verizon

VERIZON SECURITY OPERATIONS SERVICE +

1. GENERAL

1.1 **Service Definition.** Verizon Security Operations Service (VSOS) provides security monitoring from the Verizon Security Operations Center (SOC) of Customer's in-scope Security AP located on Customer's premises, in the cloud, or hosted by a third party. The Security AP interfaces with Verizon's security orchestration, automation, and response (SOAR) platform for Verizon to provide the security monitoring services to Customer. The SOAR platform will provide bidirectional communication with the Security AP and Ticketing System provided by Customer. Security monitoring includes threat analysis, Security Incident handling and escalation, Detection Content development, and reporting.

1.2 **Service Implementation.** Verizon will provide VSOS services set forth in the Order. Verizon will conduct a remote kickoff meeting to identify the appropriate Customer contacts, provide an overview of VSOS, and obtain initial information from Customer. The kickoff date must take place within four weeks after the Commencement Date of VSOS. Such meeting marks the beginning of VSOS onboarding. No later than 10 days after the kickoff meeting, Customer will provide to Verizon documents and written technical information about Customer's information technology (IT) environment, Security AP and Ticketing System including network architecture and topography information and diagrams, critical asset information, device counts, and other information requested by Verizon to provide VSOS. Verizon will onboard Customer as described in Section 1.3 following the kickoff meeting and Verizon's receipt of such Customer documents, technical information, and diagrams. VSOS implementation will include onboarding of one instance of a Security AP. Additional instances of a Security AP can be included in the Service Implementation for an additional charge. In addition to onboarding services in Section 1.3, installation or deployment of a Security AP or Ticketing System or additional project management services may be contracted separately with Verizon pursuant to a separate statement of work and the Professional Services Service Attachment (PSSA) at the Applicable Rates.

1.3 **Onboarding.** Verizon will onboard Customer to VSOS per the VSOS Onboarding section of the Verizon MSS – Additional Services Service Attachment. Upon completion, Verizon will notify Customer that VSOS is Ready For Operations.

1.4 **Service Context.** Verizon will develop a Service Context collected from Customer that contains information that Verizon will use to provide VSOS. This Service Context is set up during the onboarding phase described in Section 1.3 and is maintained via the agreed change management process. Customer can update and change information in the Service Context upon prior written notice (email is acceptable) to Verizon. Customer will obtain, collect, and maintain Customer-specific Contextual

Information. Customer will provide such Contextual Information to Verizon for use within VSOS and Customer will pay any cost, such as license and/or API integration, associated with third party Contextual Information providers. The use of such third party Contextual Information providers may require Customer to contract separately for any Verizon services that relate to third-party Contextual Information at the Applicable Rates.

1.5 **Service Features.** The Security AP will ingest Security Events from Customer's environment. Verizon will use the SOAR to triage Security Incidents generated from Detection Content. Verizon security analysts triage Security Incidents using Threat Intelligence, Contextual Information, and the Detection Content that triggered such incidents. Verizon may develop Customer-specific playbooks to respond to Security Incidents. Security Incidents may be created based on the Security Alerts generated by the Detection Content, reports produced by the Security AP or by manual analysis by the SOC. VSOS is delivered in the English language. Subject to Section 2.3.9, Customer may engage Verizon pursuant to separate terms and conditions and at the Applicable Rates to translate any part of the service such as reports and escalations into languages other than English.

1.5.1 **Analytics Levels of Service.** VSOS is available with either VSOS Standard Analytics (VSOS Standard) or VSOS Extended Analytics (VSOS Extended) levels of service.

