulate data. In some examples, the enterprise network 120 includes multiple assets. Example assets include, without limitation, users 122, computing devices 124, electronic documents 126, and servers 128.

[0039] In some implementations, the agile security platform is hosted within the server system 108, and monitors and acts on the enterprise network 120, as described herein. More particularly, and as described in further detail herein, one or more AAGs representative of the enterprise network are generated in accordance with implementations of the present disclosure. For example, the agile security platform detects IT/OT assets and generates an asset inventory and network maps, as well as processing network information to discover vulnerabilities in the enterprise network 120. The agile security platform executes automated prioritization of remedial actions of the present disclosure based on the network information.

[0040] In some examples, the agile security platform provides one or more dashboards, alerts, notifications and the like to cyber security personnel that enable the cyber security personnel to react to and remediate security relevant events. For example, the user 112 can include a cyber security expert that views and responds to dashboards, alerts, and/or notifications of the agile security platform using the client device 102.

[0041] In some examples, the agile security platform operates over multiple phases. Example phases include an asset discovery, anomaly detection, and vulnerability analysis phase, a cyber resilience risk analysis phase, and a cyber resilience risk recommendation phase.

[0042] With regard to the asset discovery, anomaly detection, and vulnerability analysis phase, discovering what vulnerabilities exit across the vertical stack and the relevant use cases is imperative to be conducted from the enterprise IT to the control systems. A focus of this phase is to generate the security backlog of issues, and potential remediations.

[0043] Rather than managing each technology layer separately, the agile security platform addresses lateral movements across the stack. Through devices, communication channels (e.g., email, TCP/IP), and/or operation systems, vulnerabilities are addressed within the context of a service (e.g., a service that the enterprise offers to customers), and a cyber kill chain to a target in the operation vertical, generating operation disturbance by manipulation of data. The notion of a CI assists in mapping dependencies between IT/OT elements within a configuration management DB (CMDB). A so-called security CI (SCI) maps historical security issues of a certain managed security element and is mapped into a security aspect of a digital twin.

[0044] As a result, a stack of technologies is defined, and is configured in a plug-in reference architecture (replaceable and extensible) manner. The stack addresses different aspects of monitoring, harvesting, and alerting of information within different aggregations views (dashboards) segmented according to owners and relevant IT and security users. An example view includes a health metric inserted within the dashboard of an enterprise application. In some examples, the health metric indicates the security condition of the underlying service and hence, the reliability of the provided data and information. Similar to risks that can be driven by labor, inventory, or energy, security risk concern can be presented and evaluated in the operations-level, drilled-through for additional transparency of the issue, and can be optimally remediated by allocating investments to automation or to security and IT personal with adequate operations awareness.

[0045] With regard to the cyber resilience risk analysis phase, each vulnerability may have several remediations, and each has a cost associated with it, either per internal personnel time, transaction, service, or retainer, as well as the deferred cost of not acting on the issue. A focus of this phase is to enable economical decision-making of security

investments, either to be conducted by the IT and security team or directly by automation, and according to risk mitigation budget.

[0046] In further detail, observing a single-issue type and its remediations does not reflect the prioritization between multiple vulnerabilities. Traditional systems are based on global risk assessment, yet the context in which the SCI is part of is missing. The overall risk of a process matters differently for each enterprise. As such, remediation would occur according to gradual hardening of a process according to prioritization, driven in importance and responsibility by the enterprise, not by gradual hardening of all devices, for example, in the organization according to policy, without understanding of the impact on separated operational processes. Hardening of a system should be a decision of the enterprise to drive security alignment with the enterprise.

[0047] In addition, as the system is changed by gradual enforcement and hardening, new issues are detected and monitored. Hence, making a big bang decision may be not relevant to rising risks as they evolve. Prioritization according to value is the essence of this phase. It is a matter of what is important for the next immediate term, according to overall goals, yet considering changes to the environment.

[0048] With regard to the cyber resilience risk recommendation phase, a focus is to simplify approved changes and actions by proactive automation. In traditional systems, the action of IT remediation of security issues is either done by the security team (such as awareness and training), by creating a ticket in the IT service system (call for patch managements), and/or by tools that are triggered by security and monitored by IT (automatic deployment of security policies, change of authentication and authorization, self-service access control management, etc.). Some operations can be conducted in a disconnected mode, such as upgrading firmware on an IoT device, in which the operator needs to access the device directly. Either automated or manual, by IT or by security, or by internal or external teams, the entire changes are constantly assessed by the first phase of discovery phase, and re-projected as a metric in a context. Progress tracking of these changes should also occur in a gradual manner, indicating maintenance scheduling on similar operational processes, hence, driving recommendations for frequent actions that can be automated, and serve as candidates to self-managed by the operations owners and systems users.

[0049] In the agile security platform, acting is more than automating complex event processing (CEP) rules on alerts captured in the system logs and similar tools. Acting is started in areas highlighted according to known patterns and changing risks. Pattern detection and classification of events for approved automation processes (allocated transactions budget), are aimed at commoditization of security hardening actions in order to reduce the attention needed for prioritization. As such, a compound backlog and decision phase, can focus further on things that cannot be automated versus those that can. All issues not attended yet are highlighted, those that are handled by automation are indicated as such, and monitored to completion, with a potential additional value of increasing prioritization due to changing risks impact analysis.

[0050] FIG. 2 depicts an example conceptual architecture 200 of an agile security (AgiSec) platform. The conceptual architecture 200 depicts a set of security services of the AgiSec platform, which include: an agile security prioritization (AgiPro) service 204, an agile security business impact (AgiBuiz) service 206, an agile security remediation (AgiRem) service 210, an agile security hacker lateral movement (AgiHack) service 208, an agile security intelligence (AgiInt) service 212, and an agile security discovery (AgiDis) service 214. The conceptual architecture 200 also includes an operations knowledge base 202 that stores historical data provided for an enterprise network (e.g., the enterprise network 120).

[0051] In the example of FIG. 2, the AgiDis service 214 includes an adaptor 234, and an asset/vulnerabilities knowledge base 235. In some examples, the adaptor 234 is specific to an asset discovery tool (ADT) 216. Although a single ADT 216 is depicted, multiple ADTs can be provided, each ADT being specific to an IT/OT site within the enterprise network. Because each adaptor 234 is specific to an ADT 216, multiple adaptors 234 are provided in the case of multiple ADTs 216.

[0052] In some implementations, the AgiDis service 214 detects IT/OT assets through the adaptor 234 and respective ADT 216. In some implementations, the AgiDis service 214 provides both active and passive scanning capabilities to comply with constraints, and identifies device and service vulnerabilities, improper configurations, and aggregate risks through automatic assessment. The discovered assets can be used to generate an asset inventory, and network maps. In general, the AgiDis service 214 can be

used to discover assets in the enterprise network, and a holistic view of network and traffic patterns. More particularly, the AgiDis service 214 discovers assets, their connectivity, and their specifications and stores this information in the asset/vulnerabilities knowledge base 235. In some implementations, this is achieved through passive network scanning and device fingerprinting through the adaptor 234 and ADT 216. The AgiDis service 214 provides information about device models.

[0053] In the example of FIG. 2, the AgiInt service 212 includes a vulnerability analytics module 236 and a threat intelligence knowledge base 238 (e.g., CVE, CAPEC, CWE, iDefence API, vendor-specific databases). In some examples, the AgiInt service 212 discovers vulnerabilities in the enterprise network based on data provided from the AgiDis service 214. In some examples, the vulnerability analytics module 236 processes data provided from the AgiDis service 214 to provide information regarding possible impacts of each vulnerability and remediation options (e.g., permanent fix, temporary patch, workaround) for defensive actions. In some examples, the vulnerability analytics module 236 can include an application programming interface (API) that pulls out discovered vulnerabilities and identifies recommended remediations using threat intelligence feeds. In short, the AgiInt service 212 maps vulnerabilities and threats to discovered IT/OT assets. The discovered vulnerabilities are provided back to the AgiDis service 214 and are stored in the asset/vulnerabilities knowledge base 235 with their respective assets.

[0054] In the example of FIG. 2, the AgiHack service 208 includes an analytical attack graph (AAG) generator 226, an AAG database 228, and an analytics module 230. In general, the AgiHack service 208 generates AAGs using the resource-efficient AAG generation of the present disclosure, and evaluates hacking exploitation complexity. In some examples, the AgiHack service 208 understands attack options, leveraging the vulnerabilities to determine how a hacker would move inside the network and identify targets for potential exploitation. The AgiHack service 208 proactively explores adversarial options and creates AAGs representing possible attack paths from the adversary's perspective.

