# 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 Service Summary

The purpose of Internal Penetration Testing (the "**Service**") is to identify the feasibility of an attack and to determine the extent of the impact of the successful exploitation of internal systems against one or more realistic objectives in an assumed breach scenario. The testing will employ intrusion analysis and testing methodologies to test the vulnerability of specific Customer assets to malicious activities. The process will mimic typical attacker techniques, including actual attempts to exploit identified vulnerabilities from a foothold within the network. SilverSky consultants will meet with key members of the Customer's staff to determine the scope and 'rules of engagement' for performing the testing. This includes clarifying or determining specific aspects such as the objective and target(s) of the test, notification requirements, and the timing of testing. The Customer will provide SilverSky with initial access to the internal network to simulate an assumed breach scenario as part of this assessment.

**Project Deliverables:**

Comprehensive Report is structured as follows:

An executive summary outlining at a business level the review conducted, the key issues found and the business impact of any vulnerabilities discovered

Narrative descriptions of the scope and approach of the testing done

Assessment information including the environment description, narrative, key findings (including severity, description, affected hosts, recommendation, references and evidence)

## 1.2 Phases of Penetration Testing

Phases of penetration testing activities include the following:

- Planning – Customer goals and rules of engagement (RoE) obtained
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities and exploits
- Attack – Confirm potential vulnerabilities through exploitation and perform further enumeration
- Reporting – Document all found vulnerabilities and exploits, failed attempts and company strengths

## 1.3 Project Summary

SilverSky will provide the following primary tasks, subject to modification or extension based on the engagement:

1. Kick-off Meeting
2. Reconnaissance (Passive / Active)

3. Scanning and Enumeration
4. Exploitation and Vulnerability Validation
5. Analysis of Findings
6. Draft Report and meeting on Initial Findings
7. Comprehensive Report

# 2 Scope

## 2.1 SilverSky Obligations:

**Kick-off Meeting** – Meet to discuss and agree on customer goals and the rules of engagement for the project. This includes project scoping (determining the target systems to be included in the testing), testing style (white box, black box or grey box testing), 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.

**Objective-setting** - SilverSky will propose a number of objectives according to Customer's size, industry vertical, and potential adversaries in the threat landscape. The Customer may accept SilverSky' proposed objectives or may request alternative objectives. SilverSky will accept alternative objectives that SilverSky considers reasonable. Additional fees and a Change Order may be required if the proposed alternative objectives materially impact the scope of the engagement.

**Primary Objectives** - These objectives are the critical success factors for the goal-based penetration test. If these objectives are completed, the test is considered a success.
**Secondary Objectives** - These objectives are considered 'stretch goals' to be attempted once the primary objectives are completed. SilverSky will pursue secondary objectives SilverSky considers reasonably possible in the time allocated for the project, not to exceed the limits stated in the applicable tier below.

The Primary and Secondary Objectives defined will be assessed by SilverSky to ensure they are 'SMART' (Specific, Measurable, Achievable, Reasonable, Time-Bound) prior to the parties' agreement on the objectives to be completed under this SOW. Two examples of potential objectives are:

**Domain Admin** - With credentialed access to the Customer network, elevate privileges to the point where the SilverSky testing team has access to or control of an account in the 'Domain Admins' group on Active Directory in the Customer domain before the end date of the test.
**Email Access** - With credentialed access to the Customer network, gain access to the mailbox of USER@CUSTOMER.COM and send an email to the project liaison before the end of the test.

In some cases, the Customer may be required to make minor changes to its environment to allow the test to be conducted without disruption to the Customer's operations. For example, if the Customer chooses the 'Email Access' objective, SilverSky recommends creating and properly provisioning a new mailbox for the duration of the test, rather than using an actual employee mailbox. SilverSky may use both manual and automated toolsets as part of this assessment which may require changes to the customer environment as part of the setup and configuration of the toolsets.

**Security Testing Phase** - Steps taken may include:

**A) Information Gathering & Reconnaissance**
SilverSky may gather information about the target for potential use in later phases or for attack positioning. This

might include personal information (for phishing and social engineering), technical information (for exploitation and vulnerability identification), and/or physical information (for physical intrusion). Information gathered during this phase will support the testing and will be included in the report to the extent that SilverSky believes it is pertinent to the narrative. (This phase is not a replacement for a full open-source intelligence assessment.)

**B) Scanning and Enumeration**

With an initial foothold on the network, SilverSky will perform scanning and enumeration to identify potential vulnerabilities and attack vectors in an effort to move laterally through the network and identify potential opportunities for privilege escalation. This could involve identifying unpatched software or systems, weak security controls or misconfigurations,

**C) Attack Execution, Network Traversal & Escalation**

Following the Scanning and Enumeration phase, SilverSky conducts initial actions to traverse the Customer's network and exploit vulnerabilities on the target (both technical and non-technical) within the boundaries of the scope previously agreed upon by the parties. Lateral and vertical movement takes place within Customer's network to locate key systems and escalate access and privilege levels. Persistence via multiple routes into and out of the network may be established.

**D) Actions on Target & Data Exfiltration**

Agreed-upon actions are executed once the key targets have been located. Such actions may include: (i) compromise of assets; (ii) interception of key information; or (iii) network positioning to allow for disruption, degradation, or destruction, alongside exfiltration of any target data or assets.