1.5.1.1 **VSOS Standard Analytics.** VSOS Standard Analytics includes: (i) 24x7 security handling for Security Incidents generated from the Detection Content; (ii) Security Incident investigation and analysis in Verizon's SOAR platform in addition to the Security AP; (iii) Threat hunting at HMM1, (iv) Detection Content Tuning; (v) "out of the box" Detection Content from the Security AP vendor and Customer-specific Detection Content; (vi) a monthly VSOS service report; and (vii) an initial review of the Security AP's existing Detection Content during onboarding to determine relevance, accuracy, timeliness and VSOS service readiness. If during the initial review Verizon identifies that the existing Detection Content does not meet these requirements, Customer will contract separately for Verizon to provide detection content development services at the Applicable Rates.

1.5.1.2 **VSOS Extended Analytics.** VSOS Extended Analytics includes: (i) all of the features of VSOS Standard Analytics level of service included in Section 1.5.1.1; (ii) enhanced Security Incident investigation SLAs set forth in Section 3; (iii) an extended analysis of a Security Incident as further described in Section 1.5.7; (iv) additional Security Incident investigation and analysis as further described in Section 1.5.7; and (v) a weekly VSOS service report.

1.5.2 **Detection Content Enrichment (Threat Intelligence).** Verizon will use Customer's Threat Intelligence feeds and Verizon's own standard-provided Threat Intelligence to develop specific search criteria and Detection Content.

1.5.3 **Detection Content Management.** Verizon will use Customer's Threat Intelligence feeds and Verizon's own standard-provided Threat Intelligence to develop specific search criteria and Detection Content. Verizon will develop a customized Security Incident schema, add Customer Context, amend event investigation processes, and adjust Verizon's SOAR playbooks and operations playbooks as agreed with Customer during onboarding.

1.5.4 **Security Incident Handling.** Verizon will implement manual and automated procedures to identify, categorize, classify, analyze, prioritize, route and escalate Security Incidents following the Security Incident management workflow agreed with Customer. Verizon will provide recommendations that can assist Customer with remediation actions that Customer will implement, if applicable.

1.5.5 **Incident Escalation.** Security Incidents identified during investigative analysis will be escalated to Customer after Verizon's reasonable analysis to verify findings. Customer agrees that the quality of Verizon's analysis and classification of Security Incidents depends in part on the quality, timeliness and completeness of the information that Verizon receives on the monitored Security AP and from Customer's environment, including comprehensive Security Event information, up-to-date

Vulnerability scanning (network, host, and web application), and user and asset criticality data. The quality and completeness of information received from Customer's environment including from the Security AP will contribute to decreasing the number of False Positives generated by the Security AP and Customer's IT environment and triaged by Verizon.

1.5.6 **Report and Analyze.** Verizon will develop and provide Customer with trend cyberthreat analysis reports. For Customer's with VSOS Extended service, Verizon will create standard reports for use by Verizon during the Security Incident triage process. Verizon can develop custom reports and report templates for Customer if Customer purchases additional engineering resource allocation pursuant to an Order.

1.5.7 **Security Operations Center.** VSOS Standard and VSOS Extended will generally be delivered from a Verizon SOC location and region designated by Verizon as set forth in the Order. Customer may purchase SOC support from a specific Verizon SOC regional location at the relevant price specific to such region. Verizon provides physical, environmental, and logical security safeguards for Verizon SOC facilities. The 24x7 Verizon VSOS SOC team will use the SOAR to triage Security Incidents generated from the Detection Content using Threat Intelligence, Contextual Information, and the Detection Content that triggered such incident and provide Security Incident escalation and guidance to Customer's designated incident response team. Verizon's VSOS SOC team typically includes SOC Analysts, Tier 3 security analysts, SSEs, and SSAs and will be allocated based on the resource model for VSOS Standard or VSOS Extended as set forth in the Order.

