US 20160164917A1

(19) **United States**

(12) **Patent Application Publication**

Friedrichs et al.

(10) **Pub. No.: US 2016/0164917 A1**

(43) **Pub. Date: Jun. 9, 2016**

(54) **ACTION RECOMMENDATIONS FOR COMPUTING ASSETS BASED ON ENRICHMENT INFORMATION**

(71) Applicant: **Phantom Cyber Corporation**, Palo Alto, CA (US)

(72) Inventors: **Oliver Friedrichs**, Woodside, CA (US); **Sourabh Satish**, Fremont, CA (US); **Atif Mahadik**, Fremont, CA (US); **Govind Salinas**, Sunnyvale, CA (US)

(21) Appl. No.: **14/675,075**

(22) Filed: **Mar. 31, 2015**

Related U.S. Application Data

(60) Provisional application No. 62/087,025, filed on Dec. 3, 2014, provisional application No. 62/106,830, filed on Jan. 23, 2015, provisional application No. 62/106,837, filed on Jan. 23, 2015.

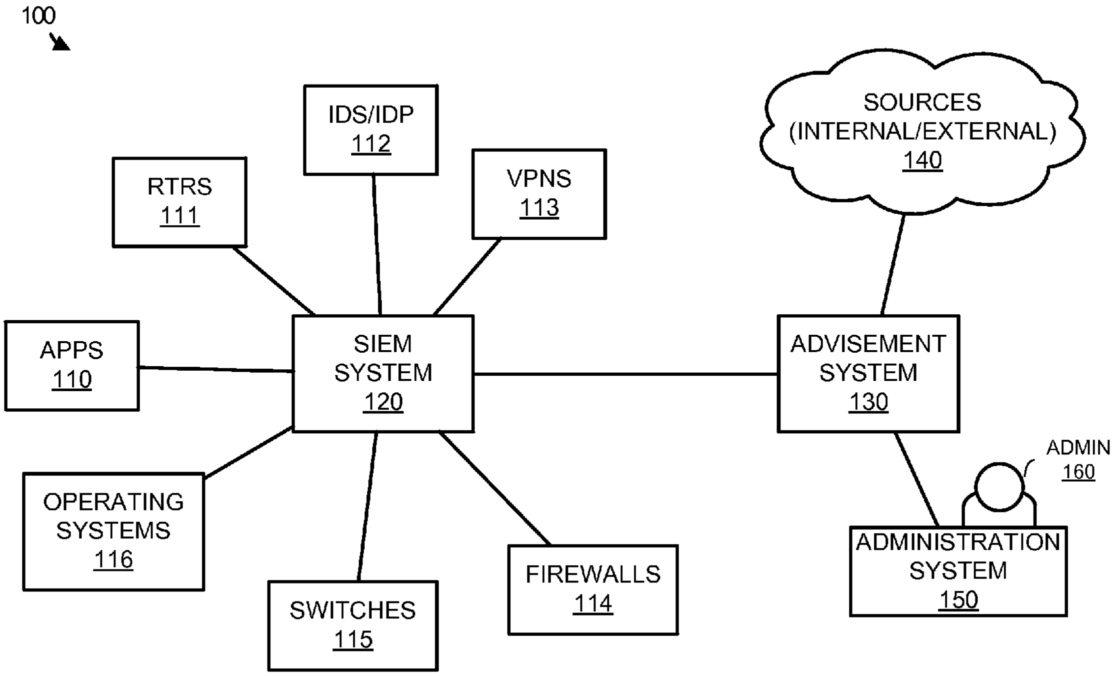
Publication Classification

(51) **Int. Cl.**
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/20*** (2013.01); ***H04L 63/0236*** (2013.01)

(57) **ABSTRACT**

Systems, methods, and software described herein provide security action recommendations to administrators of a computing environment. In one example, a method of operating an advisement system to provide action recommendations in a computing environment includes identifying a security incident for an asset in the computing environment. The method further includes, in response to identifying the security incident, gathering enrichment information about the security incident, and determining a rule set for the security incident based on the enrichment information. The method also provides recommending one or more actions to an administrator based on the rule set.



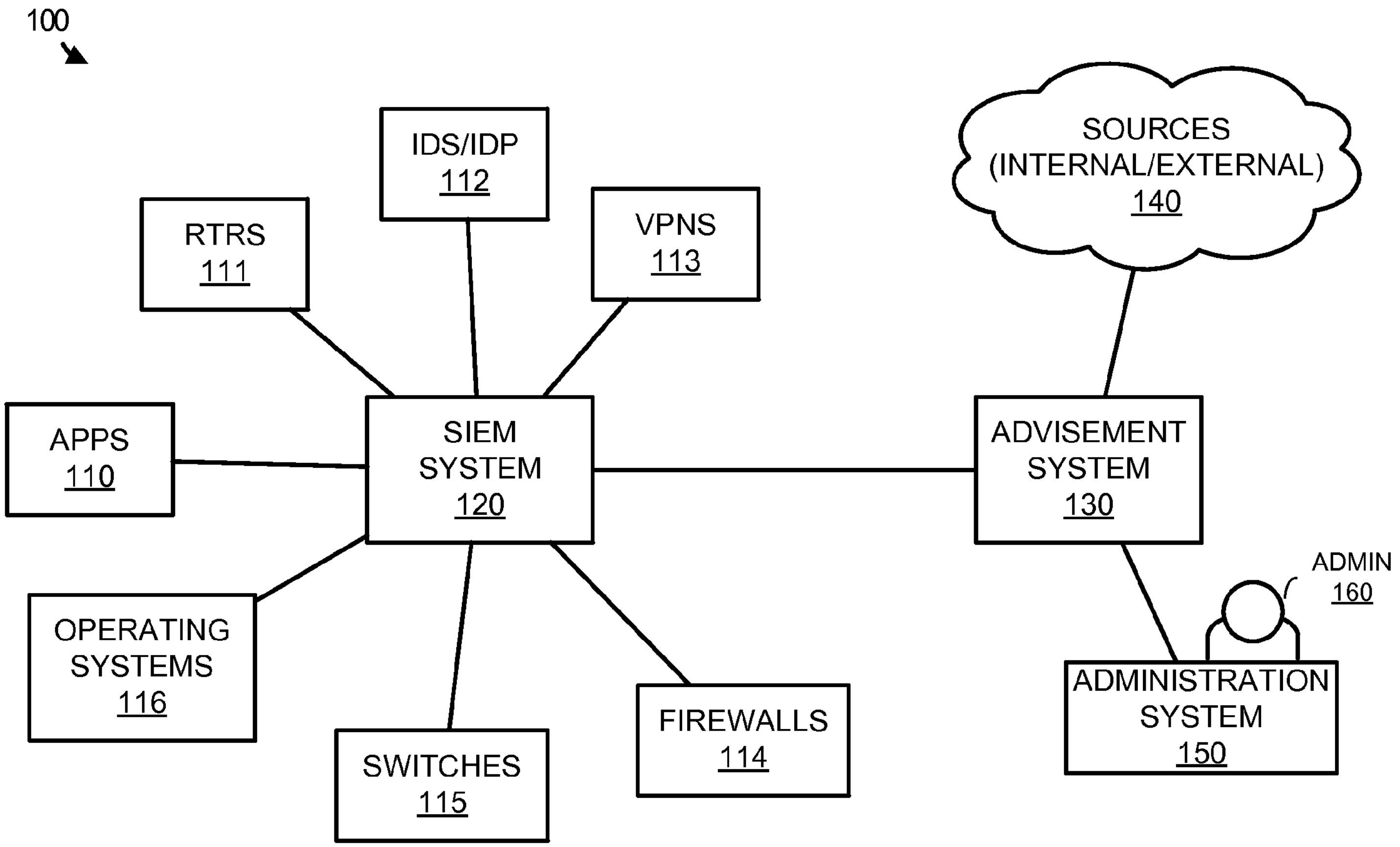

100
IDS/IDP
112
RTRS
111
VPNS
113
SOURCES
(INTERNAL/EXTERNAL)
140
APPS
110
SIEM
SYSTEM
120
ADVISEMENT
SYSTEM
130
ADMIN
160
OPERATING
SYSTEMS
116
FIREWALLS
114
ADMINISTRATION
SYSTEM
150
SWITCHES
115

