Service Description for Unit 42 Public Sector Expertise on Demand Subscription

Palo Alto Networks' Unit 42 Public Sector Expertise on Demand Subscription ("EOD Subscription") is available to federal government (where applicable) , state and local government, and education (both K-12 and higher education) entities ("Customer(s)"). This Service Description outlines the EOD Services available to an EOD Subscription Customer. This EOD Subscription shall be subject to the terms and conditions in the End User Agreement and Unit 42 Public Sector Expertise on Demand Subscription Addendum.

1. Description of Services Available for Use

In purchasing the EOD Subscription, Customer will receive on-demand access to the Services set forth in the attached Appendix A (Unit 42 Public Sector Expertise on Demand Subscription Services List), subject to fixed annual maximum number of consulting hours.

2. Delivery of Service

Unit 42 consulting hours are delivered in fifteen (15) minute increments and may be used to obtain any of the EOD Services described in Appendix A, all of which are provided remotely in the United States unless otherwise agreed to in writing. If Customer requires more Unit 42 consulting hours than originally purchased, Customer may upgrade its subscription to a higher service tier as described in Section 5 of this Service Description. Upon Customer's request, Palo Alto Networks will provide Customer with an estimate of the Unit 42 consulting hours needed to perform the relevant EOD Services, BUT MAKES NO REPRESENTATION OR WARRANTY AND PROVIDES NO GUARANTEE THAT SUCH EOD SERVICES WILL BE ACCOMPLISHED WITHIN THE ESTIMATED TIME.

3. Palo Alto Networks' Responsibilities

There are no pre-set deliverables as part of the EOD Subscription. Depending on the EOD Services performed, Palo Alto Networks may provide the following:

- Verbal Status Updates: Unit 42 will provide verbal status updates for major findings or as requested. Verbal status updates will include findings to date, activities completed, plans for the next reporting period, issues requiring attention, and budgetary updates if requested.
- Executive Summary Report: At the request of the Customer, Unit 42 will generate a written summary report that details the analysis performed and subsequent findings.

4. Kickoff and Notification

Unit 42 will, with Customer's participation, conduct an initial kickoff to review Customer's primary focus and objectives under this Service Description. Customer and Unit 42 will identify key activities and work streams, with associated prioritization and Customer team members. Subsequent requests by Customer to obtain any of the EOD Services described in Appendix A shall be provided in writing by sending an email to the designated Unit 42 EOD email address, which will be provided to Customer at kickoff. Unit 42 will provide Customer with periodic updates summarizing the number of EOD hours consumed and the number remaining in the Term.

5. Limitation on Total Annual Hours

In purchasing the EOD Subscription, Customer shall receive on-demand access to Services, up to an annual maximum number of consulting hours as set forth in the table below. In addition, Customer may purchase additional tiers of service hours for their EOD Subscription, as needed, by upgrading to a higher service tier at any time during the Term.

As reflected in the table below, a Service Level Agreement ("SLA") for response times for Incident Response services is included for each subscription level. The SLA is for remote responses, does not apply to on-site services, and is not applicable to services other than Incident Response services as described in the Appendix.

Service Tier Level	Annual Maximum Consulting Hours	SKU	Incident Response SLA
Level 1	124 hours	PAN-CES-EOD-LVL1	24 hours remote
Level 2	274 hours	PAN-CES-EODLVL2	12 hours remote
Level 3	449 hours	PAN-CES-EOD-LVL3	8 hours remote
Level 4	500 hours	PAN-CES-EOD-LVL4	4 hours remote

6. Assumptions

In order for Palo Alto Networks to provide the EOD Services in Appendix A, Customer will provide written consent from the legal owner or other applicable legal authorization to Palo Alto Networks prior to commencement, if Customer is not the owner of the computer system provided for assessment(s); ensure that Palo Alto Networks personnel may access and use Customer's and third-party licensors' proprietary materials and data, as necessary, for Palo Alto Networks to perform the EOD Services; and, where installation and use of any software is required, Customer will provide approval for and facilitate the installation and maintenance thereof. Customer warrants and represents that it has the right and authority to grant such access and use to Palo Alto Networks and hereby grants Palo Alto Networks the rights to use and access such proprietary materials as needed for Palo Alto Networks to perform the EOD Services.