[0055] In further detail, the AgiHack service 208 provides rule-based processing of data provided from the AgiDis service 214 to explore all attack paths an adversary can

take from any asset to move laterally towards any target (e.g., running critical operations). In some examples, multiple AAGs are provided, each AAG corresponding to a respective target within the enterprise network. Further, the AgiHack service 208 identifies possible impacts on the targets. In some examples, the AAG generator 226 uses data from the asset/vulnerabilities knowledge base 236 of the AgiDis service 214, and generates an AAG. In some examples, the AAG graphically depicts, for a respective target, all possible impacts that may be caused by a vulnerability or network/system configuration, as well as all attack paths from anywhere in the network to the respective target. In some examples, the analytics module 230 processes an AAG to identify and extract information regarding critical nodes, paths for every source-destination pair (e.g., shortest, hardest, stealthiest), most critical paths, and critical vulnerabilities, among other features of the AAG. If remediations are applied within the enterprise network, the AgiHack service 208 updates the AAG.

[0056] In the example of FIG. 2, the AgiRem service 210 includes a graph explorer 232 and a summarizer 234. In general, the AgiRem service 210 provides remediation options to avoid predicted impacts. For example, the AgiRem service 210 provides options to reduce lateral movement of hackers within the network and to reduce the attack surface. The AgiRem service 210 predicts the impact of asset vulnerabilities on the critical processes and adversary capabilities along kill chain/attack paths and identifies the likelihood of attack paths to access critical assets and prioritizes the assets (e.g., based on shortest, easiest, stealthiest). The AgiRem service 210 identifies remediation actions by exploring attack graph and paths. For example, the AgiRem service 210 can execute a cyber-threat analysis framework that characterizes adversarial behavior in a multi-stage cyber-attack process, as described in further detail herein.

[0057] In further detail, for a given AAG (e.g., representing all vulnerabilities, network/system configurations, and possible impacts on a respective target) generated by the AgiHack service 208, the AgiRem service 210 provides a list of efficient and effective remediation recommendations using data from the vulnerability analytics module 236 of the AgiInt service 212. In some examples, the graph explorer 232 analyzes each feature (e.g., nodes, edges between nodes, properties) to identify any condition (e.g., network/system configuration and vulnerabilities) that can lead to cyber impacts. Such

conditions can be referred to as issues. For each issue, the AgiRem service 210 retrieves remediation recommendations and courses of action (CoA) from the AgiInt service 212, and/or a security knowledge base (not shown). In some examples, the graph explorer 232 provides feedback to the analytics module 230 for re-calculating critical nodes/assets/paths based on remediation options. In some examples, the summarizer engine 234 is provided as a natural language processing (NLP) tool that extracts concise and salient text from large/unstructured threat intelligence feeds. In this manner, the AgiSec platform can convey information to enable users (e.g., security teams) to understand immediate remediation actions corresponding to each issue.

[0058] In the example of FIG. 2, the AgiBuiz service 206 includes an impact analyzer 220. In general, the AgiBuiz service 206 associates services that are provided by the enterprise with IT/OT assets, generates a security map, identifies and highlights risks and possible impacts on enterprise operations and industrial processes, and conducts what-if prediction analyses of potential security actions remediations on service health levels. In other words, the AgiBuiz service 206 identifies risk for each impact predicted by the AgiHack service 208. In some examples, the impact analyzer 220 interprets cyber risks and possible impacts (e.g., financial risk) based on the relative importance of each critical asset and its relative value within the entirety of the enterprise operations. The impact analyzer 220 processes one or more models to compare the financial risks caused by cyber-attacks with those caused by system unavailability due to shutdown time for replacing/patching critical assets.

[0059] In the example of FIG. 2, the AgiPro service 204 includes a prioritizing engine 222 and a scheduler 224. In some implementations, the AgiPro service 204 prioritizes the remediation recommendations based on their impact on the AAG size reduction and risk reduction on the value. In some examples, the AgiPro service 204 determines where the enterprise should preform security enforcement first, in order to overall reduce the risks discovered above, and evaluate and probability to perform harm based on the above lateral movements by moving from one CI to another. In some examples, the AgiPro service 204 prioritizes remediation actions based on financial risks or other implications, provides risk reduction recommendations based on prioritized

remediations, and identifies and tracks applied remediations for risks based on recommendations.

[0060] In some examples, the prioritizing engine 222 uses the calculated risks (e.g., risks to regular functionality and unavailability of operational processes) and the path analysis information from the analytics module 230 to prioritize remediation actions that reduce the risk, while minimizing efforts and financial costs. In some examples, the scheduler 224 incorporates the prioritized CoAs with operational maintenance schedules to find the optimal time for applying each CoA that minimizes its interference with regular operational tasks.

[0061] As introduced above, cyber-threat analysis for a computer network leverages one or more AAGs. In some examples, an AAG is generated by a cyber security platform, such as the AgiSec platform described herein. In mathematical terms, an AAG can be described as a directed graph modeled as $AAG(V, E)$ with a set of nodes $V = \{v_1, \ldots, v_n\}$ and a set of edges $E = \{e_1, \ldots, e_m\}$ connecting nodes together, where $|V| = n$ and $|E| = m$.

[0062] FIG. 3 depicts an example portion 300 of an example AAG to illustrate implementations of the present disclosure. As depicted in the example of FIG. 3, the AAG can include different node types to show how a set of network and system configurations result in unauthorized actions to specific targets. The example portion 300 is depicted in a database structure (e.g., Neo4j graph database structure). Nodes in an AAG are of different types: circular nodes representing system or network configurations that are the conditions that provide possibilities for actions by an attacker; circle-shaped nodes representing reasoning rules that represent the attack methodology leveraged by an attacker to achieve a particular goal; and square nodes that represent an impact as a sub-goal for a certain action an attacker could take. The AAG includes two types of edges: configuration-to-rule edges that represent logical AND (i.e., all configuration conditions have to be true to cause the impact; and rule-to-impact edges that represent logical OR (i.e., the impact happens if at least one rule is satisfied).

[0063] In general, the AAG is created by taking into account the configurations directed by some rules in order to make some impacts on the target network. In some examples, all configuration nodes, impact nodes, and rule nodes can be provided in sets

N_p, N_d, N_r, respectively. Accordingly, $N_p = \{n_{p,j} | n_{p,j} \in V, \forall n_{p,j}\ is\ a\ configuration\}$, $N_d = \{n_{d,j} | n_{d,j} \in V, \forall n_{d,j}\ is\ an\ impact\}$, and $N_r = \{n_{r,j} | n_{r,j} \in V, \forall n_{r,j}\ is\ a\ rule\}$. Consequently, the combination of these sets accounts for all vertices of the graph. In some examples, a configuration node is referred to herein as an input fact node indicating facts that are provided as input within a configuration. In some examples, impact nodes are referred to herein as derived fact nodes indicating a derived fact that results from applying one or more input facts and/or one or more derived facts to a rule.

[0064] AAGs can be used in cyber-threat analysis to determine attack paths of external attackers into and through a computer network. Use of AAGs in mitigating attacks on computer networks is described in further detail in commonly assigned U.S. App. No. 16/554,846, entitled Generating Attack Graphs in Agile Security Platforms, and filed on August 29, 2019, the disclosure of which is expressly incorporated herein by reference in the entirety for all purposes. Further, generation of AAGs is described in further detail in commonly assigned U.S. App. No. 16/924,483, entitled Resource-efficient Generation of Analytical Attack Graphs, and filed on July 9, 2020, the disclosure of which is expressly incorporated herein by reference in the entirety for all purposes.

[0065] To provide further context for implementations of the present disclosure, the AAG model presented in MulVAL will be briefly discussed. MulVAL can be described as an automatic end-to-end AAG generation framework. In general, MulVAL takes a specification, such as, but not limited to, MITRE Common Vulnerabilities and Exposures (CVE), describing the configuration of an enterprise network and rules that depict how an attacker can exploit the system configurations to advance in the enterprise network towards a target goal. MulVAL uses datalog as a specification language. In datalog, logical and physical entities of the enterprise network are formally modelled by datalog predicates; n-ary relations between entities are defined by datalog relations; and attack rules are modelled as datalog derivation rules in a datalog program. Derivation rules define preconditions (set of predicates connected by logical 'and') that, if met, derive new predicates. The specification of the predicates and derivation rules can be referred to as the datalog program of the system (enterprise network).

