Sentinel360 Managed Vulnerability Management System

Service Description

Numerous regulatory and compliance frameworks require organizations to perform vulnerability scanning of key assets, remediate identified vulnerabilities, and develop status reports. Managers and auditors must ensure that their organization's security posture meets organizational risk management and compliance requirements.

Sentinel360's Vulnerability Management Service provides the flexibility needed to create a vulnerability scanning program specifically designed to fit Client's requirements.

Overview

Features of the Sentinel360's Vulnerability Management service include the following:

- **External and Internal Scanning Options** – External vulnerability scanning will specifically examine Client's security profile from an external perspective. Internal vulnerability scanning will be used to identify real and potential vulnerabilities inside Client's network. This proposal includes licensing for a single vulnerability scanner to be installed with Client's network.
- **Managed Scanning** – Vulnerability Management offers flexibility in scan management – scans will be managed and executed by expert analysts in Sentinel360's Security Operation Center (SOC).
- **Policy Templates and Customization** – Effective vulnerability scanning of enterprise environments requires use of scanning templates customized for Client's unique network and focused on Client's own internal requirements.
- **Vulnerability Threat Correlation** – Vulnerability Threat Correlation (VTC) will enable Client to map potential threats to known vulnerabilities that exist in assets in Client's network and highlight risks associated with threats that are targeting known vulnerabilities. VTC is only available to Sentinel360 Vulnerability Management clients that are also subscribe to Sentinel360 Managed Security Services. As Client is already a Managed Security Service client, this VTC service will be provided as part of this offering.

- **Reporting Flexibility** – Sentinel360's Vulnerability Management service includes customizable vulnerability and remediation reports, with dozens of available metrics to help Client measure the performance of their vulnerability management program.
- **Vulnerability Management** – Sentinel360 will work with Client in managing and tunning the vulnerability management system to ensure false positives and other conditions are filtered out of future reports. As a result, Client will spend time remediating vulnerabilities, not digging through repetitive false positive laden reports.

The benefits include:

- **Flexibility** - custom program development, designed for organizational requirements.
- **Enhance the intelligence** – the Sentinel360 monitoring program via the Vulnerability Threat Correlation service enhancement provides up to date and accurate Threat Intelligence.
- **Repeatable and transparent** – processes that integrates and supports Client's vulnerability management program.
- **Cost effective** – by leveraging Sentinel360's skilled analysts which may augment or replace staff that lack of internal subject matter expertise for managing a vulnerability management program.
- **Compliant** – through certification and against regulations such as PCI-DSS, HIPAA, and NERC-CIP.
- **Timely** – gain visibility into threats and vulnerabilities across network environments and cloud assets 7X24X365.
- **Transform and execute** – threat and vulnerability data into actionable intelligence to assist in eliminating attack vectors and accelerating remediation.

Scan Configuration & Tuning

Sentinel360 will work with Client to configure the appropriate number of Scan Configuration templates. A configuration template is used for a single scan. For example, if you would like to have one Scan Configuration template for all Desktops, one scan for all assets in a DMZ, one scan for all printers, and one scan for detection of specific Common Vulnerabilities and Exposures (CVEs), that would require four (4) scan configurations.

Scan Scheduling & Maintenance

Sentinel360 manages and maintains all Scan Configuration schedules once deployed.

Reporting

Sentinel360 generates reports as defined in the Vulnerability Management platform. The default reports included in the Vulnerability Management service are described below:

- **Executive** - This report, appropriate for non-technical management, compares vulnerability assessment results over a time period, providing security trend information in summary format. A bar graph shows the number of vulnerabilities by severity, and a flow graph shows the number of vulnerabilities over time. This report includes no detailed vulnerability information.
- **Technical** - This report, appropriate for technicians, displays detailed results from the most recent vulnerability scan. This report includes vulnerability information sorted by host as well as a detailed description of each vulnerability, the recommended solution to remove the vulnerability, when the vulnerability was first and last detected, the consequences if the vulnerability is exploited, as well as the scan test result, where appropriate, showing how it was possible to confirm the vulnerability existed, such as the existence or lack of a registry key.
- **High Severity** - This report identifies all severity level 4 and 5 vulnerabilities, the highest severity levels and thus the vulnerabilities that pose the most serious threat to network security. Included in the summary are two graphs, identifying operating systems detected and services detected. Detailed host and vulnerability data, sorted by host, is provided.
- **Score Card** - The Vulnerability Scorecard Report gives you the latest vulnerability status about selected asset groups. By configuring a business risk goal, you can quickly review the comprehensive risk posture of different groups or business units. Additional vulnerability management metrics give managers a way to track remediation efforts.
- **Patching** - The Patch Report identifies hosts that are missing required patches and software. Each targeted asset group is listed with the hosts from each group that are missing required patches and software.

SOC Scan Reviews

The Sentinel360 SOC will perform in depth scan review status calls with Client. SOC review calls are intended to be consultative regarding the Vulnerability Management program design or program guidance. The SOC will review findings, discuss scan results, and discuss general strategies to improve Client's Vulnerability Management program and or enhance potential reporting initiatives.

On-Demand Scans

Sentinel360 will perform the number of on demand scans as requested by Client.

Authentication Scans

Sentinel360 will facilitate the deployment and configuration of Authenticated scan credentials within the platform in support of the scan configuration templates.

Vulnerability Management Support

Sentinel360 makes use of service workflow management functionality to aid in classification and management of False Positives issues. The SOC will manage the Vulnerability Management system.

