



(51) International Patent Classification:
G06F 11/00 (2006.01)

(21) International Application Number:
PCT/IB2021/051474

(22) International Filing Date:
22 February 2021 (22.02.2021)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/978,852 20 February 2020 (20.02.2020) US

(71) Applicant: CELESTYA LTD. [IL/IL]; 5 Dolev Street,
P.O. Box 10, 24959 Tefen Tower Industrial Area (IL).

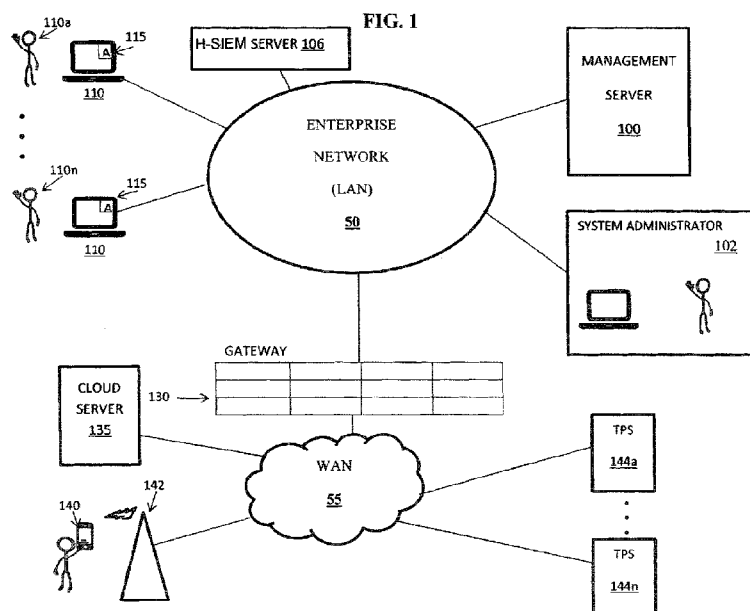
(72) Inventor: GROSSMAN-AVRAHAM, Limor; P.O. Box
183, D.N. Galil Maaravi, 25180 Moshav Hosen (IL).

(74) Agent: A.C. ENTIS-IP LTD. et al.; 6 Raoul Wallenberg,
69719 Tel Aviv (IL).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

(54) Title: METHOD AND SYSTEM FOR ONLINE USER BEHAVIOR MANAGEMENT



(57) Abstract: A method for providing an automated response to user behavior comprising: receiving, by a computer system, data of user actions taken on a computer of the user, the computer of the user in communication with the computer system; analyzing the received data against the knowledge level of the user as determined by the computer system, and/or, the user's responses to simulations generated by the computer system, to determine a score for the user; and, in response to the score, making a behavior recommendation for the user and/or making a decision to take an action associated with the computer of the user.

Published:

- *with international search report (Art. 21(3))*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

METHOD AND SYSTEM FOR ONLINE USER BEHAVIOR MANAGEMENT

RELATED APPLICATIONS

[0001] The present application claims the benefit under 35 U.S.C. 119(e) of U.S. Provisional Application 62/978,852 filed on February 20, 2020, the disclosure of which is incorporated herein by reference.

TECHNICAL FIELD

[0002] The present invention is directed to managing the behavior of users of computers, and in particular, to behavior management of computer users along an enterprise network.

BACKGROUND

[0003] Cyber-attacks can cripple an organization, costing it heavy losses in soft costs such as down time and lost production, as well as hard costs, where the business is not running and not producing revenues. In a business or enterprise, almost all employees, agents and contractors have access to the enterprise network, as well as access to large public and wide area networks, such as the Internet. It is through any one of these computers that a cyber-attack can enter the enterprise network.

SUMMARY

[0004] The present disclosure realizes that various users of the computers, who link to the enterprise network have different computer behaviors. Some users constantly surf the net, and of these users, many surf to dangerous sites, such as pornography, dating, hacking, gambling, and social media web sites, that are rife with malware for causing cyber-attacks. Also, some users are not conscientious about opening emails and accordingly, open emails from unknown senders, another way a cyber-attack can enter an enterprise network. Additionally, while the enterprise may have set policies as to computer usage, some users may simply not follow the policy, partially follow the policy, or simply attempt to bypass the policy, without understanding or being aware of the dangers of not following the policy.

[0005] To determine a computer user's level of risk, behavior and awareness, the present disclosed subject matter employs an agent at the user computer, to monitor user behavior on the user computer. Such user behavior may include dangerous behavior which may expose the computer to cyberattacks and malware, jeopardizing security of the entire enterprise network and the machines linked thereto. The agent is, for example, a browser add-on, or other computerized component, which links to a central computer associated with the enterprise network.

[0006] The agent sits at endpoints, user computers, along the network, for example, a local or enterprise network. The agent collects data from the user's computer and automatically ranks the user's behavior and risk level. When there is the same user's report (on a suspicious event/website/email, and the like), the information is also collected. This information affects the rating of the user according to actual behavior plus practical behavior in simulations, plus the user's theoretical knowledge or user knowledge level, having been presented tutorials. It is also possible to know the reliability of the reports in relation to the rating of the user's awareness, knowledge and work habits in comparison with the organizational policies.

[0007] The system of the invention collects information about the user's actual behavior on his computer, awareness, knowledge, simulations and ranking of the user, and if there is an abnormal operation/action on the computer (end point). The system then compares this behavior with organization policies, to automatically render decisions about which actions to take to maintain the security of the enterprise network and the computers, devices, and the like, linked thereto.

[0008] This Summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This Summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used to limit the scope of the claimed subject matter.

BRIEF DESCRIPTION OF FIGURES

[0009] Non-limiting examples of embodiments of the invention are described below with reference to figures attached hereto that are listed following this paragraph. Identical features that appear in more than one figure are generally labeled with a same label in all the figures in which they appear. A label labeling an icon representing a given feature of an embodiment of the invention in a figure may be used to reference the given feature. Dimensions of features shown in the figures are chosen for convenience and clarity of presentation and are not necessarily shown to scale.

[00010] FIG. 1 is a diagram of an exemplary environment for the system in which embodiments of the disclosed subject matter are performed;

[00011] FIG. 2 is a block diagram of an architecture of a system in of the disclosed subject matter;

[00012] FIG. 3A is a flow diagram of an example process of the disclosed subject matter;

[00013] FIG. 3B is a flow diagram in accordance with another example process of the disclosed subject matter; and,

[00014] FIG. 3C is a flow diagram in accordance with another example process of the disclosed subject matter.

DETAILED DESCRIPTION OF THE DRAWINGS

[00015] Before explaining at least one embodiment of the invention in detail, it is to be understood that the invention is not necessarily limited in its application to the details of construction and the arrangement of the components and/or methods set forth in the following description and/or illustrated in the drawings. The invention is capable of other embodiments or of being practiced or carried out in various ways.

[00016] As will be appreciated by one skilled in the art, aspects of the present invention may be embodied as a system, method or computer program product. Accordingly, aspects of the present invention may take the form of an entirely hardware embodiment, an entirely software embodiment (including firmware, resident software, micro-code, etc.) or an embodiment combining software and hardware aspects that may all generally be referred to herein as a "circuit," "module" or "system." Furthermore, aspects of the present invention may take the form of a computer program product embodied in one or more non-transitory computer readable (storage) medium(s) having computer readable program code embodied thereon.

[00017] FIG. 1 shows an example environment in which the invention is performed. An enterprise network, which is a local area network (LAN) 50, is representative of a network of an organization, for explaining the invention. A management server 100, which supports some or all of the system 100', which performs the invention, links to the LAN 50. A system server 102 (representative of a system administrator), also links to the LAN 50. The management server 100, for example, operates automatically, while the system server 102, for example, is operated by personnel associated with the enterprise.

[00018] A Human Security Information and Event Management (H-SIEM) server 106 links to the LAN 50. The H-SEIM server 106 collects data on activity in the LAN 50, which is traceable to users (endpoints), for example, user computers, represented by computer 110, and is used for determining a score (also known as a behavior score for example, for trustworthiness/security risk)) for each user (at each endpoint). This H-SIEM server 106 is optional, as the data collected thereby may be collected by alternate hardware and software, or combinations thereof.

[00019] The H-SIEM server 106, if present on the enterprise network 50, is a type of SIEM server (a security analytics tool), which, for example, receives and collects reports in a single

location. The H-SEIM server 106, for example, collects big data about the user 110a, in terms of computer behavior, knowledge of the user, and the like.

[00020] A user computer 110 associated with a user 110a is representative of multiple users associated with their computers of the enterprise, which are linked to the LAN 50, with each of these computer(s) 110 being representative of endpoints of the LAN 50. An agent (A) 115 sits on the user computer 110, and maps to the management server 100, or any other enterprise determined destination. The agent 115 sends the data which it detects, to the management server 100, where the data is collected and analyzed in accordance with the processes detailed herein. The agent 115 may be a hardware component, software, or a combination of hardware and software.

[00021] While a traditional desktop computer 110 is shown as the endpoint computer, other suitable endpoint computers include, for example, laptop computers, smart phones, iPads®, and other equipment. Both the LAN 50 and WAN 55 include components, such as firewalls 130, switches, routers, network access controllers (not shown), which can be controlled, by the system 100', for example, automatically, and/or system administrator 102, to control the endpoints and endpoint computers 110, devices and the like.

[00022] However, should the computer 110, e.g., desktop computer, laptop computers, smart phones, iPad® computers, and other equipment lack access to the WAN 50, a cloud server 135 may be employed. The cloud server 135, to the which the desktop computer, laptop computers, smart phones, iPads®, and other equipment will report, and from the server settings, for example, will send recommendations to the management server 100, and optionally, the system administrator 102. Additionally, there is, for example, a default preset configuration that the system administrator 102 can edit/delete/add, desktop computers, laptop computers, smart phones, iPads®, and other equipment. The cloud server 135 is formed of hardware components, software, or combinations thereof.

[00023] Additionally, the cloud server 135 relays and shares information that is trusted with servers in other organizations. This information can be accessed or automatically transmitted to the management server 100 and/or the system administrator 102. The management server 100, for example, can automatically take action based on information received from the cloud server 135, for example, making a behavior recommendation, and/or taking an action against the user computer, as detailed below. The system administrator 102 can also take action, similar to that of the management server 100, based on the information received from the cloud server 135.

[00024] For example, the cloud server 135: 1) can collect reports from customers, such as enterprises, and send recommendations to the customers, which may be passed onto computer users 110a of the enterprise; 2) can send warnings to end user equipment, such as user computers 110; 3) provides solutions for equipment not on the enterprise network 50; and, 4) can update customer servers, such as the management server 100, and, the system administrator server 102, as to the presence of threats, for example, suspicious or malicious websites to block, some of these web sites which may even be benign. Additionally, the cloud server 135 can collect data about the users 110a-110n and their computers 110 of the enterprise, while these users are not online. The collected data may be, for example, part of reports, received by the system 100', and, as a result of one or more reports being received, the management server 100 may automatically issuing a behavioral recommendation to the user or taking action on the associated user computer 110.

