SERVICE ORDER ATTACHMENT STATEMENT
OF WORK

S-266-2431 EXTERNAL INFRASTRUCTURE ASSESSMENT

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 Service Summary

In today's interconnected digital landscape, organizations' external-facing infrastructure represents an accessible attack surface for potential threat actors. Our External Infrastructure Assessment service provides a comprehensive evaluation of the underlying infrastructure hosting your publicly accessible systems, services, and applications.

We employ a methodical approach that combines automated scanning, manual testing techniques, and an adversarial mindset to identify vulnerabilities, misconfigurations, and security weaknesses that malicious actors could exploit to gain unauthorized access to your systems and data.

2 Scoping Information

This service aims to assess and identify the threat landscape and applicable attack vectors against your organization's external perimeter, specifically the underlying infrastructure. We can conduct this assessment in two different styles, each with its own pros and cons:

Privileged Internet Source: This modifier is intended to assess the entire underlying infrastructure, not just what is exposed. You will allow-list our public IP addresses so we can see past firewalls, WAFs, and similar protective measures. This provides a more comprehensive view of vulnerabilities that could be exploited if perimeter defenses are bypassed.

Unprivileged Internet Source: This modifier assesses what is publicly exposed to the 'typical' Internet-based source. No modifications to your infrastructure are necessary. This provides a realistic view of what an actual attacker would see from the open internet.

Scope Requirements

To be able to scope and deliver the External Infrastructure Assessment, we require the following information:

- Total number of in-scope Public IP addresses
- Estimate of publicly accessible services
- Useful contextual information for the consultant
- Out of scope requirements

3 Assessment Requirements

Credentials: This service is unauthenticated by default and does not require privileges. Skip this step if it does not apply.

Network Configurations: This service can be conducted from either an unprivileged or privileged Internet source. Ensure that you have completed the relevant action.

Unprivileged Internet Source – ensure that SilverSky's Pentest public IPs are not allow-listed.

Privileged Internet Source – ensure that SilverSky's Pentest public IPs are allow-listed in your perimeter controls.

Communications: Inform your chosen support lead about the engagement. Ensure they are aware of their role in aiding and are available for the duration of the engagement. Inform any necessary third parties and/or departments about the engagement, especially if authorization is required.

4 Testing Methodology

Our External Infrastructure Assessment follows a structured and comprehensive approach combining automated tools with expert manual analysis:

Information Gathering and Enumeration:

- Systematic port scanning across all in-scope targets to map exposed services
- Detailed service fingerprinting to identify versions and technologies
- Comprehensive vulnerability scanning using enterprise-grade tools
- Precise CVE identification and impact assessment
- Detection of inadvertently exposed sensitive information
- Targeted OSINT research on user accounts, including breach analysis and credential exposure
- Cloud infrastructure usage mapping

Blended Expert Analysis:

- Thorough review of enumeration data to identify viable attack vectors
- Controlled password testing within defined parameters to prevent service disruption (if in scope)
- Targeted manual testing of vulnerable services to validate exploitability
- Collection of evidence and proof-of-concept demonstrations for verified vulnerabilities
- Exploitation path analysis to determine potential impact on critical assets

Strategic Recommendations

- Security findings prioritized by risk level and exploitation potential using an Impact x Likelihood = Risk model and/or CVSS version 4. and/or CVSS version 4
- Actionable and tailored remediation guidance from experienced cloud security specialists
- Comprehensive reporting with clear visualization of your security posture

5 Project Deliverables

At the conclusion of the assessment, SilverSky will provide a comprehensive report composed of an executive summary and a detailed findings section. The Customer will have the opportunity to review draft versions of the report, and SilverSky will deliver the final version following a joint review with the Customer.

Executive Summary - This section summarizes the results of the assessment. It is intended for upper management and the Board of Directors and includes:

- Overview of assessment results
- Itemization of the risk ratings for each area reviewed during the assessment
- Key findings and recommendations

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

5.1 Out of Scope

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.

6 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 success of the engagement.

6.1 Customer Obligations

- **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.
- **Documentation** – Deliver in a timely fashion all documentation requested by SilverSky, including the Customer's security policies, network diagrams, server listings, and procedures.

6.2 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's obligations.
- SilverSky will immediately notify the 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.

7 PROJECT PARAMETERS

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	Typically, within 30 days of the Effective Date
Project Duration	Approximately 1-3 weeks, subject to project variables
Project Scope Exclusions	Internal and Web Application Testing, unless contracted under a separate agreement
S-266-2431 External Infrastructure Assessment	Up to 100 IP addresses in scope. Work hours not to exceed 40
S-266-2431 External Infrastructure Assessment	Up to 200 IP addresses in scope. Work hours not to exceed 60
S-266-2431 External Infrastructure Assessment	Up to 300 IP addresses in scope. Work hours not to exceed 80

7.1 Location and Travel Reimbursement

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

7.2 Acceptance

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