[0066] For purposes of illustration, a non-limiting example is introduced in Listing 1, below, which shows a specification of an example datalog program for an enterprise network (system).

```
## predicates
.decl domainUser(_user: UserFqdn, _domain: Domain)
.decl groupContains(_group: GroupFqdn, _principal: Principal)
.decl isUser(_user: UserFqdn)
.decl localGroup(_host: Host, _groupName: GroupName, _groupFqdn:
GroupFqdn)
.decl userInLocalGroup(_host: Host, _groupName: GroupName, _user:
UserFqdn)
.decl isUser(_user: UserFqdn, rule_id: String)
.decl groupContainsDirect(_group: GroupFqdn, _principal:
Principal)

## attack rules
groupContains(Group,Principal):-
groupContainsDirect(Group,Principal).  # rule label: 28
isUser(User):-domainUser(User,_). # rule label: 80
userInLocalGroup(Host,GroupName,User):-
localGroup(Host,GroupName,GroupFqdn),groupContains(GroupFqdn,User
,_),isUser(User,_). # rule label: 25
```

Listing 1: Example datalog program

The example datalog program of Listing 1 lists seven predicates. Each predicate is a function that maps objects of different types to a Boolean value. For example, the predicate `domainUser` maps objects of type `User` and objects of type `Domain` to `True` if the user belongs to the domain, and `False` otherwise.

[0067] The example datalog program of Listing 1 lists three attack rules. The first attack rule indicates that a predicate `groupContains` is derived from the predicate `groupContainsDirect` (with the corresponding objects). The third attack rule indicates that three precondition predicates: `isUser`, `localGroup`, `groupContains` derive the predicate `userInLocalGroup` (with the corresponding objects). Each rule has a unique identifier (id). For example, 28 for the first attack rule and 25 for the third attack rule.

The system configuration (e.g., instance of hosts, users, privileges on host, etc.) is provided as an array of facts (also referred to as grounds), each fact associated with a predicate of the datalog program.

[0068] Table 1: Example Input Facts for `domainUser`Table 1, below, lists four input facts of the `isDomain` predicate.

<ADMINISTRATOR>@CYBER.LOCAL	CYBER.LOCAL
BERTHA.DAVIES@CYBER.LOCAL	CYBER.LOCAL
BRANDON.DAVIS@CYBER.LOCAL	CYBER.LOCAL
DANIELLE.HINTON@CYBER.LOCAL	CYBER.LOCAL

Table 1: Example Input Facts for `domainUser`

The listed user-domain pairs represent mappings that are `True`. Combinations (of user and domain) that are not listed in the input facts are considered `False`, until proven otherwise (i.e., derived by a rule).

[0069] MulVAL uses a datalog solver on the program specification to check whether there exists an attack path from the input facts to a target goal. It does this by iteratively applying the derivation rules on facts until either reaching a target goal (a path exists) or reaching a fixed point, from which no new fact can be derived. In this case, no attack path to the target exists and the system is considered to be secure.

[0070] The derivation process from the grounded facts to the target goals is represented in the resulting AAG. An AAG is provided as a data object that records nodes and edges between nodes, described herein. The data object underlying an AAG can be processed to generate a visual representation, a graph, of the AAG.

[0071] In further detail, MulVAL generates an AAG that shows the derivation of grounded facts by the application of rules. Formally, the AAG is defined as: $AAG = (N_r, N_p, N_d, E, L, Args, G)$, where N_r, N_p, N_d are the sets of nodes (rules (r), input facts (p), and derived facts (d), respectively), E is a set of edges that connect from facts to derivation rules (precondition) and from derivation rules to derived facts, L is a mapping from a node (i.e., an input fact, a derived fact, a rule) to its label (i.e., the predicate or rule that it is associated with), $Args$ is a mapping of facts to their arguments (i.e., objects they are associated with), and $G \in N_d$ describes the target goal (e.g., crown jewel that may be a target for hackers). N denotes the union of all node elements in the graph (i.e., $N = N_r \cup N_p \cup N_d$). In some examples, primitive nodes and derived nodes (i.e., fact nodes)

are denoted by N_f, where $N_f = N_p \cup N_d$. Every fact node in the graph is labeled with a logical statement in the form of a predicate applied to its arguments. In some examples, $Args$ and L are separately encoded. For example, a configuration $c = \{"DomainUser","BERTHA.DAVIES@CYBER.LOCAL","CYBER.LOCAL"\}$ can be encoded as $N_p = \{node\_1\};\ L(node\_1) = "DomainUser";\ Args(node\_1) = ["BERTHA.DAVIES@CYBER.LOCAL","CYBER.LOCAL"]$.

[0072] Every element of the AAG is uniquely identifiable. Each fact (input fact, derived fact) node is uniquely defined by its arguments and predicate label (i.e., no two nodes may have the same label and arguments). As described in further detail herein, a unique identifier (index) for each fact node can be provided based on this information. Every rule node is uniquely defined by its label, preconditions and derived fact. As also described in further detail herein, a unique index for each rule node can be provided based on this information. The AAG size can be defined as the number of nodes and edges in the AAG.

[0073] In some implementations, each node and each edge is uniquely identified by a respective identifier that is generated by encoding. Each identifier enables the respective node or edge to be indexed within dictionaries and/or libraries in a time- and resource-efficient manner. In some examples, each fact node includes a respective identifier that is determined based on a concatenation of the predicate label and the arguments of the fact node. In some examples, each rule node includes a respective identifier that is determined based on a concatenation of the rule label, the unique identifier(s) of predicate node(s) (i.e., one or more fact nodes input to the rule node), and the unique identifier(s) of derivative node(s) (i.e., one or more derived fact nodes output by the rule node). In some examples, lexicographical ordering is used for the precondition nodes and/or derived nodes to provide the order used in the concatenation. In some examples, each edge includes a respective unique identifier that is determined based on a concatenation of the unique identifier of the source node and the unique identifier of the target node. In some implementations, a concatenation is itself the encoding used to uniquely identify a respective node. In some implementations, each concatenation is processed through a hash function (e.g., a deterministic hash function) to generate a hash value, the hash value being the encoding used to uniquely identify a respective node.

[0074] In accordance with implementations of the present disclosure, and as described in further detail herein, automated prioritization of remedial actions is provided. In some implementations, a risk assessment of an enterprise network (or a portion thereof) is determined based on a process-aware AAG that is representative of the enterprise network. A risk tolerance profiled is provided that represent a risk tolerance per risk aspect. A mitigation simulator processes the risk assessment and the risk tolerance profile to generate a prioritized list of remedial actions. In some examples, a remedial action (also referred to as a security control) is in action that can be executed to mitigate (e.g., reduce) risk within the enterprise network. For example, a remedial action can be executed to mitigate a fact (e.g., input fact, derived fact).

[0075] FIG. 4 depicts a conceptual architecture 400 for prioritizing risk mitigation for cyber security in accordance with implementations of the present disclosure. In the example of FIG. 4, the conceptual architecture 400 includes a process-aware risk assessment module 402 and a mitigation simulator 404. The process-aware risk assessment module 402 receives a process-aware AAG 410 and a risk tolerance profile 414, and generates a risk assessment 414. The mitigation simulator 404 receives the process-aware AAG 410, the risk assessment 412, and the risk tolerance profile 414, and generates a prioritized risk mitigation profile 416. In some examples, the prioritized risk mitigation profile 416 includes a prioritized list of remedial actions that can be executed within the enterprise network to mitigate cyber security risk therein.

[0076] In further detail, process-aware risk assessment module 402 performs a process-aware risk assessment based on the process-aware AAG 410 and the risk tolerance profile 412. In some examples, the process-aware AAG 410 is generated as described herein and/or as described in commonly assigned U.S. App. Nos. 16/554,846 and 16/924,483, introduced above.

[0077] In some examples, a process-aware AAG, such as the process-aware AAG 410, includes fact nodes (i.e., configuration (condition) nodes of FIG. 3), impact nodes (i.e., impact (effect) nodes of FIG. 3), and rule nodes (i.e., reasoning rule nodes of FIG. 3). An entry point to the process-aware AAG, and thus the enterprise network represented by the process-aware AAG, is fact node (e.g., potential entry point of an attacker). In some examples, a so-called crown-jewel is an asset within the enterprise network (e.g.,

administrator credentials) that is targeted by attackers (e.g., a target asset). In some examples, an attack goal can refer to an impact node that is considered as a capability that an attacker could get over a crown-jewel.

[0078] In some examples, attributes of a process-aware AAG include, without limitation, hardness scores, impact vectors, asset identifier, and process context. In some examples, each rule (represented as a rule node) holds a hardness score (e.g., in range [0, 1]) that represents a measure on a required maturity level of an adversary to be able to execute the rule, resulting in an impact. In some examples, the hardness this score is set as an attribute of an outgoing edge of the rule node (e.g., incoming edge(s) have value of 0 set as hardness score). In some examples, each hardness score is specified by domain experts and embedded within an ontology per rule. In some examples, an attack goal holds an impact vector that includes a set of impact scores (e.g., each in range [0, 1]), each impact score corresponding to a respective risk aspect. Example risk aspects include, without limitation, safety, availability, integrity, and confidentiality. In some examples, an impact vector expresses the potential impact caused by execution of a rule. In some examples, impact vectors are specified by domain experts and are embedded within the ontology per impact type (e.g., denial of service (DoS) has a high impact on availability). In some examples, each asset (represented as a node that represents an asset), has an asset identifier, which enables mapping to the asset (e.g., rules are mapped to assets based on asset identifiers according to outgoing impacts).