FIGURE 1

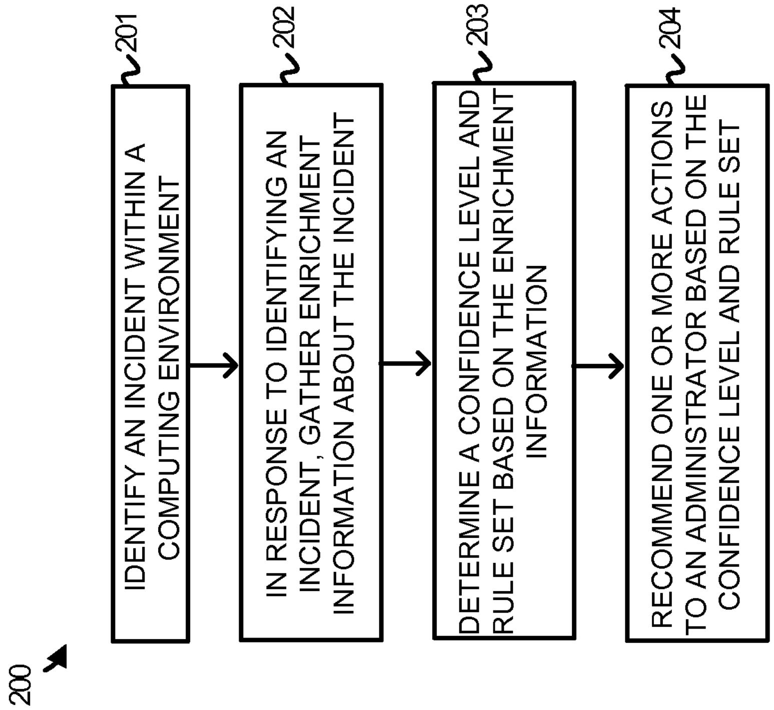

200
201
IDENTIFY AN INCIDENT WITHIN A COMPUTING ENVIRONMENT
202
IN RESPONSE TO IDENTIFYING AN INCIDENT, GATHER ENRICHMENT INFORMATION ABOUT THE INCIDENT
203
DETERMINE A CONFIDENCE LEVEL AND RULE SET BASED ON THE ENRICHMENT INFORMATION
204
RECOMMEND ONE OR MORE ACTIONS TO AN ADMINISTRATOR BASED ON THE CONFIDENCE LEVEL AND RULE SET

FIGURE 2

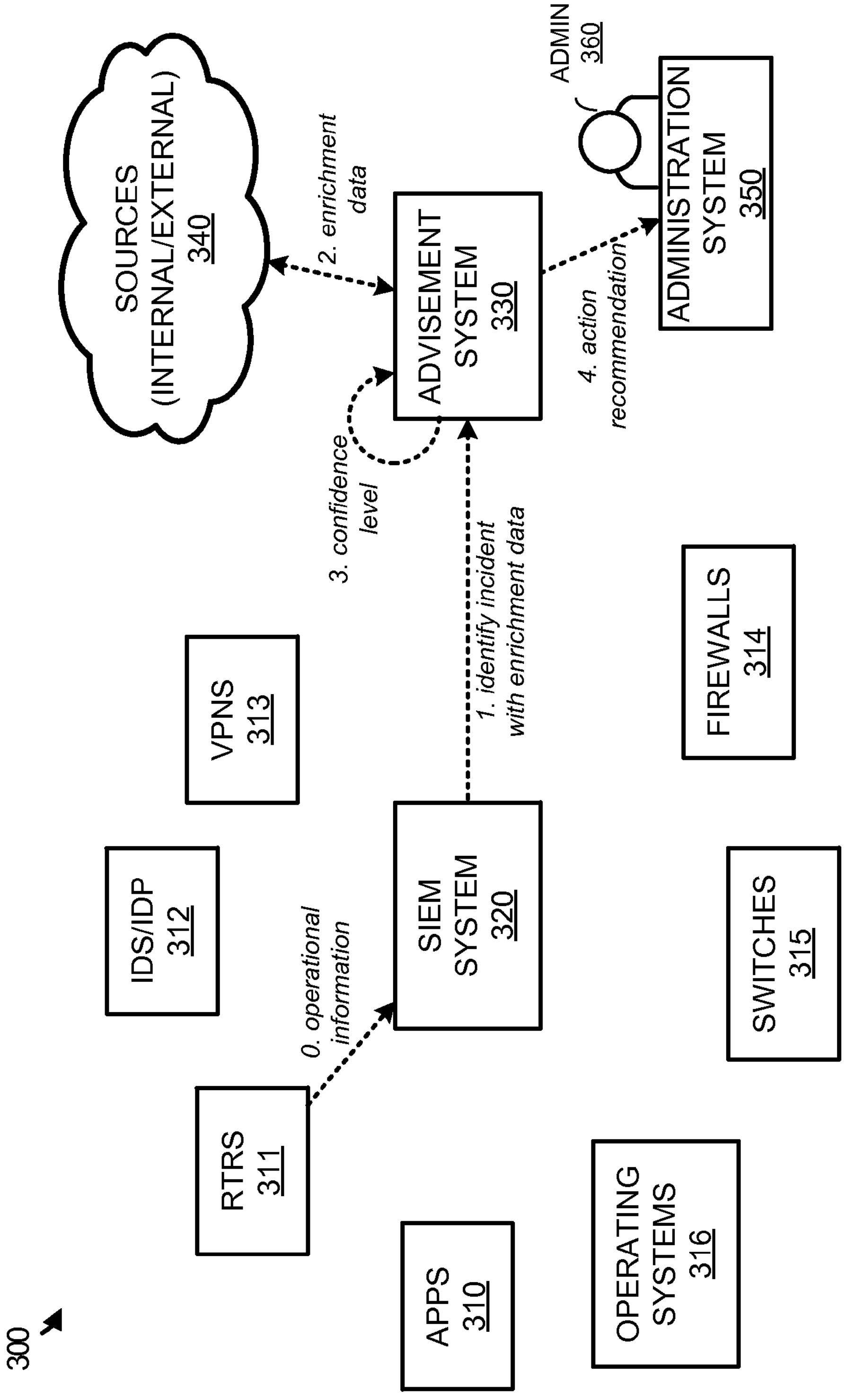

300
APPS 310
RTRS 311
IDS/IDP 312
VPNS 313
FIREWALLS 314
SWITCHES 315
OPERATING SYSTEMS 316
0. operational information
SIEM SYSTEM 320
1. identify incident with enrichment data
ADVISEMENT SYSTEM 330
2. enrichment data
SOURCES (INTERNAL/EXTERNAL) 340
3. confidence level
4. action recommendation
ADMINISTRATION SYSTEM 350
ADMIN 360