[00025] For example, when an offline user wants to surf the Internet while he is not inside the enterprise (corporate or corporate internal) network 50, a request is sent through the cloud server 135, to the management server 100, to open the Internet (WAN) 55 for browsing, or alternately, open a wireless network on the computer 110, for example, a laptop computer, tablet (iPad®), or the like, through the agent 115. Subsequently, automatically and according to a preset configuration on the management server 100, if, for example, the user's cyber awareness (trustworthiness/risk) score, also known as a behavior score or a score, is high, and the user has also passed a safe surfing tutorial, the management server 100 will send an instruction (command) for action, through the cloud server 135, that the user can surf the Internet. However, if the user's score is low, and the user did not complete the tutorial, then the user will first have to attend a tutorial and only then, will the user be able to surf the Internet. The aforementioned occurs, for example, when the user 110 is not within the enterprise (corporate internal) network.

[00026] The agent 115 is configured to monitor and detect the behavior of a user 110a (also known as "user behavior" with respect to the computer 110 and the LAN 50, as the computer 110 serves as an endpoint. The agent 115 monitors the computer 110 for example, for actual computer behavior of the user, email behavior, web browsing behavior (the "actual computer behavior", "email behavior" and "web browsing behavior" collectively referred to herein as "actual computer behavior"), file downloads, threat and website (e.g., URL) reporting, and, devices used in conjunction with the computer, and communicates this actual behavior (e.g., as raw data), records thereof, and/or data associated therewith, to the management server 100. The agent 115 is such that the user 110a can report to the management server 100 and/or the

system server 102, or the agent 115 itself can automatically report to the management server 100 and/or the system server 102, unusual user computer events such as, slowdowns of computer workflow, changes of file types/extensions, browser direction to suspicious websites (which may actually be benign), infrequent user behavior, user behavior at times when the user is not normally on the computer 110, a user who rarely or never browses to malicious or unauthorized web sites is suddenly browsing to such sites regularly, and the like, regardless of whether the websites are malicious, suspicious, or benign. The agent 115 can also report unusual user computer behavior to the management server 100 and/or the system server 102, such as user browsing to web sites for which the user lacks permissions, credentials or the like, and, web sites for which the user lacks permissions, credentials or the like, and continues to attempt to access these web sites.

[00027] Email behavior monitored and detectable by the agent 115, and transmitted to the management server 100, for example as actual actions (e.g., raw data), data and/or records, includes, for example, which emails are opened, the time after receipt when the emails are opened, the sources of the emails being opened, any attachments being opened from the emails being opened, any known viruses and/or malware in the attachments being opened, attempts to open emails which have been blocked, quarantined, or otherwise disabled, emails being sent including the recipients, and any attachments being included therein, receiving an alert or antivirus or other block when attempting to open an attachment and continuing to attempt to open the attachment.

[00028] Web browsing (surfing) behavior being monitored by the agent 115 includes, for example, the type of web sites to which the browser is directed, such as pornography sites, gambling sites, social media sites, sites which violate the enterprise policy, known to be rife with viruses and/or malware, as well as interactions with various web sites, including data transmissions, file uploads and downloads, and openings of the downloaded files, as well as files and downloads of applications from the Internet, e.g., Skype®, and opening the applications. Additionally, web browsing behavior may include, for example, monitoring the time of the web browsing, and/or the certain web sites (Uniform Resource Locators (URLs)), being viewed at certain times or time periods.

[00029] For example, should the user 110a, via computer 110 attempt to direct his web browser to a particular website (regardless of the email link, but standard web browsing), and the website is blocked by a technology protection solution (e.g., URL filtering), then this information is also collected by the agent 115. This information is used to influence user (employee) awareness rankings, based on actual and practical behavior, and one or the other

of, the user's simulations behavior and the theoretical level of knowledge (user knowledge level) from the answers the user provided to his tutorials. As a result of this data collection and analysis by the management server 100 from the data obtained by the agent 115, the system 100' defines the level of reliability of user reports in relation to the rating of the level of awareness, knowledge and work habits and actual behavior of the user 110a and in comparison with the organizational policy.

[00030] As another example, the system administrator 102 can configure the system 100', such that over a predetermined number of unsuccessful attempts to access a file, email, email attachment or the like, or browsing to an unauthorized web site for a predetermined number of times, make a predetermined number of attempts to use an unauthorized device on the computer 110, such as an unapproved disk on key, or other unapproved portable storage device, or commit another system policy violation for a predetermined number of times, the user 110a-110n will be blocked automatically from accessing the network 50, for example, by the management server 100 automatically taking action, and/or will need to request permission from the help desk center (e.g., system administrator 102 operated) and/or automatically report to authorized personnel, to be again provided access to the network 50. A user who attempts more than the predetermined number of tries to perform a prohibited action, including actions prohibited by system policies, then one (or more) of actions, to limit the user's access and usage of the network 50 will automatically occur, for example, as automatically directed by the management server 100 taking action and/or in accordance with defaults or settings that the system administrator 102 has set.

[00031] As another example, a user may be asking the management server 100 to open a web site, allow use of an external device on his computer, or other permission, such as a temporary permission. Should the user 110a have a high score for trustworthiness/low security risk, the management server 100 automatically takes the action on the computer 110 and/or the network 50, to provide the user 110a with the requested permission. However, should the user score be low, the management server 100, may automatically deny the request, or send the request to the system server 102, where the system administrator will decide as to granting of the permission.

[00032] Devices being monitored for by the agent 115 also include, for example, portable storage devices, portable drives, disk on key, and other Universal Serial Bus (USB) devices, WIFI™ devices, Bluetooth™ devices, which connect to the computer via physical (e.g., wired) connections, such as ports, or are linked wirelessly.

[00033] The agent 115 is, for example, a browser add-on, and operates with the existing web browsers, of the computer 110 and the computer's 110 operating system. The agent 115 is also designed to allow users to report security breaches, their own and those of others, suspicious files, suspicious and malicious web sites and devices, which may be known to contain malware, viruses, and other threats, and the like, which are in turn, transmitted to the management server 100 for data collection and analysis. As a browser add-on, the agent 115 can filter or otherwise block access to web sites as well as report browsing of these disallowed web sites. Also, the agent 115 may be such that the user may be allowed to access this web site for a limited time. The agent 115 can work with browsing programs (browsers), such as Internet Explorer™ from Microsoft, or Chrome™ from Google.

[00034] The management server 100 interacts or otherwise communicates with the agent 115, for example, such that the agent 115 acts as a go between with the management server 100. For example, through the agent 115, the user may make a report to the management server 100; the agent may be used to send instructions to the user at the user computer; from the management server 100 and/or the system server 102, the management server 100 and/or the system server 102 can send instructions to the user at the user computer 110, through the agent 115; and, the agent 115 can send reports to the management server 100 and/or the system server 102.

[00035] The agent 115 also includes a push-button feature, which detects a web site and/or web page, and responds by displaying a push button, which is activated by a mouse click, swipe, contact or the like. When the button is activated, data for the web site/web page is sent to the management server 100, for example, as a request. The management server 100, automatically attends to the request, returning an answer, whether the site is suspicious or not, and whether the user 110a is permitted to enter personal data, play videos or download files from the site, or the like. Should an automatic answer not be provided in a predetermined time, the management server then sends the request to a system administrator 102, who provides a manual response.

[00036] The agent 115 also allows the user 110a-110n, via the computer 110, to communicate with the system 100' and report suspicious or malicious web pages (URLs), attachments, files, viruses and the like. For example, this may result in the system 100' taking automatic and immediate action, as detailed below, such as blocking the user 110a computer's 110 access to the LAN 50.

[00037] A gateway 130, such as a firewall or other inspection or security device, sits between the LAN 50, and a wide area network (WAN) 55 or public network, such as the Internet. An

Internet caller device 140 links to the WAN 55 via a cellular tower 142. Third party servers (TPS) 144a-144n also link to the WAN 55. For example, one or more of the third party servers 144a-144n, looks for malicious, suspicious or threatening web sites and other network threats, and sends updates to customers, such as the management server 100 and/or the system server 102.

[00038] The networks LAN 50 and WAN 55, although shown as single networks, may be a combination of networks and/or multiple networks including, for example, data networks, cellular networks, communications networks, and the like. "Linked" as used herein, includes both wired and/or wireless links, either direct or indirect, such that the computers, including, servers, components and the like, are in electronic and/or data communications with each other.

[00039] FIG. 2 shows an example architecture of the management server 100, as a system 100'. The system 100', also known as a computer system, is shown, for example, within the management server 100, but may be distributed external to the management server 100, for example, among multiple servers, computers, components and the like along the LAN 50 and/or the WAN 55. The management server 100, for example, is formed of hardware components, software, or combinations thereof.

[00040] The architecture of the system 100', for example, includes a central processing unit (CPU) 202 formed of one or more processors. The CPU 202 is electronically linked, and in electronic and/or data communication, directly or indirectly with computer components including: a storage/memory 204, a data collection module or data collector 211a, a HUMAN SIEM data collection module or HUMAN SIEM data collector 211b, a data analysis module or data analyzer 212, a reports module 213, a report analysis module 214, a tutorials and education module 215, a simulated cyber-attacks/phishing module 216, a push-button requests and responses module 217, a web site data bases and policies module 218, a communications interface 219, data storage media 220, and a behavior recommendation engine 230. While components 202, 204, 211a-220, and 230 of the system 100' are shown within the management server 100, any one or more of these components 202, 204, 211a-220, and 230 may be external to the management server 100, and be linked to the management server 100 from their external location. As used herein, a "module", for example, includes a component for storing instructions (e.g., machine readable instructions) for performing one or more processes, and including or associated with processors, e.g., the CPU 202, for executing the instructions. While the aforementioned components are shown for the system 100', other components may also be used.

[00041] The Central Processing Unit (CPU) 202 is formed of one or more processors, including microprocessors, for performing the management server 100 functions and operations detailed herein, including controlling the components 204 and 211a-220 and 230, executing the instructions provided and/or obtained therefrom. The Central Processing Unit (CPU) 202 processors are, for example, conventional processors, such as those used in servers, computers, and other computerized devices, including data processors and hardware processors, for performing the management server 100 and system 100' functions and operations detailed herein. For example, the processors may include x86 Processors from Advanced Microdevices (AMD) and Intel, Xenon® and Pentium® processors from Intel, as well as any combinations thereof.

[00042] The storage/memory 204 is associated with the CPU 202, and is any conventional storage media. The storage/memory 204 also includes machine executable instructions associated with the operation of the CPU 202 and the components 211a-220 and 230, and along with the processes and subprocesses shown in FIG. 3, detailed herein. The storage/memory 204 also, for example, stores rules and policies, such as security policies, for the system 100' and the management server 100.

[00043] The data collection module or data collector 211a collects data received from the agent 115 on each computer or other endpoint of the LAN 50, as well as the Human SIEM server 106, and cloud servers, represented by the cloud server 135.

[00044] The Human SIEM data collection module or Human SIEM data collector 211b collects Human SEIM data on the system 100', when the LAN 50 does not have a Human SIEM Server.

