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

Our Simulated Breach Assessment is a comprehensive service that simulates user-initiated attacks (such as Ransomware) and malicious user journeys against physical devices and remote access solutions, with the goal of demonstrating and mapping device vulnerabilities, access pathways, and security exposures.

This service provides an attacker-centric perspective on your endpoint and remote access infrastructure to demonstrate the repercussions of a compromised device, unauthorized physical access, or insider threats.

Typically Identified Issues:

- Lack of Network Segregation
- Outdated and Unsupported Software
- Bypassable Security Controls
- Cleartext Credentials
- Weak Credentials & Password Reuse
- Unsecured Applications
- Administrative Tool Access

1.2 In-Scope Service Details

This service is scoped to cover x1 VDI solution as a foundational level, but is a modular service that can be scoped to cover one or more of the following surfaces:

- Laptops, workstations, servers
- Thin clients
- Containers
- VPNs
- VDIs (Citrix, VMware Horizon)
- Virtual apps

1.3 Technical Requirements

There are prerequisites and Customer preparation steps required before initiating a Simulated Breach Assessment for Virtual Desktop Infrastructure (VDI) environments. Proper preparation ensures optimal testing conditions and maximizes the value of the security assessment.

- Credentials
    - Create user account(s) that can access the in-scope VDI solution.
        - This should be an accurate reflection of the number of accounts and types discussed during scoping.

        - Accounts should represent realistic user privilege levels (standard user, power user, administrator) as agreed upon in scoping.

    - Test the credentials internally to ensure that no problems exist with the configuration.
        - Verify successful authentication to the VDI environment
        - Confirm access to expected applications and resources
        - Test from multiple network locations if applicable

    - Securely provide credentials using our secure email solution.
        - Include username, password, and any additional authentication factors
        - Specify any password policies or expiration dates
        - Note any account lockout thresholds or restrictions

1.4 Assessment Requirements

Typical requirements to facilitate commencement of the project will include;

- Remote Access
    - Determine access method for your VDI environment:
        - External/Internet Access: VDI accessible from any public IP address
        - Allow-listed Access: VDI accessible only from specific IP ranges
        - VPN-Required Access: VDI accessible only through corporate VPN

    - For externally accessible VDI:
        - Provide the external URL/FQDN for VDI access
        - Confirm any IP allow-listing requirements for our testing IPs
        - Document any geographic restrictions or access policies

    - For VPN-required access:
        - Provide VPN credentials and connection details
        - Share VPN client software or configuration files
        - Test VPN connectivity and confirm access to VDI resources
        - Document any multi-factor authentication requirements for VPN

1.5 Project Summary

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

1. Kick-off Meeting
2. x1 VDI simulated breach assessment
3. Exploitation and Vulnerability Validation
4. Analysis of Findings
5. Draft Report and Review of Initial Findings
6. Final Comprehensive Report

1.6 Methodology:

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

- Reconnaissance & Environment Mapping
- Credential Access & Authentication Weaknesses

- Privilege Escalation & Lateral Movement
- Active Directory & Identity Security Testing
- Impact Simulation & Security Control Evaluation
- 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

1.7 Final Report Delivery

SilverSky will deliver a final version after a joint review with the Customer, and any changes will be addressed in the draft report.

- Comprehensive Report detailing
    - Methodology followed
    - Successful exploitation achieved
    - Detailed recommendations for improvements

1.8 Out of Scope

Any activity not explicitly included in this SOW is considered out of scope.

- Any retesting of the infrastructure after remediations are addressed, unless specifically included in the SOW scope.
- Any testing not outlined in the in-scope testing section

If the Customer requests additional services, those services will be subject to a change request.

2 CUSTOMER OBLIGATIONS & REQUIREMENTS

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

2.1 Customer Obligations

- **Project Liaison** - Designate an authorized representative to authorize 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 Customer that 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.

2.2 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's personnel with detailed knowledge of Customer's security architecture, network architecture, computing environment, and related matters.
- 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 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 cannot perform the Service due to Customer's delay or other failure to fulfill its obligations under this Statement of Work.

3 PROJECT PARAMETERS

3.1 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 Duration	Approximately 1-2 weeks, subject to project variables; comments on findings preliminary to the comprehensive report to be delivered to SilverSky within 30 days of receipt of the initial report
Simulated Breach Assessment x1 user account **S-266-3163**	1x VDI solution using 1 user account
Simulated Breach Assessment x2 user accounts **S-266-3163**	1x VDI solution using x2 user accounts

3.2 Location and Travel Reimbursement

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

3.3 Acceptance

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