SERVICE ORDER ATTACHMENT
STATEMENT OF WORK
S-266-3156 AZURE CLOUD PENETRATION TESTING

1.1 Overview

This Statement of Work ("SOW"), with any appendices included by reference, is part of any agreement that incorporates this document by reference.

1.2 Services Summary

While more and more organizations are adopting the use of cloud providers to host critical infrastructure, it is essential for organizations to be aware of potential challenges and risks associated with cloud adoption. Typical security challenges organizations face with cloud implementations include lack of visibility, control, dependency on service providers, and misconfigurations due to shared responsibilities. These challenges create an extended security risk that goes beyond the boundaries of a traditional network.

SilverSky's Cloud Penetration testing service (the "**Service**") provides validation that your cloud implementation is secure. Many organizations now use Azure AD as an Identity and Access Management platform using the hybrid cloud model. This makes it imperative to understand the risks associated with Azure as it contains an enterprise's infrastructure, apps, identities, and a lot more. In addition to cloud-only identity, the ability to connect on-prem Active Directory, applications and infrastructure to Azure AD brings some very interesting opportunities and risks too. Often complex, this setup of components, infrastructure, and identity is a security challenge.

Cloud Penetration testing is becoming increasingly common and follows a different methodology than traditional pen testing. This type of testing differs from on-prem AD testing, and the tools and techniques leveraged are different. While in an on-prem AD assessment, SilverSky is assessing the security posture of the AD domain, including patchable vulnerabilities and misconfigurations, Azure AD testing looks at services, containers, enterprise applications, and more." During a typical Cloud Penetration test, SilverSky will attempt to abuse Azure, Azure AD, and several services offered by it and perform in-depth testing of your cloud-based architecture. Testing will cover multiple complex attack lifecycles against the target environment's Azure tenant(s).

SilverSky's Cloud penetration testing is a proactive and strategic approach to identifying and addressing security risks in cloud environments while ensuring an organization's infrastructure's overall security and resilience.

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. Security Testing Phase
3. Analysis of Findings
4. Draft Report and meeting on Initial Findings
5. Comprehensive Report

1. **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.

2. **Security Testing Phase** - A typical cloud penetration testing methodology covers discovery, initial access, enumeration, privilege escalation, lateral movement, persistence, and data mining. Based on the results, we will attempt to exploit any found issue and recommend appropriate remediation guidance.

   Some of the attack chains we will explore include:

   - Illicit Consent Grant
   - Managed Identity Abuse
   - Automation Account Abuse
   - App Service Abuse
   - Anonymous Access to Storage Containers
   - Key Vault Abuse
   - Enterprise Applications Abuse
   - Token Theft
   - Application Proxy Abuse

3. **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 risk associated with the findings.

4. **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.

1.4 Deliverables

SilverSky will provide a Detailed Findings Report following its review.

The Detailed Findings Report describes the review results in detail. It is intended for mid-level management, administrators, and other operations personnel and includes:

- Itemized listing and description of the areas reviewed.
- Identified deficiencies.
- Overall risks associated with deficiencies.
- Detailed recommendations for addressing deficiencies.

1.5 Out of Scope

Any activity not explicitly included in this SOW is considered out of scope. If the Customer requests additional services, such services will be the subject of a change request.

- Internal, wireless, application and other cloud penetration testing are not outlined within this scope of work.
- Physical Security and Social Engineering services

2 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.

2.1 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 can access key personnel and requested data.
- **Resources** - Furnish SilverSky with Customer personnel, facilities, resources, and information and perform tasks promptly.
- **Cooperation** - Ensure all the Customer's employees and contractors cooperate fully and promptly with SilverSky. SilverSky will advise the Customer if an increased level of Customer participation is required for SilverSky to perform the Services under this SOW.
- **Documentation** - Timely delivery of all documentation SilverSky requests, including the Customer's security policies, network diagrams, server listings, and procedures.

2.2 SilverSky Assumptions

- The Customer will provide SilverSky with reasonably requested information upon which SilverSky can rely to be current, accurate, and complete.
- The Customer will provide access to the Customer's personnel with detailed knowledge of the Customer's security architecture, network architecture, computing environment, and related matters.

- The Customer will provide access to the Customer's personnel who understand the Customer's security policies, regulations, and requirements.
- The Customer will evaluate SilverSky deliverables and immediately notify SilverSky of any perceived problems or issues with SilverSky obligations.
- SilverSky will immediately notify Customer of any perceived problems or issues regarding Customer's obligations.
- Customer is responsible for any additional costs if SilverSky cannot perform the Services 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	SilverSky will reach out within 30 days of the Effective Date with a date for a kickoff call.
Project Duration	Approximately 1-2 weeks, subject to project variables
Cloud Penetration Testing (Azure) Tier 1	Work hours not to exceed 40 hours of penetration testing work
Cloud Penetration Testing (Azure) Tier 2	Work hours not to exceed 60 hours of penetration testing work
Cloud Penetration Testing (Azure) Tier 3	Work hours not to exceed 80 hours of penetration testing work

3.2 Location and Travel Reimbursement

The Services defined in this SOW will be performed remotely and do not require any onsite travel.

3.3 Acceptance

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