[00045] The data analysis module 212 analyzes data including the collected data from data collectors 211a, 211b, and the agent 115, including, for example, actual computer behavior, email behavior, and web browsing behavior, coupled with reports (produced by the reports module 213) on the user, the user's position, the user having been educated by tutorials as to cyber security policies of the organization, the user's responses to simulated cyber-attacks, simulated phishing, as provided by the system 100', and actual computer behavior, and the like, the sensitivity of data the user has attempted to obtain, and the like. The analyzed data is then converted to a score for the user, which reflects the trustworthiness and/or risk associated with this user. For example, the score may change each time user behavior (and user data obtained therefrom), is again detected. The score also serves as a ranking/rating of the user, when compared to other users in the organization for risk and trustworthiness of the user. The score may be the basis for a report or provided in a report along with other computer behavioral data reported for or by the user. For example, the score may be based on a set time period, or

aggregated over time. When determining the score, one or more of the user data, such as the various behavior actions, reports, and other factors used to determine the score may be given various weights, for example, depending on importance, relevance, and the like. Also, for example, a “high” score may be for a more trustworthy and low risk user, while a “low” score may be for a less trustworthy and high risk user, the parameters for the score are, for example, programmed into the module 212 (FIG. 2).

[00046] The score created by the data analysis module 212 is, for example, based on one or more factors. A first factor is theoretical behavior/theoretical knowledge or user knowledge level, based on tutorials and quizzes other tests, and webinars (network-based education) sent to the user at his computer, provided to the user. The second factor is practical or practical behavior, such as user performance in simulations, such as simulated phishing attacks, simulated cyber-attacks and the like. The third factor is the actual behavior of the user, how the user interacts and behaves on a daily or regular basis with actual interactions and situations. Additional factors may include, for example, reports, such as those made by the user, as to malicious, suspicious, as well as potentially malicious and suspicious, web sites, emails, downloads, and the like. For example, should a report made by a user be accurate, this may positively influence the user’s score.

[00047] For example, monitored and detected user 110a behavior includes detecting a user 110a continuing to browse a web site, which is against the enterprise’s security policy. While the enterprise may not actually block this web site, as it may not have the means to do so, or there is a technology, such as a URL (uniform resource locator) filtering engine so that the user is blocked when browsing in contravention of enterprise policy and the server still records the browsing attempts in violation of policy - this is actual behavior, that will affect the score given to this user. Also affecting the score is the system knowing the user 110a has been warned about browsing certain web sites, which are against company policy, but continues to do so, which is part of his actual behavior factored into his score.

[00048] The data analysis module 212 also performs comparison functions. For example, the data collected from data collector 211a, 211b is analyzed by comparing it against system 100’/enterprise rules and policies, e.g., in the module 218. The results of this comparison are used in determining the score, for example, as part of the user’s actual behavior.

[00049] The reports module 213 creates reports on user activity on their computers, and stores the reports created. Reports made for the enterprise, for or any computer 110 (or other endpoint) along the enterprise network 50, regardless of the time when made, are stored in the reports module 213. Reports are made by users, as well as about users, by third parties, and

the like. Reports may be consolidated with other reports into a single report. The activity reported, which makes up a report, includes, for example, user actions on the computer, as well as indications of the user having received various tutorials and education about computer security (theoretical knowledge/behavior or user knowledge level), and their behavior when faced with simulated cyber-attacks, phishing attempts, and other malicious and potentially malicious situations (practical knowledge/behavior), and, the user's actual behavior when using his computer - how the user interacts and behaves on a daily basis (actual knowledge/behavior), such as what web sites (browser directions to URLs) are viewed, what time is the computer normally used, and what web sites are viewed at what times, does the user attach any external devices such as external drives, disk on keys, and the like, to the computer, does the user report certain web sites, or others viewing certain web sites, at what time and with what frequency, does the user request permission to browse web sites against company policy and when, does the user request exceptions to company computer policies, does the user continue to attempt to open unopenable files, such as email attachments, or files not permitted to be opened by company policies, such as certain file types, or other files from external sources, such as from web sites, portable storage devices, and the like, which are against company policy, or failing to take protective action against external files (e.g., virus scanning and/or reporting these files as suspicious), downloads made and downloads attempted, and the like. The reports module 213 is typically provided with the user's score, from module 212, and factors this score into the report on the user. The report analysis module 214 provides analysis for each report created, as well as received from users, such as this website is suspicious. For example, should a user with a low score report a web site as suspicious, the system 100' may not render a decision on the web site, and instead, pass the data on to the system administrator 102, who makes the decision on the web site. However, should a user with a high score report a web site as suspicious, or there are a minimum number of users who report a particular website as a suspect, the system 100' (e.g., via a command issued by the engine 230) may take action against users attempting to direct their browsers to this web site, as it is now "suspicious" in the system 100', or to send a prompt for action to the enterprise URL filtering technological solution. For example, user reports, the frequency the user makes reports and the accuracy of the report, influence the user's score, and are factored into the calculation thereof.

[00050] The Tutorials and Education module 215 stores various media, such as tutorials and educational programs for the users 110 of the system, which they can access or be sent. The tutorials and educational programs are, for example, used to explain company policies as well as explain damage which can occur to computers, networks, and machines on a network, should

a policy be breached and/or a virus or the like enter the enterprise network. The tutorials and educational programs may also include quizzes and the like on computer security, company policies and the like, for the user to understand and answer, to gauge the user's awareness of these topics. The tutorials, education, and quizzes may also be presented as network based training, such as in webinars, live and recorded.

[00051] The simulated cyber-attack/phishing module 216 stores simulated cyber-attacks and simulated phishing attempts, such as email phishing, SMS (short message service) phishing (smishing), web phishing, Wi-Fi® phishing, cellular application phishing, media device phishing and voice phishing (vishing), which are presented to users 110 via their computers (and/or mobile devices), for example, either as programmed into the system 100' or via the system administrator 102. The results of the user's 110a-110n handling of these simulations, for example, user actions as part of user behavior, are collected, for example, by the agent 115 and ultimately by the data collection module 211a.

[00052] The push-button requests and responses module 217 operates on web site access requests from users, including sending the request for a manual decision from the system administrator 102. This module 217 records the decisions on the web site access, both made automatically by the module 217, and manually.

[00053] The web site database and policies module 218 stores rules and policies and information about web sites, emails, file types, downloads, and the like, so that automatic decisions can be made about allowing a computer 110 access to the web site, email, file type, download, or the like, or whether the decision as to access to the web site, email, file type, download, or the like must be sent to the system server 102, to made manually.

[00054] The communications interface 219 provides for communications between the system 100' and computers, components and the like, which are linked to the LAN 50, and/or the WAN 55.

[00055] The storage media 220 provides storage, both temporary and permanent, for data collected and created by the system 100'.

[00056] The behavior recommendation engine 230 is a processor based computer component which analyzes all of the user data (also known as user computer data) including behavior data (e.g., obtained as data elements (or data portions) from the user's theoretical knowledge or user knowledge level, practical knowledge, and actual knowledge) from the user's behavior on his computer 110, and/or other user data, email behavior and web browsing behavior, obtained as data elements (data portions) including one or more of, scores, risk ratings, company (enterprise) rules and policies, and reports for and/or from a user at any given time. The user

data and behavior data, for example, is on the order of hundreds or thousands of data elements (or parameters) which are analyzed by the behavior recommendation engine 230. The analysis is, for example, such that different data elements may have different weights, as designated and provided for by weighting algorithms. The analysis of these hundreds or thousands of data elements is performed, for example, contemporaneously, and may be performed simultaneously, and accordingly is a “big data” analysis, that is performed by special purpose computers. The “big data” analysis, for example, includes analyzing and systematically extracting information, or otherwise dealing with data sets that are too large or complex to be dealt with by traditional data-processing application software and/or software tools, for example, by specialized computer hardware and/or software, to capture, curate, , manage, and process data within a tolerable elapsed time, for example, on the order of seconds, and, for example, in real time.

[00057] From this user data and analysis the behavior recommendation engine 230, performs one or more of recommending action for influencing user behavior, and/or taking or initiating the taking of action against a user computer for mitigating user behavior. For example, the taking action is performed to mitigate against threats, malware and other damaging agents to the individual user computer 110 as well as the enterprise network (LAN), and the computers linked thereto.

[00058] Recommendations may include, for example, whether the user should be warned about his computer behavior, and directed to, or sent, for example, automatically by the management server 100, media, such as tutorials and education, webinar (e.g., Zoom™-<https://zoom.us>) as provided by module 215 and/or a third party server 114a-114n. For example, after reporting and learning the user’s behavior, the engine 230 provides recommendations regarding teaching methods, recommendations for practice and/or blockages, and appropriate technology/network permissions (email/browsing/password selection/file access and the like). The recommendations may also include not providing any recommendations, or waiting to do so at a later time. For example, waiting to issue behavior recommendations at a later time may be based on further monitoring of user behavior to determine whether such behavior has improved to a level deemed satisfactory in accordance with system rules and policies.

[00059] The taking action against the user computer includes, for example, directing the system 100’ to block access to web sites, disable certain components of the computer, deny the user access to the company network and/or the internet, not allow the user computer to work with any external components, such as external drives and disk on key, and the like. The taking action may also include not taking any action, or waiting to do so at a later time.

[00060] The behavioral recommendation engine 230 can recommend and direct the system 100' or components thereof, such as firewalls (e.g., gateway 130), switches, routers, network access controllers in the LAN 50 or WAN 55 to perform actions automatically. The automatic actions are performed, for example, according to one or more of: reports, employee awareness rank and reliability, employee (user) scores (e.g., risk scores), according to presets or defaults in the system 100' regarding the number of users reported (Employee Notification Website). Automatic actions performed may also include, blocking browsing to suspicious sites from the one or more user computers 110 linked to the network 50, and, reporting to servers of information security solutions and propulsion technology solutions for operations, including, for example, automatic reporting to an enterprise Uniform Resource Locator (URL) filtering server (not shown) about the site to be blocked/reporting an antivirus/mail filtering server, and the like. The automatic actions also include turning off or deactivating network components such as firewalls, switches, routers, network access controllers in the LAN 50 or WAN 55.

[00061] The recommendations to take action, and actual actions, may also be, for example, from a list of actions. These actions result in commands sent by the engine 230 to the agent 115, as well as network peripheral components, such as computers (e.g., end points), firewalls, network access controllers in the LAN, switches, routers, other LAN components, and cyber security technology solutions. The commands may be performed (issued) automatically by the management server 100, or by the system administrator 102, who can take action, including issuing commands, manually.

[00062] The behavioral recommendation engine 230 can also cause reporting of an event and/or actionable recommendation to all users or users via an outbreak message or via email. For example, an outbreak message to employees about a suspicious URL for a website which is a phishing site, or a URL of website that is currently infected and prohibited from browsing until further notice. The behavioral recommendation engine 230 can also cause reporting of an event and/or an actionable recommendation to the system administrator 102 or similar official, via an outbreak message or via email.