7. Term

The term of an EOD subscription is twelve (12) months ("Term") and shall commence upon Palo Alto Networks' receipt of a purchase order. Any unused Services or service hours will expire at the end of the Term and are non-transferable and non-refundable.

Appendix A:

Unit 42 Public Sector Expertise on Demand Subscription Services List

Services Type	**Description**
Incident Response	● Incident Response ○ Investigate and recover from security incidents and data breaches: ■ Contain and eradicate the threat ■ Determine the initial point of access ■ Determine the extent of unauthorized activity ■ Determine what, if any, data was accessed or stolen ○ Malware analysis and reverse engineering ● Ransomware Investigation ○ Engage the threat actor on Customer's behalf ○ Seek proof that the attacker can decrypt the data ○ Refer Customer to service providers of payment services to acquire encryption keys for data recovery ○ Reverse engineer the attacker-provided decryption utility to ensure no malicious code exists ○ Provide tutorial to the Customer's team to demonstrate how to decrypt files ○ Provide remote troubleshooting support ● Business Email Compromise ○ Contain the incident and recommend additional safeguards; Investigate and determine root cause, window of compromise, attacker activity, and review data accessed to quantify sensitive information. ● Web Compromise ○ Contain threat and implement safeguards, analyze logs, review code, quantify exposure or loss of sensitive information, and recommend design hardening countermeasures. ● Cloud Breach Response ○ Identify initial attack vector and extent of unauthorized access and exfiltration, contain incident, identify scope of systems for remediation and recommend/implement additional safeguards and ongoing checks. ● PCI Investigation ○ Contain the incident and implement safeguards, navigate the PFI process, respond to alleged violations, identify the attack vector and window of compromise, quantify the number of exposed cards.

	● Malware Analysis ○ Conduct analysis on samples using open source intel., sandboxing, reverse engineering, and deliver a detailed report focused on the behavior and functionality of the malware. ● Data Mining ○ Identify data at risk using industry standard tools to index, search for, and produce data for review and to identify PII and PHI affected after a data breach.
Digital Forensics	● Digital Investigations, including matters related to insider threats, departed employees, and intellectual property theft. ● Perform forensic analysis of digital media, including desktop/laptop computers, servers, mobile phones/tablets, and/or log data to meet specific objectives, including identifying data access, movement, exfiltration and/or destruction. ● Hardware forensics to determine the functionality of a device, or extract data from IoT devices, new technologies, or attacker-made hardware ● Structured Data Investigations ○ Advise on the collection and lead the analysis of SQL and NoSQL database environments, including but not limited to the review of schemas, tables, procedures, and logs collected from impacted database systems, to assess threat actor activity and data exposure risk.
Testing & Assessment Services	● Breach Readiness Review (BRR) ○ Targeted cybersecurity risk assessment focused on detective controls, people, processes, and technologies necessary to effectively respond to cyber threats. ○ Includes remediation recommendations, control enhancements, and a strategic roadmap to achieve a target state of breach readiness.
	● Incident Response Program Development ○ Facilitate the development of an incident response program to assist in establishing or enhancing current incident response plan, policies, procedures, and playbooks.
	● Penetration Tests - Purple and Red Team Exercises ○ Simulates a real-world cyber-attack to assess the strength of countermeasures and identify hidden security vulnerabilities.

	○ Define a scope, rules of engagement, and establish goals, and then identify attack paths and exploit chains a threat actor would likely leverage to gain access to sensitive data or critical business applications.
	● Vulnerability Assessment ○ Internal and/or external technical assessment designed to yield as many vulnerabilities as possible in environment, along with the severity and recommended remediation priority.
	● Web Application Assessment ○ Evaluate web applications for vulnerabilities, including flaws in development, configuration, deployment, upgrade process, API integrations, maintenance or third-party add-ons.
	● Cloud/SaaS Security Assessment ○ Perform a targeted assessment and deep dive review of the security configuration specific to critical business services, including Office365, Microsoft Azure, G Suite, or Google Cloud Platform. ○ Assess Customer's current configurations against multiple hardening standards and industry best practices. ○ Following the assessment, Palo Alto Networks can supervise the implementation of recommended enhancements in an advisory capacity.
	● Tabletop Simulation ○ Simulate the response to a severe data security incident with key stakeholders. ○ We build customized scenarios based on Customer's industry-specific threats, and real world breaches the Palo Alto Networks team has responded to.
	● Mobile Application Assessments ○ Test and improve the security of mobile applications. Enumerate the attack surface, looking for vulnerabilities, misconfigurations, or logic flaws that lead to likely paths of compromise and/or the exfiltration of data.
	● Email Phishing Exercises ○ Test and improve Customer's employees' cybersecurity awareness and reduce susceptibility to phishing attacks.