FIGURE 3

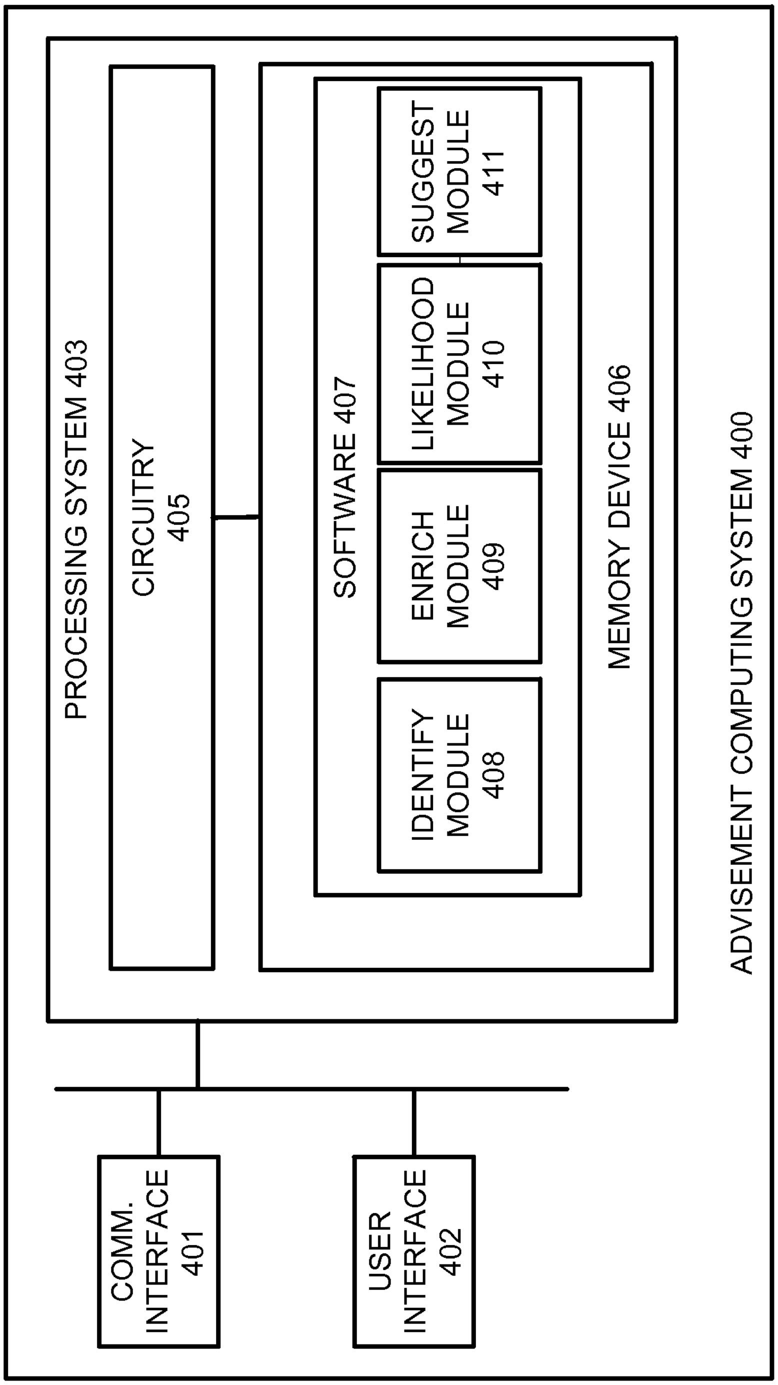

PROCESSING SYSTEM 403
CIRCUITRY
405
SOFTWARE 407
IDENTIFY
MODULE
408
ENRICH
MODULE
409
LIKELIHOOD
MODULE
410
SUGGEST
MODULE
411
MEMORY DEVICE 406
ADVISEMENT COMPUTING SYSTEM 400
COMM.
INTERFACE
401
USER
INTERFACE
402

FIGURE 4

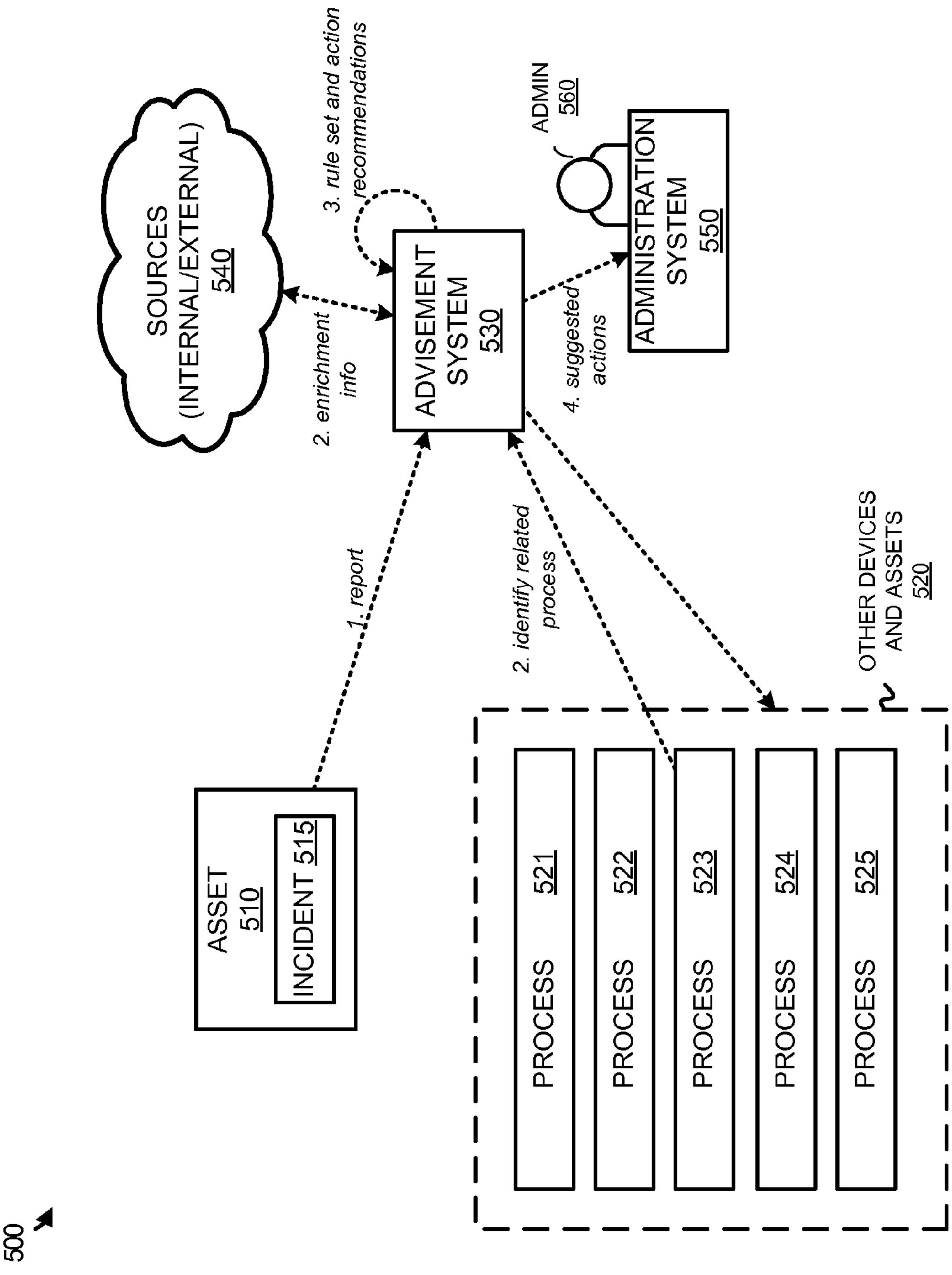

500
SOURCES (INTERNAL/EXTERNAL) 540
3. rule set and action recommendations
2. enrichment info
ADVISEMENT SYSTEM 530
ADMIN 560
ADMINISTRATION SYSTEM 550
4. suggested actions
1. report
2. identify related process
ASSET 510
INCIDENT 515
OTHER DEVICES AND ASSETS 520
PROCESS 521
PROCESS 522
PROCESS 523
PROCESS 524
PROCESS 525

