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

Internal networks often house the most sensitive systems and data, making them prime targets once attackers gain a foothold. Our Internal Infrastructure Assessment evaluates your organization's internal infrastructure — including Active Directory, workstations, servers, and internal network segmentations to identify vulnerabilities, misconfigurations, and weaknesses that could enable lateral movement, privilege escalation, or full domain compromise.

We emulate realistic post-exploitation techniques to assess internal risks from the perspective of a compromised asset or insider threat. Active Directory testing is included by default.

1.2 Service Importance

The speed, scale, and stealth of post-breach intrusions continue to increase across all sectors, with no signs of slowing. In fact, it will only get worse as automated tooling and agentic AI systems improve. Notable information includes:

- "Breakout time — how long it takes for an adversary to start moving laterally across your network — reached an all-time low in the past year:
- The average fell to 48 minutes, and the fastest breakout time we observed dropped to a mere 51 seconds.
- Valid account abuse was responsible for 35% of cloud-related incidents, reflecting attackers' growing focus on identity compromise as a gateway to broader enterprise environments.

2 Scoping

This service can be delivered remotely via ScreenConnect, VPN, or internal jump host. We offer two engagement styles:

Authenticated Assessment – You provide a standard domain user account and network access. We simulate an insider threat, evaluating lateral movement, privilege escalation, and access controls from a legitimate user's perspective.

Unauthenticated Network Assessment – We operate as an unprivileged system on the internal network, emulating a rogue or compromised device.

Our default approach begins unauthenticated, attempting to compromise systems or users to gain access naturally. If this is unsuccessful, we request a standard Active Directory account to ensure we can still evaluate internal risks. This ensures a comprehensive assessment.

Scope Requirements

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

- Total number of in-scope IP addresses
- Will a list of alive IP addresses be provided, or is there a network discovery requirement?
- Confirmation of access method (e.g., VPN, SSH to internal server, physical)
- Useful contextual information for the consultant
- Out of scope requirements

Assessment Requirements

Minimal prerequisites, but access must be provided as agreed:

- Internal network connectivity (on-site, VPN, or hosted VM)
- Access (VPN/RDP/VDI/SSH/VM) to the environment with working network access to the scope.
- Accurate and updated scope that contains IP addresses, ranges, and fully qualified domain names.
- Credentials if agreed and necessary.

3 Testing Methodology

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

Reconnaissance & Environment Mapping

- 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
- Enumeration of internal service exposures (e.g., file sharing, remote desktop, databases, AD-related ports)
- Identification of deprecated or vulnerable protocols that may allow impersonation or traffic interception (e.g., LLMNR, NetBIOS, mDNS, IPv6 spoofing)
- Detection of misconfigured or excessive protocol permissions, such as unauthenticated SMB shares or null sessions

Credential Access & Authentication Weaknesses

- Controlled use of credential harvesting and reuse techniques across services and hosts
- Identification of plaintext credentials or sensitive files on open shares, endpoints, or domain controllers
- Targeted abuse of authentication protocols (e.g., NTLM relaying, LDAP/S authentication downgrade, Pass-the-Hash)
- Detection of insecure delegation, shared local administrator use, and excessive permissions
- Kerberos-focused attacks (e.g., Kerberoasting, AS-REP Roasting) to extract credentials from service accounts
- Enumeration of exposed certificates or misconfigurations within Active Directory Certificate Services (ADCS)

Privilege Escalation & Lateral Movement

- Analysis of privilege boundaries within systems and accounts, including excessive group membership or local admin rights
- Identification of paths for lateral movement, such as through service misconfigurations or protocol abuse
- Controlled exploitation of known privilege escalation vectors in the operating system or endpoint management agents
- Use of real-world attacker techniques to simulate compromise of sensitive systems or access to critical data
- Testing segmentation controls between user zones, server networks, and administrative infrastructure

Active Directory & Identity Security Testing

- Enumeration of trust relationships, domain group policy issues, and delegation vulnerabilities
- Testing for unauthorized access to domain objects and high-value users (e.g., Domain Admins, service accounts)
- Analysis of directory permissions and ACLs to identify privilege escalation paths (e.g., DCSync, DCShadow)
- Identification of misconfigured or overly permissive certificate templates enabling ADCS abuse (e.g., ESC1–ESC8 techniques)
- Assessment of exposure through stale accounts, weak passwords, or lack of MFA on privileged users

Impact Simulation & Security Control Evaluation

- Controlled proof-of-concept attacks demonstrating risks of credential compromise, data access, or domain control

- Simulation of man-in-the-middle attacks via rogue devices to intercept or relay credentials
- Evaluation of endpoint protection, network monitoring, and incident response controls
- Mapping of attacker paths from initial foothold to critical asset access
- Review of logs, telemetry, and response capability to detect and respond to simulated incidents

Strategic Recommendations

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

4 Project Deliverables:

Comprehensive Report structured as follows:

1. An Executive Summary outlining at a business level the review conducted, the key issues found, and the business risk impact of any vulnerabilities discovered.
2. A Detailed Findings section containing descriptions of the scope and testing methodology applied.
3. Assessment information, including the environment description, narrative, key findings (including severity, description, affected hosts, recommendation, references, and evidence).

5 SilverSky Obligations

Kick-off Meeting – Meet to discuss and agree on customer goals and the rules of engagement for the project.

Objective-setting - SilverSky will propose a set of objectives based on the Customer's size, industry vertical, and potential adversaries in the threat landscape. The Customer may accept SilverSky's proposed objectives or may request alternative objectives.

Primary Objectives: These 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 below.

6 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 joint review with the Customer.

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

Consultant Findings – This 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

7 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. If Customer requests additional services, such services will be the subject of a change request or additional SOWs, depending on the nature of the Customer requests.

8 Customer Obligations and Assumptions

Services, fees, and work schedule are based upon the assumptions, representations, and information supplied by Customer. Customer's fulfillment of the obligations listed below is critical to the success of the engagement.

8.1 Customer Obligations

8.2 Pre-Technical

This section covers the non-technical prerequisites that ensure details of the engagement are accurate, lawful, and all relevant parties have been informed.

Scoping Documents:

- Complete the provided scoping documents with accurate and updated information that encapsulates all in-scope assets and requirements. This ensures both parties have a clear understanding of the engagement's scope and objectives.

Legal Documents:

- Complete and sign the Order Form. This document is critical for legal and compliance purposes, authorizing us to conduct the engagement under a finalized, agreed-upon scope.

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.

8.3 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, 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.
- 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 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.

9 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 Exclusions	Web Application Testing and External Penetration Testing, unless contracted separately
Project Duration	Approximately 2-3 weeks, depending on project variables
S-266-2821 Internal Infrastructure Assessment	AD testing and up to 250 devices (servers, workstations, network equipment)
S-266-2821 Internal Infrastructure Assessment	AD testing and up to 500 devices (servers, workstations, network equipment)
S-266-2821 Internal Infrastructure Assessment	AD testing and up to 1000 devices (servers, workstations, network equipment)

All penetration testing services are performed as time-bound exercises by skilled, 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 operations 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 the issue is resolved or the penetration testing is ruled out as the cause.

9.1 Location and Travel Reimbursement

The Service defined in this SOW is performed remotely.

9.2 Acceptance

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