SERVICE ORDER ATTACHMENT
STATEMENT OF WORK

S-200-3192 CONTINUOUS VALIDATION SERVICES

1 Overview

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

1.1 SilverSky Continuous Validation Services

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

Each of these security systems is susceptible to human error and misconfiguration. Every application or operating system evolves and introduces vulnerabilities. As IT networks grow and expand, the probability of misconfiguring 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 organization's cyber strategy.

While penetration testing has proven to be a critical part of most cyber programs, it is expensive, talent-dependent, and 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 not enough. The move to SilverSky's Continuous Validation service will solve this problem by providing more frequent views into your evolving threat landscape and continuous remediation guidance to help keep your risk at an acceptable level.

1.2 Service Summary

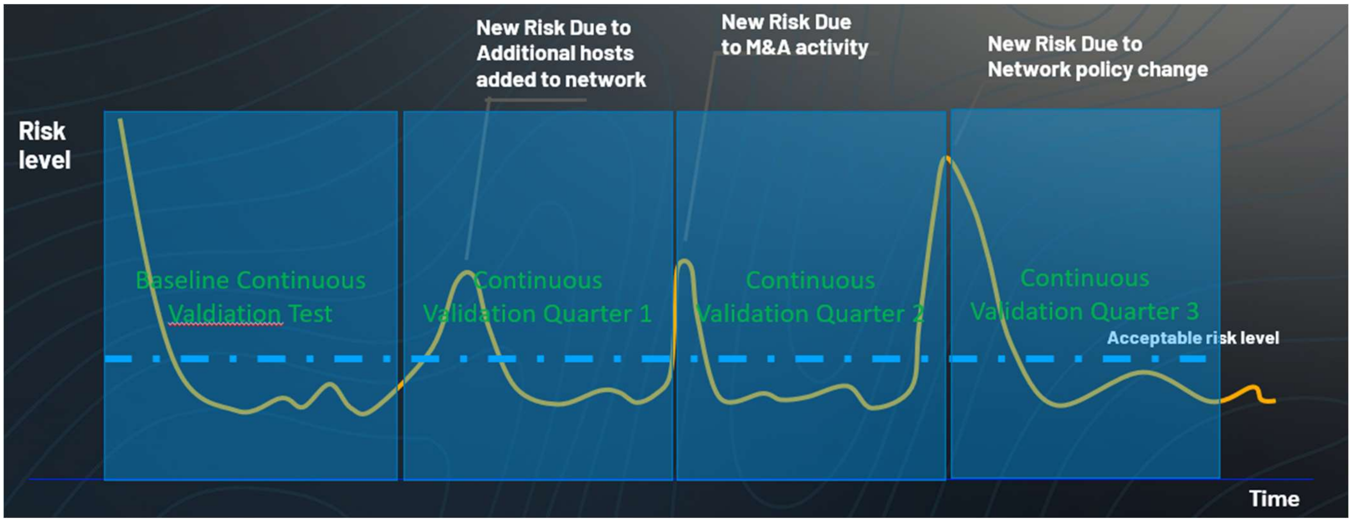
SilverSky's Continuous Validation service allows organizations to harness efficiencies and knowledge of your environment to empower our seasoned penetration testers to perform traditional ethical hacker penetration testing at scale without needing agent installation. Armed with only network access, SilverSky can 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 lack compensating controls. Once identified, we attempt to exploit these weaknesses at scale without malicious intent or harming your network.

Our penetration testing team are able to consistently challenge your security from a hacker's perspective, covering all areas of your network and delivering a cost-effective service on a more frequent basis.

Your penetration tester performs testing, oversees delivery, provides insight into the results, and provides strategic recommendations to enhance your internal security posture.

Services are performed during four quarterly testing cycles throughout the year. Each cycle consists of a new Continuous Validation test, a brief consultation meeting with your assigned penetration tester to discuss findings, and a remediation period reserved for you to review and resolve any identified issues. At the start of the next cycle's testing, we perform validation testing to ensure all findings were remediated successfully and perform new testing to identify any issues that may have appeared due to changes in your environment or new attack patterns.

Figure 1. The lifecycle of a continuous validation assessment shows risk spikes due to environmental changes and shows how continuous validation assessments help keep risk to an acceptable level.



The figure above depicts the 4 cycles of testing as new risks are introduced and our ability to reduce your risk back down to acceptable levels.

Project Deliverables:

- Comprehensive Quarterly Internal Findings Report
- Dashboard of findings and trends that your penetration tester will review in their quarterly engagements

1.3 Service Summary

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

1. Kick-off Meeting
2. Assess the performance of quarterly Continuous Validation reviews
3. Hold strategic quarterly review meetings

2 Scope

2.1 SilverSky Obligations:

Kick-off Meeting—This is a meeting to discuss and agree on the 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.

Assess the performance of quarterly Continuous Validation reviews - SilverSky will deploy and manage the service on the Customer's internal and external network and provide a Continuous Validation assessment of the Customer's internal attack surface.

- Work with the Customer to determine the scope of testing and quarterly review schedule
- Review of network architecture to determine the appropriate performance of validation service

- Determine any custom rules of engagement with the Customer
- Perform continuous threat landscape validation of the Customer's 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.

Hold strategic quarterly review meetings– SilverSky's penetration testers oversee the service delivery and meet with the Customer quarterly to provide strategic recommendations as a dedicated penetration testing team resource to include:

- Validating exercises using the same tactics and techniques utilized by adversaries
- Make recommendations to improve security posture and validate the removal of prior findings
- Prioritize remediation recommendations based on actual risk and potential impact rather than CVSS ranking alone to accelerate efficient remediation
- Gain visibility through continuous internal assessments to uncover the Customer's exploitable attack surface, identify possible impacts, 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 any attack surface findings need attention. The reports will consist of the following:

Continuous Validation Detailed Findings - The detailed findings section describes the assessment results. 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. If the Customer requests additional services, such services will be subject to a change request.

3 Customer Obligations and Assumptions

Services, fees, and work schedules are based on the assumptions, representations, and information supplied by the Customer. The Customer's fulfillment of these responsibilities is critical to the engagement's success.

3.1 Customer Obligations

- **Service Deployment**—The Customer will make available resources to assist with the initial installation/connectivity of the service and ongoing connectivity for each quarterly assessment so that SilverSky can 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 the completion of key project phases, assign resources, and serve as project liaison.
- **Access** - Ensure SilverSky consultants can access key personnel and requested data.
- **Resources** - Furnish SilverSky with Customer personnel, facilities, resources, and information, and perform tasks promptly.
- **Cooperation**—Ensure all of the Customer's employees and contractors cooperate fully and in a timely manner with SilverSky. SilverSky will advise the Customer if increased Customer participation is required 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 with detailed knowledge of Customer security architecture, network architecture, computing environment, and related matters.
- Customer will provide access to personnel who understand the 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 the Customer of any perceived problems or issues regarding Customer obligations.
- Customer is responsible for additional costs if SilverSky cannot perform the Service due to Customer's delay or 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 contract term, including 4 testing cycles per year.
Project Scope Exclusions	Exclusions – External and Web Application Testing unless contracted under a separate agreement
Project Scope	Project is limited to the device counts contracted. Internal and external IP addresses will be combined to provide the total number of in-scope devices.

4.2. Location and Travel Reimbursement

The Service defined in this SOW does not require SilverSky staff to participate on-site at the Customer's location(s).

4.3. Acceptance

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