[00063] Additional functionalities of the behavioral recommendation engine 230 include causing the system 100' to automatically report to user (employee) personal managers, automatically report to user (employee) personal files, provide automatic feedback, both positive or negative, and repeat notifications to users (employees) by reporting a site or suspicious event, for example, whether the site is safe to continue browsing or suspicious. Also the engine 230 can recommend causing automatic blocking of certain web sites for certain users and/or certain computers, as well as automatically blocking a predetermined number of

computers 110 at the same time, based on, for example, IP address, domain, usernames, computer names, and the like.

[00064] Still other additional functionalities of the engine 230 include rendering recommendations which cause the system 100' to automatically disconnect the computer from the network 50 if the computer 50 is suspected of being compromised, and/or the attacker will propagate across the network 50 according to a set of settings. For example, this is done automatically by commanding a switch to block certain ports or all ports or internal firewall blocking (internal signaling). Also, an automatic block of access to an external device, can be caused by a recommendation from the engine 230.

[00065] The engine 230 can also make recommendations, which will cause automatic authorization for a user who submits a request through the agent 115 to open a site for a predefined and limited time (with/without the option to extend time), for example, a predetermined time, e.g., on the order of minutes or hours, or predefined Universal Serial Bus (USB) access for a user who requested access to the network 50.

[00066] Attention is now directed to FIG. 3A, FIG. 3B, and FIG. 3C, which show flow diagrams detailing computer-implemented processes and sub-processes in accordance with embodiments of the disclosed subject matter. These processes, for example, are performed by a computer system, such as the computer system 100' of FIG. 2. The aforementioned processes and sub-processes are, for example, performed automatically and in real time.

[00067] The process begins at the START block 300, where, for example, a user is seeking to access a random browsing web site. Moving to block 302, a score (e.g., a behavior score) and/or ranking is assigned to the user by the system 100', e.g., data analysis scoring/ranking module 212, from data collected from the agent 115 at the endpoint, e.g., computer 110, of the respective user 110a-110n, and his computer behavior, known as user behavior.

[00068] The user behavior includes web browsing activity, attempts and continued attempts to access web sites blocked by the organization, email opens and open attempts, email attachment opens and open attempts, web site requests for browser direction, devices used by or associated with the computer, such as portable storage devices, WIFI™ and Bluetooth™ devices, and the like, responses to simulated threats, e.g., simulated cyber-attacks and simulated phishing attempts, simulated emails, any training and/or education as to company policy/cyber security, the user's position in the company, any permissions or credentials the user has, the accuracy and/or credibility of reports the user makes, the frequency of reports made by the user, any reports about the user, or behaviors of the user, from inside or outside the enterprise network 50, the time the user is typically active on his computer, and the like.

[00069] The assigned score will allow the system 100' to determine future actions or permissions and/or issue user behavior recommendations, which are provided to the user 110a-110n.

[00070] Moving to block 304, user activity is monitored by the agent 115, with captured data sent to the data collection module 211a, for analysis.

[00071] At block 306, the collected data is analyzed to determine whether the user's browsing activity, as well as other user behavior, has made the user a security risk, in browsing to the web site. This collected data includes user awareness data. For example, user awareness data includes a user having viewed a tutorial about cyber security (theoretical behavior/knowledge or user knowledge level), but continues to attempt to open a blocked attachment to an email, attempts to open an email which is from an unknown source, attempts to download a file from a web site, where the web site and/or the file type are against company policy, and the user continues to do so after multiple failed attempts, has a suspicious file attachment, or the like (the user's actual behavior/knowledge). Also, this user, who viewed the tutorial, may not have permission to access a particular file in the network, but repeatedly tries to do so. Also at block 306, group behavior may be taken into the analysis, for example, at a first time, user behavior, such as browsing to a certain web site may have been permitted, but now at a time later than the first time, after a group of system 100' users has reported the web site, the user's browsing to that web site may no longer be permitted by the system 100', and may be considered a security risk.

[00072] The process moves to block 308, where the user's position in the company, the type of the user, and/or the department in the company of the user, may be taken into consideration.

[00073] From block 308, the process moves to block 310, where the system 100' for example, via the management server 100, automatically determines whether action should be taken against the user computer. If no, or not at the present time, the process moves to block 314. If yes, at block 310, the process moves to block 312. At block 312, the system 100', for example, via the management server 100, automatically takes action, and/or sends a command to the agent 115, computer (endpoint), firewall, switch, router, network access controllers router, or other peripheral component associated with the user computer 110, to take an action. This action may include, for example, blocking the email or web site the user's computer is seeking or attempting to access, block the user computer from the LAN 50, or the like.

[00074] From block 312, and also from block 310, the process moves to block 314, where the behavior recommendation engine 230 determines whether a behavioral recommendation should be issued to the user, via the user computer 110. The engine 230 analyzes all of the

user behavior data and other user data at any given time, and recommends whether the user should be warned about his computer behavior, and directed to, or sent, for example, media, such as tutorials and education, including webinars (live and recorded), as provided by module 215 and/or a third party server 114a-114n. If yes, at block 314, the behavior recommendation engine 230 issues the behavior recommendation, and the system 100', for example, via the management server, automatically sends the recommendation to the various system modules 211a-220, and the user (user computer 110), who receives the behavior recommendation engine 230 selected tutorials and/or educational materials, for viewing, interacting with, and the like by the user at his computer 110. With the behavior recommendation issued, the process returns to block 302, from where it resumes with the user's score/ranking assigned, for example to the user's trustworthiness/risk. Similarly, if no at block 314, the process also returns to block 302, from where it resumes with the user's score/ranking is assigned. The assigned score may be changed, for example, raised or lowered, or remain the same. The score/ranking may, for example be for a particular time or over a time period.

[00075] FIG. 3B is a flow diagram of another exemplary process in accordance with another embodiment of the disclosed subject matter. The process begins at the START block 350. At this time, the computer user may or may not have a score (e.g., trustworthiness/risk), also known as a behavior score, and/or security rating, assigned to the user, whose behavior is the subject of the process.

[00076] The process moves to block 352, where the user's theoretical knowledge and/or behavior or user knowledge level, as to network and computer security, and the like, is determined. This determination is made by knowing that the user has viewed, interacted with, or otherwise consumed, various media, typically provided to the user by the system 100', such as tutorials and/or educational materials, presentations, and network based training, such as live or recorded webinars, and has communicated, typically by electronic communication, his completed consumption of this media (e.g., materials and presentations) to the system 100'. For example, one or more educational materials, tutorials, network based training, such as live or recorded webinars, and the like, such as videos, quizzes, interactive documents, is provided to the computer user, who indicates having completed these educational materials, tutorials and the like, to the system 100'. For example, the user may be provided with a time period in which to consume the media, such as educational materials, tutorials and the like, and indicate his completion of this media to the system 100'.

[00077] The process moves to block 354, where the practical behavior/practical knowledge of the user is determined. The system 100' has selected and sent one or more simulated security activities or other simulated computer activities, to the computer of the user, who has received and completed the educational materials, and has recorded the user's actions (behavior) in response to the one or more simulated security and/or simulated computer activities. These simulated security activities and/or simulated computer activities may be, for example, simulated emails, simulated downloads, simulated phishing communications, simulated cyber-attacks, and the like, where the user's actions in response to these simulations are recorded, and presented to the system 100' as data for analysis.

[00078] The process moves to block 356, as the actual behavior and/or knowledge of the user is determined. For example, this is done by the system 100' doing one or more of recording computer activity, for example, obtained from the agent 115, as detailed above, and computer actions made by the user, during computer activity in daily computer operation, email sending and handling, web browsing, reviewing reports on the user, and the like.

[00079] The process moves to block 358, where an analysis of the user behavior and/or knowledge is performed, for example by the components 211a-220 and 230 of the system 100', for example, associated with the management server 100. The analysis, for example, is based on the theoretical behavior and/or knowledge (knowledge level) of the user, which includes, for example, knowing what materials (media) and the content of the materials that were consumed by the user, the practical behavior and/or practical knowledge of the user, for example, how was the user's computer behavior in handling system 100' generated simulations, and, the actual user computer behavior and/or actual knowledge, and/or additional factors such as reports, group behaviors, information about the user, company (enterprise) rules and policies, and the like, to determine a Score (trustworthiness/security risk) and/or rating (Security Rating) for the user.

[00080] Actual computer behavior of a user includes, for example, user actions and interactions to show the user interacts and behaves on a daily basis and/or over a time period, email behavior, web browsing behavior and the like, for example, in the form of data, such as data of user actions, for example, for analysis by the system 100' and its components 211a-220 and 230. These user actions, include interactions between the user computer and various computers, components, network components, servers, and the like includes, for example, web sites (browser directions to URLs) that are viewed, and which web sites at what time, what time is the computer normally used, external devices and/or drives, such as disk on keys, and the like, connected to the computer, any reports made by or about the user, including for

example, reports made by the user which are accurate and credible which may positively influence the user's score, does the user report certain web sites, or others viewing certain web sites, at what time and with what frequency, does the user request permission to browse web sites against company policy or unauthorized or suspicious web sites, when, does the user request exceptions to company computer policies, does the user continue to attempt, and/or continue multiple times (for example, beyond a system permitted number of times) to attempt, to open unopenable files, such as email attachments, or files not permitted to be opened by company policies, such as certain file types, or other files from external sources such as web sites (regardless whether the web sites and/or files are benign) against company policy, or failing to take protective action against external files (e.g., virus scanning and/or reporting these files as suspicious), downloads made and downloads attempted, terminating the LAN and/or WAN connection when leaving the computer 110, changes of file types/extensions, the user's position in the company, any permissions or credentials, including temporary permissions or credentials, of the user, sudden or irregular behavior on the computer by the user, abnormal computer behavior, such as slowdowns, longer than normal times for the computer to boot, and the like. The system administrator 102 may also provide a list or one or more additional user actions, behaviors or criteria from reports made by or about the user, which are considered dangerous and affect the user's score, for example, to the analysis module 212.

[00081] The score (e.g., behavior score) and/or rating for the user may change at this point, or remain the same, provided a score and/or rating was present at the START block 250.

[00082] Based on the score and/or rating of the user, at block 360, the system 100', for example, via the behavior recommendation engine 230, determines whether action should be taken against the user computer, issue a behavioral recommendation for the user, and/or do nothing at this time. The taking action is in accordance with that described above, and is performed, for example, to mitigate threats, including malware, spyware, and damaging agents, and the like. The behavioral recommendation is in accordance with that described above, and includes, for example, providing the user with media, such as educational materials and tutorials, including, for example, the management server 100 automatically sending the user educational materials, tutorials, quizzes, warnings, network based training, live or recorded, to understand computer security, computer safety, company computer rules and policies, and the like.

[00083] The process moves to block 362 where it ends. At this block, the user score and/or rating is updated, and stored in the system 100', and should a process for the user start again, carries over to the START block 350. The process may be repeated, for example, from the START block 350, for as long as desired.