FIGURE 5

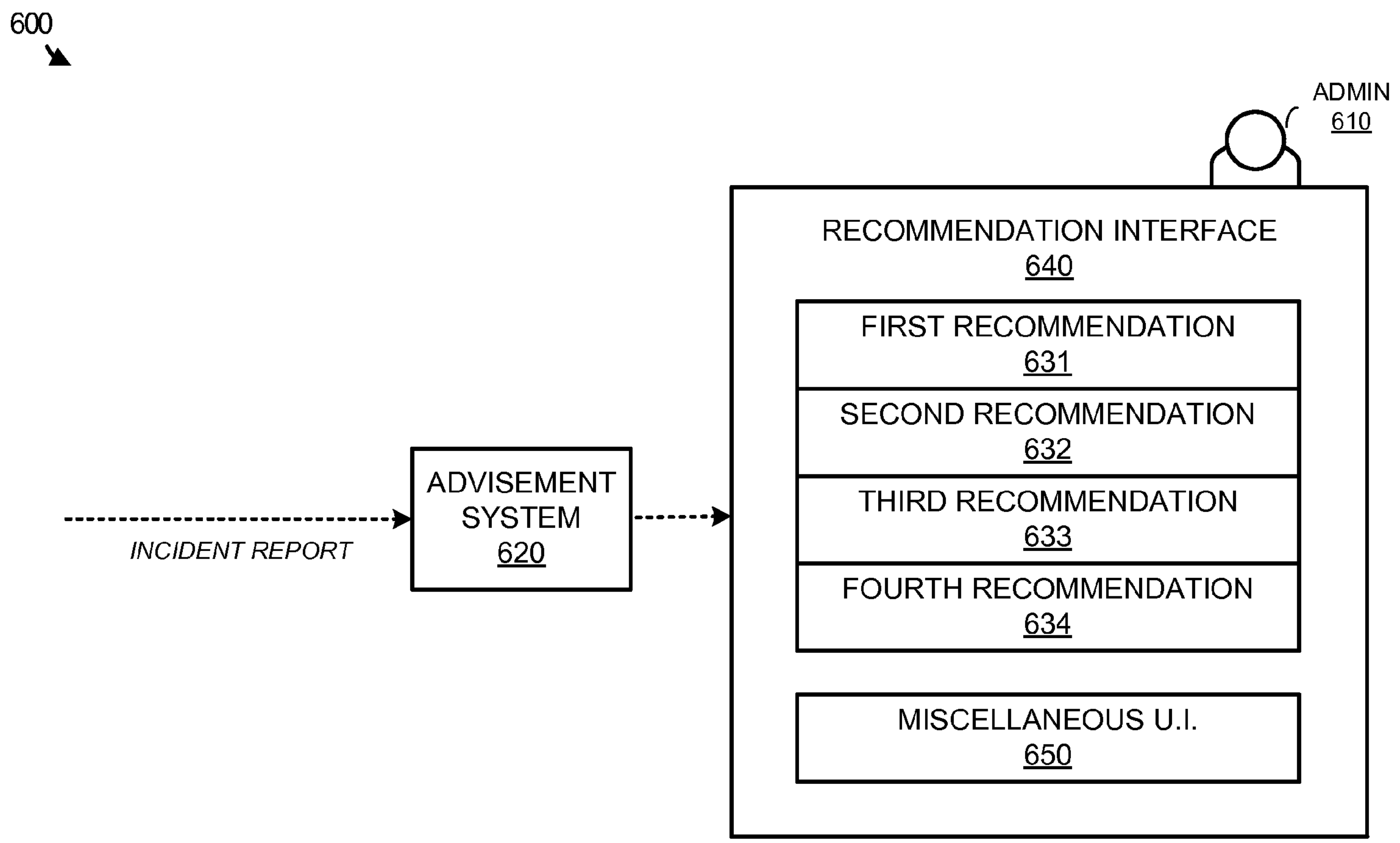

600
ADMIN
610
INCIDENT REPORT
ADVISEMENT SYSTEM
620
RECOMMENDATION INTERFACE
640
FIRST RECOMMENDATION
631
SECOND RECOMMENDATION
632
THIRD RECOMMENDATION
633
FOURTH RECOMMENDATION
634
MISCELLANEOUS U.I.
650

FIGURE 6

ACTION RECOMMENDATIONS FOR COMPUTING ASSETS BASED ON ENRICHMENT INFORMATION

RELATED APPLICATIONS

[0001] This application is related to and claims priority to U.S. Provisional Patent Application No. 62/087,025, entitled "ACTION RECOMMENDATIONS FOR COMPUTING ASSETS BASED ON ENRICHMENT INFORMATION," filed on Dec. 3, 2014, U.S. Provisional Patent Application No. 62/106,830, entitled "ACTION RECOMMENDATIONS FOR ADMINISTRATORS IN A COMPUTING ENVIRONMENT," filed on Jan. 23, 2015, and U.S. Provisional Patent Application No. 62/106,837, entitled "SECURITY ACTIONS IN A COMPUTING ENVIRONMENT," filed on Jan. 23, 2015, and which are hereby incorporated by reference in their entirety.

TECHNICAL FIELD

[0002] Aspects of the disclosure are related to computing environment security, and in particular to providing action recommendations to administrators based on enrichment information.

TECHNICAL BACKGROUND

[0003] An increasing number of data security threats exist in the modern computerized society. These threats may include viruses or other malware that attacks the local computer of the end user, or sophisticated cyber attacks to gather data and other information from the cloud or server based infrastructure. This server based infrastructure includes real and virtual computing devices that are used to provide a variety of services, such as data storage, cloud processing, web sites and services, amongst other possible services. To protect applications and services, various antivirus, encryption, and firewall implementations may be used across an array of operating systems, such as Linux and Microsoft Windows.

[0004] Further, computing environments may implement security information and event management (SIEM) systems to provide real-time analysis of security alerts generated by network hardware and applications. In particular SIEM systems allow for real-time monitoring, correlation of events, notifications, and console views for end users. Further, SIEM systems may provide log storage capable of managing historical information about various security events within the network. Although SIEMs generate security alerts within the network, administrators may be forced to translate each of these alerts into particular action. Thus, time and resources that could be used on other tasks may be used in researching and determining the course of action to handle the possible security threat.

OVERVIEW

[0005] Provided herein are methods, systems, and software to provide action recommendations for a plurality of network assets in a computing environment. In one example, a method of operating an advisement system to provide action recommendations in a computing environment comprising a plurality of computing devices includes identifying a security incident for an asset in the computing environment. The method further includes, in response to identifying the security incident, identifying enrichment information about the security incident. The method also provides determining a rule set for the security incident based on the enrichment information, and identifying one or more action recommendations for an administrator based on the rule set.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] Many aspects of the disclosure can be better understood with reference to the following drawings. While several implementations are described in connection with these drawings, the disclosure is not limited to the implementations disclosed herein. On the contrary, the intent is to cover all alternatives, modifications, and equivalents.

[0007] FIG. **1** illustrates a computing environment to provide action recommendations for a plurality of network assets.