[0079] In some examples, nodes of the AAG hold a process attribute based on a node-to-process mapping. In some examples, the node-to-process mapping maps a process to nodes (e.g., assets) that execute the process within the enterprise network. For example, the mapping can map different levels (e.g., process, sub-process, activity, task) of a process to one or more assets. Accordingly, assets of the enterprise network, as represented in the AAG, are mapped to processes the assets contribute to. In this manner, the AAG is considered to be a process-aware AAG.

[0080] FIG. 5 depicts an example user interface (UI) 500 depicting an example process-aware AAG.

[0081] Referring again to FIG. 4, the risk assessment 414 is provided as a risk vector representative of the context of process, crown-jewel, and attack goals. More particularly,

the risk vector holds configurable risk aspects (e.g., availability, confidentiality, integrity, safety).

[0082] FIG. 6 depicts an example UI 600 displaying an example process-aware risk assessment in accordance with implementations of the present disclosure.

[0083] Referring again to FIG. 4, in some implementations, a total score is calculated based on a user-defined risk tolerance. During mitigation simulation by the mitigation simulator module 404, a single risk aspect (e.g., safety) can be minimized or the total score can be minimized.

[0084] In further detail, the risk tolerance profile 412 defines a minimal risk level for each risk aspect in a set of configurable risk aspects (e.g., availability, confidentiality, integrity, safety). In some examples, the risk tolerance profile includes user-assigned acceptance scores to each risk aspect, an acceptance score represents an enterprise's minimal acceptance rate of a risk aspect. For example, if an enterprise accepts 50% safety risk, the acceptance score for the safety risk aspect is set to 0.5. The risk tolerance profile 412 is a risk vector holding the acceptance scores of all of the configurable risk aspects.

[0085] In some examples, a risk vector is calculated for each attack goal. For example, a risk vector per attack goal is calculated as a multifaction between the impact vector and the easiest way of reaching the attack goal. As long as it is easier to reach the attack goal, the risk vector converges to the impact vector, and as long as it is harder to reach the attack goal, the risk vector converges to 0. The following example relationship is provided:

$$\overrightarrow{AGR_i} = \overrightarrow{IV_i} \cdot e^{\frac{\sum_{r=1}^{R} H_r}{\alpha}}$$

where:

$\overrightarrow{AGR_i}$ – risk vector over attack goal *i*

$\overrightarrow{IV_i}$ - impact vector over attack goal *i*

R - set of rule nodes that compose the shortest path reaching the attack goal from all entry points

H_r - hardness of rule instance r

α - normalizes the power number

[0086] In some examples, a risk vector is calculated for each crown-jewel level. For example, a risk vector per crown-jewel is determined as the maximal risk over the attack goals that relate to the respective crown-jewel, where calculation is performed per risk aspect. The following example relationship is provided:

$$\overrightarrow{CJR_J} = \max_{i \in [n]}(AGR_{ia}) \ \ for\ a\ in\ A$$

where:

$\overrightarrow{CJR_J}$ - risk vector over crown-jewel j

n - set of attack goals related to crown-jewel j

A – set of risk aspects a

AGR_{ia} risk aspect a of attack goal i

[0087] In some examples, a risk vector is calculated for process-level risk. For example, a risk vector per process is determined as the maximal risk over the crown-jewels that relate to the process, where calculation is performed per risk aspect. The following example relationship is provided:

$$\overrightarrow{BPR_p} = \max_{j \in [k]}(CGR_{ja}) \ \ for\ a\ in\ A$$

where:

$\overrightarrow{BPR_p}$ - risk vector over process p

k - set of crown-jewels related to process p

A – set of risk aspects a

CGR_{ja} risk aspect a of crown-jewel j

[0088] In some implementations, a total score is calculated as a sigmoid function of the sum of differences between risk aspects to their tolerance. In general, a sigmoid function is a mathematical function having a characteristic "S"-shaped curve (sigmoid curve). In some examples, when the sum of differences is equal to 0, the total score is equal to 0.5. As long as risk exceeds tolerance total, the total score converges to 1. As long as risk decreases from tolerance, the total score converges to 0. The following example relationship is provided:

$$BPT_p = S\left(\sum_{a}^{A}(BPR_{pa} - TOL_a)\right)$$

where:

BPT_P- total score of process p

S – sigmoid function defined as $S(x) = \frac{e^x}{e^x+1}$

A – set of risk aspects a

BPR_{pa} – risk aspect a of process p

$\overrightarrow{TOL}$ – risk tolerance vector

TOL_a risk tolerance of aspect a

[0089] In accordance with implementations of the present disclosure, the mitigation simulator (e.g., executed by the mitigation simulator module 402) takes a process-aware AAG and a risk tolerance as input, and automatically outputs mitigation priority in a manner that minimizes risk in the context of the process. As noted above, the mitigation priority can be based on minimizing a single risk aspect (e.g. safety) or the total score. In some examples, the mitigation priority is provided as a prioritized list of ordered facts (input facts, derived facts) that should be addressed (e.g., repaired). In some implementations, the mitigation simulator is provided as a greedy algorithm that, in each step, searches for the attack goal with the maximal process-level risk loss and mitigates the attack goal.

[0090] In mitigation simulation, the following example functions are defined:

Function	Description	Input	Output
calculateRisk()	Calculates process-level risk assessment according to formulas above	Process name Process-aware AAG Risk score type (total score /single aspect score)	Process-level score (if total score, then BPT_P; if risk aspect, then BPR_{pa}) Crown-jewel level score (if total score, then $\overrightarrow{CJR_j}$; if risk aspect, then CJR_{ja}) Attack-goal level score (if total score, then $\overrightarrow{AGR_i}$; if risk aspect, then AGR_{ia})
threshold()	Returns stop criteria for simulation	Risk Tolerance Vector Risk score type (total score /single aspect score)	Threshold (if risk score type is 'total', then threshold is 0.5; if risk score type is a specific aspect, then threshold is TOL_a)
greedyRiskLoss()	Gets risk model results (initial process level risk) and search for the attack goal with the maximal process level risk loss (the different between the initial risk and the risk if attack goal would be removed)	Process-level score Crown-jewel level score Attack-goal level score	Attack goal with maximal process level risk loss
allShortestPaths()	Gets entry points and attack-goal with maximal process level risk loss, then retrieves all shortest paths between entry points to attack goal, and create a new graph based on these paths	Entry points Attack goal Process-aware AAG	Process aware attack sub-graph
factInfluence()	Gets a process aware attack sub-graph, then calculates eigenvector centrality in reverse order, and returns list of facts ordered by their eigenvector centrality	Process aware attack sub-graph	List of facts ordered by their eigenvector centrality
graphGeneration()	Gets mitigation list (list of facts ordered by eigenvector centrality) and generates a new attack graph (considering facts removal)	List of facts ordered by their influence rank (eigenvector centrality)	

[0091] The following algorithm of Listing 1 represents a mitigation simulator in accordance with implementations of the present disclosure:

Listing 1: Mitigation Simulator

```
Input: Process aware attack graph, risk tolerance, risk score type, process name
process_risk, crown_jewel_risk, attack_goal_risk = calculateRisk(process name, process
aware attack graph, risk score type)
t = threshold(risk tolerance, risk score type)
while (process_risk > t) do:
    attack_goal = greedyRiskLoss(process_risk, crown-jewel_risk, attack_goal_risk)
    subgraph = allShortestPaths(entryPoints, attack_goal)
    mitigation_list = factInfluence(subgraph)
    mitigation_priority.append(mitigation_list)
    new_graph = graphGeneration(mitigation_list)
    process_risk, crown_jewel_risk, attack_goal_risk = calculateRisk(new_graph)
return mitigation_priority
```

In some implementations, the mitigation list output by the mitigation simulator is input to an automatic remediation system. In some examples, the automatic remediation system maps each fact of the mitigation list to a pre-defined automatic remediation action. For example, a remediation action can be associated with a fact, as a known remediation action for mitigating the fact (e.g., preventing the fact from occurring). The remediation actions are executed to mitigate risk within the enterprise network.

