Vulnerability Management

Service Overview

Vulnerability Management Services (referred herein as “VMS” or the “service”) delivers vulnerability assessments of Customer’s environment. VMS consists of automated and recurring vulnerability and compliance scanning.

VMS delivers vulnerability scanning and remediation data reporting of a Customer’s environment.

VMS provides unlimited scanning recurrence of Customer’s internal, external, and cloud-based live IP addresses. Scans of external IPs are conducted remotely. Scans of internal and cloud-based IPs are conducted from one or more ISO images placed on Customer’s network or in Customer’s leased virtual datacenter. IP level is based on Customer's technical scanning requirements.

Service Objectives: VMS service provides the customer with the following:

- Infrastructure scanning of the internal and external customer network infrastructure
- 24x7 Service support with online ticketing and alerting through the customer portal

Service Deliverables: VMS service will deliver to the customer the following:

- Agreed on list of IP addresses
- ISO image(s) for internal or cloud based IPs
- Customer portal access as well as ticketing system to view scan logs
- 24x7 SILVERSKY security support coverage

Service Description

Conduct scanning of the Customer infrastructure (for example servers, applications, network devices and end user devices) using a recognized industry vulnerability scanning tool , against the list of IP addresses as agreed, provided that those IP addresses are accessible from the Internet or through the supplied ISO image(s) and subject to the maximum numbers of IP addresses specified on the Order Form.

Scanning may be conducted as an ‘internal’ scan utilizing an ISO images within the Customer Network, as an ‘external’ scan utilizing a web based portal.

‘External’ scans can only be conducted on network assets and infrastructure with an internet-facing external IP address.

‘Internal’ scans can only be conducted on network assets and infrastructure that are accessible from the ISO images from its location within the Customer Network.

24x7 SOC Access

VMS Customers can contact SilverSky 24X7 via email or telephone. The Customer can use help desk calls for:

- Asking questions about the results of the Service, troubleshooting, or reviewing scan results, which will result in a ticket to the VMS SOC team.
- Changing contact information or rescheduling test dates and times.
- Solving issues associated with accessing the VMS service.
- Stopping scans during a network impacting event.

NOTE: Help desk calls cannot be used for general consulting advice that does not directly pertain to the results of the Service.

Vulnerability Reporting

We provide Customer with access to the Security Portal to view reports. Report capabilities are restricted to the capabilities of the platform and are Customer's responsibility to generate.

Additional scan report result information is as follows:

- Vulnerability reporting with a description of each vulnerability, level of severity, business and technical impact, remediation suggestions, and links to relevant sites
- Discovery reporting, detailing live hosts discovered on the network
- Vulnerability remediation data

Security portal

We provide Customer with access to the Security portal. The Security portal may only be accessed by the named individuals specified by Customer. All information received by Customer through the Security portal is solely for Customer's internal use and may not be re-distributed, resold, or otherwise transmitted outside of Customer's organization.

Profile Setup

We will assist Customer in selecting individual scan engine profiles as requested by Customer.

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:

<u>VMS Delivery</u>

The following procedures apply to the delivery of Vulnerability Management Services:

- Total IP quantities selected are limited to unique live IP instances and may not be rotated throughout the term of the contract for Customer accounts.
- Scan results and suggested remediation guidance are made available after the scan is completed.

Data Backups

The Customer acknowledges and agrees that the scanning of IP addresses and/or domain names may expose vulnerabilities and, in some circumstances, could result in the disruption of Services or corruption or loss of data. The Customer agrees that it is Customer's responsibility to perform regular backups of all data contained in or available through the devices connected to Customer's IP address and/or domain names.

Cloud-Based IP Address Acknowledgement

The Customer acknowledges that the IP address of cloud-based assets is subject to change. The Customer agrees that it is Customer's responsibility to identify the specific IP addresses of cloud-based assets that are to be scanned.

Third Party IP Addresses: Authority and Indemnification

Except as set forth herein, Customer may use the Services only to scan the IP Addresses owned by and registered to Customer, or for which Customer otherwise has the full right, power, and authority to consent to have the Services scan and/or map. Customer may not rent, lease, or loan the Services, or any part thereof, or permit third parties to benefit from the use or functionality of the Service via timesharing, service bureau arrangements or otherwise. In the event one (1) or more of the IP Addresses identified by Customer are associated with computer systems that are owned, managed, and/or hosted by a third party service provider ("Host"), Customer warrants that it has the consent and authorization from such Host(s) necessary for SilverSky to perform the Services. Customer agrees to facilitate any necessary communications and exchanges of information between SilverSky and Host.