Vulnerability & Cyber Risk Management Service ("Insight")

With over 20 years of experience and supporting hundreds of customers, SilverSky has developed an approach to protecting organizations from known network, system, and application vulnerabilities. SilverSky Insight takes the complexity out of detecting and prioritizing issues in your environment. Vulnerabilities, from software errors to improper configurations, pose a critical risk to businesses. Understanding what needs to be improved, in what order, and how quickly can significantly improve the effectiveness of a security team.

SilverSky has developed our vulnerability and cyber risk management service in partnership with CODA Intelligence, which addresses the challenges of identifying new vulnerabilities, prioritizing remediation based on corporate business impact, and gaining complete visibility into asset inventory.

Key Benefits

- Continuous autonomous security validation leads to zero overhead for managing scans, validating fixes, and reviewing alerts and reports on a daily basis.
- Automated translation of vulnerabilities to business risk by leveraging our contextual risk scoring system to establish your organization's true cyber risk exposure.
- Prioritization of the remediation plan using our unique Real Life Exploit Validation (RLEV) system based on Threat Intelligence.
- Complete attack surface visibility means complete visibility into your asset inventory and kill chain prediction across your organization.
- Automated compliance & risk reporting.
- Actionable remediations. Instant revalidation is one click away.
- 24x7 Service support with online ticketing and alerting through the customer portal.

Scope of Work

SilverSky Insight delivers:

- Vulnerability assessment of the customer's environment, consisting of automated and recurring vulnerability and compliance scanning.
- Remediation data reporting of the customer's environment. Note that the creation of a remediation plan, schedule, and actions to remediate vulnerabilities is the customer's responsibility.
- Continuous scanning of the 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 Virtual Scanners and/or Agents placed on the customer's network or in the customer's leased virtual data center. This scanning type is based on the customer's technical scanning requirements.

Service Deliverables:

- Agreed on the list of IP addresses.
- Virtual Machine image(s) for internal or cloud-based IPs.
- Customer portal access to view scan logs.
- 24x7 SilverSky security support coverage.

SERVICE IMPLEMENTATION

The onboarding process will be performed in three stages:

1. Service Orientation Call

Your assigned Project Coordinator will contact you to schedule a Service Orientation Call attended by the implementation team who will be assisting during deployment. The goals of the call will be:

- Introduce the SilverSky team members.
- Review any hardware, software, or connectivity requirements for the service.
- Review customer infrastructure to be scanned, including IP ranges.
- Discuss notification and escalation procedures and customer points of contact.

2. Installation Call

After your Service Orientation Call, the implementation team will work with you to install the service:

- Provide the list of IPs to be scanned.
- Provide the list of approved Users of the service.
- Customer to validate the whitelisting of the SilverSky service IPs.
- Install a scanner (if scanning the internal IPs) and/or Agents.
- Test and validate toolset connectivity.
- Set initial configurations and provide an overview of the reporting console.
- Discuss a timeline for initial scans to avoid potential downtime.

3. Service Onboarding

After your Installation Call has been performed, the implementation team will work with you to:

- Run the first scan.
- Ensure reports are available for download.
- Train the customer on the use of the portal.
- Verify the customer has the tools and training to set up new and scheduled scans.

Note that SilverSky defines a completed Insight service deployment as the date when the following steps have been completed:

(1) Customer knows how to deploy scanner(s) and configure scan targets.
(2) Customer is trained on viewing and using reports in the Insight Customer Portal.

Any changes requested after that date will be managed through our service operations, customer portal service tickets or customer support team.

Service Features:

SilverSky Insight provides clients with the following deliverables:

Service	Deliverable
Scanning the customer infrastructure	Conduct scanning of the customer infrastructure (for example, servers, 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 Virtual Scanners or Agents within the customer's network, as an 'Internal 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 accessible from the virtual machines located within the customer network.
24x7 SOC Access	Customers can contact SilverSky 24X7 via email or telephone. The customer can use help desk calls for: • Asking questions about technical issues with the scanner operation or troubleshooting will result in a ticket to the SOC team. • Change contact information or reschedule scan dates and times. • Solving issues associated with accessing the Insight 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 Service results.
Vulnerability Reporting	SilverSky provides access to the Insight Portal to view reports. Report capabilities are restricted to the platform's capabilities and are the customer's responsibility to generate. Additional scan report result information is as follows: • Vulnerability reporting with a description of each vulnerability, level of severity, remediation suggestions, and links to relevant sites • Discovery reporting, detailing live hosts discovered on the network • Vulnerability remediation data

Security Portal	SilverSky provides access to a portal for the service. The Insight portal may only be accessed by the named individuals specified by the customer. All information received by the customer through the Insight portal is solely for the customer's internal use and may not be re-distributed, resold, or otherwise transmitted outside of the customer's organization.
Profile Setup	SilverSky will assist the customer in selecting individual scan engine profiles as requested by the customer.