	● Compromise Assessment / Threat Hunting ○ Review Customer’s networks and endpoint behaviors to determine whether there is evidence of unauthorized access or activity.
	● Email Security Assessment ○ Conduct a comprehensive review of the security configuration of the Customer’s email environment that includes the review of account management, email forwarding rules, inbox policies, authentication controls, etc.
Strategic Advisory Services	● Virtual Chief Information Security Officer (vCISO) ○ A Palo Alto Networks vCISO assists with developing and implementing a cybersecurity strategy, identifying risk, and providing recommendations for risk reduction measures. ○ A vCISO can answer board of directors’ or senior management’s questions about benchmarks and security program’s maturity, breach readiness, effectiveness, and adequacy, etc.
	● Cyber Risk Strategy and Mitigation Roadmaps ○ Develop customized strategic plans that lay out a path, timeline, and budget to achieve an organization's cyber resilience goals.
	● BoD Security Strategy Review ○ Assessment and review to identify cyber risk, create a current state profile, and build a clear security strategy to share with your executives and Board.
	● Cyber Program, Policy & Standards Development Maturation ○ Develop or improve cybersecurity policies and standards. Taking into consideration industry-specific standards, customer objectives, and future goals.
	● SOC Assessment ○ Design and advise on build of a next gen security operations center and/or infosec program based on best practices.
	● Discrete Cyber Project Implementation ○ Expert assistance with the architecture, overseeing implementation, and tuning of a critical cybersecurity project.

	○ Strategic and tactical services, e.g., advise on hardening critical business applications, enterprise email, and next-gen detective controls.
	● Post breach strategic recovery and remediation advisory services ○ Strategic remediation guidance and prioritization to avoid further spread of any persistence related to Incident. ○ Assessment of state of security controls, systems, managed services providers, team design and procedures intended to identify and prevent the specific Incident. ○ Based on assessment, develop and deliver a strategic remediation plan including, short, medium and long-term prioritized objectives to address security weaknesses exposed by a specific incident and reduce risk of any ongoing or recurrence of an incident.
Governance, Risk, & Compliance Services	● CIS V8 Assessment ○ CIS V8 Report & Tailored Recommendations. ○ 12 – 24 Month Implementation Roadmap,
	● NIST Cybersecurity Framework (NIST CSF) Assessment ○ NIST CSF Findings Workbook. ○ Thematic Findings Executive Report. ○ 12 – 24 Month Implementation Roadmap.
	● Regulated and Contract-based Cybersecurity Assessments (e.g. CCPA, NYDFS, HIPAA, FINRA, PCI DSS, C2M2, GDPR) ○ Perform an assessment mapping to the control requirements of contractual, state, and/or regulatory frameworks. ○ Assess control requirements, find and remediate gaps, and demonstrate compliance.
	● M&A Cyber Due Diligence Reviews ○ Targeted assessment in connection with pending merger/acquisition activity. Focused and tactical, this assessment is designed to provide transparency to deal participants. ○ Identify potential red flags, highlight hidden cybersecurity risks, and obtain an independent assessment of overall information security program maturity.

	● Third Party Vendor Cybersecurity Risk Assessment ○ Evaluation of third-party vendor-based cybersecurity risk. ○ Evaluate and improve information security-related contract requirements. ○ Develop and/or enhance security operations related to third party vendor compliance with security requirements.
	● Cybersecurity Training and Awareness ○ Remote or on-site training modules for groups ranging from 5 to 5,000+. ○ Development of employee cyber training programs.