[00084] FIG. 3C is a flow diagram of another exemplary process in accordance with another embodiment of the disclosed subject matter. The process begins at the START block 370. At this time, the computer user subject to the process has a score (behavior score) (e.g., trustworthiness/risk) and/or security rating, assigned to him. For example, the score is determined by processes, such as those detailed in one or more of blocks 352, 354, 356 and 358 of FIG. 3B. The process moves to block 372, where the user makes a request to the management server 100, and the management server 100 receives the request. For example, the request may be to use a disk on key and access the website www.example.sportsscores.com, a gambling web site prohibited by company policy, but is known to be benign from various reports received by the management server 100, or from an existing web filtering solution in the organization (enterprise).

[00085] The process moves to block 374, where the management server 100 automatically checks the user's score from the data analysis module 212. If the user's score is above a predetermined upper threshold, at block 376, the process moves to block 378. At block 378 the management server 100 automatically allows the request, either as requested, or modifies the request, for example, allows the disk on key, but not access to the web site www.example.sportsscores.com, and, for example, for a limited time period, such as one hour. For example, if the user has a very high score, the disk on key and access to www.example.sportsscores.com may be allowed, such as for one day.

[00086] Returning to block 376, if the user's score is below the predetermined upper threshold, the process moves to block 380. At block 380, if the user's score is below the lower threshold, the process moves to block 382, where the management server 100 automatically denies the user's request. From block 382, the process moves to block 388, where it ends.

[00087] If "no" at block 380, the process moves to block 384, where the management server 100 automatically passes the score and the responsibility for the decision to allow (including modify) or deny the user's request to the system administrator 102. Should the system administrator 102 deny the request, at block 384, the process moves to block 388, where it ends.

[00088] From block 378, and if "yes" at block 384, the process moves to block 386. At block 386, the original or modified request, the one which has been allowed, is acted on by the management server 100 (from block 378), which automatically directly configures the computer and/or the various network components responsible for the allowed actions, or automatically sends a command or signals to the system administrator 102, to make the aforementioned computer and network configurations. Alternately, if from block 384, the

system administrator 102 makes the aforementioned computer and network configurations to accommodate the allowed request, or sends a recommendation for actions to other technological information security solutions that exist in the organization (enterprise).

[00089] From block 386, the process moves to block 388, where the process ends. Here, the user's score and/or rating may be changed. The process may be performed again for as long as desired.

[00090] The following examples show various aspects of the behavior recommendation engine 230 analyzing various user activity and user data to provide a recommendation to the user, and/or cause the system 100', for example, via the management server 100, to take action, such as issue a behavioral recommendation including a warning and/or tutorials and other education, and/or send a command from the engine 230 to cause the system 100', for example, via the management server 100, to issue a behavioral recommendation including a warning and/or media, such as tutorials and other educational documents, presentations, and the like, and/or take action. The taking action is, for example, for the purpose of mitigating threats such as malware, viruses and other threats, which could harm the user's computer, company network and its computers, and the like.

[00091] EXAMPLE 1 – A user who works every day from 8am to 8pm is suddenly showing activity on his computer as being active at 11 pm. The behavioral recommendation engine 230 analyzes this change in time of activity and recommends that action be taken by the system 100', for example, via the management server 100. The action recommended and taken is one of blocking the user computer from accessing the network 50, alerting before blocking, or asking for a certain code to make sure it is the user (similar to a two factor authentication).

[00092] EXAMPLE 2 – The behavioral recommendation engine 230 analyzes a combination of awareness, rating, ongoing behavior, detection of exceptions and automated actions. Here, the user has never tried to download software and has a high cybersecurity awareness training and behavior rating, but is now suddenly trying to download software from a website, which is unacceptable under the organization's policies. The recommendation is to take action by automatically blocking the user computer from accessing the network 50, and automatically reporting to the system administrator 102 (by email) of the blocking. The recommendation engine 230 can also send commands to the requisite network components and computers to take the recommended action.

[00093] EXAMPLE 3 – A user who has never attempted to browse malicious websites, and now suddenly tries to browse websites not previously visited, or a user who suddenly tries to transmit information to third parties, both users having a very high cybersecurity awareness

training and behavior rating, the engine 230 recommends automatic action in the form of blocking the user computers from the network 50 and/or alerting the system administrator. The recommendation engine 230 can also send commands to the requisite network components and computers to take the recommended action.

[00094] EXAMPLES 2 and 3 illustrate how to combine an action that happened on a computer, which is in violation of an organization's policy, with a user's level/rating of his cybersecurity awareness training and behavior. The behavior recommendation engine 230 recommends automatic behavioral recommendations and/or actions to block the user computers from accessing the network 50.

[00095] EXAMPLE 4 – A user wants to use a disk on key to download/upload some documents. Disk on keys are against the enterprise's security policy and the user knows this, hence, he is requesting permission from the management server 100. Since the user has a high score, he is considered trustworthy, and accordingly, the system administrator 102 grants the user permission for one hour to use this disk on key, and the management server 100 automatically configures the user's computer (endpoint) accordingly, or automatically sends instructions to the system administrator 102 to do so.

[00096] EXAMPLE 5 – A user wants to browse a web site against the enterprise's security policy (regardless of whether the web site is benign) and the user knows this, hence, he is requesting permission from the management server 100. As the user's score is high, the user is considered to be trustworthy, and the management server 100 automatically unblocks the web site for a limited time, such as an hour, whereby the user may access this web site, or alternately sends instructions to the system administrator 102 to do so. Alternately, the management server 100 may automatically send a recommendation for actions to other technological information security solutions that exist in the organization.

[00097] EXAMPLE 6 - Once an action is performed at the end point computer 110, that is in violation of company (enterprise) policy, or an employee fails in a simulation - the system 100', for example, of the management server 100, via the behavior recommendation engine 230, will automatically send the employee a quiz/tutorial according to the action taken. For example - after the employee has browsed the Internet more than 10 times for websites that must not be browsed (and blocked) – the engine 230, via the management server 100, automatically sends a command to the requisite computer or network device to block this endpoint computer 110 from accessing the Internet will be blocked. Additionally, the engine 230 may automatically send a command to the tutorials and education module 215, to send the user a tutorial on

cybersecurity and enterprise policy, which the user will need to successfully pass. Only then be able to continue surfing the Internet.

[00098] EXAMPLE 7 – At a first time t1, a user with a low score reports a web site as suspicious, to the system 100'. At subsequent second, third and fourth times, t2, t3, t4, users with high scores report this web site as suspicious to the system 100'. As of time t4, company network users may still access this web site. At a subsequent fifth, sixth and seventh time, t5, t6 and t7, high score users report this web site as suspicious to the system 100'. Now, at an eighth time t8, after time t7, the system 100', for example, via the management server 100, automatically blocks all access to this web site for all computers on the company network, regardless of the user's score, as a minimum number of high score users have reported this web site as suspicious. Alternately, the management server 100 automatically allows high score users to access this web site, while low score users are blocked from accessing this web site. The management server 100 can send one or more notifications to the cloud server 135. The cloud server 135 can then, for example, send these notifications to other management servers for their enterprise networks.

[00099] EXAMPLE 8 – Data Leak Protection (DLP). A user is sending credit card numbers/credit card information over the network 50. Sending credit card numbers, and using credit card processing electronic forms, is against company policy. This user behavior is monitored, for example, the activity in violation of the company (enterprise) policy is monitored by a DLP solution (if there is one in the organization (enterprise)) and the DLP is the one that reports to the management server 100 the user's attempt to send data in violation of the policy. This behavior of the user affects his score, and is automatically reported, for example, as a report to the analysis module 212 and the behavior recommendation engine 230. The management server 100 acts automatically, such that the analysis module adjusts the user's score, for example, negatively, and/or causes the computer 110 of the user and/or the gateway 130 to block this email or other transmission of credit card numbers/information (the automatic taking of action).

[000100] The processes of EXAMPLES 1-8 may be performed automatically by the system 100', of the management server 100, or by manual operation, according to the system administrator 102 settings, or combinations thereof. This includes sending instructions for action from the management 100 server for technological solutions possessed by the organization (enterprise).

[000101] In other embodiments, the cloud server 135 links to the management server 100, and, for example transmits reports as to malicious or suspicious web pages, for every predetermined number of instances the web page is determined to be suspicious or malicious. The system

100' now has this information and can analyze user behavior knowing that a web site is suspicious or malicious. This information can also be shared with the system administrator 102, and with a relevant technological solution that exists in the organization, either from the cloud server 135 or the management server 100, which can take action accordingly.

[000102] Embodiments of the disclosed subject matter are directed to a method for providing an automated response to user behavior, for example, for user computer behavior management. The method comprises: receiving, by a computer system, data of user actions taken on a computer of the user, the computer of the user in communication with the computer system; analyzing the received data against the knowledge level of the user as determined by the computer system, and/or, the user's responses to simulations generated by the computer system, to determine a score for the user; and, in response to the score, making a behavior recommendation for the user and/or making a decision to take an action associated with the computer of the user.

[000103] Optionally, the method additionally comprises providing an agent to the computer of the user for obtaining the user actions taken on the computer of the user and transmitting data of the user actions to the computer system. Optionally, the agent monitors the computer of the user to obtain the user actions taken on the computer of the user. Optionally, the knowledge level of the user is determined by the computer system, based on the user having been provided media about the computer and/or the computer system, by the computer system. Optionally, the knowledge level of the user is additionally determined by the computer system receiving indications of interaction by the user with the provided media, from the user of the computer. Optionally, the media includes materials in electronic formats. Optionally, the computer system automatically generates electronic reports on the user of the computer, and, the analyzing additionally includes analyzing one or more of the electronic reports on the user of the computer. Optionally, the simulations generated by the computer system include one or more of: cyber-attacks, phishing, email handling, document handling, file handling, and web browsing. Optionally, the making a behavior recommendation for the user and/or a decision to take an action on the computer of the user, includes not making a behavior recommendation for the user and/or not making a decision to take an action on the computer of the user. Optionally, the behavior recommendation includes transmitting, to the computer of the user, a warning to the user of the computer, and/or sending materials to the computer of the user, associated with the behavior of the user on the computer of the user. Optionally, the decision to take action on the computer of the user, includes causing an action to be taken by the

computer of the user and/or the computer system. Optionally, the computer system includes at least one computer comprising at least one processor and a memory.

[000104] Optionally, the method is such that it additionally comprises, receiving a request from a user of the computer. Optionally, the making a decision to take an action on the computer of the user includes allowing or not allowing the request. Optionally, the allowing the request includes causing the computer of the user to operate in accordance with the request.

[000105] Embodiments of the disclosed subject matter are directed to a system for managing computer behavior of users. The system comprises: a storage medium for storing computer components; and, at least one processor for executing the computer components. The computer components comprise: a first module for receiving data of user actions taken on a computer of the user, the computer of the user in communication with a computer system; a second module for analyzing the received data of user actions against a knowledge level of the user, and/or, the user's responses to simulations generated by the computer system, to determine a score for the user; and, a third module, which responds to the determined score to make a behavior recommendation for the user and/or make a decision to take an action associated with the computer of the user.