[0092] As described herein, implementations of the present disclosure enable enterprise to have clear visibility into security postures in the context of processes (at least partially) executed within enterprise networks. Further implementations of the present disclosure prioritizes mitigation efforts according to the impact over enterprise processes. Further, both the simulation and the risk assessment are based on a process-aware AAG. Implementations of the present disclosure are driven by information that is embedded within the a twin ontology of risk vectors and rule hardness, and are instantiated to the instance level to the favor of risk calculation and mitigation prioritization. Considering risk-tolerance to automatically prioritize mitigations enables implementations of the present disclosure to be sensitive to user preferences.

[0093] FIG. 7 depicts an example process 700 that can be executed in accordance with implementations of the present disclosure. In some implementations, the example

process 700 may be performed using one or more computer-executable programs executed using one or more computing devices.

[0094] A process-aware AAG and a risk tolerance profile are received (702). For example, a process-aware AAG representative of an enterprise network (or portion thereof) and a risk tolerance representative of risk tolerances of the enterprise across a set of risk aspects are received by each of a process-aware risk assessment module and a mitigation simulator module. A risk assessment is generated (704). For example, the process-aware risk assessment module generates a risk assessment based on the process-aware AAG and the risk tolerance profile. The risk assessment is received (706). For example, the mitigation simulator receives the risk assessment from the process-aware risk assessment module.

[0095] A mitigation list is generated (708). For example, the mitigation simulator executes a simulation (e.g., per Listing 1) based on the process-aware AAG, the risk tolerance profile, and the risk assessment and outputs a mitigation list. As described herein, the mitigation list includes a prioritized list of facts (input facts, derived facts) that can be mitigated to reduce risk. A set of remediation actions is determined (710). For example, one or more facts of the mitigation list is mapped to at least one mitigation action. In some examples, a fact-to-mitigation action mapping can be retrieved from computer-readable memory, which identifies remediation actions that can be executed for respective facts. Remediation actions are executed (712). For example, a remediation action is executed to mitigate risk resulting from a respective fact.

[0096] Implementations and all of the functional operations described in this specification may be realized in digital electronic circuitry, or in computer software, firmware, or hardware, including the structures disclosed in this specification and their structural equivalents, or in combinations of one or more of them. Implementations may be realized as one or more computer program products, i.e., one or more modules of computer program instructions encoded on a computer readable medium for execution by, or to control the operation of, data processing apparatus. The computer readable medium may be a machine-readable storage device, a machine-readable storage substrate, a memory device, a composition of matter effecting a machine-readable propagated signal, or a combination of one or more of them. The term “computing system”

encompasses all apparatus, devices, and machines for processing data, including by way of example a programmable processor, a computer, or multiple processors or computers. The apparatus may include, in addition to hardware, code that creates an execution environment for the computer program in question (e.g., code) that constitutes processor firmware, a protocol stack, a database management system, an operating system, or a combination of one or more of them. A propagated signal is an artificially generated signal (e.g., a machine-generated electrical, optical, or electromagnetic signal) that is generated to encode information for transmission to suitable receiver apparatus.

[0097] A computer program (also known as a program, software, software application, script, or code) may be written in any appropriate form of programming language, including compiled or interpreted languages, and it may be deployed in any appropriate form, including as a stand alone program or as a module, component, subroutine, or other unit suitable for use in a computing environment. A computer program does not necessarily correspond to a file in a file system. A program may be stored in a portion of a file that holds other programs or data (e.g., one or more scripts stored in a markup language document), in a single file dedicated to the program in question, or in multiple coordinated files (e.g., files that store one or more modules, sub programs, or portions of code). A computer program may be deployed to be executed on one computer or on multiple computers that are located at one site or distributed across multiple sites and interconnected by a communication network.

[0098] The processes and logic flows described in this specification may be performed by one or more programmable processors executing one or more computer programs to perform functions by operating on input data and generating output. The processes and logic flows may also be performed by, and apparatus may also be implemented as, special purpose logic circuitry (e.g., an FPGA (field programmable gate array) or an ASIC (application specific integrated circuit)).

[0099] Processors suitable for the execution of a computer program include, by way of example, both general and special purpose microprocessors, and any one or more processors of any appropriate kind of digital computer. Generally, a processor will receive instructions and data from a read only memory or a random access memory or both. Elements of a computer can include a processor for performing instructions and one

or more memory devices for storing instructions and data. Generally, a computer will also include, or be operatively coupled to receive data from or transfer data to, or both, one or more mass storage devices for storing data (e.g., magnetic, magneto optical disks, or optical disks). However, a computer need not have such devices. Moreover, a computer may be embedded in another device (e.g., a mobile telephone, a personal digital assistant (PDA), a mobile audio player, a Global Positioning System (GPS) receiver). Computer readable media suitable for storing computer program instructions and data include all forms of non-volatile memory, media and memory devices, including by way of example semiconductor memory devices (e.g., EPROM, EEPROM, and flash memory devices); magnetic disks (e.g., internal hard disks or removable disks); magneto optical disks; and CD ROM and DVD-ROM disks. The processor and the memory may be supplemented by, or incorporated in, special purpose logic circuitry.

[00100] To provide for interaction with a user, implementations may be realized on a computer having a display device (e.g., a CRT (cathode ray tube), LCD (liquid crystal display), LED (light-emitting diode) monitor, for displaying information to the user and a keyboard and a pointing device (e.g., a mouse or a trackball), by which the user may provide input to the computer. Other kinds of devices may be used to provide for interaction with a user as well; for example, feedback provided to the user may be any appropriate form of sensory feedback (e.g., visual feedback, auditory feedback, or tactile feedback); and input from the user may be received in any appropriate form, including acoustic, speech, or tactile input.

[00101] Implementations may be realized in a computing system that includes a back end component (e.g., as a data server), or that includes a middleware component (e.g., an application server), or that includes a front end component (e.g., a client computer having a graphical user interface or a Web browser through which a user may interact with an implementation), or any appropriate combination of one or more such back end, middleware, or front end components. The components of the system may be interconnected by any appropriate form or medium of digital data communication (e.g., a communication network). Examples of communication networks include a local area network ("LAN") and a wide area network ("WAN") (e.g., the Internet).

[00102] The computing system may include clients and servers. A client and server are generally remote from each other and typically interact through a communication network. The relationship of client and server arises by virtue of computer programs running on the respective computers and having a client-server relationship to each other.

[00103] While this specification contains many specifics, these should not be construed as limitations on the scope of the disclosure or of what may be claimed, but rather as descriptions of features specific to particular implementations. Certain features that are described in this specification in the context of separate implementations may also be implemented in combination in a single implementation. Conversely, various features that are described in the context of a single implementation may also be implemented in multiple implementations separately or in any suitable sub-combination. Moreover, although features may be described above as acting in certain combinations and even initially claimed as such, one or more features from a claimed combination may in some cases be excised from the combination, and the claimed combination may be directed to a sub-combination or variation of a sub-combination.

[00104] Similarly, while operations are depicted in the drawings in a particular order, this should not be understood as requiring that such operations be performed in the particular order shown or in sequential order, or that all illustrated operations be performed, to achieve desirable results. In certain circumstances, multitasking and parallel processing may be advantageous. Moreover, the separation of various system components in the implementations described above should not be understood as requiring such separation in all implementations, and it should be understood that the described program components and systems may generally be integrated together in a single software product or packaged into multiple software products.

[00105] A number of implementations have been described. Nevertheless, it will be understood that various modifications may be made without departing from the spirit and scope of the disclosure. For example, various forms of the flows shown above may be used, with steps re-ordered, added, or removed. Accordingly, other implementations are within the scope of the following claims.