1.5.7.1 **SOC Analyst.** The SOC Analyst, which may be either a Tier 1 or Tier 2 analyst, is a shared resource available on an 24x7 basis. SOC Analyst responsibilities for VSOS Standard may include: (i) performing active security monitoring and triaging of Security Incidents; (ii) analyzing and escalating Security Incidents to Customer; (iii) managing incoming requests and correspondence relating to Security Events, Security Incidents and reports applicable to the Security AP and VSOS; (iv) identifying recurring Security Incidents as potential Security AP tuning candidates; (v) coordinating with Tier 3 security analysts for high priority Security Incidents; (vi) contributing to the development of documentation such as procedures, playbooks, and standard operational metrics reports; (vii) maintaining security knowledge base; (viii) following documented playbook and escalation procedures; and (ix) providing Security AP-based Threat hunting activities at the HMM1 level. For VSOS Extended, additional responsibilities include advanced Security Event detection and Threat analysis for complex and/or Escalated Security Incidents, malware analysis leveraging Customer sandboxing tools, and providing remediation recommendations of Security Incidents that Customer is responsible to implement.

1.5.7.2 **Tier 3 Security Analyst.** The Tier 3 security analyst is a shared resource that is available on an 8x5 basis. For VSOS Standard, Tier 3 security analyst responsibilities may include: (i) providing guidance to Verizon SOC Analysts; (ii) focusing on the continuous improvement of the Verizon VSOS SOC team; (iii) performing analysis and tuning of the Detection Content; (iv) providing Security AP-based Threat hunting activities using automated IOC searches only; (v) providing reports on Threat intelligence, operational metrics, and service performance; (vi) collaborating with the Verizon VSOS delivery teams on Detection Content development lifecycle; (vii) communicating with Customer senior management and other Verizon teams on VSOS service improvement initiatives; (viii) performing quality assurance reviews of SOC Analyst Security Incident triage, and escalation; and (ix) supervising Verizon staff and providing escalation management and SOC Analyst training. For VSOS Extended, additional responsibilities may include leading research and resolution of complex and/or escalations issues, including technical troubleshooting calls with Customer and Verizon teams, providing Threat hunting activities at HMM1 level, managing changes to Detection Content development, opening tickets with the Security AP vendor on behalf of Customer, and creating security documentation including policies and procedures, training documents, playbooks and operations manuals tailored to Customer.

1.5.7.3 **Security AP and SOAR Engineer (SSE).** The SSE is a shared resource available on an 8x5 basis.

The SSE responsibilities may include: (i) tuning and creating Customer's security Detection Content; (ii) reporting; (iii) creating SOAR playbooks; and (iv) helping to enhance Threat Intelligence feeds on the Security AP. The amount of SSE hours included is based on Customer's anticipated number of Security Incidents per day as set forth in the Order. Customer may purchase additional SSE services in an Order.

1.5.7.4 **Security Services Advisor (SSA).** The SSA is a shared resource available on an 8x5 basis. The SSA will oversee the following activities as part of overseeing the entire VSOS Service: (i) escalation support; (ii) coordination with the security monitoring capability; (iii) Threat detection and analysis; (iv) review of Threat Intelligence; (v) VSOS operational review and service delivery reporting with Customer; and (vi) publication of intelligence reports. The SSA will act as the primary interface between Customer and Verizon and monitor Customer service-related cases and escalations. For VSOS Standard, Verizon will provide SSA support for up to 4 hours per week. For VSOS Extended, Verizon will provide up to 10 hours per week of SSA time. Customer may purchase additional SSA services as set forth in an Order.

1.5.7.5 **Client Security Engineer (CSE).** The CSE is an optional shared resource that is available on an 8x5 basis that Customer may purchase in an Order to: (i) configure and maintain the Detection Content on the Security AP considering best practices; (iii) provide parser and Data Source creation, management, and maintenance, (iv) provide Security AP feature enablement, Security AP configuration, and support for agreed third party integrations supported by VSOS; and (v) participate in scheduled review calls about VSOS between Verizon and Customer.

1.5.7.6 **Designated SOC Analyst (DSA)**. The designated DSA is an optional Tier 3 security analyst. Customer may purchase DSA services as set forth in an Order.

1.5.7.7 **Additional Security Resources.** Customer may separately purchase additional Verizon security services and resources at the Applicable Rates.

