Event Monitoring and Response Service

Service Overview:

Security Event and Response service (the "Service") consolidates and organizes security log events from a variety of network systems, devices, applications, and other tools, providing detailed visibility into the security of your network and bringing it into compliance with applicable regulatory information security mandates. The Security Operations Center (SOC) is trained to handle each event and contact the customer based on predefined incident handling policies.

Service Objectives: Security Event and Response service provides the customer with the following:

- Organization of security events from systems, devices, applications and other tools
- Detailed visibility into the security of your network
- Service support 24x7 with online ticketing

Service Deliverables: Security Event and Response service will deliver to the customer the following:

- Monitoring and reporting of security events delivered to SilverSky
- Online ticketing support for change management and reporting

Service Description

A proprietary threat intelligence platform provides the foundation for delivery of our Security Event Monitoring and Response service. Security Event Monitoring and Response service correlates event source data to report and provide responses to the customer about the latest viruses, spyware, and other content-level threats found within event data. Security Event Monitoring and Response services uses industry-leading advanced detection and correlation engines to report both new and evolving threats inside your network.

- Ingest event data from customer managed security appliances to provide correlations, responses and reporting.
- Provides incident handling policies based on security events from customer data feeds

Other Services

Any other services are out-of-scope. Upon request, SilverSky may provide out-of-scope technical support on a time and materials basis pursuant to a separate service description or statement of work ("SOW"). Examples of such out-of-scope support include but are not limited to:

- On-site installation and provisioning of device
- Integration of complementary products that are not managed by SilverSky (e.g., antivirus software; web reporting software)
- Custom analysis and/or custom reports
- Forensics
- Any change requests not specified above

- Rule set design, validation, and troubleshooting
- Policy Auditing, Policy/Rule Utilization, and Security Best Practice Consulting

CUSTOMER REQUIREMENTS

Customer agrees to perform the following obligations and acknowledges and agrees that SilverSky System's ability to perform its obligations, and its liability under the SLAs below, are dependent upon Customer's compliance with the following:

Hardware/Software Procurement

The Customer is responsible for purchasing the firewall hardware and service necessary for SilverSky to deliver the Service. Additionally, the Customer is responsible for ensuring that their hardware/software stays within Fortinet's supported versions. SilverSky System's SLAs will not apply to platforms that are end of life, end of support, or are otherwise not receiving updates by Fortinet.

Support Contracts

Customer is responsible for maintaining appropriate levels of hardware support and maintenance for the Customer-owned firewall and connectivity to prevent network performance degradation and maintain communications between the customer's contracted firewall devices and SilverSky System's security operations centers (Secure Operations Centers" or "SOC(s)").

RMA Responsibilities

The Customer is responsible for initiating and fulfilling the return materials authorization ("RMA") process directly with SilverSky in the event that the hardware/software being managed by SilverSky is determined to be in a failed or faulty state and requires replacement.

Connectivity

Customer will provide access to Customer-premises and relevant appliance(s) necessary for SilverSky to manage and monitor the contracted firewall devices. Additionally, Customer should communicate any network or system changes that could impact service delivery to the SOC via a ticket in the SilverSky SMC customer portal. Service activation which may require device downtime will depend on customer deliverables such as on-site assistance with initial configuration of the appliance to get connectivity between Fortinet appliance and SilverSky data centers. SLAs will not apply to devices that are experiencing Customer-caused connectivity issues.