Vulnerability Management Service Process

The Vulnerability Management Service process includes, but is not limited to, capturing information of Client's service requirements, SLAs, Configuration Items, site and contact details, configuration of connectivity and the implementation and activation of the Manage Centre portal and Security portals.

Sentinel360 utilizes a multi-phased approach to coordinate and perform the scanning service:

- Vulnerability Management Program Design PSS Services are available for Complex and Enterprise scale engagements.
- Phase 1 - Scanning Configuration
- Phase 2 – Vulnerability Discovery and Processing
- Phase 3 – Scanning Results and Reporting.

Sentinel360 assigns an Account Team to work with you throughout the performance of Services and may consist of one or more of the following: Service Delivery Manager, Information Security Analyst.

Sentinel360 will work with Client to complete the services questionnaire, which details Client's 'in-scope' IPs and escalation procedures. If Sentinel360 is contracted to provide more in-depth vulnerability management consultative services, we will work with Client to complete questionnaire.

Phase 1 – Scanning Configuration

Discovery Scans are not required but may be run at the start of each assessment window. The SOC uses Discovery Scans to help validate scope, or other concerns Client or the SOC may have before an assessment starts.

Sentinel360 configures the scanning system with the appropriate IPs and scan configurations as defined by Client. The SOC will schedule the scan start time per Client direction. All scans run until completion and may not be paused.

Phase 2 – Vulnerability Discovery and Processing

Sentinel360 scans network devices to identify potential vulnerabilities. Detection of vulnerabilities is based on specific scan settings among other factors. Information collected during this phase includes, but is not limited to, the following:

- Open / Closed Port detection
- Service type and version fingerprinting
- Service Interrogation for vulnerabilities
- Rudimentary Application Form / Variable Interrogation
- Operating System (OS) identification

Phase 3 – Scanning Results and Reporting

The Vulnerability Management service reports are delivered through the Security Portal and regular monthly reports. Scanning review and service delivery calls are performed with Client. Sentinel360 SOC support is available 24/7 for technical questions via email or telephone.

Sentinel360 SOC Support will be available to aid, investigate and troubleshoot scan issues, assist with access to the vulnerability management systems, starting and stopping scans and general vulnerability management service questions.

On Demand Scans

Client can request On-Demand scans, as well as the following conditions. The Client requesting On-Demand scans must submit an On-Demand scan request via the SOC at least 24 hours prior to the required start time. Requests must include an authorized scan window and be directed from an authorized employee within Client's organization.

Assumptions

Sentinel360 VMS Services has made the following specific assumptions while specifying the Service detailed in this Service Description:

- All information provided by Customer regarding site technical requirements and architecture is materially correct.

Exclusions

While the Service is intended to assist Customer to identify and reduce risk, it is impossible to completely eliminate risk, and Sentinel360 makes no guarantee that intrusions, compromises, or any

other unauthorized activity will not occur in the Customer IT environment. For the avoidance of doubt, the following activities are not included in the scope of this Service Description:

- Any services, tasks or activities other than those specifically noted in this Service Description.
- The Service does not include the development of any intellectual property created solely and specifically for the Customer.
- Troubleshooting or fixing any existing system/server problems unless otherwise described in this Service Description.
- Testing integration between a Sentinel360 VMS product and other third-party products, such as, but not limited to, third-party encryption or security products.
- Remediation or mitigation of any of the performance issues identified by the analysis of the Customer environment unless otherwise described in this Service Description.
- Sentinel360 VMS Services responsibility (including financial responsibility) for any Customer and/or third-party personnel, hardware, software, equipment or other assets currently utilized in the Customer's operating environment, unless otherwise set forth in this Service Description.
- Installation of the Endpoint Protection Software on Customer's on-site servers.
- Resolution of compatibility issues or other issues that cannot be resolved by the manufacturer or for configuring hardware, software, equipment, or assets in contradiction to the settings supported by the manufacturer.
- Purchase of software or software as a service licenses.

Offer-Specific Customer Responsibilities

Customer agrees to cooperate with Sentinel360 Services in its delivery of Sentinel360 VMS Services, and agrees to the following responsibilities:

- Customer must provide the Sentinel360 VMS Services technician access to all required environments for the period of delivery.
- Customer must be present or provide a Customer nominated representative who will be present and available for all planning and review sessions.
- Customer must participate as appropriate in the provision of the Sentinel360 VMS Service. Customer understands that without proper participation, including goal setting, Sentinel360 cannot work towards meeting Customer needs or perform the Service.
- Customer will cooperate with and follow the instructions given by Sentinel360 analysts.
- Review and agree to pre-engagement check lists and test plans.
- Ensure availability of sufficient network bandwidth and access to perform Service.
- Ensure all device integrations function and continue to function appropriately.
- Provide appropriate access to Sentinel360 for integrations as required for Sentinel360 Services.
- Ensure Customer security controls are compatible with Sentinel360 Integrations.
- Manage credentials and permissions for integrations with Sentinel360.
- Ensure list of Customer authorized contacts remains current, including permissions and associated information.
- Provide information and assistance (e.g., files, logs, IT environment context) promptly during investigations that Sentinel360 conducts for threats against Customer.

- Identify and authenticate all users Customer authorizes to use the Service.
- Control against unauthorized access by users, and maintain the confidentiality of usernames, passwords, and account information.
- Customer is responsible for all activities by the users it has authorized and will notify Sentinel360 immediately of any unauthorized use the Service.
- Use of two-factor authentication, where available, to access the Service.
- Accept all updates and upgrades to the VMS support systems necessary for the proper function and security of the Service.