1.5.8 **Security Incident Status.** A Security Incident is generated in, and assigned by, the Security AP and ingested into the Verizon SOAR. The status values applied during the Security Incident lifecycle will depend on the Security AP and Ticketing System and the status of the Security Incident will be changed throughout its lifecycle. Status changes are displayed on the Security AP. A Security Incident classification and status may change based on additional analysis, intelligence information or after Customer feedback. A Security Incident can have the following status:

Security Incident Status	Conditions
Open	A Security Incident is generated based on Detection Content. UTC time is assigned when the Security Incident is received in the Verizon SOAR.
Active	The Verizon SOC begins the investigation and determines if the Security Incident needs to be escalated to the Customer's designated security team or closed.
Escalated	The Verizon SOC has completed the triage investigation and determined that the Security Incident needs to be escalated to Customer's designated security team. A Security Incident Ticket is created with information to allow the mitigation, containment, or resolution of the risk.
Closed	The Security Incident is auto-closed or closed by the Verizon SOC analyst including after a Security Incident has been escalated to Customer. False Positives or incidents resulting from a Security Incident Flood may be closed by the Verizon SOC instead of being escalated.

1.5.9 **Threat Analysis.** Customer provides Verizon with a variety of Customer-specific Contextual Information to triage Security Incidents and to tune the Detection Content. VSOS will analyze Security Events and Data Sources in the context of such information, looking for patterns, to identify possible Security Incidents.

1.5.10 **Security Incident Classification.** The definitions for the Security Incident severity classifications (Priority 1 - Critical, Priority 2 - High, Priority 3 - Medium, and Priority 4 - Low) will be documented and agreed between Verizon and Customer during the onboarding process and assigned to Security AP Detection Content. After initial incident status and investigation, Verizon may reclassify a Security Incident into one of the following four incident classification categories based on the following descriptions as supplemented with knowledge of specific Threats or risks, definitions of assets and/or business processes agreed during onboarding:

Security Incidents Classification

Security Incident Classification	Risk Level	Description
Priority 1	Critical	Impact on majority of, or all information, applications and services or disruption of business-critical processes. Will require prompt incident response and escalation to Customer security leadership. Examples: Critical asset(s) impacted Critical business information exfiltration Disruption of critical network communications Confirmed Ransomware attack
Priority 2	High	Impact on widely used information, applications and services, or disruption of important business processes. May require timely incident response and escalation to Customer security leadership. Examples: Non-critical asset(s) impacted Possible business information exfiltration Disruption of network communications Possible Ransomware scenario
Priority 3	Medium	Impact on shared information, applications or services, with a limited group of users. May not require escalation to Customer's security team. Examples: Limited asset(s) impacted Limited business information exfiltration Limited network communication disruption Non-Ransomware Malware detection

Priority 4	Low	Impact limited to a single entity information, applications or services on a single end point. Does not require escalation to Customer's security team. Examples: Minimal asset(s) or information impacted Minimal network communication disruption Malware activities with low risk

1.5.11 **Near Real-Time Security Incidents.** When applicable, Verizon will implement Detection Content on the Security AP to create Security Incidents in near real time. All Detection Content are categorized to help: (i) increase insight into Security Incidents and, (ii) reduce the number of False Positive incidents. The incident descriptions provide recommendations on possible actions Customer can take to address the Security Incident.

1.5.12 **Non-Near Real Time Security Incidents.** When applicable, Verizon will implement Detection Content to find cyberthreat patterns over a longer period of time and to allow low confidence indicators to be analyzed more effectively. Security analysts will review these incidents periodically as a group of security information. If an incident or a combination of incidents is considered to be important, the Verizon SOC Analyst will escalate it. The VSOS SLA does not apply to non-near real time Security Alerts handling.