[0008] FIG. **2** illustrates a method of operating an advisement system to provide action recommendations for a plurality of network assets.

[0009] FIG. **3** illustrates an overview of generating action recommendations for a network asset.

[0010] FIG. **4** illustrates an advisement computing system to provide action recommendations for a plurality of network assets.

[0011] FIG. **5** illustrates a computing environment to identify rule sets and recommend security actions for security incidents.

[0012] FIG. **6** illustrates an overview of providing a recommendation interface for an administrator of a computing environment.

TECHNICAL DISCLOSURE

[0013] Security information and event management (SIEM) systems provide analysis of security alerts generated by network hardware and processes. The network hardware and processes may include routers, firewalls, operating systems, applications executing on one or more computing devices, switches, or intrusion detection systems, amongst a variety of other network devices and processes. During the analysis of the particular network, a SIEM system may identify an issue and flag the issue as a possible security threat. Once flagged, the SIEM system may provide information to an administrator or store information about the threat to be analyzed for a possible solution.

[0014] Here, in addition to the operations provided by the SIEM system or other security monitoring systems within a computing environment, an advisement system may be used to identify and recommend the appropriate course of action to the related administrator. For example, if a SIEM system identified a possible security threat within a router of the network, information about the threat could be transferred to the advisement system, supplementary information about the threat could be identified from internal and external sources, and a recommendation could be determined based on the gathered supplementary information and a preconfigured rule set. Once the action recommendations are determined, the recommendations may be provided to an administrator, allowing the administrator to select a desired action and implement the action within the computing environment. In some implementations, the advisement system may be configured to provide a workflow allowing the administrator to step through the necessary steps of implementing the action. In other implementations, the advisement system may include connector or translator software modules that may automate or script the process of implementing the desired modification to the asset or computing environment. Thus, for each different type of asset within the environment, a connector may be provided to implement actions, such as blocking a particular process, blocking a particular network address, taking a snapshot of a computing environment, or other possible actions.

[0015] In some implementations, to manage the various rule sets for the advisement system, one or more data structures may be accessible by the advisement system that relate rule sets to assets, incidents, and enrichment information. For example, an incident may be reported for an unknown process executing on a virtual machine asset. Once enrichment information is gathered about the unknown process, the advisement system may identify a rule set that applies to virtual machines, unknown processes, and the enrichment information determined about the unknown process. Accordingly, an unknown process that is known to be malicious from the enrichment information may be associated with a different rule set than an unknown process that cannot be confirmed to be malicious.

[0016] To further illustrate the operation of an advisement system within a computing network, FIG. **1** is provided. FIG. **1** illustrates a computing environment **100** to provide action recommendations for a plurality of network assets. Computing environment **100** includes computing assets **110-116**, SIEM system **120**, advisement system **130**, sources **140**, and administration system **150**. Computing assets **110-116** include applications **110**, routers **111**, intrusion detection systems and intrusion prevention system (IDS/IDP) **112**, virtual private networks (VPNs) **113**, firewalls **114**, switches **115**, and operating systems **116**, although other assets may exist. Assets **110-116** may execute via any number of computing systems or devices. In addition to the routers and switches, these computing devices may include server computers, desktop computers, laptop computers, and the like. Although not illustrated in the present example, in some implementations, assets may be defined at computing system level. Accordingly, assets may be defined as servers, end user computing systems, host computing systems, and the like that each include an operating system, applications, processes, and firewalls.

[0017] SIEM system **120**, advisement system **130**, sources **140**, and administration system **150** may each include communication interfaces, network interfaces, processing systems, computer systems, microprocessors, storage systems, storage media, or some other processing devices or software systems, and can be distributed among multiple devices. SIEM system **120**, advisement system **130**, and sources **140** may comprise one or more server, desktop, laptop, or other similar computing devices. Administration system **150** may comprise an end user device, such as a desktop computer, laptop computer, smartphone, tablet, or any other similar computing device.

[0018] Advisement system **130** communicates with SIEM system **120**, sources **140**, and administration system **150** via communication links that may use Time Division Multiplex (TDM), asynchronous transfer mode (ATM), internet protocol (IP), Ethernet, synchronous optical networking (SONET), hybrid fiber-coax (HFC), circuit-switched communication signaling, wireless communications, or some other communication format, including combinations and improvements thereof. Similarly, SIEM system **120** may gather information from assets **110-116** via a plurality of communication links to the computing systems associated with the assets, wherein the links may use TDM, ATM, IP, Ethernet, SONET, HFC, circuit-switched communication signaling, wireless communications, or some other communication format, including combinations and improvements thereof. While not illustrated in the present example, it should be understood that advisement system **130** might communicate with the assets over various communication links and communication formats to implement desired security actions.

[0019] In operation, SIEM system **120** receives data and performance information from assets **110-116** and performs inspections to identify possible security issues. Once SIEM system **120** identifies a possible security threat, information about the security threat is transferred to advisement system **130**. Advisement system **130** identifies the security threat and analyzes the threat using sources **140** to determine suggested actions against the security threat. Once the suggested actions are determined, the actions are transferred, via email, text message, or other similar format, to administration system **150** to be presented to administrator **160**.

[0020] To further illustrate the operation of computing environment **100**, FIG. **2** is provided. FIG. **2** illustrates a method **200** of operating advisement system **130** to provide action recommendations for a plurality of network assets. In particular, as described in FIG. **1**, SIEM system **120** receives information from a plurality of network assets **110-116** and identifies security threats based on the information. Once a threat is identified, the threat is transferred to advisement system **130**. Advisement system **130** identifies the security threat or incident within computing environment **100** (**201**), and in response to identifying the incident, gathers enrichment information about the incident (**202**). Specifically, advisement system **130** may identify properties or traits of the incident, such as internet protocol (IP) addresses associated with the incident, the firewall associated with the incident, the computing device for the incident, the host, the user, any uniform resource locators (URLs) associated with the incident, or any other information specific to the security incident. Once the properties are identified, advisement system **130** may identify information related to the threat using internal and external sources **140**. These sources may include databases or websites that keep track of malicious IP addresses or domain names, the type of threats presented from the particular domain names, identifies of malware, Trojans, and viruses, amongst a variety of other information.

[0021] Upon determining enrichment information related to a particular incident, administration system **130** may determine a rule set based on the enrichment information (**203**). This rule set is related to the type of threat presented to the network and computing environment **100**. For example, as enrichment information is gathered related to a particular incident, administration system **130** may use predefined criteria to establish how likely the identified incident is a security threat to computing environment **100**. Based on this likelihood and a corresponding related rule set, one or more actions may be recommended to administrator **160** on administration system **150** (**204**).

[0022] For instance, SIEM system **120** may identify that an application of applications **110** is receiving a large amount of inbound requests from a particular IP address and flag these requests as a possible incident. Once flagged, information or traits regarding the inbound requests and the application is transferred to advisement system **130** including the IP address, the type of data requested, or any other information related to the request. Upon identifying the flagged incident, advisement system **130** determines enrichment information for the incident via sources **140**. If advisement system **130** determines that the incident is likely a security threat based on the enrichment information, advisement system **130** may determine suggested actions based on an identified rule set, and provide the actions to an administrator responsible for the application via email, text message, or some other form of communication. These actions may include preventing the application from future execution, sand boxing the computing system executing the application, taking an image of the computing system executing the application, removing the security threat within the application, amongst a variety of other actions. For example, if the enrichment information identifies that the inbound requesting IP address is associated with malicious operations, advisement system **130** may recommend sand boxing the computing system, or implementing a firewall configuration that prevents generating a response to requests from the particular IP address. In contrast, if the IP address is unknown or sources **140** do not indicate that the IP address is malicious, advisement system **130** may select a different rule set and corresponding action recommendations that could allow further monitoring of the interactions between the asset and the unknown IP address.

