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;

wherein the SOC services module 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.

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 heath 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 claims 7 or 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 further 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 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.

13. 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.

14. 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.

15. 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.

16. The method of claim 15 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.

17. The method of claim 16 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.

18. 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.

19. 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;

wherein the SOC services module 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.