SERVICE ORDER ATTACHMENT
STATEMENT OF WORK

S-200-3043 CONTINUOUS INTERNAL VALIDATION SERVICES (ADVANCED)

1 Overview

This Statement of Work ("SOW"), with any appendices included by reference, is part of any agreement which incorporates this document by reference.

1.1 SilverSky Continuous Internal Validation Services

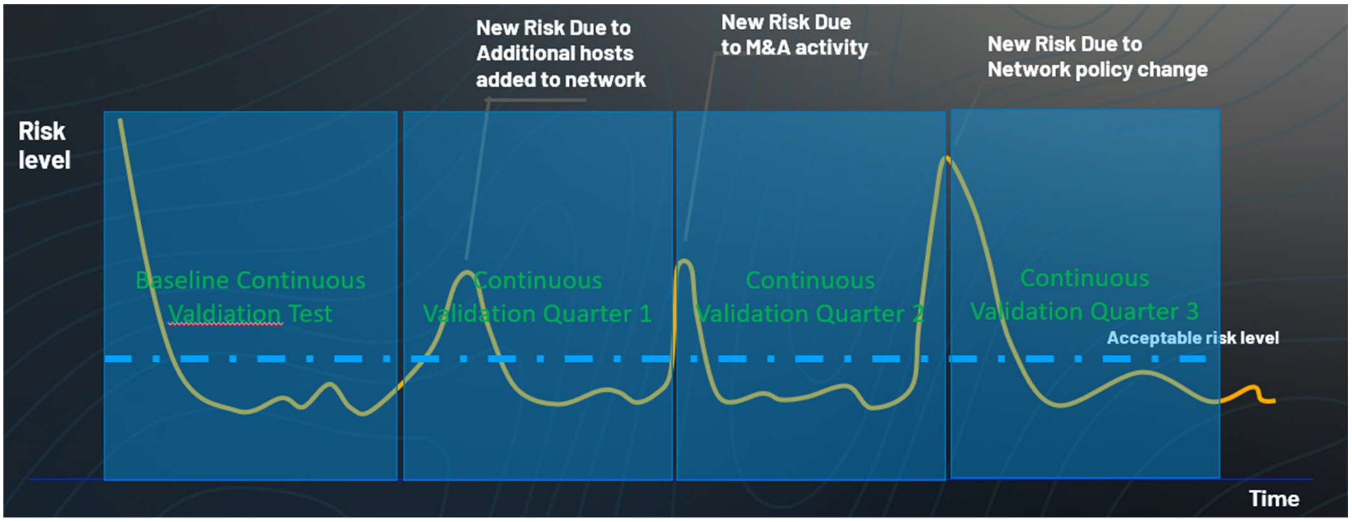
Companies are investing significant resources to build and improve their cybersecurity posture in efforts to keep up with their continuously evolving threat landscape.

Each one of these security systems has a probability of human error and misconfiguration. Every application or operating system introduces vulnerabilities as it evolves. As IT networks grow and expand, the probability for misconfigurations of controls and vulnerabilities increases, as does their operational complexity. While these preventive and detective controls are important, validation of these controls is becoming an indispensable part of an organizations cyber strategy.

While penetration testing has proven to become a critical part to most cyber programs, its expensive, talent dependent and as a result is usually limited in time, scope and frequency. With these constraints, pen-tests are typically only performed once a year on a small segment of the infrastructure deemed most business-critical, leaving most of the attack surface unvalidated.

In today's environment with rapidly changing threat profiles and dynamically changing networks, one time testing is simply not enough anymore. The move to SilverSky's continuous validation service will solve this problem by providing more frequent views into your evolving threat landscape and provide continuous remediation guidance to help keep your risk at an acceptable level.

Figure 1. Lifecycle of a continuous validation assessment showing risk spikes due to environment changes and how continuous validation assessments help keep risk to an acceptable level.



1.2 Service Summary

SilverSky's continuous internal validation service allows organizations to harness efficiencies and knowledge of your environment to empower our seasoned penetration testers to perform traditional ethical hacker penetration testing at scale with no need for agent installation. Armed with only network access SilverSky is able to perform every action a hacker would on a continuous service basis including — scanning, reconnaissance, sniffing, spoofing, cracking, (harmless) malware injection, file-less exploitation, post-exploitation, lateral movement and privilege exploitation all the way to data exfiltration. Our objective is to seek out and identify vulnerabilities correlated with exploits that are lacking a compensating control. Once identified, we then attempt to exploit these weaknesses, at scale, without malicious intent or harm to your network.

Along with oversight from the SilverSky Cyber Advisory Penetration testing team, we are able to provide a consistent means of challenging your security from a hacker's perspective, covering all areas of your network and delivering a cost effective service on a more frequent monthly or quarterly basis.

Your dedicated SilverSky Cyber Service advisor penetration tester overlays to the service to perform testing, oversee delivery, provide insight into the results and provide strategic recommendations to enhance your internal security posture.

Project Deliverables:

- Comprehensive Quarterly Internal Findings Report

1.3 Service Summary

SilverSky will undertake the following primary tasks, subject to modification or extension based on the investigation findings.

1. Kick-off Meeting
2. Performance of Quarterly Internal Continuous Validation Reviews
3. Strategic Quarterly Review Meetings

2 Scope

2.1 SilverSky Obligations:

Kick-off Meeting - Meet to discuss and agree on customer goals and the rules of engagement for the services. This includes project scoping, the timeframe for testing, the extent to which system exploits can be performed, and procedures to follow should any issues occur during the testing. Any additional precautions or provisions are also considered before testing.

