Statement of Services

Supra ITS Network External Penetration Testing

Purpose of this Document

This document represents the scope of included services of Supra ITS (Provider) External Penetration Testing and the deliverables and unique features of the included services.

External Penetration Testing

External Penetration Testing simulates the actions of an external attacker. Using emerging tactics, techniques and procedures, the penetration tester attempts to exploit systems and gain access to data. Exercise results in identification of systematic weaknesses with areas of remediation ranked by criticality.

Scope: The scope of work for the one-time External Penetration Testing involves simulating the actions of an external attacker to identify and exploit vulnerabilities, assess the effectiveness of security controls, and provide actionable insights for remediation. This process includes using emerging tactics, techniques, and procedures to attempt exploitation of systems and data access. Thorough assessments are conducted to identify vulnerabilities and weaknesses in the system, with areas of remediation ranked by criticality. Detailed technical reports and executive-level summaries of findings and recommendations are provided to enable comprehensive understanding and strategic planning. The effectiveness of existing prevention and detection mechanisms is evaluated, utilizing methodologies such as OWASP (Open Web Application Security Project) and OSSTMM (Open Source Security Testing Methodology Manual). The robustness and effectiveness of external security controls are verified, and areas of very high risk are identified with prioritized remediation recommendations. Compliance with regulatory standards is validated, leveraging the expertise of credentialed professionals to produce high-quality and reliable testing outcomes.

Deliverables:
The following deliverables are associated with the scope of work:

- Vulnerability Assessment Report: Detailed documentation of identified vulnerabilities and weaknesses.
- Remediation Plan: Prioritized recommendations for addressing identified issues.
- Technical Report: Comprehensive technical analysis of the penetration testing activities and findings.
- Executive Summary: High-level overview of the testing results and strategic recommendations.
- Compliance Report: Documentation demonstrating compliance with relevant standards and regulations.
- Risk Assessment: Identification and ranking of areas of very high risk.
- Methodology Documentation: Description of the methodologies used during the testing process.
- Validation Report: Confirmation of the effectiveness of external security controls.
- Training Materials: Resources for educating the client/customer's (Client) team on findings and remediation strategies.

Unique Features:

- Client will provide a designated point of contact for testing, remediation guidance and verification requests.
- Provider will provide remediation guidance based on industry standard practices and vulnerability severity. Client is responsible for implementing remediation actions.
- Usage and Counts: Based on total number of IP addresses, Cloud assets, and Web Applications within scope.
- Does not include retesting after the first test is completed.
- Client shall provide Provider with accurate, correct, and complete information. Client acknowledges that inaccurate information provided to Provider may result in adverse consequences to Client or other third parties, including, but not limited to, an inaccurate Report of Compliance (ROC) or Assessment. Client acknowledges that Provider is not responsible for any errors, inaccuracies, or negative consequences that relate to, or arise from, inaccurate information provided by Client to Provider.
- Client shall not misrepresent any ROC, Assessment, or other statement made by Provider concerning Client's information security practices.
- Client acknowledges Provider does not guarantee, represent, or warrant that Client's computers, equipment, information systems, or network "Network) will not be accessed by an unauthorized third party, or that Provider will be able to identify, in all instances, if Client's Network has been accessed by an unauthorized third party. Provider shall not be liable, directly or indirectly, for any unauthorized third party that accesses Client's Network or any harm or injury incurred by Client that arises from such access.
- If the scope of the Services includes payment card industry (PCI) certification then the Client allows Provider to release, directly to PCI Security Standards Council (SSC), without any additional consent, approval, or permission of Client, and to the extent necessary to provide the Services, (i) all Reports on Compliance (ROCs) and related risk assessments (Assessments) results generated in connection with the Provider's assessment of Clients' working papers, notes and other materials, and any and all information generated in connection with conducting, or obtaining, such ROCs or Assessments and (ii) any and all additional agreements or other materials necessary in the future to enable Provider to comply with the PCI SSC reporting requirements.
- Provider will treat information received from Client as confidential unless otherwise in the public domain or already known, or otherwise becomes known from a third party, to Provider. Provider will not publish or disclose to any persons other than agents, employees or associates of the parties, except upon the written approval of Client. This provision also does not preclude Provider from disclosing information or documents in the following situations:
    - Provider may disclose information, as necessary, to PCI SSC, as required by PCI Certification.
    - Provider may disclose information in response to a valid court order. To the extent feasible Provider will notify Client that it has received such an order and will provide Client with an opportunity to request that the issuing court revoke or rescind the order prior to the disclosure.
    - Provider may disclose information to a government agency in response to a subpoena, civil investigative demand, or non-public inquiry.
- Provider's Services may include scanning, penetration, intrusion testing or related analysis of Client's information systems or enterprise (Testing Services), for which Provider may use intrusive or passive techniques and software tools. Client shall obtain all necessary consents from its third-party service providers in connection with Testing Services. If Testing Services will be performed with respect to any information systems, applications or components that are hosted by a third party, such as an internet service provider or application service provider, its consent shall be obtained by the Client prior to the commencement of testing by Provider.
- The objective of this assessment is not to identify all vulnerabilities existing in the systems in scope for testing and is intended to identify relevant security gaps present during the testing time.
    - In any event, under no circumstances shall Client consider or claim Provider to be liable for damages or costs that may be caused by the penetration testing, network intrusion by any third party, any interruptions in network service that may occur, or any other damage to Client data or devices that might result from the penetration test.
    - Client understands that testing may result in disruptions of and/or damage to its or a third party's information systems and/or the information and data contained therein, including, without

limitation, denial of access to a legitimate system user, automatic shut-down of information systems caused by intrusion detection software or hardware, or failure of the information system. Client is solely responsible for understanding the testing steps that are included in any Testing Services and for arranging alternative means of operation should such disruptions or failures occur. Client is solely responsible for any damage caused by Testing Services. Provider shall have no responsibility or liability for, and Client shall have no recourse and shall bring no claim, against Provider in connection with or arising out of, any Testing Services, including with respect to any of its claims or third-party claims against Client related thereto.

Covered Items

This Statement of Services applies to the following SupraITS External Penetration Testing Services

7489C014 - SupraITS - External Penetration Test (1-10 IP's)
7489C015 - SupraITS - External Penetration Test (10-25 IP's)
7489C016 - SupraITS - External Penetration Test (25-50 IP's)
7489C017 - SupraITS - External Penetration Test (50-100 IP's)

Any product, service, or deliverable not expressly set forth in the foregoing is out of scope of this Service.

About Supra ITS

Supra ITS, a Canon IT Managed Services partner, is based in Canada, established in 1999 and blends deep enterprise know-how with a “customer-first” mindset to deliver everything-as-a-service for growing organizations. Supra ITS has offices in the US, UK, India and Canada. More than 200 certified professionals operate four tier-3 data centers and run tightly integrated 24 × 7 SOC and NOC teams, so clients get prompt, around-the-clock support. The company’s portfolio spans managed IT and cloud, cyber-security, business-process outsourcing, and custom application development, all backed by top-tier credentials and strategic alliances. This combination of scale, pedigree, and nimble execution lets Supra ITS safeguard critical workloads, speed digital transformation, and simplify compliance.

Canon U.S.A., Inc.