Managed Web Application Firewall Service

Service Overview

Managed Web Application Firewall (the "Service") provides advanced features that defend web applications from known and zero-day threats. Using an advanced multi-layered and correlated approach, Managed Web Application Firewall provides complete security for your external and internal web-based applications from the OWASP Top 10 and many other threats.

Service Objectives: Managed Web Application Firewall service provides the customer with the following:

- 24x7 Monitoring of input, output and access attempts of your Web-based applications
- 24x7 Service support with online ticketing and alerting through the customer portal
- Blocking of any malicious activity that is detected
- Event/Incident triage with security service support. Triage will work towards identification and remediation.
- Protection against application vulnerabilities

Service Deliverables: Managed Web Application Firewall service will deliver to the customer the following:

- Web Application Firewall provisioning, signatures and policy definitions
- Collection of WAF log data through VPN tunnel
- Customer portal access to monitor alerts and ticketing
- 24x7 SilverSky security support coverage

Service Description

Managed Web Application Firewall service protects your Web-based applications from attack by monitoring input, output and access attempts, and dropping any malicious activity. When attacks are detected, Web Application Firewall alerts security analysts in one of the SilverSky Security Operations Centers (SOCs). The service protects against the full range of application vulnerabilities including cross-site scripting (XSS), injection flaws (SQL, LDAP, Xpath and others), malicious file execution, insecure direct object references, cross-site request forgery (CSRF), information leakage and improper error handling, broken authentications and session management, insecure cryptographic storage, insecure communications, and failure to restrict URL access.

- Deployed in front of web applications to scan and protect from application layer attacks and vulnerabilities.
- Deployed in transparent, transparent proxy, or reverse proxy modes.

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