SERVICE ORDER ATTACHMENT
STATEMENT OF WORK

S-266-2166 DYNAMIC (DAST) WEB APPLICATION PENETRATION TESTING

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

The purpose of Dynamic Web Application Penetration Testing (the "Service") is to identify the feasibility of an attack on the Customer's Internet-facing web application(s) and to determine the extent of the impact of successful exploitation of that intrusion. The testing will employ intrusion analysis and testing methodologies to test the potential for Internet-based penetration of the systems. The process will involve mostly automated dynamic scanning methods followed by manual validation to mimic typical attacker techniques and actual attempts to exploit identified vulnerabilities.

1.2 In Scope Service Details

Dynamic Web Application Security Testing (DAST) scanning provides the customer with a cost-effective solution for performing web application level testing of a customer's web applications. DAST application testing relies heavily on automated web application tools to scan an application to determine potential weaknesses. Once the application is scanned, the penetration tester will perform manual validation to help assess the ability to exploit the vulnerability discovered successfully.

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. Dynamic Application Security Testing (DAST)
3. Exploitation and Vulnerability Validation
4. Analysis of Findings
5. Draft Report and Review of Initial Findings
6. Final Comprehensive Report

1.4 SilverSky Methodology:

Kick-off Meeting - Meet personnel to discuss and agree on customer goals and the project engagement rules. This includes project scoping (determining the target systems to be included in the testing), testing style (authenticated versus unauthenticated and the privilege level of authentication for users provided), 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.

Dynamic Application Security Testing – SilverSky penetration testers will use automated toolsets to perform web application scanning of the targets. Once this information is gathered, the dynamic web app scanning tools help identify potential security vulnerabilities in the web application and architectural weaknesses. DAST tools allow sophisticated scans, detecting vulnerabilities with minimal user interactions once configured with host name, crawling parameters and authentication credentials.

Vulnerability Validation - Once issues are identified, SilverSky's web application penetration testing team will perform manual validation within the remaining testing time allotted to validate any findings from the DAST application tools. SilverSky processes and techniques for manual validation will vary significantly depending on the type of weakness identified but may include manual verification of open ports, listening services and vulnerable versions evidenced in the report and proof of concept screenshots or code snippets of successful exploitation of identified vulnerabilities.

Analysis of Findings Phase – SilverSky will compile and analyze the data generated from the assessment tools and manual checks and categorize vulnerabilities by severity, depending on the potential impact each can have on the affected network. This analysis is the basis for recommendations to address the risks associated with the vulnerabilities potentially.

Draft Report and Review of Initial Findings

At the conclusion of the assessment, SilverSky will provide a comprehensive draft report composed of an executive summary and a detailed findings section. The Customer will have an opportunity to review drafts of the report and make any comments on findings.

Final Report Delivery

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

- Comprehensive Report detailing
  - Methodology followed
  - Successful exploitation of the web application
  - Detailed recommendations for improvements

1.5 Out of Scope

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

- Any web applications not identified as in-scope
- Any retesting of the application 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, such services will be the subject of a change request.

2 CUSTOMER OBLIGATIONS AND ASSUMPTIONS

Services, fees and work schedule are based upon the assumptions, representations and information supplied by the Customer's fulfilment 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 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, including Customer's security policies, network diagrams, server listings, and procedures

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 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 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	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; comments on findings preliminary to comprehensive report to be delivered to SilverSky within 30 days of receipt of the initial report
DAST Web Application Testing Project Scope	Dynamic Web App Penetration Testing is priced per web application with up to 25 hours of project work per application.

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.