Customer Responsibilities

The effective delivery of the SilverSky Insight service requires a collaboration between the Customer and SilverSky team. Below outlines both sets of responsibilities, recognizing that SilverSky's ability to deliver the service is dependent upon the Customer's compliance with these steps:

SilverSky Insight Procedures

The following procedures apply to the delivery of the SilverSky Insight services:

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

Data Backups

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

Cloud-Based IP Address Acknowledgement

The customer acknowledges that the IP addresses of cloud-based assets are subject to change and agrees that it is the 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, the customer may use the Services only to scan the IP Addresses owned by and registered to the customer or for which the customer otherwise has the full right, power, and authority to consent to have the Services scan and/or map. The 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 the customer are associated with computer systems that are owned, managed, and/or hosted by a third-party service provider ("Host"), the customer warrants that it has the consent and authorization from such Host(s) necessary for SilverSky to perform the Services. The customer agrees to facilitate any necessary communications and exchanges of information between SilverSky and the Host.

Service Definition

Service Feature	Description	Benefit
Internal and external vulnerability scanning	Continuous scanning of the customer's internal, external, and cloud-based live IP addresses.	Consistent, predictable program to test for known vulnerabilities of systems, networks, and applications
24x7 Support	SilverSky provides email and telephone support for the service to report issues with scan completion or troubleshooting	Support to guide the customer to ensure they understand how to perform the scans and interpret the results
Reporting Portal	SilverSky provides a reporting portal, restricted to a list of approved users, to view reports and plan remediation steps. Reports include a description of each vulnerability, level of severity, remediation suggestions, and links to relevant sites	Reporting to show current vulnerability status, list of live hosts on the network, and remediation data

RACI Matrix

Roles and Responsibilities are used to assign the level of task responsibility for various components of the SilverSky services:

Responsible	The person who is responsible for doing the work
Accountable	The person who is ultimately accountable for the process or task being completed properly
Consulted	People who are not directly involved with carrying out the task but who are informed
Informed	Those who receive output from the process or task or need to stay in the know

Task ownership for the SilverSky Insight service:

Activity	SilverSky	customer
PLATFORM		
Solution evaluation	A	CIR
Provide a list of IP addresses to be scanned, blackout windows	IC	RA
Participation in kickoff and ongoing meetings	AC	IR
Technical customer resource to assist with implementation & testing	IC	RA
Pre-launch Setup of the Platform	RA	IC
Initial User Access Configuration	RA	IC
Deployment of the solution and Initial scan	IC	RA
Validation of results: Initial scan flowing into the reporting platform	RA	IC
Management of the platform	RA	IC
VULNERABILITY SCANNING		
Installation of virtual vulnerability scanner/agent (internal scans)	ACI	R
Validation that the agent follows the scanner requirements	CI	RA
Configuration of vulnerability scanner/agent	RA	CI
Maintenance of vulnerability scanner/agent	RA	I
Review of automated scanning schedule	CI	RA
Technical validation of scan results	CI	RA
Tracking of new, remediated, and persistent vulnerabilities	RA	CI
Return results and notification of risks and vulnerabilities to the customer	RA	CI
Setup email notifications	IC	RA
Ongoing Monitoring of Vulnerabilities, Risks, Alerts, User Activity	IC	RA
Validate remediation effect on fixing/reducing the risk, providing business risk scoring to the customer	RA	IC
Continuous review of scanning logs	IC	RA
Create and manage remediation plans	IC	RA
Develop a remediation schedule	IC	RA
Implement remediations	IC	RA
IP inventory (classification of assets)	IC	RA
Provide 24x7 support of the platform and manage ongoing support issues	RA	IC