SERVICE ORDER ATTACHMENT
STATEMENT OF WORK

S-266-2721 VULNERABILITY ASSESSMENT

Service Overview

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

Our Vulnerability Assessment ("VA") service provides essential security scanning capabilities for organizations requiring systematic identification of network-based vulnerabilities and Misconfigurations. This service can be conducted against both internal and external infrastructure environments to meet specific compliance and/or risk management requirements.

Nessus Professional powers our service and follows a structured approach for broad vulnerability coverage using known signatures and heuristics.

Service Methodology

Our approach focuses on comprehensive automated scanning with expert validation and false positive elimination.

Network Discovery & Port Enumeration

- Systematic scanning (Nmap) across all in-scope targets to identify active services and open ports
- Service version detection and operating system fingerprinting to establish an accurate asset inventory
- Identification of non-standard ports and services that may indicate security risks

Automated Vulnerability Scanning

- Comprehensive vulnerability scanning using Nessus Professional against all discovered services
- Systematic identification of known vulnerabilities, misconfigurations, and security weaknesses
- Coverage of operating system vulnerabilities, application flaws, and service-specific issues
- Detection of missing security patches and outdated software versions (where applicable)
- Assessment of SSL/TLS configurations, certificate validity, and cryptographic implementations

Expert Validation & False Positive Elimination

- Manual review and validation of all identified vulnerabilities to eliminate false positives
- Contextual analysis to determine actual exploitability and business impact

Service Deliverables

SilverSky will provide an automated report composed of an executive summary and a detailed findings section. The Customer will have an opportunity to review drafts of the report.

Executive Summary - This section summarizes the results of the assessment. It is intended for upper management and boards of directors and includes;

- Overview of assessment results
- CVSS risk ratings for each area reviewed during the assessment
- Key findings

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

- An itemized listing of individual vulnerabilities
- A description of each vulnerability
- The severity of the threat likely posed by each vulnerability
- Potentially affected resources
- Recommendations for remediation

Scope

SilverSky Obligations:

Scope Gathering Phase - Meet with key Customer staff to understand the environment and capture and confirm the “in-scope” IP range before project kick-off.

Security Testing Phase - Perform vulnerability scans using tools that are continually updated and contain checks for known vulnerabilities and exploits

Analysis of Findings Phase - SilverSky will compile and analyze data generated by the assessment tools and categorize vulnerabilities by severity based on their potential impact on the affected network. This analysis is the basis for recommendations to potentially address risks associated with identified vulnerabilities.

Scope Exclusions:

Any activity not explicitly included in this SOW is considered out of scope. In the event that the

Customer requests additional services; such services will be the subject of a change request.

- The engagement is solely limited to the agreed-upon scope.
- Any activity not explicitly included in this SOW is considered out of scope.

Customer Obligations

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 success of the engagement. The Customer will provide, as required;

- **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 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 the Customer's employees and contractors cooperate fully with SilverSky and in a timely manner. SilverSky will advise the Customer if increased Customer participation is required in order for SilverSky to perform the Service under this SOW.

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's personnel who have detailed knowledge of Customer's security architecture, network architecture, computing environment, and related matters.
- Customer will provide access to Customer's personnel who understand Customer's security policies, regulations, and requirements.
- Customer will evaluate SilverSky deliverables and immediately notify SilverSky of any perceived problems or issues with SilverSky's obligations.
- SilverSky will immediately notify the Customer of any perceived problems or issues regarding the Customer's obligation.
- 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.

Project Parameters

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

Project Component	**Parameter(s)**
Project Start Date	Typically, within 30 days of the Effective Date
Project Duration	Approximately 1 week, subject to project variables
S-266-2721 Internal Vulnerability Assessment	Up to 200 IP addresses in scope.
S-266-2721 Internal Vulnerability Assessment	Up to 500 IP addresses in scope.
S-266-2721 EXTERNAL Vulnerability Assessment	Up to 100 public IP addresses
S-266-2721 EXTERNAL Vulnerability Assessment	Up to 300 public IP addresses

Location and Travel Reimbursement

The Service defined in this SOW is delivered entirely remotely.

Acceptance

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