1.5.13 **Security Incident Escalation.** Verizon will only escalate Security Incidents that meet the Escalated Security Incident criteria established during the onboarding period. Verizon will examine the characteristics and context of the Security Alerts and Security Incidents, and evaluate the possible impact of a threat/attack before creating a Security Incident Ticket in the Ticketing System for escalation and routing to Customer's designated security contact. Verizon will provide additional information to support the investigation of a Security Incident and may propose possible recommendations for next actions. Customer will contract separately for any remedial efforts or mitigation activities Customer undertakes. Customer will report any Customer remediation action to Verizon. Customer will repair the integrity of affected applications and infrastructure for Data Sources.

1.5.14 **Security Incident Information.** When a Security Incident is escalated to the Customer's designated security contact, Verizon will notify the Customer via the agreed escalation path defined during onboarding and in the Ticketing System. Verizon will escalate a Security Incident Ticket with the following information:

- "5Ws + H" analysis including who, what, where, when, why, and how;
- Security Incident Ticket number;
- UTC timestamp of the Security Incident creation and the affected entity/entities; and,
- Detection Content ID, name, and description.

1.5.14.1 **Security Incident Information – VSOS Extended.** If Customer has ordered VSOS Extended, Verizon will also provide the following information for each Escalated Security Incident Ticket: (i) extended analysis of Security Incidents; (ii) historical Security Incident analysis, and (iii) additional Security Incident investigation and analysis in the Security AP.

1.5.15 **Detection Content Management.** Verizon may implement Detection Content from the Verizon Detection Content Library and from the Security AP vendor's standard Detection Content library as agreed with Customer in accordance with the Detection Content Development Process. Alternatively, Verizon can develop custom Detection Content per Customer's requirements if scoped by Verizon in an implementation statement of work. Verizon will provide recommendations to maintain and enhance the Detection Content in line with new Threats and changes in Customer's IT environment. Customer may receive notification that an update to Verizon's Threat Content is available. Customer and Verizon will discuss and determine the applicability of any change to Customer's IT environment and agreed changes implemented by Customer. If Customer wants to change any Detection Content, Customer will notify Verizon of any such proposed change at least 24 hours before such change is made. The amount of Detection Content management provided by Verizon as part of VSOS during the Service Commitment is based on Customer's anticipated number of Security Incidents per day as set forth in the Order unless an additional resource allocation is contracted from Verizon pursuant to an Order.

1.5.16 **Change Management, Detection Content Development, Response Action Content Development.** If Customer requires Detection Content or Response Action Content development and Customer purchases Verizon resources to support the effort, Verizon will work with Customer to develop such content. When required and Customer purchases Verizon resources to support the effort, Verizon will work with Customer to develop and document change management processes for Detection Content development, Response Action Content development, and major Security AP changes.

1.5.17 **Verizon-initiated Detection Content Changes.** Verizon may initiate Detection Content changes to Customer's Security AP in accordance with the agreed change management processes. Verizon may also initiate Detection Content changes to Customer's Security AP or disable Detection Content and disable Threat signatures under the following circumstances:

- Verizon witnesses or is notified of a significant security event including without limitation a massive attack of malware with the risk of a Security Incident Flood of Verizon's infrastructure, which may include the SOAR;
- Verizon notes a Security Incident Flood that may be caused by changes in Customer's technology environment or infrastructure including without limitation: (i) the Security AP for which the Detection Content and security detection rules on the Security AP have not been updated, (ii) the Ticketing System, (iii) rewiring or network cabling, addressing and routing, (iv) endpoint security or application control ("allow list" or "block list") configuration, (v) new application deployment, (vi) user account changes, or (vii) misconfigured Data Sources including devices;
- If changes to the Service Context submitted to Verizon are believed to influence the Detection Content. These changes may include adding, removing, or moving servers, adding new applications or web servers, and changes made to Detection Content by or on behalf of Customer.