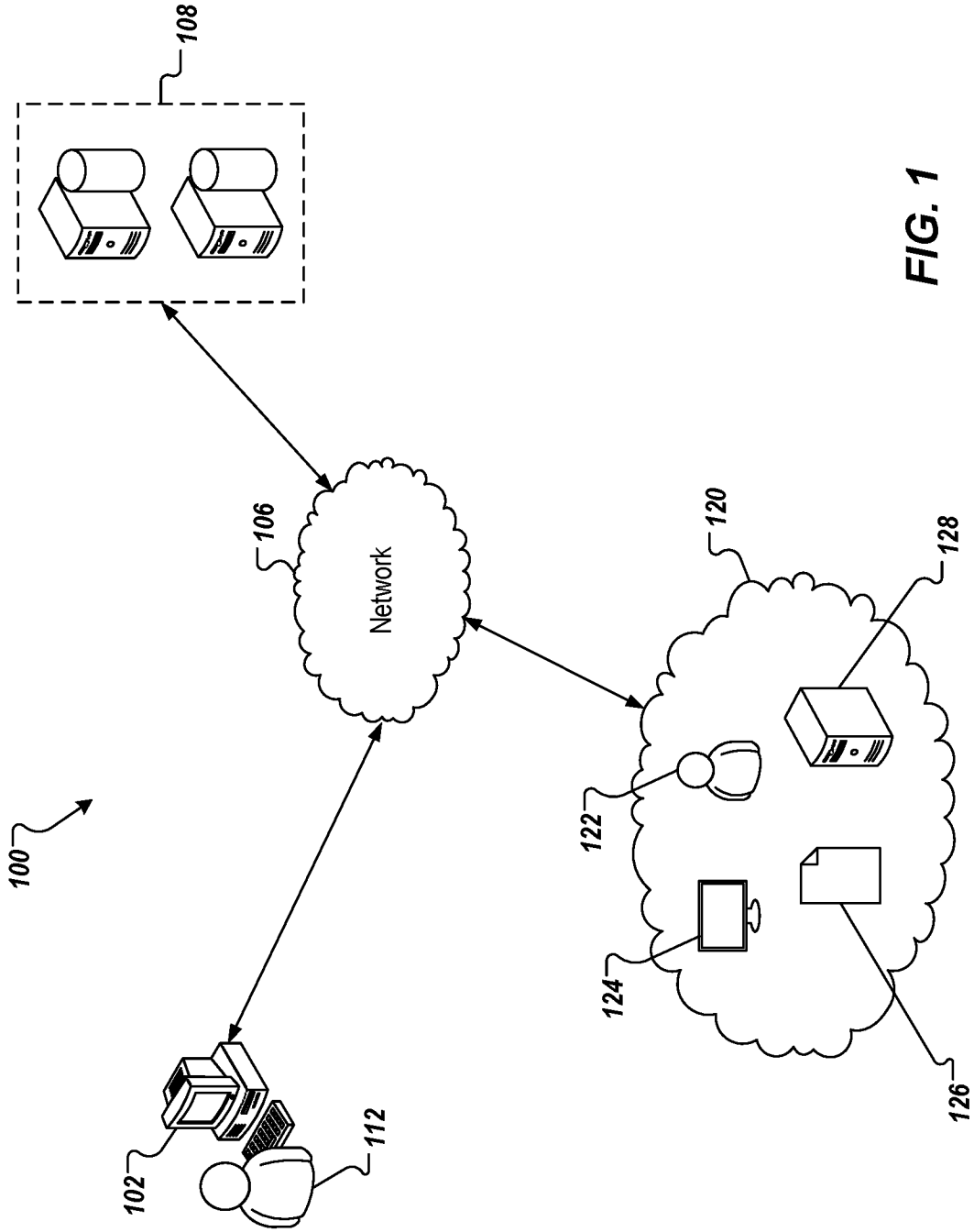


FIG. 1

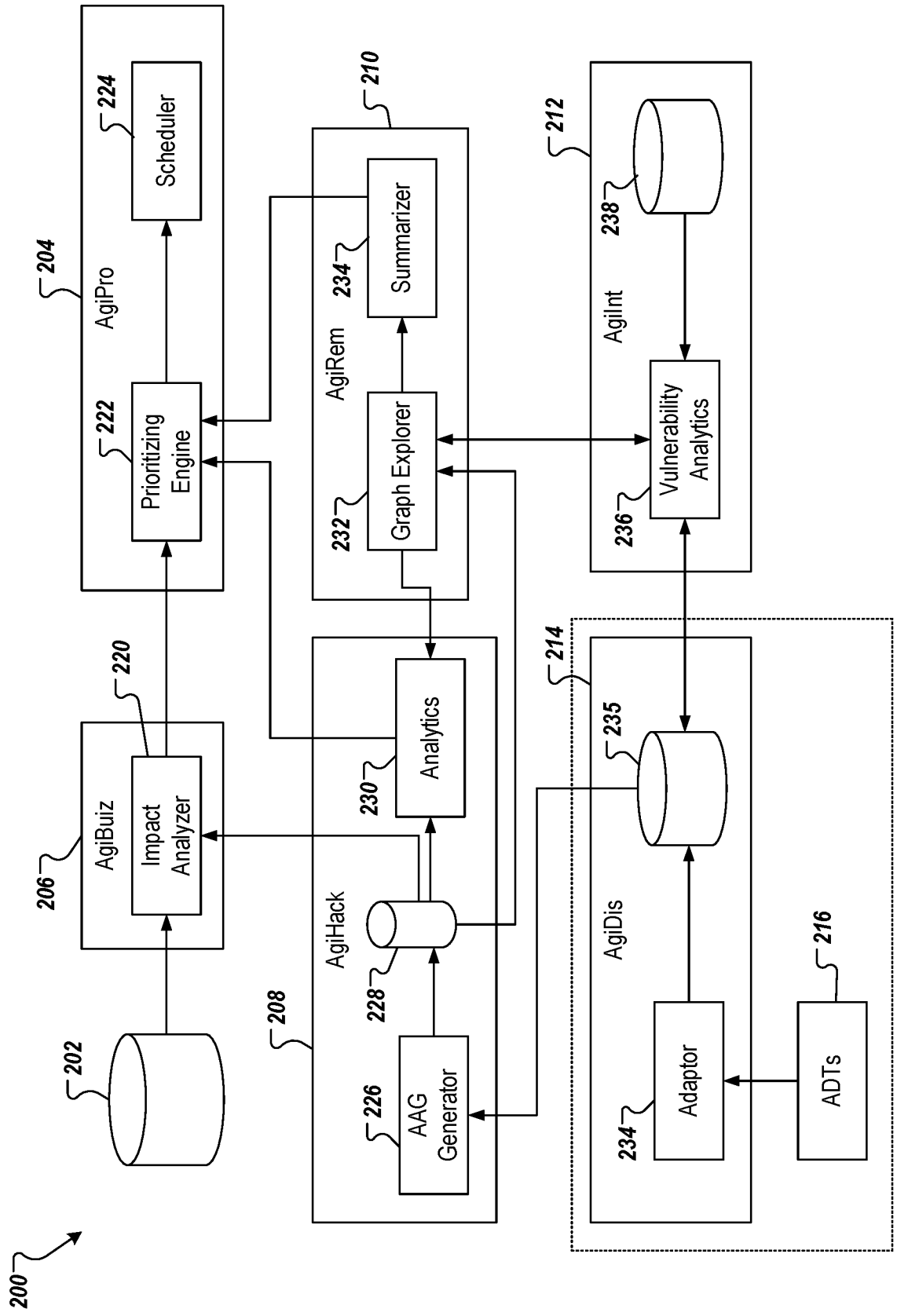

200
202
204
AgiPro
222
Prioritizing Engine
224
Scheduler
206
AgiBuiz
220
Impact Analyzer
208
AgiHack
228
226
AAG Generator
230
Analytics
210
AgiRem
232
Graph Explorer
234
Summarizer
212
AgiInt
236
Vulnerability Analytics
238
214
AgiDis
235
234
Adaptor
216
ADTs