Performance of Quarterly Continuous Validation Reviews – SilverSky will deploy and manage the service on the customer's internal and external network and provide continuous validation assessment of the customers internal attack surface.

- Work with customer to determine scope of testing and quarterly review schedule
- Review of Internal network architecture to determine appropriate performance of validation service
- Determine any custom rules of engagement with Customer
- Perform continuous threat landscape validation of customer's internal network
- Perform full scale baseline penetration testing across all network segments determined to be in scope
- Perform quarterly assessments to validate remediation and discover any new weaknesses or attack vectors
- Validate security control efficacy against the MITRE ATT&CK framework.

Service Review Meetings – SilverSky's Cyber Security Advisors oversee the service delivery and meet with the customer on a continuous basis to provide strategic recommendations as a dedicate penetration testing team resource to include:

- Validating exercises using the same tactics and techniques utilized by adversaries
- Make recommendation to improve security posture and validate the removal of prior findings
- Prioritize remediation recommendations based on true risk and potential impact, rather than CVSS ranking alone to accelerate efficient remediation
- Gain visibility through continuous internal assessments to uncover the customer exploitable attack surface, identify possible impact and realize the optimal path for exposure remediation.

2.2 Reporting

SilverSky will provide a comprehensive initial baseline report and subsequent quarterly assessment reports at the end of each quarterly cycle. SilverSky will review with the customer, help develop a remediation priority plan and identify if there are any attack surface findings that need attention. The reports will consist of the following reports:

Continuous Validation Detailed Findings - The detailed findings section describes the assessment results in detail. It is intended for management, administrators and other operations personnel and includes:

- Quarterly comparison metrics showing risk reduction per quarter
- An itemized listing of individual vulnerabilities
- A description of each vulnerability
- The severity of the threat likely posed by each vulnerability
- Potentially affected resources
- Prioritized recommendations for remediation

2.3 Out of Scope

Any activity not explicitly included in this SOW is considered out of scope. In the event that Customer requests additional services, such services will be the subject of a change request.

3 Customer Obligations and Assumptions

Services, fees and work schedule are based upon the assumptions, representations and information supplied by Customer. Customer's fulfilment of these responsibilities is critical to the success of the engagement.

3.1 Customer Obligations

- **Service Deployment –** Customer will make available resources to assist with the initial installation/connectivity of the service and ongoing connectivity for each quarterly assessment for SilverSky to provide services.
- **Computing Resource –** Customer will provide access to a dedicated VM or SilverSky scanning machine that has access to the in scope network resources to run services
- **Attendance –** Customer will be required to attend the quarterly service review meetings and provide assistance each quarter for activation of the quarterly validation runs
- **Project Liaison** - Designate an authorized representative to authorize completion of key project phases, assign resources and serve as project liaison.
- **Access** - Ensure SilverSky consultants have access to key personnel and data requested.

- **Resources** - Furnish SilverSky with Customer personnel, facilities, resources and information and perform tasks promptly.
- **Cooperation** - Ensure all of Customer's employees and contractors cooperate fully with SilverSky and in a timely manner. SilverSky will advise Customer if increased Customer participation is required in order for SilverSky to perform the Service under this SOW.
- **Documentation** – Deliver in a timely fashion all documentation requested by SilverSky including Customer's security policies, network diagrams, server listings, and procedures.

3.2 SILVERSKY Assumptions

- Customer will provide SilverSky with reasonably requested information upon which SilverSky can rely to be current, accurate, and complete.
- Customer will provide access to Customer personnel who have detailed knowledge of Customer security architecture, network architecture, computing environment, and related matters.
- Customer will provide access to Customer personnel who have an understanding of Customer's security policies, regulations and requirements.
- Customer will evaluate SilverSky deliverables and immediately notify SilverSky of any perceived problems or issues with SilverSky obligations.
- SilverSky will immediately notify Customer of any perceived problems or issues regarding Customer obligations.
- Customer is responsible for any additional costs if SilverSky is unable to perform the Service due to Customer's delay or other failure to fulfill its obligations under this Statement of work.

4. PROJECT PARAMETERS

4.1. Project Scope

The scope of the project is based on the above description with the additional details listed as follows:

Project Component	Parameter(s)
Project Start Date	SilverSky will reach out within 30 days of the Effective Date with a date for a kickoff call.
Project Duration	Services will be performed quarterly for the term of the contract including 1 baseline assessment and 3 quarterly runs for a total of 4 assessments per year.
Project Scope Exclusions	Exclusions – External and Web Application Testing unless contracted under a separate agreement
Project Scope Tier 1	Project is limited up to 50 devices. Not to exceed 35 hours of testing and documentation time per quarter.
Project Scope Tier 2	Project is limited up to 250 devices. Not to exceed 40 hours of testing and documentation time per quarter.
Project Scope Tier 3	Project is limited up to 500 devices. Not to exceed 40 hours of testing and documentation time per quarter.
Project Scope Tier 4	Project is limited up to 1000 devices. Not to exceed 45 hours of testing and documentation time per quarter.

4.2. Location and Travel Reimbursement

The Service defined in this SOW does not require onsite participation by SilverSky staff at Customer location(s).

4.3. Acceptance

Delivery of all stated project deliverables will constitute acceptance of services provided under this SOW.