[000106] Optionally, the system additionally comprises: an agent associated with the computer of the user for transmitting the data of user actions to the first module. Optionally, the agent is configured to monitor the computer of the user to obtain the user actions taken on the computer of the user. Optionally, the system additionally comprises a fourth module for determining the knowledge level of the user, based on media provided to the user. Optionally, the system additionally comprises a fifth module for providing simulations to the computer of the user, the simulations including one or more of: cyber-attacks, phishing, email handling, document handling, file handling, and web browsing. Optionally, the behavior recommendation for the user and/or a decision to take an action on the computer of the user, by the third module includes not making a behavior recommendation for the user and/or not making a decision to take an action on the computer of the user. Optionally, the system additionally comprises a sixth module for handling requests from users of computers, and based on a score associated with the user who made the request, rendering a decision to allow, modify or deny the request.

[000107] Embodiments of the disclosed subject matter are directed to a computer usable non-transitory storage medium having a computer program embodied thereon for causing a suitably programmed system to manage computer behavior of users, by performing the following steps when such program is executed on the system. The steps comprise: receiving data of user actions taken on a computer of the user, the computer of the user in communication

with a computer system; analyzing the received data of user actions against a knowledge level of the user, and/or, the user's responses to simulations generated by the computer system, to determine a score for the user; and, responding to the determined score to make a behavior recommendation for the user and/or make a decision to take an action associated with the computer of the user.

[000108] Optionally, the computer usable non-transitory storage medium additionally comprises: determining the knowledge level of the user, based on media provided to the user of the computer. Optionally, the computer usable non-transitory storage medium additionally comprises: providing simulations to the computer of the user, the simulations including one or more of: cyber-attacks, phishing, email handling, document handling, file handling, and web browsing. Optionally, the behavior recommendation for the user and/or a decision to take an action on the computer of the user, includes not making a behavior recommendation for the user and/or not making a decision to take an action on the computer of the user. Optionally, the computer usable non-transitory storage medium additionally comprises: handling requests from users of computers, and based on a score associated with the user who made the request, rendering a decision to allow, modify or deny the request.

[000109] According to actual instrumentation and equipment of embodiments of the method and/or system of the disclosed subject matter, several selected tasks could be implemented by hardware, by software or by firmware or by a combination thereof using an operating system or a cloud-based platform.

[000110] For example, hardware for performing selected tasks according to embodiments of the invention could be implemented as a chip or a circuit, or a virtual machine or virtual hardware. As software, selected tasks according to embodiments of the invention could be implemented as a plurality of software instructions being executed by a computer using any suitable operating system. In an exemplary embodiment of the invention, one or more tasks according to exemplary embodiments of method and/or system as described herein are performed by a data processor, such as a computing platform for executing a plurality of instructions. Optionally, the data processor includes a volatile memory for storing instructions and/or data and/or a non-volatile storage, for example, non-transitory storage media such as a magnetic hard-disk and/or removable media, for storing instructions and/or data. Optionally, a network connection is provided as well. A display and/or a user input device such as a keyboard or mouse are optionally provided as well.

[000111] For example, any combination of one or more non-transitory computer readable (storage) medium(s) may be utilized in accordance with the above-listed embodiments of the

present invention. A non-transitory computer readable storage medium may be, for example, but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, or device, or any suitable combination of the foregoing. More specific examples (a non-exhaustive list) of the computer readable storage medium would include the following: a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), a portable compact disc read-only memory (CD-ROM), an optical storage device, a magnetic storage device, or any suitable combination of the foregoing. In the context of this document, a computer readable non-transitory storage medium may be any tangible medium that can contain, or store a program for use by or in connection with an instruction execution system, apparatus, or device.

[000112] A computer readable signal medium may include a propagated data signal with computer readable program code embodied therein, for example, in baseband or as part of a carrier wave. Such a propagated signal may take any of a variety of forms, including, but not limited to, electro-magnetic, optical, or any suitable combination thereof. A computer readable signal medium may be any computer readable medium that is not a computer readable storage medium and that can communicate, propagate, or transport a program for use by or in connection with an instruction execution system, apparatus, or device.

[000113] As will be understood with reference to the paragraphs and the referenced drawings, provided above, various embodiments of computer-implemented methods are provided herein, some of which can be performed by various embodiments of apparatuses and systems described herein and some of which can be performed according to instructions stored in non-transitory computer-readable storage media described herein. Still, some embodiments of computer-implemented methods provided herein can be performed by other apparatuses or systems and can be performed according to instructions stored in computer-readable storage media other than that described herein, as will become apparent to those having skill in the art with reference to the embodiments described herein. Any reference to systems and computer-readable storage media with respect to the following computer-implemented methods is provided for explanatory purposes, and is not intended to limit any of such systems and any of such non-transitory computer-readable storage media with regard to embodiments of computer-implemented methods described above. Likewise, any reference to the following computer-implemented methods with respect to systems and computer-readable storage media is provided for explanatory purposes, and is not intended to limit any of such computer-implemented methods disclosed herein.

[000114] The flowcharts and block diagrams in the Figures illustrate the architecture, functionality, and operation of possible implementations of systems, methods and computer program products according to various embodiments of the present invention. In this regard, each block in the flowchart or block diagrams may represent a module, segment, or portion of code, which comprises one or more executable instructions for implementing the specified logical function(s). It should also be noted that, in some alternative implementations, the functions noted in the block may occur out of the order noted in the figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved. It will also be noted that each block of the block diagrams and/or flowchart illustration, and combinations of blocks in the block diagrams and/or flowchart illustration, can be implemented by special purpose hardware-based systems that perform the specified functions or acts, or combinations of special purpose hardware and computer instructions.

[000115] The descriptions of the various embodiments of the present invention have been presented for purposes of illustration, but are not intended to be exhaustive or limited to the embodiments disclosed. Many modifications and variations will be apparent to those of ordinary skill in the art without departing from the scope and spirit of the described embodiments. The terminology used herein was chosen to best explain the principles of the embodiments, the practical application or technical improvement over technologies found in the marketplace, or to enable others of ordinary skill in the art to understand the embodiments disclosed herein.

[000116] As used herein, the singular form "a", "an" and "the" include plural references unless the context clearly dictates otherwise.

[000117] The word "exemplary" is used herein to mean "serving as an example, instance or illustration". Any embodiment described as "exemplary" is not necessarily to be construed as preferred or advantageous over other embodiments and/or to exclude the incorporation of features from other embodiments.

[000118] It is appreciated that certain features of the invention, which are, for clarity, described in the context of separate embodiments, may also be provided in combination in a single embodiment. Conversely, various features of the invention, which are, for brevity, described in the context of a single embodiment, may also be provided separately or in any suitable subcombination or as suitable in any other described embodiment of the invention. Certain features described in the context of various embodiments are not to be considered essential features of those embodiments, unless the embodiment is inoperative without those elements.

[000119] The above-described processes including portions thereof can be performed by software, hardware and combinations thereof. These processes and portions thereof can be performed by computers, computer-type devices, workstations, processors, micro-processors, other electronic searching tools and memory and other non-transitory storage-type devices associated therewith. The processes and portions thereof can also be embodied in programmable non-transitory storage media, for example, compact discs (CDs) or other discs including magnetic, optical, etc., readable by a machine or the like, or other computer usable storage media, including magnetic, optical, or semiconductor storage, or other source of electronic signals.

[000120] The processes (methods) and systems, including components thereof, herein have been described with exemplary reference to specific hardware and software. The processes (methods) have been described as exemplary, whereby specific steps and their order can be omitted and/or changed by persons of ordinary skill in the art to reduce these embodiments to practice without undue experimentation. The processes (methods) and systems have been described in a manner sufficient to enable persons of ordinary skill in the art to readily adapt other hardware and software as may be needed to reduce any of the embodiments to practice without undue experimentation and using conventional techniques.

[000121] In the description and claims of the present application, each of the verbs, “comprise” “include” and “have”, and conjugates thereof, are used to indicate that the object or objects of the verb are not necessarily a complete listing of components, elements or parts of the subject or subjects of the verb.

[000122] Descriptions of embodiments of the invention in the present application are provided by way of example and are not intended to limit the scope of the invention. The described embodiments comprise different features, not all of which are required in all embodiments of the invention. Some embodiments utilize only some of the features or possible combinations of the features. Variations of embodiments of the invention that are described, and embodiments of the invention comprising different combinations of features noted in the described embodiments, will occur to persons of the art. The scope of the invention is limited only by the claims.

CLAIMS

1. A method for providing an automated response to user behavior comprising:
 - receiving, by a computer system, data of user actions taken on a computer of the user, the computer of the user in communication with the computer system;
 - analyzing the received data against the knowledge level of the user as determined by the computer system, and/or, the user's responses to simulations generated by the computer system, to determine a score for the user; and,
 - in response to the score, making a behavior recommendation for the user and/or making a decision to take an action associated with the computer of the user.
2. The method of claim 1, additionally comprising: providing an agent to the computer of the user for obtaining the user actions taken on the computer of the user and transmitting data of the user actions to the computer system.
3. The method of claim 2, wherein the agent monitors the computer of the user to obtain the user actions taken on the computer of the user.
4. The method of claim 1, wherein the knowledge level of the user is determined by the computer system, based on the user having been provided media about the computer and/or the computer system, by the computer system.
5. The method of claim 4, wherein the knowledge level of the user is additionally determined by the computer system receiving indications of interaction by the user with the provided media, from the user of the computer.
6. The method of claim 5, wherein the media includes materials in electronic formats.
7. The method of claim 1, wherein the computer system automatically generates electronic reports on the user of the computer, and, the analyzing additionally includes analyzing one or more of the electronic reports on the user of the computer.

8. The method of claim 1, wherein the simulations generated by the computer system include one or more of: cyber-attacks, phishing, email handling, document handling, file handling, and web browsing.
9. The method of claim 1, wherein the making a behavior recommendation for the user and/or a decision to take an action on the computer of the user, includes not making a behavior recommendation for the user and/or not making a decision to take an action on the computer of the user.
10. The method of claim 1, wherein the behavior recommendation includes transmitting, to the computer of the user, a warning to the user of the computer, and/or sending materials to the computer of the user, associated with the behavior of the user on the computer of the user.
11. The method of claim 1, wherein the decision to take action on the computer of the user, includes causing an action to be taken by the computer of the user and/or the computer system.
12. The method of claim 1, wherein the computer system includes at least one computer comprising at least one processor and a memory.
13. The method of claim 1, additionally comprising, receiving a request from a user of the computer.
14. The method of claim 13, wherein the making a decision to take an action on the computer of the user includes allowing or not allowing the request.
15. The method of claim 14, wherein the allowing the request includes causing the computer of the user to operate in accordance with the request.
16. A system for managing computer behavior of users comprising:
 - a storage medium for storing computer components; and,

at least one processor for executing the computer components, the computer components comprising:

a first module for receiving data of user actions taken on a computer of the user, the computer of the user in communication with a computer system;

a second module for analyzing the received data of user actions against a knowledge level of the user, and/or, the user's responses to simulations generated by the computer system, to determine a score for the user; and,

a third module, which responds to the determined score to make a behavior recommendation for the user and/or make a decision to take an action associated with the computer of the user.

17. The system of claim 16, additionally comprising: an agent associated with the computer of the user for transmitting the data of user actions to the first module.

18. The system of claim 17, wherein the agent is configured to monitor the computer of the user to obtain the user actions taken on the computer of the user.

19. The system of claim 16, additionally comprising: a fourth module for determining the knowledge level of the user, based on media provided to the user.

20. The system of claim 16, additionally comprising a fifth module for providing simulations to the computer of the user, the simulations including one or more of: cyber-attacks, phishing, email handling, document handling, file handling, and web browsing.

21. The system of claim 16, wherein the behavior recommendation for the user and/or a decision to take an action on the computer of the user, by the third module includes not making a behavior recommendation for the user and/or not making a decision to take an action on the computer of the user.

22. The system of claim 16, additionally comprising a sixth module for handling requests from users of computers, and based on a score associated with the user who made the request, rendering a decision to allow, modify or deny the request.

23. A computer usable non-transitory storage medium having a computer program embodied thereon for causing a suitably programmed system to manage computer behavior of users, by performing the following steps when such program is executed on the system, the steps comprising:

receiving data of user actions taken on a computer of the user, the computer of the user in communication with a computer system;

analyzing the received data of user actions against a knowledge level of the user, and/or, the user's responses to simulations generated by the computer system, to determine a score for the user; and,

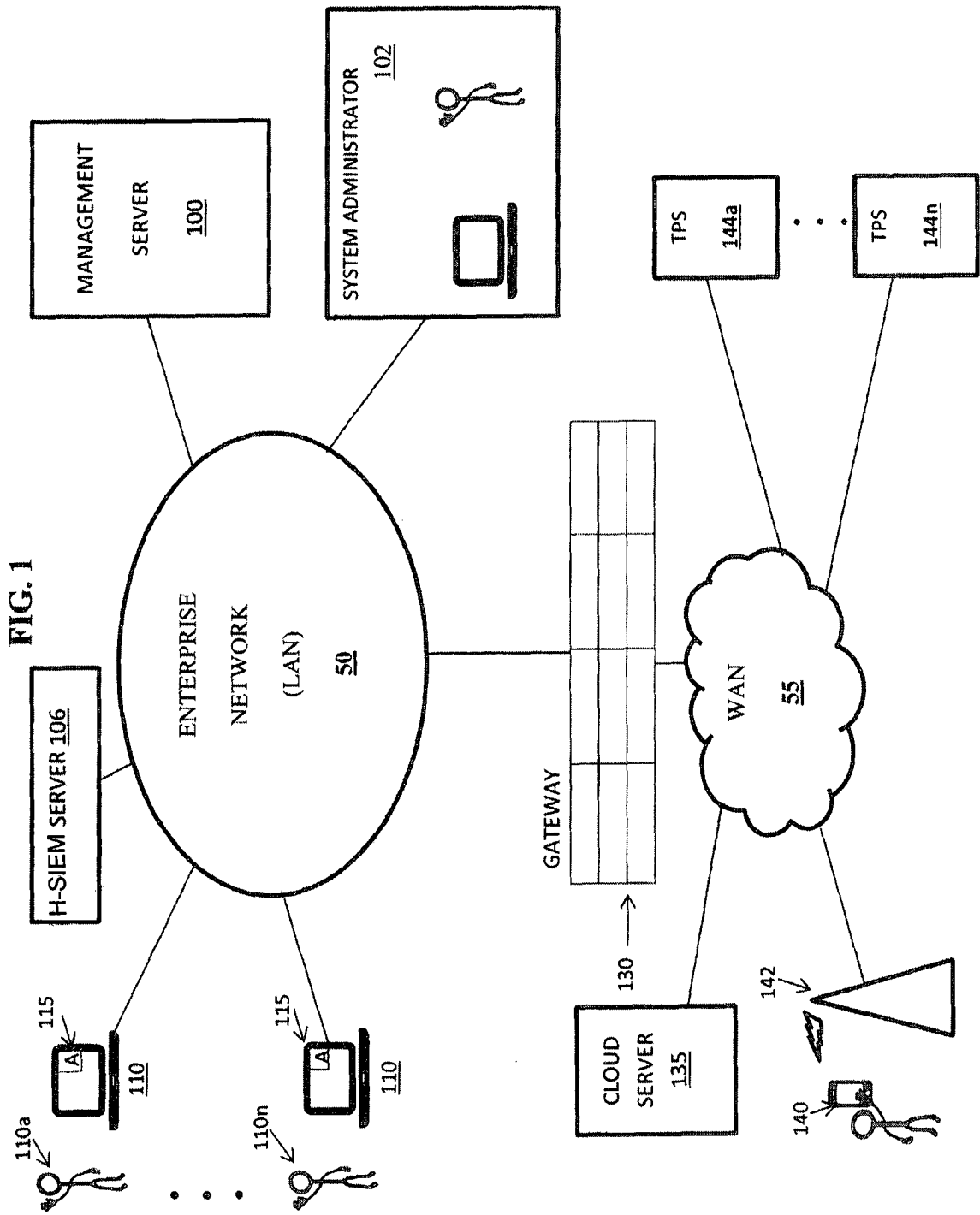
responding to the determined score to make a behavior recommendation for the user and/or make a decision to take an action associated with the computer of the user.

24. The computer usable non-transitory storage medium of claim 23, additionally comprising: determining the knowledge level of the user, based on media provided to the user of the computer.

25. The computer usable non-transitory storage medium of claim 23, additionally comprising: providing simulations to the computer of the user, the simulations including one or more of: cyber-attacks, phishing, email handling, document handling, file handling, and web browsing.

26. The computer usable non-transitory storage medium of claim 23, wherein the behavior recommendation for the user and/or a decision to take an action on the computer of the user, includes not making a behavior recommendation for the user and/or not making a decision to take an action on the computer of the user.

27. The computer usable non-transitory storage medium of claim 23, additionally comprising: handling requests from users of computers, and based on a score associated with the user who made the request, rendering a decision to allow, modify or deny the request.



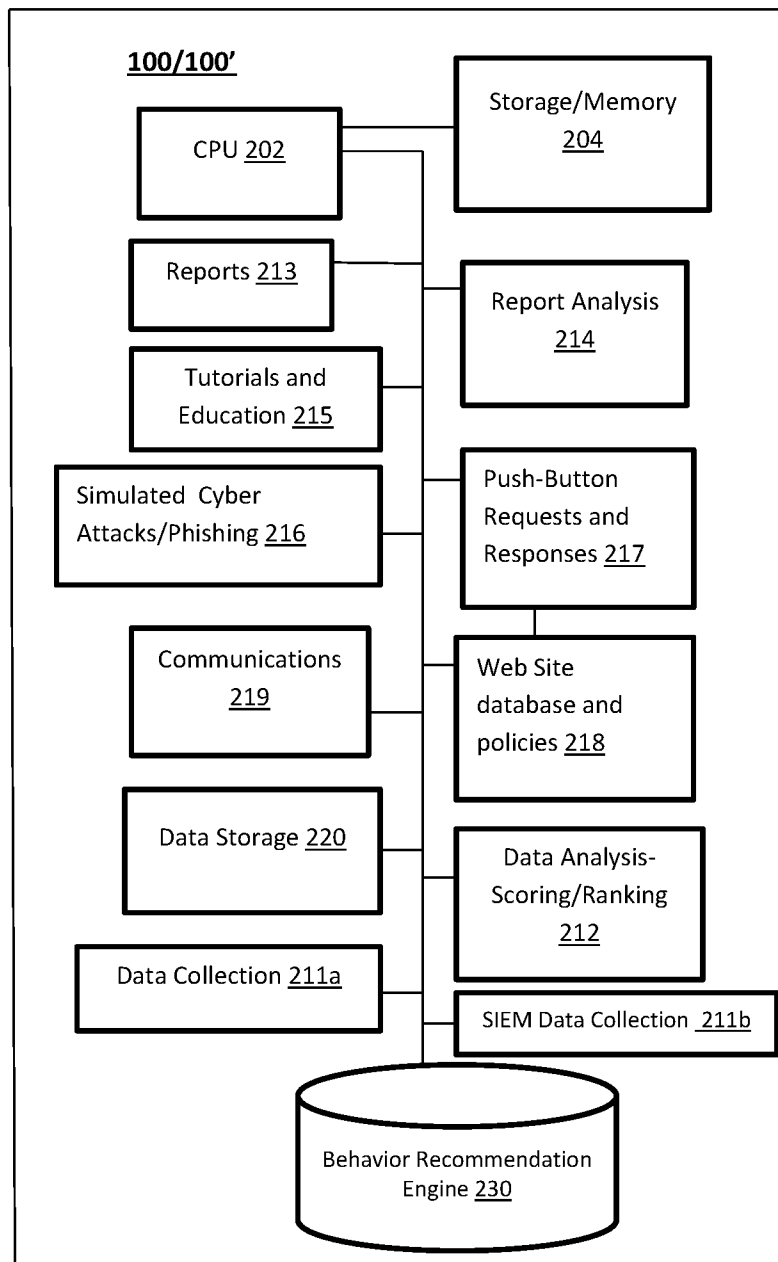


FIG. 2

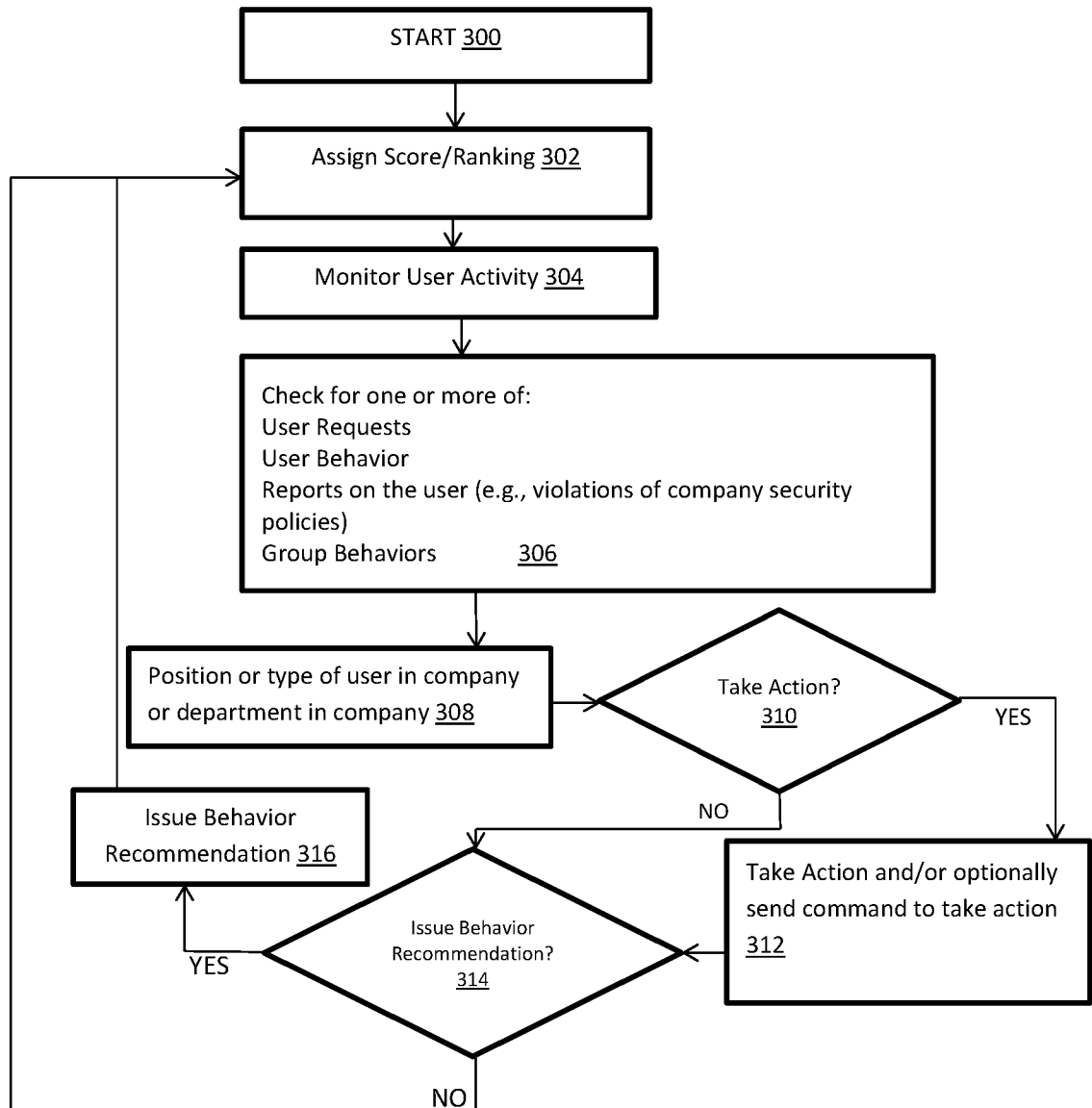


FIG. 3A

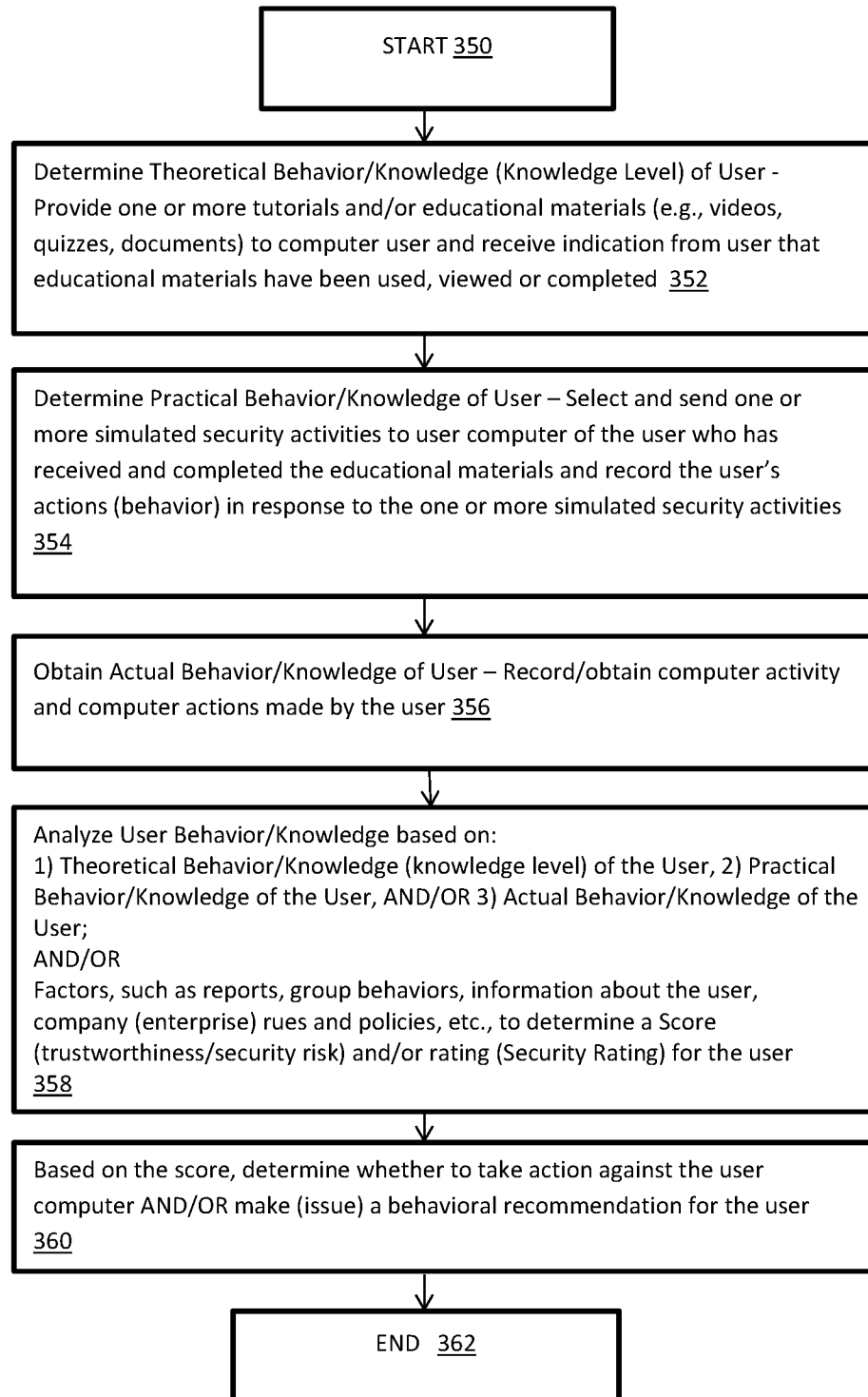


FIG. 3B

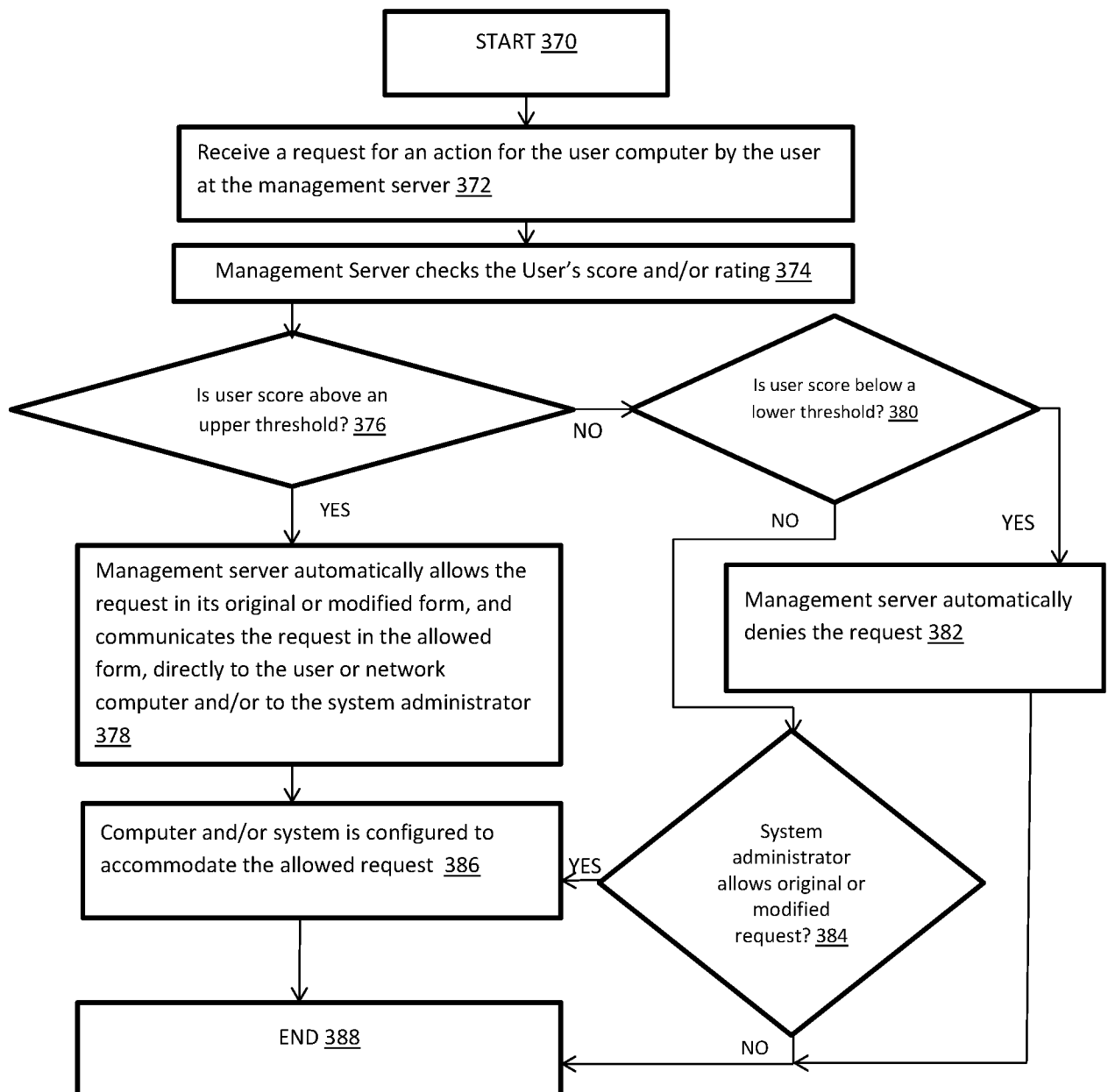


FIG. 3C

INTERNATIONAL SEARCH REPORT

International application No.

PCT/IB 21/51474

A. CLASSIFICATION OF SUBJECT MATTER

IPC - G06F 11/00 (2021.01)

CPC - G06F 21/577, H04L 63/1433, H04L 63/1416, H04L 63/20, H04L 63/1408, G06F 21/10, G11B 20/00086, G11B 20/0021, H04L 63/0428, H04N 21/4405, H04L 63/20, H04L 63/102, G06F 21/6218, G06F 21/604, H04L 63/0227

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

See Search History document

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

See Search History document

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

See Search History document

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2020/0021620 A1 (Securityadvisor Technologies, Inc.) 16 January 2020 (16.01.2020), entire document, especially, Abstract; Figs 11A-11B, 20; paras [0003], [0008]-[0011], [0042], [0044], [0048], [0051], [0053], [0056], [0059]-[0061], [0070]-[0071], [0080], [0082], [0093], [0097]-[0099], [0102], [0104]-[0105].	1-27
A	US 2019/0260764 A1 (Darktrace Limited) 22 August 2019 (22.08.2019), entire document.	1-27
A	US 2018/0375886 A1 (Oracle International Corporation) 27 December 2018 (27.12.2018), entire document.	1-27
A	US 2014/0310235 A1 (Oracle International Corporation) 16 October 2014 (16.10.2014), entire document.	1-27

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

* Special categories of cited documents:

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

"D" document cited by the applicant in the international application

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

18 May 2021 (18.05.2021)

Date of mailing of the international search report

JUN 11 2021

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450

Facsimile No. 571-273-8300

Authorized officer

Lee Young

Telephone No. PCT Helpdesk: 571-272-4300