1.5.18 **Reporting.** Verizon will provide the following reports to the Customer:

1.5.18.1 **Monthly Service Status and Trend Report for VSOS Standard and VSOS Extended.** This report will: (i) summarize trends related to Security Alerts and Security Incidents over the immediately preceding month; (ii) summarize Security Incident Tickets; (iii) review Threat Intelligence; and (iv) describe any significant changes to the overall VSOS, including Detection Content development. Verizon will deliver such report to Customer via email or an agreed file sharing mechanism and in accordance with the timing agreed with Customer.

1.5.18.2 **Weekly Service Status for VSOS Extended.** This report may: (i) summarize key observations, VSOS service issues, and daily Security Incident Tickets for the month; (ii) summarize significant VSOS service changes such as updates to the Escalation Matrix, or Security Alert schema, or incident handling processes made during the previous month; (iii) summarize significant Threat Intelligence; (iv) describe development of Detection Content during the preceding month; and (v) summarize key observations, recommendations and trend analysis. Verizon will deliver such report via email or an agreed file sharing mechanism and in accordance with the timing agreed with Customer.

1.5.18.3 **Custom Reporting.** Customers may purchase additional or customized reporting for an additional charge.

1.5.19 **Data Availability and Retention.** Customer agrees that Verizon may store and maintain a copy of

Customer's Security Incident and relevant event data that correlates to the particular Security Incident including without limitation source and destination IP addresses and any notes from Verizon's security analysts. Verizon may store data elements collected in the provision of VSOS for up to 365 days. At the end of the retention period, such data will be disposed of in accordance with the relevant Verizon asset classification and handling policy.

2. SUPPLEMENTAL TERMS

2.1 **Maximum Daily Ingested Security Incidents.** VSOS is contracted based on Customer's anticipated volume of Security Incidents generated by the Security AP and ingested in the SOAR that require triage by Verizon as such volume is set forth in an Order.

2.2 **Maximum Daily Ingested Security Incident Volume Overage and Charges.** If, on any single day Customer's actual Daily Ingested Security Incident Volume exceeds Customer's maximum Daily Security Incident volume as set forth in the applicable Order, Verizon will charge Customer the amount of any overage incurred.

2.3 Security AP and Ticketing System

2.3.1 **Maintenance and Maintenance Contracts.** Customer will, at its own expense, procure and maintain with each vendor adequate maintenance contracts and all licenses necessary to enable Verizon to properly perform the VSOS including for the Security AP and Ticketing System. Customer is responsible for maintaining and providing operational support for Customer's devices, software, and other assets within its environment including for the Security AP, Ticketing System, and Data Sources. Customer will provide Verizon reasonable prior notice of any maintenance including emergency, preventative, and corrective maintenance services. Verizon will provide Customer reasonable prior notice of any maintenance including emergency, preventative, and corrective maintenance services on the tools and software provided as part of VSOS including the SOAR. Verizon's service levels set forth in Section 3 will not apply during times of Customer or Verizon maintenance.

2.3.2 **Interoperability.** Customer acknowledges that modifications or changes to the Security AP, the Ticketing System, and any Data Sources including future releases to the operating software of the Security AP or Ticketing System or to the Customer environment may cause interoperability problems or an inability to transmit data to Verizon. Customer will give Verizon written notice of any modifications or changes within seven days before making any such changes or modifications and any impact to the Verizon services from such modifications or changes may result in additional charges via a change order. Customer will maintain the Customer environment to ensure interoperability with each Data Source, device, the Security AP, and the Ticketing System.

