SERVICE ORDER ATTACHMENT
STATEMENT OF WORK

S-266-3156 SIMULATED CLOUD BREACH 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

Our Microsoft Cloud Breach Assessment service is a streamlined offering that simulates user-initiated attacks and malicious user journeys against Azure and M365 environments (including Copilot), to demonstrate and map user permissions, access, and threats.

This service and our Cloud Security Review service are two sides of the same coin; this service provides an attacker-centric perspective of your cloud environment to demonstrate the repercussions of a compromised user or an insider threat.

Typically Identified Issues:

- Default Configurations
- Conditional Access Policy Weaknesses
- Poor SharePoint/OneDrive Hygiene
- Misconfigured SSO Access
- Lack of Monitoring and Alerting

1.2 In-Scope Service Details

Can be conducted against Azure and/or M365. Purely Microsoft Cloud-focused.

1.3 Scope Requirements

To scope and deliver the Microsoft Cloud Breach Assessment, we require information for the following sections. Please note that we only require information for the in-scope sections.

- Azure
    a. Is Azure in scope?
    b. Number of in-scope Azure tenants
    c. Number of in-scope subscriptions
    d. Number of total resources
    e. Is everything within the tenant(s) in scope? If not, please clarify what is and out of scope

- Entra ID
    - Is Entra ID in scope?
    - Number of in-scope Azure tenants

- M365
    - Is M365 in scope?

- Number of unique M365 tenants/instances
- Is everything in scope? If not, please clarify what is in and out of scope

1.4 Assessment Requirements

Typical requirements to facilitate commencement of the project will include;
The following requirements are needed to conduct the assessment.

- Azure
  - Entra ID account for the consultant with Global and Security Reader roles and Reader RBAC permissions to the most applicable scope (tenant, management group(s), subscription(s), resource group(s), resources.
  - For example, if you have one tenant and two subscriptions, and everything within the subscriptions is in scope, you would assign the Reader RBAC assignments to both subscriptions or a management group that contained both subscriptions.
  - We suggest that you create a new Entra ID user within the tenant rather than inviting our consultants as guest/external users.

- Entra ID
  - Entra ID account with Global and Security Reader roles.

- M365
  - Entra ID account with Global and Security Reader roles.

- Conditional Access Policy Requirements
  - Exclude the consultant(s) accounts from any conditional access policies that prevent access to the target environment(s) and applications such as Azure CLI and Azure PowerShell.

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

- Breach 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 Cloud Breach Assessment x1 User Account **S-266-3156**	Conducted using x1 User Account
Simulated Breach Assessment x2 User Accounts **S-266-3156**	Conducted 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.