FIG. 2

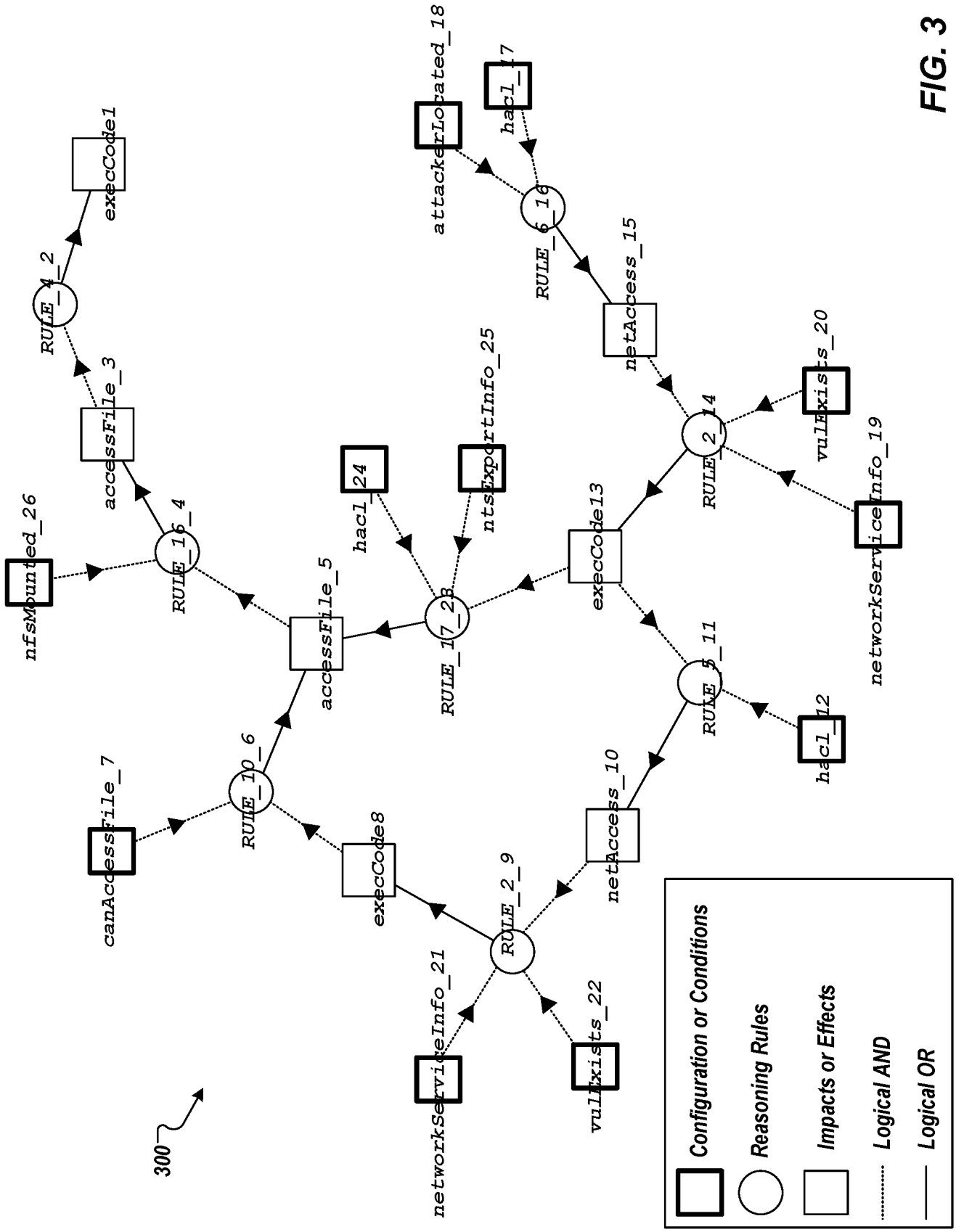

300
execCode1
RULE_4_2
accessFile_3
RULE_16_4
nfsMounted_26
canAccessFile_7
RULE_10_6
accessFile_5
execCode8
networkServiceInfo_21
RULE_2_9
vulExists_22
hacl_24
ntsExportInfo_25
RULE_17_23
netAccess_10
execCode13
RULE_3_11
hacl_12
attackerLocated_18
hacl_17
RULE_6_16
netAccess_15
RULE_2_14
vulExists_20
networkServiceInfo_19
Configuration or Conditions
Reasoning Rules
Impacts or Effects
Logical AND
Logical OR

FIG. 3

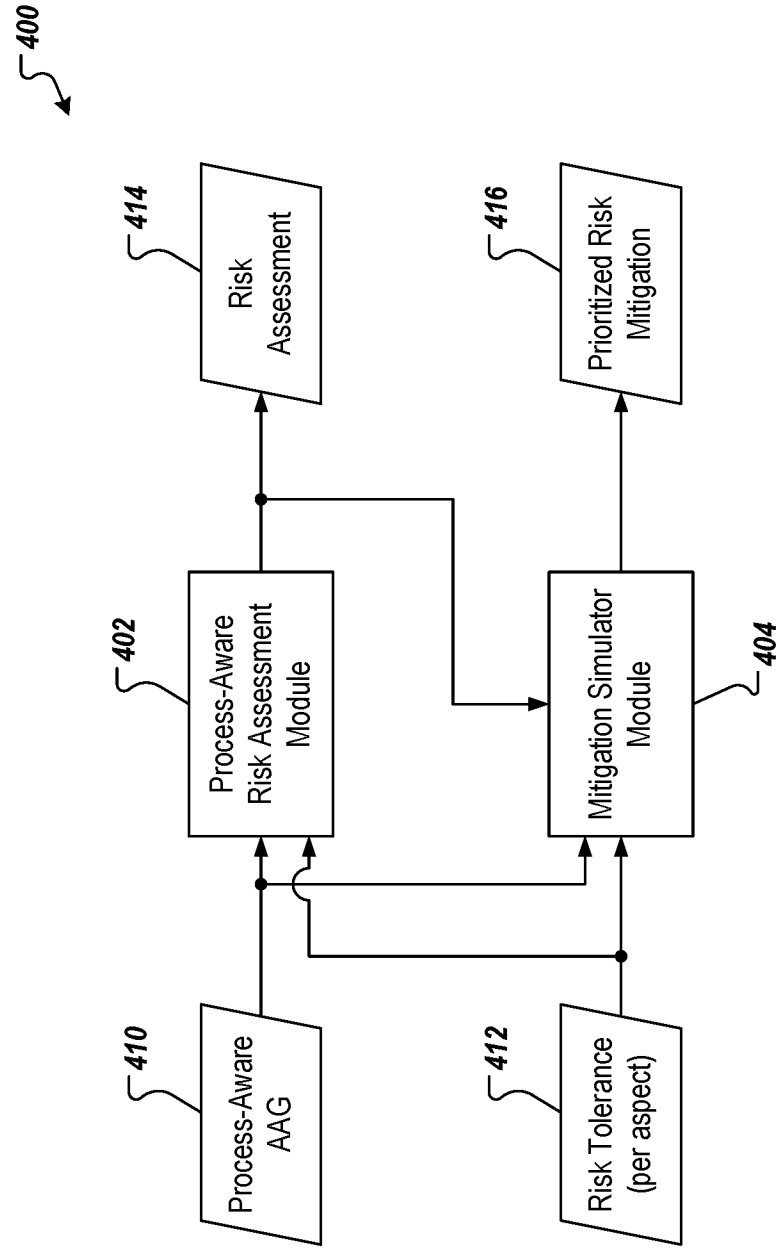

400
414
Risk Assessment
416
Prioritized Risk Mitigation
402
Process-Aware Risk Assessment Module
404
Mitigation Simulator Module
410
Process-Aware AAG
412
Risk Tolerance (per aspect)

FIG. 4

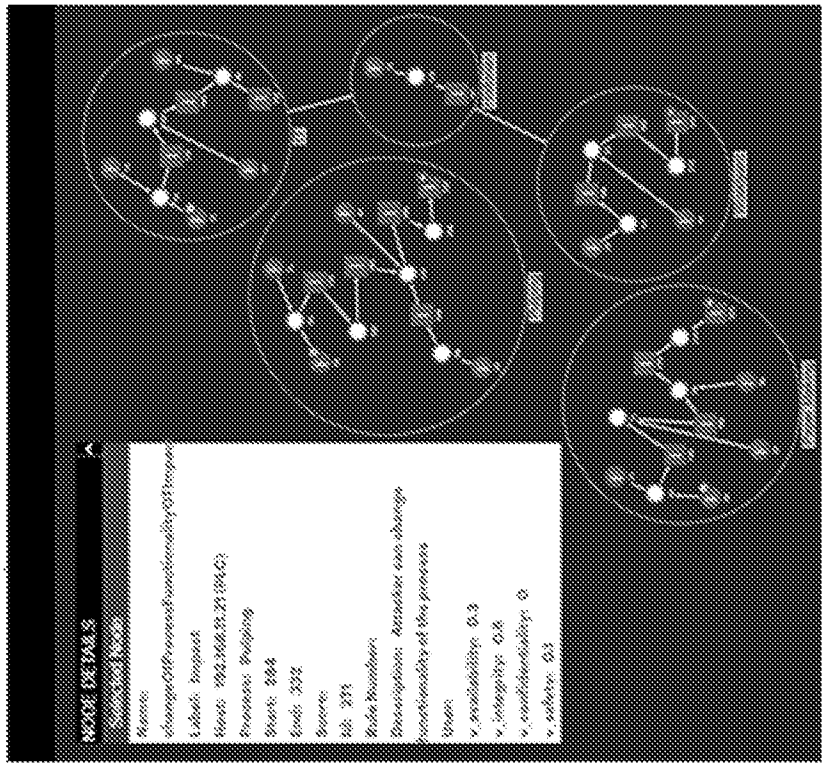


FIG. 5

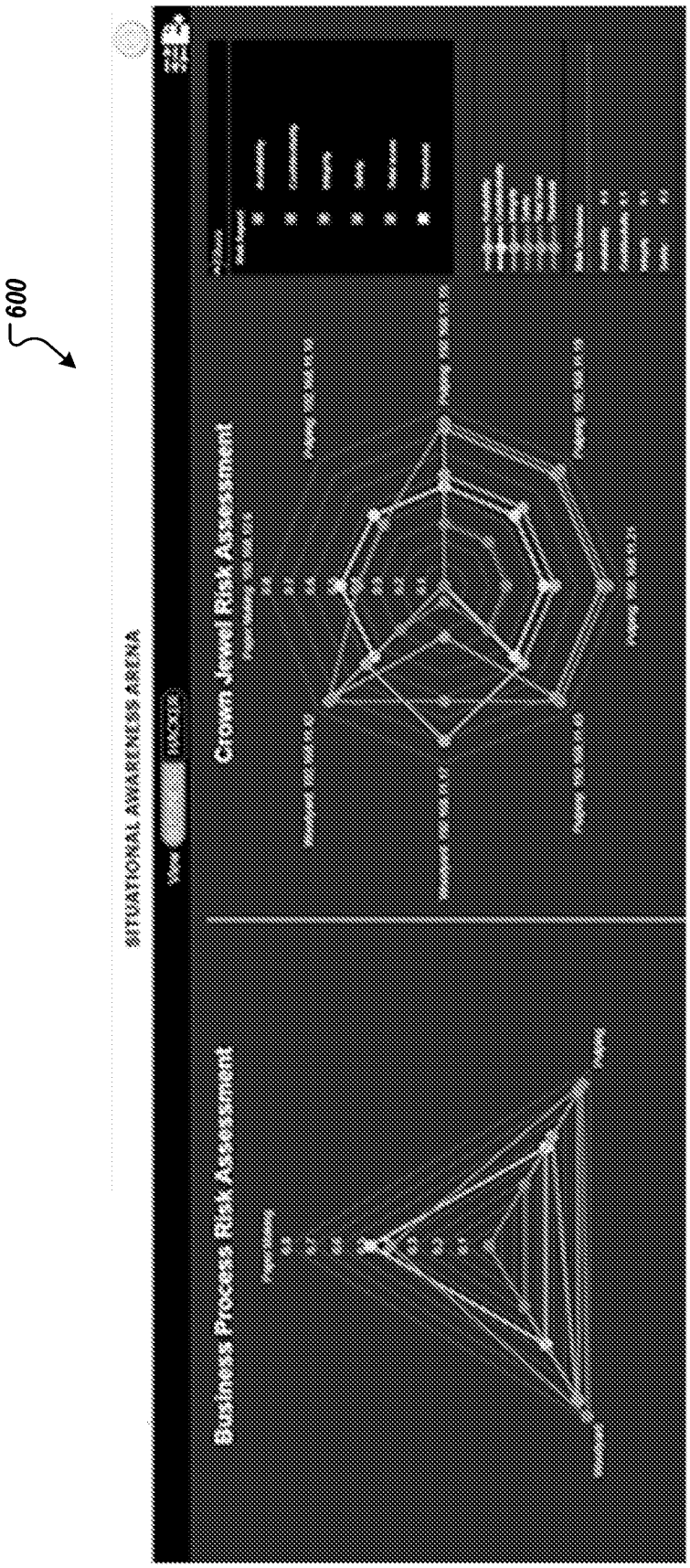

600
SITUATIONAL AWARENESS ARENA
Crown Jewel Risk Assessment
Business Process Risk Assessment

FIG. 6

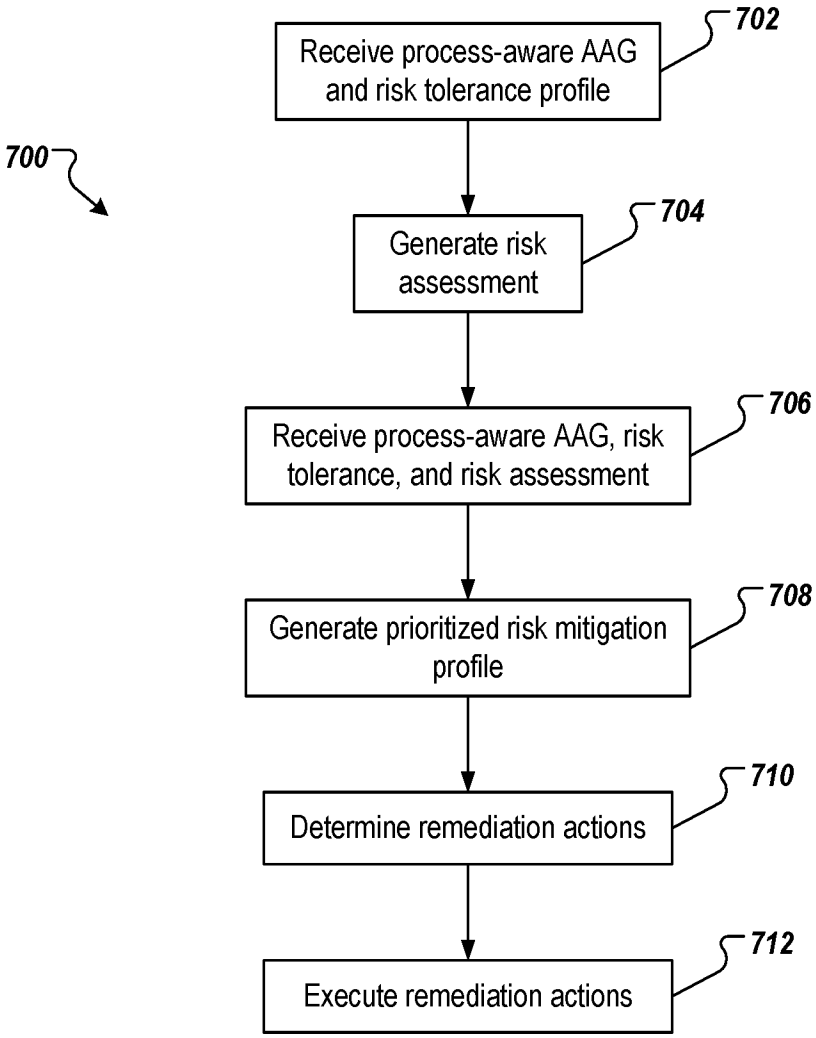

700
Receive process-aware AAG and risk tolerance profile
702
Generate risk assessment
704
Receive process-aware AAG, risk tolerance, and risk assessment
706
Generate prioritized risk mitigation profile
708
Determine remediation actions
710
Execute remediation actions
712

FIG. 7

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	AUTOMATED PRIORITIZATION OF PROCESS-AWARE CYBER RISK MITIGATION
First Named Inventor/Applicant Name:	Gal Engelberg
Filer:	Ryan McCarthy/Veronica Juarez
Attorney Docket Number:	12587-0887P01

Filed as Large Entity

Filing Fees for Provisional

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
PROVISIONAL APPLICATION FILING	1005	1	300	300
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**300**

Electronic Acknowledgement Receipt

EFS ID:	41953390
Application Number:	63150664
International Application Number:	
Confirmation Number:	2805
Title of Invention:	AUTOMATED PRIORITIZATION OF PROCESS-AWARE CYBER RISK MITIGATION
First Named Inventor/Applicant Name:	Gal Engelberg
Customer Number:	26212
Filer:	Ryan McCarthy/Veronica Juarez
Filer Authorized By:	Ryan McCarthy
Attorney Docket Number:	12587-0887P01
Receipt Date:	18-FEB-2021
Filing Date:	
Time Stamp:	12:08:18
Application Type:	Provisional

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$300
RAM confirmation Number	E20212HC08312369
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Provisional Cover Sheet (SB16)	12587-0887P01_TRANS.PDF	115178 7544becfc10a1274c31bc31383e610c81ddb5a5a	no	2
Warnings:					
This is not a USPTO supplied Provisional Cover Sheet SB16 form.					
Information:					
2	Application Data Sheet	12587-0887P01_ADS.pdf	1822903 d24ab4b5530cfb92fa50652ff5b16d7819ebebcb	no	9
Warnings:					
Information:					
3		12587-0887P01_APPLN.PDF	434907 799ada4c4bb95a84e8370ec098e7058014eb57ef	yes	36

Multipart Description/PDF files in .zip description

Document Description	Start	End
Abstract	36	36
Claims	34	35
Specification	1	33

Warnings:					
Information:					
4	Drawings-other than black and white line drawings	12587-0887P01_FIGs.pdf	1006672 896f53ebd25d2bd78f3faaeb420595639962f76f	no	7
Warnings:					
Information:					

5	Fee Worksheet (SB06)	fee-info.pdf	30060 d89905e6245cb1c163ac99cf6f2be737f239c093	no	2

Warnings:	
Information:	
Total Files Size (in bytes):	3409720

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

New Applications Under 35 U.S.C. 111

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

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

DocCode – SCORE

SCORE Placeholder Sheet for IFW Content

Application Number: 63150664 Document Date: 02/18/2021

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

- Drawing

At the time of document entry (noted above):

- USPTO employees may access SCORE content via DAV or via the SCORE web page.
- External customers may access SCORE content via PAIR using the Supplemental Content tab.

Form Revision Date: March 1, 2019