2.3.3 **Customer Responsibilities.** During the Service Commitment for VSOS, Customer must timely: (i) maintain its contract for (a) Security AP and Ticketing System licensing and implementation services with the applicable third party vendors and (b) provide Verizon secure access to the Security AP and Ticketing System for provision of Service; (ii) continue to provide Verizon a secure method to access the Security AP and Ticketing System through a connection to Verizon's SOAR; and (iii) continue to provide a secure method for delivering Data Sources to the Security AP instance, and maintain such access and secure Data Source delivery method for the duration of the Verizon Security Operations Service. Customer will resolve any interoperability problems such as with software versions, parsers, Security AP or Ticketing System within 48 hours after Verizon's written notice (email is acceptable). Customer will be responsible for maintaining the Security AP and Ticketing System (including the necessary licenses, required hardware, maintenance agreements, and necessary storage systems), and Customer's Data Sources including data collectors, virtual log collectors, and other such sources. Customer will notify the Verizon SSA in writing (email is acceptable) at least seven days prior to any changes to the Ticketing System, Security AP or Customer's related IT environment and any changes in the VSOS Services due to such changes will require a change order. Any delay or failure of

Customer or its third party suppliers to perform the responsibilities in this Section 2.3.3 could delay or impact Verizon's ability to provide the services herein, may result in additional charges via a change order, and Verizon is not responsible for any impacts on the services or schedule as a result of such delays or failures. Other than Verizon's responsibility for Verizon's SOAR, Customer is responsible for managing and maintaining any Data Sources, devices and applications in its environment including any patching.

2.3.4 **Third Party Warranties.** For any third party products and/or services incorporated as part of VSOS, Customer will receive only the warranties offered by such third party either directly to Customer or to the extent Verizon may pass through such warranties to Customer.

2.3.5 **Third Party Products or Services.** Verizon is not liable for any damages caused by hardware, software, or other products or services furnished by parties other than Verizon, its agents, subcontractors, or any damages caused by the products and/or services delivered by or on behalf of Verizon which have been modified, serviced, or otherwise attended to by parties other than Verizon or without Verizon's prior written and express consent. Customer acknowledges that Verizon will not be liable for any damages resulting, directly or indirectly, from any act or failure to act by Customer or any third party including, without limitation, any failure to perform Customer responsibilities, any disconnection to Verizon's systems including the SOAR or the non-performance, defaults, omissions or negligence of any third party that provides telecommunications services in the country or countries in which Customer's premises or systems are situated and other countries from, across, to or in respect which VSOS is provided by or on behalf of Verizon.

2.3.6 **Protected Health Information.** VSOS is implemented without specific controls that may generally be required or customary for customers in any particular industry and is not designed to satisfy any specific legal obligations. Customer agrees to use VSOS in accordance with all applicable laws and not to use VSOS in any manner that imposes obligations on Verizon under any laws other than those laws with which Verizon agrees to comply as specifically set forth in the Agreement. Without limiting the generality of the foregoing, Customer agrees not to cause, or otherwise request that Verizon create, receive, maintain or transmit protected health information (as defined at 45 C.F.R. § 160.103) for or on behalf of Customer in connection with VSOS or in any manner that would make Verizon a business associate (as defined at 45 C.F.R. § 160.103) to Customer. In the event Customer acts or uses VSOS in a manner not permitted under this Section 2.4.6, Customer shall (i) take, at Customer's expense, prompt action to correct and/or mitigate the effects of Customer's breach of this Section 2.3.6; and (ii) provide Verizon with cooperation and support in connection with Verizon's response to Customer's breach of this Section 2.3.6. Customer shall assume and be solely responsible for any reporting requirements under law or contract arising from Customer's breach of this Section 2.3.6.

2.3.7 **Industry Alerts and Third Party Updates and Patches.** With regard to services which provide information sharing and/or industry alerts, Verizon disclaims any liability to Customer, and Customer assumes the entire risk for: (i) information from third parties provided to Customer which to the best of Verizon's information, knowledge and belief did not contain false, misleading, inaccurate or infringing information; (ii) Customer's actions or failure to act in reliance on any information furnished as part of VSOS; and/or (iii) the use of any third party links, patches, updates, upgrades, enhancements, new releases, new versions or any other remedy suggested by any third party as part of VSOS.

2.3.8 **Restriction on Encryption Functionality in India.** Prior to connecting any encryption equipment to Verizon Facilities in India, