

A METHOD FOR PRE-BUILDING AND DEPLOYING A SECURITY OPERATIONS CENTER

FIELD OF THE INVENTION

[0001] The invention pertains to security operations centers.

BACKGROUND

[0002] A security operations center (SOC) is a centralized unit inside an organization that continuously monitor and enhance the security posture of an organization leveraging on people, process and technology methodology. A computer implemented SOC for an organization can comprise servers implementing SIEM and / or analytics, endpoint protection, web protection, email protection and deception technologies.

[0003] Currently, if a customer organization wishes to implement a SOC, the SOC has to be designed to suit the organization requirements, and the SOC has to be built and assembled from scratch at the customer's premises. This process can take on average 9 to 12 months. This length of time is too long as during this period, the organization will be vulnerable to malicious attacks. This problem is further compounded if the organization does not have any employees with the necessary security expertise. In addition, an organization can lack well-defined processes that impedes the efficiency and effectiveness to operate a SOC. Technology can evolve rapidly and an organization can have difficulty keeping up with technology changes.

[0004] Thus, what is required is a novel method and system which addresses the above problems by providing a pre-assembled or pre-built deployable SOC, to reduce the time it takes to implement the SOC at the customer's environment. Furthermore, the SOC should also be modular so that it can be easily integrated with the customer's existing systems, and so that obsolete modules can be easily replaced with updated modules. Furthermore, other desirable features and characteristics will become apparent from the subsequent detailed description and the appended claims, taken in conjunction with the accompanying drawings and this background of the disclosure.

SUMMARY OF INVENTION

[0005] According to a first aspect of the invention, a method for pre-building a computer implemented security operations center (SOC) system is disclosed, the system for subsequent deployment at a customer environment. The system comprises a hardware module, an operating environment module, a common services module, a SOC services module and a sensors and log collectors module. The method comprising the steps of assembling the hardware module, and housing the hardware module in a portable assembly, the hardware module comprising computing resources, storage resources and networking resources; and adding the operating environment module into the computing resources and the storage resources of the hardware module, the operating environment module comprising a hypervisor module configured to consolidate the computing resources, the storage resources and the networking resources of the hardware module to provide a virtual machine for each of the common services module, the SOC services module and the sensors and log collectors module.

[0006] The method further comprises the steps of implementing the common services module on the virtual machine, the common services module configured to protect the system from security threats; implementing the sensors and log collectors module on the virtual machine, the sensors and log collectors module configured to detect and/or protect entry points of the customer environment from security threats; and implementing the SOC services module on the virtual machine, the SOC services module configured to continuously monitor the security posture of the customer environment.

[0007] The method further comprises the steps of integrating the common services module with the hardware module, the operating environment module, the SOC services module and the sensors and log collectors module; integrating the common services module, the SOC service module and the sensors and log collectors module with a cloud service; and transporting the portable assembly to a customer premises for the deployment of the system at the customer environment.

[0008] According to a second aspect of the invention, a portable assembly is disclosed, the portable assembly housing a prebuilt computer implemented security operations center (SOC) system, the system for deployment at a customer environment. The system comprising a hardware module, the hardware module comprising computing resources, storage resources

and networking resources; a common services module, the common services module configured to protect the system from security threats; and a sensors and log collectors module, the sensors and log collectors module configured to protect entry points of the customer environment from security threats.

[0009] The system further comprises a SOC services module, the SOC services module configured to monitor the security posture of the customer environment; and an operating environment module comprising a hypervisor module, the hypervisor module configured to consolidate the computing resources, the storage resources and networking resources of the hardware module to provide a virtual machine for each of the common services module, the SOC services module and the sensors and log collectors module.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] The accompanying figures, where like reference numerals refer to identical or functionally similar elements throughout the separate views and which together with the detailed description below are incorporated in and form part of the specification, serve to illustrate various embodiments, by way of example only, and to explain various principles and advantages in accordance with a present embodiment.

[0011] Figure 1 depicts a computer implemented security operations center (SOC) system for deployment at a customer environment, in accordance with certain embodiments.

[0012] Figure 2 depicts a hardware module, in accordance with certain embodiments.

[0013] Figure 3 depicts an operating environment module, in accordance with certain embodiments.

[0014] Figure 4 depicts a common services module, in accordance with certain embodiments.

[0015] Figure 5 depicts a SOC services module, in accordance with certain embodiments.

[0016] Figure 6 depicts a sensor and log collection module, in accordance with certain embodiments.

[0017] Figure 7 depicts a method for pre-building a computer implemented security SOC system, prior to its deployment to a customer environment, in accordance with certain embodiments.

[0018] Figure 8 depicts a method for deploying a pre-built computer implemented SOC system at a customer environment, in accordance with certain embodiments.

[0019] Skilled artisans will appreciate that elements in the figures are illustrated for simplicity and clarity and have not necessarily been depicted to scale. For example, the dimensions of some of the elements in the block diagrams or steps in the flowcharts may be exaggerated in respect to other elements to help improve understanding of the present embodiment.

DETAILED DESCRIPTION

[0020] The following detailed description is merely exemplary in nature and is not intended to limit the invention or the application and uses of the invention. Furthermore, there is no intention to be bound by any theory presented in the preceding background of the invention or the following detailed description.

[0021] It is the intent of certain embodiments to disclose a method for pre-building a computer implemented security operations center (SOC) system for subsequent deployment at a customer environment, the system comprising a hardware module, an operating environment module, a common services module, a SOC services module and a sensors and log collectors module, the method comprising the steps of assembling the hardware module, and housing the hardware module in a portable assembly, the hardware module comprising computing resources, storage resources and networking resources; and adding the operating environment module into the computing resources and the storage resources of the hardware module, the operating environment module comprising a hypervisor module configured to consolidate the computing resources, the storage resources and the networking resources of the hardware module to provide a virtual machine for each of the common services module, the SOC services module and the sensors and log collectors module.

[0022] The method further comprises the steps of implementing the common services module on the virtual machine, the common services module configured to protect the system from security threats; implementing the sensors and log collectors module on the virtual machine, the sensors and log collectors module configured to detect and/or protect entry points of the customer environment from security threats; and implementing the SOC services module on the virtual machine, the SOC services module configured to continuously monitor the security posture of the customer environment.

[0023] The method further comprises the steps of integrating the common services module with the hardware module, the operating environment module, the SOC services module and the sensors and log collectors module; integrating the common services module, the SOC service module and the sensors and log collectors module with a cloud service; and transporting the portable assembly to a customer premises for the deployment of the system at the customer environment.

[0024] As described above, by pre-building and pre-assembling the SOC system off-site, before delivering the SOC system to customer's premises for deployment, the time it takes to implement an operational SOC for the customer can be advantageously reduced. Furthermore, the design of the system is modular, in that the common services module, the SOC services module and the sensors and log collectors module are logically separated into distinct modules according to functionality. Moreover, because each of the common services module, the SOC services module and the sensors and log collectors module run on a virtual machine with a dedicated operating system, or are virtual appliances, this promotes the swap-ability of the modules – for example, if the sensors and log collectors module or one of its sub-modules needs to be replaced with an updated module/sub-module.

[0025] Even further still, the specific mix of the 5 modules (the hardware module, the operating environment module, the common services module, the SOC services module and the sensors and log collectors module) fulfil the fundamental requirements of a SOC and therefore act as a “one size fits all”, to cater to a majority customers and their needs.

[0026] Figure 1 shows a computer implemented security operations center (SOC) system 100 for deployment at customer environment 110, in accordance with certain embodiments. SOC

system 100 can comprise hardware module 101, operating environment module 102, common services module 103, SOC services module 104 and sensors and log collection module 105.

[0027] Hardware module 101 is for providing the hardware components necessary for the operation of SOC system 100. For example, hardware module 101 can comprise computing resources, storage resources and networking resources. As shown in figure 2, hardware module 101 can comprise network/network security sub-module 201, network/network security sub-module 201 for providing the networking resources. Networking resources such as network capabilities of SOC system 100 (for example, router, switch, hub), and network security of SOC system 100 (for example, firewall, network intrusion prevention system (IPS) and the virtual private network (VPN)).

[0028] Hardware module 101 can also comprise storage sub-module 202, storage sub-module 202 for providing the storage resources (e.g. servers, hard disks etc). The storage resources can include storage capability to store and run operating environment module 102, common services module 103, SOC services module 104 and sensors and log collection module 105. The storage resources can also store backups of SOC system 100 for backup protection.

[0029] Hardware module 101 can also comprise computing sub-module 203, computing sub-module 203 for providing the computing resources to provide processing power to run the workload of common services module 103, SOC services module 104 and sensors and log collection module 105. Computing sub-module 203 can include multiple central processing units (CPU), including graphic processing units (GPU) and Field Programmable Gate Arrays (FPGA) to enhance the computing engine. Computing sub-module 203 can also include mass high-speed dynamic memory or a hybrid of memory technology to enhance the computing speed.

[0030] Operating environment module 102 is for providing the operating environment for common services module 103, SOC services module 104 and sensors and log collection module 105. As shown in figure 3, operating environment module 102 can comprise hypervisor sub-module 301. Hypervisor sub-module 301 is for consolidating the computing resources, the storage resources and networking resources of hardware module 101 to provide one or more virtual machines for each of common services module 103, SOC services module 104 and sensors and log collectors module 105. Hypervisor sub-module 301 can create and

run the virtual machines, and can provide the virtualization platform (for example, VMware, Hyper-V) to run the operating systems (for example, Linux, Windows OS) and virtual appliances (for example, virtual firewall).

[0031] Operating environment module 102 can also comprise OS sub-module 302. OS sub-module 302 can provide the operating systems (for example, Linux, Windows OS) to run applications for common services module 103, SOC services module 104 and sensors and log collection module 105 on the virtual machines. Operating environment module 102 can also comprise virtual appliance sub-module 303. Virtual appliance sub-module 303 can comprise virtual appliances. A virtual appliance is a virtual machine image file consisting of a pre-configured operating system environment and a single application. The purpose of the virtual appliances is to simplify delivery and operation of applications.

[0032] Common services module 103 is for providing functionality to protect SOC system 100 itself. As shown in figure 4, common services module 103 can comprise authentication sub-module 401. Authentication sub-module 401 can provide authentication services for SOC system 100 which can include directory services, two-factor authentication, to manage local and remote access and authorization, and thus provide the functionality to assign/allow roles and privileges to the accessing users or entities. Common services module 103 can also comprise endpoint protection sub-module 402. Endpoint protection sub-module 402 can provide NexGen antivirus and anti-malware protection as well as early detection and response for SOC system 100. This can include advanced endpoint (e.g. end-user computers) activity detection with or without machine learning to identify any security threats at the endpoints. Endpoint protection sub-module 402 can also be configured to collect logs, and these logs can be correlated with other security sensing logs to narrow down the cyber threats.

[0033] Common services module 103 can also comprise active monitoring sub-module 403. Active monitoring sub-module 403 can provide infrastructure and/or application monitoring for SOC system 100. Active monitoring sub-module 403 can run on a virtual appliance. Common services module 103 can also comprise public key infrastructure sub-module 404. Public key infrastructure sub-module 404 can provide the infrastructure for certificates management. This can include key generation, key storage (for example in Hardware Security Modules), and the retrieval of keys in a highly secure manner. Common services module 103 can also comprise management tools sub-module 405. Management tools sub-module 405 can

provide the necessary management tools to manage and backup infrastructure and services for SOC system 100.

[0034] Common services module 103 can also comprise patch management sub-module 406. Patch management sub-module 406 can monitor and install patches for SOC system 100, thus keeping SOC system 100 up to date. Common services module 103 can also comprise remote access sub-module 407. Remote access sub-module 407 can provide remote access functionality for remote support and maintenance of SOC system 100 via the internet. This can include application of Virtual Private Network (VPN), Remote Desktop Protocol (RDP), Secure Shell (SSH), and similar technologies. Common services module 103 can also comprise compliance sub-module 408. Compliance sub-module 408 can provide compliance check for SOC system 100 and scan SOC system 100 for vulnerabilities. Compliance sub-module 408 can also be configured to generate rules and reports based on a templates database and/or customized templates. These reports can provide an indication of what remedial actions to take. Compliance sub-module 408 can run on a virtual appliance. Common services module 103 can also comprise configuration management sub-module 409. Configuration management sub-module 409 can manage any configuration change of SOC system 100.

[0035] SOC services module 104 is for providing functionality to continuously monitor the security posture of the customer environment, once SOC system 100 has been integrated with customer environment 110. As shown in figure 5, SOC services module 104 can comprise analytics sub-module 501. Analytics sub-module 501 can provide real-time threat intel driven analysis of security events generated by information gathered by the sensors and the log collectors of sensors and log collectors module 105 deployed in customer environment 110. The analysis can include applying machine learning and/or artificial intelligence technologies to identify the threats.

[0036] SOC services module 104 can also comprise threat intel sub-module 502. Threat intel sub-module 502 can provide threat intelligence to enhance the analysis and triaging of security incidents. The threat intelligence can be stored and extracted from a single or a plurality of local databases, or from external databases in cloud services 120. The threat intelligence can be constantly evolving and updated with threat data obtained from the day to day operations of running the SOC in the customer environment 110.

[0037] SOC services module 104 can also comprise orchestration, automation and response sub-module 503. Orchestration, automation and response sub-module 503 can provide assisted incident analysis and response workflow procedures. Orchestration, automation and response sub-module 503 can also automate some of the incident responses in the SOC. SOC services module 104 can also comprise use cases sub-module 504. Use cases sub-module 504 can comprise a list of specific threat events that is configured in analytics sub-module 501 to detect threats that need to be addressed by SOC system 100. The list of use cases sub-module 504 can be adapted to meet the specific requirements of the customer environment 110.

[0038] SOC services module 104 can also comprise processes and procedures sub-module 505. Processes and procedures sub-module 505 can provide the foundation for workflow that are implemented by orchestration, automation and response sub-module 503. Processes and procedures sub-module 505 can contain a “playbook” or workflow which describes countermeasures that need to be taken in response to the detection of specific security threats. Orchestration, automation and response sub-module 503 can reference processes and procedures sub-module 505, and execute the countermeasures in response to the detection of specific security threats. SOC services module 104 can also comprise future services sub-module 506. Future services sub-module 506 can act as a placeholder to incorporate additional future services to complement existing services. These future services can include network detection and response (NDR) to monitor communications within the customer’s network using a NDR sensor and apply advanced behaviour analytics to detect threats. Future services sub-module 506 can be an open, modular and scalable platform.

[0039] SOC services module 104 can also comprise situational awareness dashboard sub-module 507. Situational awareness dashboard sub-module 507 can provide a dashboard interface, the dashboard interface providing a user with a holistic view of the state of security of client environment 110. The dashboard interface provides a security posture of customer environment 110 by displaying the log activities with the alarm trends. The dashboard interface can provide a widget that allows quick categorization of events according to the risk score. Once a “threatening” event has been selected from the dashboard interface by the user, orchestration, automation and response sub-module 503 can reference processes and procedures sub-module 505 based on the details of the event, to access a “playbook” or workflow to execute countermeasures. For example, if the “threatening” event is that a range of IP addresses have a denial of service with a firewall of customer’s infrastructure, the

“playbook” or workflow may require the user to block the range of IP addresses. The executed countermeasures can be fully autonomous, semi- autonomous, or manual. The dashboard interface can also provide a threat activity map that visualises the source of the security threats (for example, suspicious IP addresses and its country of origin can be displayed on map).

[0040] Sensors and log collectors module 105 is for providing functionality to detect and/or protect customer environment 110 from security threats, and for collecting logs, once SOC system 100 has been integrated with customer environment 110. As shown in figure 6, sensors and log collectors module 105 can comprise sensors such as web sensor sub-module 601. Web sensor sub-module 601 can protect customer environment 110 against malicious web traffic. Web sensor sub-module 601 can be configured to identify threats in the web traffic and isolate these threats. Web sensor sub-module 601 can also be configured to block malicious web sites. Web sensor sub-module 601 can reference local databases, or online threat intelligence databases in cloud services 120, and apply Universal Resource Locator (URL) filtering and anti-phishing functions for customer environment 110.

[0041] Sensors and log collectors module 105 can also comprise sensors such as email sensor sub-module 602. Email sensor sub-module 602 can provide advanced email security protection for the email accounts in the email domain of customer environment 110. The email security protection can encompass identification of, and protection against, malware, phishing activities, file sandboxing and data leakage activities. Email sensor sub-module 602 can reference local databases or external threat intelligence databases in cloud services 120 for the identification of these threats. Sensors and log collectors module 105 can also comprise sensors such as endpoint sensor sub-module 603. Endpoint sensor sub-module 603 can provide early detection and response capabilities for all the endpoints in customer environment 110. An endpoint is any device that is physically an end point in customer environment 110 and can non-exhaustively include laptops, desktops, mobile phones, tablets, servers, and virtual environments.

[0042] Sensors and log collectors module 105 can also comprise sensors such as deception sub-module 605. Deception sub-module 605 can provide traps for early threat detection and analysis for internal or external threats. Sensors and log collectors module 105 can also comprise future sensor sub-module 606. Future sensor sub-module 606 can act as a placeholder to incorporate additional future sensors (e.g. NDR sensors) to complement

existing sensors. Sensors and log collectors module 105 can also comprise log collectors such as log collector sub-module 604. Log collector sub-module 604 can collect a variety of logs from the existing infrastructure and applications in customer environment 110, and from web sensor sub-module 601, email sensor sub-module 602, endpoint sensor sub-module 603 and deception sub-module 605, and then send the collected logs to for security analysis and analytics for detection of security events. For example, the collected logs can be sent to analytics sub-module 501 in SOC services module 104.

[0043] Figure 7 shows a method 700 which describes the steps of pre-building SOC system 100, prior to its deployment to customer environment 110, in accordance with certain embodiments.

[0044] In step 701, hardware module 101 is assembled and housed in a portable assembly. The portable assembly can comprise one or a plurality of server racks. Each of the server racks can have wheels at its base Hardware module 101 can comprise network/network security sub-module 201, storage sub-module 202 and computing sub-module 203.

[0045] In step 702, operating environment module 102 is added into the computing and storage resources of hardware module 101. Operating environment module 102 can comprise hypervisor sub-module 301, OS sub-module 302 and virtual appliance sub-module 303. Hypervisor sub-module 301 provides virtual machines for each of common services module 103, SOC services module 104 and sensors and log collectors module 105 to run their applications.

[0046] In step 703, common services module 103 is implemented on the virtual machine. Common services module 103 can run on OS sub-module 302 and/or virtual appliance sub-module 303. Common services module 103 can comprise authentication sub-module 401, endpoint protection sub-module 402, active monitoring sub-module 403, public key infrastructure sub-module 404, management tools sub-module 405, patch management sub-module 406, remote access sub-module 407, compliance sub-module 408 and configuration management sub-module 409.

[0047] In step 704, sensors and log collectors module 105 is implemented on the virtual machine. Sensors and log collectors module 105 can run on OS sub-module 302 and/or virtual

appliance sub-module 303. Sensors and log collectors module 105 can comprise web sensor sub-module 601, email sensor sub-module 602, endpoint sensor sub-module 603, log collector sub-module 604, detection sub-module 605 and future sensor sub-module 606.

[0048] In step 705, SOC services module 104 is implemented on the virtual machine. SOC services module 104 can run on OS sub-module 302 and/or virtual appliance sub-module 303. SOC services module 104 can comprise analytics sub-module 501, threat intel sub-module 502, orchestration, automation and response sub-module 503, use cases sub-module 504, processes and procedures sub-module 505, future services sub-module 506, and situational awareness dashboard sub-module 507.

[0049] Steps 703, 704 and 705 can be performed sequentially. In embodiments, steps 703, 704 and 705 can be performed concurrently.

[0050] In step 706, common services module 103 is integrated with hardware module 101, operating environment module 102, SOC services module 104 and sensors and log collectors module 105.

[0051] In step 707, common services module 103, SOC services module 104 and sensors and log collectors module 105 are integrated with cloud services 120. For instance, endpoint protection sub-module 402, patch management sub-module 406 and compliance sub-module 408 of common services module 103, and analytics sub-module 501 and threat intel sub-module 502 of SOC services module 104, and web sensor sub-module 601, email sensor sub-module 602 and endpoint sensor sub-module 603 of sensors and log collectors module 105, can be integrated with cloud services 120.

[0052] Steps 706 and 707 can be performed sequentially. In embodiments, steps 706 and 707 can be performed concurrently.

[0053] In step 708, integration verification is performed on SOC system 100 and on cloud services 120.

[0054] At the conclusion of the steps of method 700, the portable assembly comprising SOC system 100 is ready for deployment to customer environment 110. The ballpark average time

it takes to assemble and pre-build SOC system 100 as depicted by method 700 can be between 4 to 5 months.

[0055] In embodiments, a health check monitoring step can also be performed prior to step 708.

[0056] Figure 8 shows a method 800 which describes the steps of deploying pre-built SOC system 100 to customer environment 110, in accordance with certain embodiments.

[0057] In step 801, the portable assembly comprising SOC system 100 is transported to the client's premises. The portable assembly can weigh between 100 to 500 Kg.

[0058] In step 802, hardware module 101 is physically connected to customer environment 110. For instance, network/network security sub-module 201 can be connected to customer environment 110 first, followed by the servers in storage sub-module 202 and the CPUs of computing sub-module 203.

[0059] In step 803, a connection is established between remote access sub-module 407 of common services module 103, and the internet. Through this connection, support and maintenance can be provided from a remote server onto SOC system 100.

[0060] In step 804, the sensors of web sensor sub-module 601, email sensor sub-module 602, and endpoint sensor sub-module 603, and also log collector sub-module 604 and deception sub-module 605 of sensors and log collectors module 105, are integrated with customer environment 110. This can include installing the sensors of endpoint sensor sub-module 603 into the endpoints in customer environment 110. This can also include adapting deception sub-module 105 to customer environment 110. Coupled with the continuous monitoring of SOC services module 104, it is ensured that emails and web traffic in customer environment 110 flow through the sensors of web sensor sub-module 601 and email sensor sub-module 602 for protection and detection.

[0061] In step 805, the logs in customer environment 110 are integrated with log collector sub-module 604 of sensors and log collectors module 105, so that the present and future logs in customer environment 110 will be onboarded to log collector sub-module 604.

[0062] In step 806, configurations are made to SOC services module 104 to adapt to customer environment 110. These configurations can include removing use cases in use cases sub-module 504 that may not be relevant to customer environment 110. These configurations can also include adapting the “playbook” or workflow of dealing with security threats in processes and procedures sub-module 505, to cater to customer’s preferences.

[0063] At the conclusion of the steps of method 800, the deployment of SOC system 100 in customer environment 110 is complete. The ballpark average time it takes to deploy pre-built SOC system 100 at customer environment 110 as depicted by method 800 can be between 2 to 4 weeks.

[0064] As such, the total ballpark average time it takes to pre-build SOC system 100, and then deploy SOC system 100 at customer environment 110 can be between 4 to 6 months. This is significantly faster than the present method of building and assembling a SOC from scratch at the customer’s premises, which on average, takes between 9 to 12 months. Thus, the approach of configuring, assembling and testing SOC system 100 offsite, before delivering to customer’s premises, is able to drastically reduce the time it takes to implement an operational SOC for a customer.

[0065] Furthermore, the design of SOC system 100 is modular. The modules of SOC system 100 (i.e. hardware module 101, operating environment module 102, common services module 103, SOC services module 104 and sensors and log collection module 105) and its sub-modules can be easily swapped out, and replaced with updated modules, or updated sub-modules. This is advantageous because technologies in cyber securities evolve very quickly. Therefore, a modular design allows obsolete modules to be replaced with updated modules, without impacting the workings of SOC system 100. For example, if web sensor sub-module 601 of sensors and log collectors module 105 has become obsolete, a new web sensor sub-module 601 can be added to sensors and log collectors module 105, to replace the previous web sensor sub-module 601, to provide reasonable assurance that the technology is relevant. Moreover, because each of common services module 102, SOC services module 104, and sensors and log collectors module 105 run on a virtual machine with a dedicated operating system or a virtual appliance, this promotes the swap-ability of the modules.

[0066] Even further still, the specific mix of the 5 distinct modules fulfil the fundamental requirements of a SOC and therefore act as a “one size fits all”, to cater to most customers and the needs. In addition, the short build time can increase the return on investment. The pre-built deployable SOC also includes well-defined processes resulting in operation efficiency. Further, the pre-built deployable SOC is pre-integrated with proven technology and future proofed.

[0067] Unless specifically stated otherwise, and as apparent from the following, it will be appreciated that throughout the present specification, discussions utilizing terms such as “receiving”, “identifying”, “initiating”, “tagging”, “transmitting”, “running”, “incrementing”, “determining”, “assigning”, “approving”, “selecting”, “sending”, “calculating”, “determining”, “replacing”, “generating”, “initializing”, “outputting”, or the like, refer to the action and processes of a computer system, or similar electronic device, that manipulates and transforms data represented as physical quantities within the computer system into other data similarly represented as physical quantities within the computer system or other information storage, transmission or display devices.

[0068] In the application, unless specified otherwise, the terms "comprising", "comprise", and grammatical variants thereof, intended to represent "open" or "inclusive" language such that they include recited elements but also permit inclusion of additional, non-explicitly recited elements.

[0069] It will be apparent that various other modifications and adaptations of the application will be apparent to the person skilled in the art after reading the foregoing disclosure without departing from the spirit and scope of the application and it is intended that all such modifications and adaptations come within the scope of the appended claims.

CLAIMS

1. A method for pre-building a computer implemented security operations center (SOC) system for subsequent deployment at a customer environment, the system comprising a hardware module, an operating environment module, a common services module, a SOC services module and a sensors and log collectors module, the method comprising the steps of:

assembling the hardware module, and housing the hardware module in a portable assembly, the hardware module comprising computing resources, storage resources and networking resources;

adding the operating environment module into the computing resources and the storage resources of the hardware module, the operating environment module comprising a hypervisor sub-module configured to consolidate the computing resources, the storage resources and the networking resources of the hardware module to provide a virtual machine for each of the common services module, the SOC services module and the sensors and log collectors module;

implementing the common services module on the virtual machine, the common services module configured to protect the system from security threats;

implementing the sensors and log collectors module on the virtual machine, the sensors and log collectors module configured to detect and protect entry points of the customer environment from security threats;

implementing the SOC services module on the virtual machine, the SOC services module configured to monitor the security posture of the customer environment;

integrating the common services module with the hardware module, the operating environment module, the SOC services module and the sensors and log collectors module;

integrating the common services module, the SOC service module and the sensors and log collectors module with a cloud service; and

transporting the portable assembly to a customer premises for the deployment of the system at the customer environment.

2 The method of claim 1 wherein the portable assembly comprises at least one server rack, the at least one server rack having wheels at a base.

3. The method of claims 1 or 2, further comprising the step of performing integration verification of the system prior to transporting the portable assembly to the customer premises for the deployment of the system at the customer environment.
4. The method of any one of the preceding claims wherein the common services module comprises a remote access sub-module, and the remote access sub-module is configured to provide remote access functionality for remote support and maintenance of the system via the internet.
5. The method of any one of the preceding claims wherein the common services module further comprises a patch management sub-module, the patch management sub-module configured to monitor and install patches for the system.
6. The method of any one of the preceding claims wherein the operating environment module further comprises a virtual appliance sub-module, the virtual appliance sub-module configured to provide virtual appliances.
7. The method of any one of the preceding claims wherein the common services module further comprises an active monitoring sub-module, and the active monitoring sub-module is configured to perform periodic health check monitoring on the system.
8. The method of any one of the preceding claims wherein the common services module further comprises a compliance sub-module, and the compliance sub-module is configured to perform compliance check for the system and scan the system for vulnerabilities.
9. The method of claim 8 wherein the active monitoring sub-module or the compliance sub-module run on virtual appliances.
10. The method of any one of the preceding claims wherein the SOC services module comprises an analytics sub-module and a use cases sub-module, the analytics sub-module configured to reference a list of threat events in the use cases sub-module to detect security threats.

11. The method of any one of the preceding claims wherein the SOC services module further comprises a threat intel sub-module, the threat intel sub-module configured to reference the cloud service to provide threat intelligence to enhance the analysis and triaging of security threats.
12. The method of any one of the preceding claims wherein the SOC services module further comprises a situational awareness dashboard sub-module, an orchestration, automation and response sub-module, and a processes and procedures sub-module; and wherein the processes and procedures sub-module contain workflows which describes countermeasures to be taken in response to the detection of specific security threats; and wherein the situational awareness dashboard sub-module is configured to render an interface, the interface displaying at least one event for a user's selection; and wherein upon selection of the at least one event, the orchestration, automation and response sub-module is configured to reference the processes and procedures sub-module based on the selected event and execute the countermeasures.
13. The method of any one of the preceding claims wherein the sensors and log collectors module comprises a web sensor sub-module, the web sensor sub-module comprising sensors configured to protect the customer environment against malicious web traffic.
14. The method of any one of the preceding claims wherein the sensors and log collectors module further comprises an email sensor sub-module, the email sensor sub-module comprising sensors configured to provide email security protection for email accounts in the email domain of the customer environment.
15. The method of any one of the preceding claims wherein the sensors and log collectors module further comprises an endpoint sensor sub-module, the endpoint sensor sub-module comprising sensors configured to provide early detection and response capabilities for endpoints in the customer environment.
16. The method of any one of the preceding claims wherein the sensors and log collectors module further comprises a deception sub-module, the deception sub-module configured to provide traps for early threat detection and analysis for internal or external threats.

17. The method of claim 16 wherein the sensors and log collectors module further comprises a log collector sub-module, the log collector sub-module configured to collect logs from the web sensor sub-module, the email sensor sub-module, the endpoint sensor sub-module and the deception sub-module, and send the collected logs to the analytics sub-module for detection of security threats.

18. The method of claim 17 further comprising the steps of:
physically connecting the hardware module to the customer environment;
establishing a connection between the remote access sub-module and the internet;
integrating the sensors of the web sensor sub-module, the email sensor sub-module and the endpoint sensor sub-module with the customer environment;
integrating the log collector sub-module and the deception sub-module with the customer environment; and
configuring the SOC services module to adapt to the customer environment.

19. The method of any one of the preceding claims wherein the common services module, the SOC services module, and the sensors and log collectors module can be swapped with updated modules.

20. A portable assembly housing a prebuilt computer implemented security operations center (SOC) system, the system for deployment at a customer environment, the system comprising: -

a hardware module, the hardware module comprising computing resources, storage resources and networking resources;

a common services module, the common services module configured to protect the system from security threats;

a sensors and log collectors module, the sensors and log collectors module configured to protect entry points of the customer environment from security threats;

a SOC services module, the SOC services module configured to monitor the security posture of the customer environment; and

an operating environment module comprising a hypervisor module, the hypervisor module configured to consolidate the computing resources, the storage resources and networking resources of the hardware module to provide a virtual machine for each of the common services module, the SOC services module and the sensors and log collectors module.