[0023] In some implementations, gathering information about the security incident may further include gathering information about related processes within the environment. For example, if an application is identified as exhibiting unusual behavior related to a possible security threat, the advisement system may identify other processes executing on one or more devices that are related to the application. Accordingly, if it is determined that the application is required by other processes, recommendations may be determined that allow the other processes to continue to use the application, but may limit or further monitor other interactions initiated by the flagged application. These recommendations may include taking a snapshot of the application or of the full computing system to identify any unusual process within the application, prevent the application from initiating communications with external systems and processes, or any other similar function that allows the required processes to continue to communicate with the required application.

[0024] In some instances, the advisement system may have access to a database of known applications and executables within the computing environment, which can be compared to the application related to the incident. For example, an executable may be titled RESEARCH.EXE. Once an incident is identified that is related to RESEARCH.EXE, the advisement system may attempt to identify any other system or process that requires or acknowledges that executable. If no other system or process requires or acknowledges the executable, recommendations may be made that can remove that application, or otherwise prevent the operation of RESEARCH.EXE.

[0025] In some examples, the rule set for a particular security incident may identify a preconfigured action to take against the threat. Thus, in addition to or in place of recommending actions to an administrator, the administrator may preapprove certain actions against particular security incidents. Although illustrated in the present example as receiving information about an incident from a SIEM system, it should be understood that other security systems, such as security processes on the individual computing devices, might provide the security threat information to the advisement system. In some implementations, a user or administrator may define a security incident in the environment, which can then be identified by the advisement system. This user or administrator defined incident may allow the personnel to define various information about the incident, including the asset involved in the incident, a computing device identifier for the incident, the type of suspected threat, or any other similar characteristic from the incident. Once defined, the advisement system may gather enrichment information related to the incident from internal and external sources. As the enrichment information is gathered, a rule set may be identified and action recommendations determined for the threat.

[0026] In some implementations, advisement system **130** may be configured to generate a display of the action recommendations and provide the display to the administrator either locally on advisement system **130**, or externally on a console such as administration system **150**. This display may include the various action recommendations as well as other relevant security event characteristics. These characteristics may include a chat room that allows the administrator to chat with any other administrator associated with the particular threat, a summary window that displays information about the threat, such as an identifier for the asset, IP address information for the security incident, a URL associated with the security incident, or other similar information.

[0027] To further demonstrate the process of generating actions for an administrator, FIG. **3** is included. FIG. **3** illustrates an overview **300** of generating action recommendations for a network asset. Overview **300** includes computing assets **310-316**, SIEM system **320**, advisement system **330**, sources **340**, and administration system **350**. Computing assets **310-316** include applications **310**, routers **311**, intrusion detection systems and intrusion prevention system (IDS/IDP) **312**, virtual private networks (VPNs) **313**, firewalls **314**, switches **315**, and operating systems **316**. Assets **310-316** may execute via any number of computing systems or devices. In addition to the routers and switches, these computing devices may include server computers, desktop computers, laptop computers, and the like.

[0028] As depicted, SIEM system **320** receives operational information from assets **310-316**. This operational information may include information about the devices connecting with the assets, the type of data be communicated over the assets, the number of times a device contacts an asset, and other similar operational information. Based on the operational information, SIEM system **320** identifies an incident with a router in routers **311**. This incident may include an unknown IP address, an improper number of requests over the router, or any other incident within the router. Once identified, the incident is forwarded to advisement system **330**, wherein advisement system **330** will identify enrichment data for the incident. This enrichment information may include information about the IP address related to the incident, the URL address associated with the incident, or any other information related to the incident. For example, SIEM system **320** may identify an incident corresponding to an unknown URL connection with the router in routers **311**. Once advisement system **330** is notified of the incident, advisement system **330** may query a database or external source to determine information about the URL, including whether the URL is malicious, the owner of the URL, the relation of the URL to the devices in the network, or any other enrichment information.

[0029] Once enrichment information is gathered, advisement system **330** may determine a confidence level of whether the incident involves a security threat and a rule set based on the enrichment information. Referring again to the previous example, advisement system **330** may determine that the particular URL has been associated with a malicious virus. Accordingly, the confidence level and rule set may reflect that there is a security threat related to the URL on the router. In contrast, if no enrichment information is available, a lower confidence level may be defined for the incident and a separate rule set may be defined for the router.

[0030] Upon determining the confidence level and rule set, one or more action recommendations may be transferred to administration system **350** and administrator **360** based on the enrichment information. In some examples, advisement system **330** may include action routing information that identifies personnel responsible for each of the assets within the computing network. For example, a first administrator may be responsible for particular applications, whereas second administrator may be responsible for the routers and the switches. Thus, once an action is identified, advisement system **330** may direct the action recommendations to the proper administration personnel. Further, in some instances, the administration personnel may be tiered to respond to each of the security threats. This use of tiers allows recommendations to be forwarded to a second personnel member if a first member has not responded to the recommendations.

[0031] Further, although illustrated as providing recommendations to an administrator in the present example, it should be understood that an administrator might preapprove particular actions as part of a rule set. Thus, if a particular threat is identified, predefined actions might be taken based on the confidence level and rule set. Additionally, the actions that are provided to an administrator may be based on previous selections of the administrator. For example, a list of recommendations is provided to the administrator for a particular threat, and the user makes an initial action selection from the list. On the next occurrence of the same or similar threat, the recommendations that are provided to the user may include a new list of recommendations based on the user's previous selection for the identified threat. Thus, as input is collected from each of the administrators within the computing environment, recommendations may improve based at least in part on previous recommendation selections.

[0032] In some examples, the action recommendations referred to administrator **360** may change in accordance with a change in the confidence level. For example, when an incident is first encountered, advisement system **330** may transfer a first set of recommended actions based on the unknown threat level of the incident. However, as further enrichment information is gathered about the incident, a second set of recommended actions may be transferred to the administrator. Thus, the action recommendations may be dynamic in accordance with the current confidence in the threat presented and the rule set corresponding to the confidence.

[0033] In some implementations, the advisement system may generate action recommendations based on the cost of the asset or the cost of the action. This cost determination may be assigned by administrators of the computing environment, may be based on the type of information that is stored on the computing asset, may be determined based on the amount of disruption that an action may cause in the environment, or may be determined by any other method. For example, a financial officer's computing system in the computing environment may have a higher cost or priority than an intern's computing system due to the data that is accessible from the computing systems. Accordingly, action recommendations for the financial officer's computing asset may be different than the action recommendations that are generated for the intern's computing asset. Further, the action recommendations may also be allocated a cost rating that relates each of the actions to an effect that the actions will have on the environment. For example, the cost of an action that places a computing asset into a virtual local area network (VLAN) may have a higher cost or be more disruptive to the computing environment than preventing the computing asset from communicating with particular IP addresses. Based on the importance or cost of the system and the cost of the actions, recommendations may be provided to the administrator. As an example, a computing asset that requires high availability may be provided with actions that do not disrupt availability of the asset. Likewise, if the system includes sensitive data, actions may be more conservative to prevent the sensitive data from being inappropriately accessed.