It may become necessary at various points during the Security Testing phase to simulate certain activities to avoid business disruption or to keep within timescales. For example, if SilverSky identifies encrypted data it estimates could be decrypted in a reasonable time, SilverSky may ask the Customer to decrypt the data.

If SilverSky identifies a significant issue during the test, SilverSky will stop to identify the issue and its potential outcome. For example, should SilverSky detect a vulnerability that provides the ability to gain access to a host, application, or service, the Customer will be given the choice of the potential outcome based upon SilverSky leveraging the exploit or the Customer providing the same level of access without exploitation.

**E) Analysis of Findings Phase**

SilverSky will compile and analyze the data generated from the testing. Then SilverSky will categorize findings by severity - based on the potential impact each can have. This analysis is the basis for recommendations to potentially address risks associated with the findings.

## 2.2 Reporting

At the conclusion of the assessment, SilverSky will provide a comprehensive report. The report will include three main sections: (i) an executive summary, (ii) a narrative, and (iii) a detailed findings section. The Customer will have an opportunity to review drafts of the report and SilverSky will deliver a final version after a joint review with the Customer.

**Executive Summary** - The executive summary summarizes the results of the assessment. It is intended for upper management and boards of directors and includes:

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

**Narrative** - The narrative details the major events and findings discovered during testing. It is interspersed with technical detail and analysis.

**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

### 2.3 Out of Scope

Any activity not explicitly stated in this SOW is considered out of scope. In particular, the Service does not include any testing of the Customer's external (public-facing) assets and does not include a comprehensive vulnerability assessment. If the Customer requests additional services, such services will be the subject of a change request or additional SOWs, depending on the nature of the Customer's requests.

## 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 the obligations listed below is critical to the success of the engagement.

### 3.1 Customer Obligations

**Project Liaison** - Designate an authorized representative to authorize the completion of key project phases, assign resources, and serve as project liaison. During the test, the Project Liaison or a nominated representative should be available at all times to support the test. If the liaison is not available to answer questions or provide technical assistance, it may affect the ability of the team to conduct the test within the allowed time.

**Access** - Ensure SilverSky consultants have access to key personnel and data requested

**Resources** - Furnish SilverSky with Customer personnel, facilities, resources, and information and perform assigned tasks promptly

**Cooperation** - Ensure all Customer employees and contractors cooperate fully with SilverSky 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** - Timely delivery of all documentation requested by SilverSky including Customer's security policies, network diagrams, server listings and procedures

**Scheduling** - SilverSky will contact the Customer to agree on a start date. Once agreed, if the Customer needs to change the scheduled start date this must be done at least two weeks (14 days inclusive) prior to the first day of the

engagement. Any change to the dates within two weeks (14 days inclusive) of the start date may result in the effort being forfeited if SilverSky cannot reassign committed resources to other customer work. The Customer will be responsible for any non-refundable travel and lodging already booked, should travel have been agreed upon.

### 3.2 SilverSky Assumptions

The Customer will provide SilverSky with reasonably requested information upon which SilverSky can rely to be current, accurate and complete.

For engagements conducted at Customer's site, Customer will provide SilverSky personnel with a workplace that meets industry standard health and safety requirements along with access to network and power. Customer will provide access to Customer's personnel who have detailed knowledge of Customer's security architecture, network architecture, computer environment, and related infrastructure. Customer will provide access to Customer's personnel who have an understanding of Customer's security policies, regulations, and requirements.

The Customer will evaluate SilverSky deliverables and notify SilverSky of any perceived problems or issues with SilverSky obligations within two weeks (14 days inclusive) of the comprehensive report delivery.

SilverSky will promptly 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.

## 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 | Typically within 30 days of the Effective Date |
| Project Exclusions | Web Application Testing and External Penetration Testing unless contracted separately |
| Project Duration | Approximately 2-3 weeks, depending on Tier level and subject to project variables |
| **S-266-2821** Internal Pen Testing Tier 4 | Up to 1000 IP addresses in scope. Work hours not to exceed 120 |
| **S-266-2821** Internal Pen Testing Tier 3 | Up to 250 IP addresses in scope. Work hours not to exceed 80 |
| **S-266-2821** Internal Pen Testing Tier 2 | Up to 100 IP addresses in scope. Work hours not to exceed 60 |
| **S-266-2821** Internal Pen Testing Tier 1 | Up to 50 IP addresses in scope. Work hours not to exceed 40 |

All penetration testing services are performed as time-bounded exercises utilizing skilled and experienced consultants following our standard, repeatable methodology.

Penetration testing is an active assessment of a defined network, system or application. The impact on the Customer's normal business operation is expected to be minimal. However, given the nature of the assignment, SilverSky makes no representations or covenants regarding actual consequences that may result from the testing. Should either SilverSky or Customer suspect that the testing has caused an issue, all work will be halted until such time as it has been resolved or the penetration testing has been ruled out as the cause.

### 4.2 Location and Travel Reimbursement

The Service defined in this SOW is performed remotely

On occasion, testing may require onsite participation by SilverSky's staff at Customer location(s).

For Customer-approved onsite participation, the Customer will be invoiced for all actual SilverSky's staff travel and living expenses associated with all onsite visits. An administration fee of ten percent (10%) of all travel and living expenses will be billed to the Customer in the event the Customer requires an itemized statement of such expenses.

| Location | Scope of Work |
|---|---|
| | |
| | |
| | |

### 4.3 Acceptance

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