Managed Intrusion Detection & Prevention

Service Overview

Intrusion Detection & Prevention service analyzes network traffic to identify and respond to threats in real time. A team of security analysts review security escalations and respond in accordance with the customer defined incident handling policies. We provide ongoing device management to ensure IDPS configurations and signatures stay up to date to combat the constantly evolving threat landscape. Certified security experts will perform all activities necessary to keep devices operating at peak performance.

Service Objectives: Managed Intrusion Detection & Prevention service provides the customer with the following:

- Detection and prevention of advanced targeted attacks, zero day attacks, ransomware, polymorphic malware and distributed denial-of-service attacks
- Multiple inspection engines, threat intelligence feeds and advanced threat protection options to defend against these unknown threats
- Service support 24x7 with online ticketing

Service Deliverables: Managed Intrusion Detection & Prevention service will deliver to the customer the following:

- Tuned and delivered policy and signature updates for the IDPS service
- Monitoring and reporting of security events that do not meet the configured policy
- Blocking of detected threats

Service Description

A proprietary threat intelligence platform provides the foundation for delivery of our Intrusion Detection & Prevention service. This developed technology facilitates Fortinet device management and detection of possible intrusions while actively attempting to prevent them. The following service components are included with the Service:

- Security Event Monitoring with Correlation
- Security Event Reporting

Security Event Monitoring with Correlation

Security Event Monitoring with Correlation monitors for zero-day, advanced targeted attacks, ransomware, polymorphic malware and distributed denial-of-service attacks using sophisticated detection engines not available in traditional standalone IDPS or in most firewalls. SilverSky uses these detection engines to then correlate events and alert the customer.

Security Event Reporting

Device log data is gathered by the device(s) and sent to the SilverSky SOC. The data is parsed, normalized, correlated, and prioritized. The security events are categorized by SilverSky based on the severity level. SilverSky also performs additional analysis using advanced detection engines to determine whether the event is a false positive. SilverSky provides the Customer with a report that contains a description of the event and any contextual information. The event is also posted on the SMC Portal and made available for reporting.

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.