[0034] Turning to FIG. **4**, FIG. **4** illustrates an advisement computing system **400** to provide action recommendations for a plurality of network assets. Advisement computing system **400** is representative of a computing system that may be employed in any computing apparatus, system, or device, or collections thereof, to suitably implement the advisement systems described herein. Computing system **400** comprises communication interface **401**, user interface **402**, and processing system **403**. Processing system **403** is communicatively linked to communication interface **401** and user interface **402**. Processing system **403** includes processing circuitry **405** and memory device **406** that stores operating software **407**.

[0035] Communication interface **401** comprises components that communicate over communication links, such as network cards, ports, RF transceivers, processing circuitry and software, or some other communication devices. Communication interface **401** may be configured to communicate over metallic, wireless, or optical links. Communication interface **401** may be configured to use TDM, IP, Ethernet, optical networking, wireless protocols, communication signaling, or some other communication format—including combinations thereof. In particular, communication interface **401** communicates with a SIEMs system that gathers security incident information from a plurality of assets within a computing environment. Further, communication interface **401** may be configured to communicate with one or more administrations systems to provide the suggested course of action to administrators.

[0036] User interface **402** comprises components that interact with a user. User interface **402** may include a keyboard, display screen, mouse, touch pad, or some other user input/output apparatus. User interface **402** may be omitted in some examples.

[0037] Processing circuitry **405** comprises microprocessor and other circuitry that retrieves and executes operating software **407** from memory device **406**. Memory device **406** comprises a non-transitory storage medium, such as a disk drive, flash drive, data storage circuitry, or some other memory apparatus. Operating software **407** comprises computer programs, firmware, or some other form of machine-readable processing instructions. Operating software **407** includes identify module **408**, enrichment module **409**, likelihood module **410**, and suggest module **411**, although any number of software modules may provide the same operation. Operating software **407** may further include an operating system, utilities, drivers, network interfaces, applications, or some other type of software. When executed by circuitry **405**, operating software **407** directs processing system **403** to operate advisement computing system **400** as described herein.

[0038] In particular, identify module **408** is configured to, when executed by advisement computing system **400** and processing system **403**, to identify a security incident for an asset within the computing environment. Once identified via a SIEM system or other security monitoring module, enrichment module **409** identifies enrichment information for the security incident. This enrichment information may be gathered from sources internal to the computing environment, as well as external sources, such as websites and databases. For example, if an asset within the computing environment was connecting in an abnormal way to a particular IP address, enrichment module **409** may contact one or more sources to determine information about the unknown IP address. These sources may include information about whether the address is malicious, whether the address belongs to a particular entity, or any other similar information regarding the IP address.

[0039] Once the enrichment information is determined, likelihood module **410** may determine a threat confidence level and rule set for the security incident based on the enrichment information. This confidence level relates the security incident to the likelihood that the incident is related to a malicious activity. For instance, if an external source verified that an IP address corresponded to malicious software activity, the confidence level and rule set would be different than for an unknown IP address. Once the confidence level and rule set is determined, suggest module **411** determines suggested security actions for an administrator based on the identified rule set. These suggestions may include suggestions to eliminate a malicious item related to the security incident, segregating the asset from other assets within the network, imaging computing system to provide further analysis on the incident, amongst a variety of other suggested security actions.

[0040] Referring now to FIG. **5**, FIG. **5** illustrates a computing environment **500** to identify rule sets and recommend security actions for security incidents. Computing environment **500** includes asset **510**, other devices and assets **520**, advisement system **530**, internal and external sources **540**, and administration system **550**. Asset **510** is further associated with incident **515**, and other devices and assets **520** execute processes **521-525**. Asset **510** and other devices and assets **520** may comprise routers, switches, operating systems, applications, processes, or any other similar asset within a computing environment.

[0041] As illustrated, advisement system **530** identifies an incident **515** related to asset **510**. This incident report may include an identifier for the asset, an identifier for the computing device associated with the asset, a URL associated with the incident, an application, process, or executable for the incident, or any other similar information about the incident. For example, if incident **515** corresponded to an executable, the report to advisement system **530** may include the name, file path, and other related information to the executable. In some implementations, the report may be generated by a SIEM system to be provided to advisement system **530**. However, in other examples, the report may be generated by other security devices including, but not limited to, the devices associated with the assets, or other security monitoring hardware.

[0042] Once a report of incident **515** is received, advisement system **530** may gather enrichment information from sources **540** to gather further data related to the particular incident. For example, if the incident were related to communications with a particular IP address, advisement system **530** may query a database, either internal or external to the computing environment, to determine if the IP address is related to malicious activity. Here, in addition to querying the internal and external sources, advisement system **530** identifies related processes to incident **515**. For example, incident **515** may be related to a particular application within the network, such as a database application or some other application. Once an incident is identified with the application, advisement system **530** may determine other applications or processes that require access to the database application. The processes may include, but are not limited to, back-end processes and data processing processes. Based on the information gathered from asset **510**, enrichment information gathered from internal and external source **540**, and related processes identified from processes **521-525**, advisement system **530** identifies a rule set for the incident.

[0043] For example, because process **523** is identified as relating to or requiring asset **510** for operation, a particular rule set may be selected based on this determination to continue to provide services to process **523**. Once the rule set is selected, advisement system **530** may determine one or more action suggestions to take against incident **515** based on the rule set and provide them to administrator **560** at administration system **550**. Although illustrated separately in the present example, it should be understood that administration system **550** might reside wholly or partially on advisement system **530**.

[0044] While illustrated in FIG. **5** as inquiring other devices and assets **520** to determine the related processes to asset **510**, it should be understood that in some examples a database might be maintained to relate the physical devices and processes to one another. Here, the action recommendations that are provided to administrator **560** might include actions that continue the operation of asset **510**. For example, because process **523** requires asset **510** for operation, the action recommendations may include taking a snapshot of asset **510**, limiting the communications that can be made by asset **510**, limit the type of data that is communicated by asset **510**, or other similar operations that continue the operation of asset **510**.

[0045] In some implementations, advisement system **530** may identify a report of a possible malicious application on a particular asset. Responsive to the report, advisement system **530** may determine if the application is a known application based on a known repository of applications within the environment. If advisement system **530** determines that the application is known for the environment, a rule set and actions may be provided to the administrator that may allow the application to continue operation with particular limitations or monitoring. In contrast, if advisement system **530** determines that the application is unknown within the environment, the rule set and action recommendations may prescribe removing the application and the related application data from the environment.

[0046] FIG. **6** illustrates an overview **600** of providing a recommendation interface for an administrator of a computing environment. Overview **600** includes advisement system **620** and recommendation interface **640**. Recommendation interface **640** further includes recommendations **631-634** and miscellaneous user interface (U.I.) **650**. As illustrated in the present example, advisement system **620** is configured to identify reports of possible security incidents within a computing environment. This computing environment includes a plurality of computing systems and devices, including switches, computers, routers, or other similar computing hardware. These reports may include information about the type of security incident, an identifier for the asset with the incident, IP address information related to the incident, information about a process or executable related to the incident, or any other similar information.

[0047] In response to receiving the report, advisement system **620** may use the information about the incident to query internal and external sources for enrichment data related to the incident. For example, if advisement system **620** received a report regarding a particular executable within the computing environment, advisement system **620** may query one or more databases to determine whether the executable was malicious. In some implementations, advisement system **620** may identify whether the asset related to the issue is required or associated with any other asset within the environment. Thus, if the asset is required by one or more processes or systems, action recommendations may be identified that allow the required processes or systems to continue to access the asset in question.

[0048] In the present example, once the enrichment information is gathered and a rule set identified, recommendations may be defined based on the rule set and provided to an administrator as recommendation interface **640**. Recommendation interface **640** may be displayed locally via a screen or other interface on advisement system **620**, or may be displayed at a user console, such as a desktop, laptop, tablet, or other similar computing device. Here, recommendation interface **640** includes four recommendations **631-634**, although any number of recommendations may be provided to an administrator, and further includes miscellaneous user interface **650**. Miscellaneous user interface **650** may include a chat window, a programming interface allowing the user to program various actions for the assets within the computing environment, amongst a variety of other possible user interactions.

[0049] For example, the chat window may allow a plurality of administrators within the organization discuss the security incidents and possible actions or responses to the incidents. In some implementations, the chatroom that is provided to administrator **610** may include administrators that are approved to take action against a particular incident. For instance, an organization may permit four administrators to take action against a malware incident within a database computing system. Accordingly, when the incident is identified, the recommendation interface that is provided to each of the administrators may allow the four approved administrators to discuss the incident, and identify the appropriate action to take against the incident.

[0050] Once administrator **610** selects a recommendation of recommendations **631-634** to be taken against the security incident, advisement system **620** may initiate the activities necessary to implement the requested action. In some implementations, advisement system **620** may provide administrator **610** with the workflow or the procedural steps to implement the desired action. For example, if the action required the modification of a firewall within the computing environment, advisement system **620** may present the user with the necessary steps to implement the change to the firewall, including logging into the necessary device and making the necessary changes.

[0051] In other implementations, rather than requiring administrator **610** to step through each phase necessary for a particular action, advisement system **620** may be configured to automate the implementation of the actions. To automate the action implementations, in some examples, advisement system **620** may be configured with various connectors or translators that are used to configure each of the assets and computing systems within the environment. These connectors may be used to take a recommendation such as “block all communications from IP address X,” and convert the recommendation into a script to implement the recommendation in a firewall. Thus, although each of the assets may require a different programming language or application program interface, advisement system **620** may implement the actions in a scripted format for each of the assets. In some implementations, the administrators of the computing environment may generate the configurations. In other examples, the connector configurations may be gathered from a database that allows the connectors to be generated and shared across various computing environments and organizations. Accordingly, an administrator for one computing environment may generate a connector that can be used by other administrators in other computing environments to script the implementation of a particular action. Once the connector information is configured with advisement system **620**, advisement system **620** may communicate with the devices, computing systems, and software of the computing environment to implement the desired security actions of administrator **610**.

[0052] For example, a computing environment may include firewall software on one or more computing devices. To manage the firewall software, an administrator of the environment may identify, via the connector database, a connector associated with the software, and configure advisement system **620** to implement the connector. Accordingly, when an action is required that relates to the particular firewall, the connector information may be used to implement the desired action in the firewall. This connector information may include the necessary commands and scripts to block a particular IP address, permit a particular IP address, block particular data requests, or any other similar configuration information.

[0053] The included descriptions and figures depict specific implementations to teach those skilled in the art how to make and use the best option. For the purpose of teaching inventive principles, some conventional aspects have been simplified or omitted. Those skilled in the art will appreciate variations from these implementations that fall within the scope of the invention. Those skilled in the art will also appreciate that the features described above can be combined in various ways to form multiple implementations. As a result, the invention is not limited to the specific implementations described above, but only by the claims and their equivalents.

What is claimed is:

1. A method of operating an advisement system to provide action recommendations in a computing environment comprising a plurality of computing devices, the method comprising:

identifying a security incident for an asset in the computing environment;

in response to identifying the security incident, identifying enrichment information about the security incident;

determining a rule set for the security incident based on the enrichment information; and

identifying one or more action recommendations for an administrator based on the rule set.

2. The method of claim **1** wherein identifying the enrichment information about the security incident comprises identifying the enrichment information in an external database related to the security incident.

3. The method of claim **1** wherein identifying the security incident for an asset comprises one of receiving the security incident from a security information and event management (SIEM) system or identifying a user defined security incident.

4. The method of claim **1** wherein the asset comprises one of a router, a switch, a firewall, an operating system, a virtual private network, or an application.

5. The method of claim **1** wherein identifying the enrichment information about the security incident comprises determining whether one or more approved processes in the computing environment relate to the security incident, and wherein determining the rule set for the security incident based on the enrichment information comprises, if one or more approved processes in the computing environment relate to the security incident, determining the rule set for the security incident based on an effect of the rule set on the one or more approved processes.

6. The method of claim **1** wherein identifying the security incident for the asset in the computing environment comprises identifying traits related to the security incident, wherein the traits comprise an identifier for the asset, and at least one of an internet protocol (IP) address related to the incident, Uniform Resource Locator (URL) related to the incident, a user name related to the incident, a computing system identifier for the asset, a file name related to the incident, or a service name related to the incident.

7. The method of claim **1** further comprising generating a display of the one or more recommendations for the administrator.

8. A computer readable storage medium having instructions stored thereon, that when executed by advisement computing system, direct the advisement computing system to perform a method of providing action recommendations in a computing environment comprising a plurality of computing devices, the method comprising:

identifying a security incident for an asset in the computing environment;

in response to identifying the security incident, identifying enrichment information about the security incident;

determining a rule set for the security incident based on the enrichment information; and

identifying one or more action recommendations for an administrator based on the rule set.

9. The computer readable storage medium of claim **8** wherein identifying the enrichment information about the security incident comprises identifying the enrichment information in an external database related to the security incident.

10. The computer readable storage medium of claim **8**, wherein identifying the security incident for an asset comprises one of receiving the security incident from a security information and event management (SIEM) system or identifying a user defined security incident.

11. The computer readable storage medium of claim **8**, wherein the asset comprises one of a router, a switch, a firewall, an operating system, a virtual private network, or an application.

12. The computer readable storage medium of claim **8**, wherein identifying the enrichment information about the security incident comprises determining whether one or more approved processes in the computing environment relate to the security incident, and wherein determining the rule set for the security incident based on the enrichment information comprises, if one or more approved processes in the computing environment relate to the security incident, determining the rule set for the security incident based on an effect of the rule set on the one or more approved processes.

13. The computer readable storage medium of claim **8**, wherein identifying the security incident for the asset in the computing environment comprises identifying traits related to the security incident, wherein the traits comprise an identifier for the asset, and at least one of an internet protocol (IP) address related to the incident, Uniform Resource Locator (URL) related to the incident, a user name related to the incident, a computing system identifier for the asset, a file name related to the incident, or a service name related to the incident.

14. The computer readable storage medium of claim **8**, wherein the method further comprises generating a display of the one or more recommendations for the administrator.

15. The computer readable storage medium of claim **9**, wherein the security incident comprises a process, and wherein identifying the enrichment information about the security incident comprises at least determining whether the process is known in the computing environment.

16. An advisement system to provide security action recommendations in a computing environment, the advisement system comprising:

a communication interface configured to:

receive a security incident for an asset in the computing environment;

a processing system, communicatively coupled to the communication interface, configured to:

in response to receiving the security incident, identify enrichment information about the security incident;

determine a rule set for the security incident based on the enrichment information; and

identify one or more action recommendations for an administrator based on the rule set.

17. The advisement system of claim **16** wherein the processing system configured to identify the enrichment information about the security incident is configured to identifying the enrichment information in an external database related to the security incident.

18. The advisement system of claim **16** wherein the asset comprises one of a router, a switch, a firewall, an operating system, a virtual private network, or an application.

19. The advisement system of claim **16** wherein the security incident comprises a process, and wherein the processing system configured to identify the enrichment information about the security incident is configured to at least determine whether the process is known in the computing environment.

20. The advisement system of claim **16** wherein the processing system is further configured to generate a display of the one or more recommendations for the administrator.

* * * * *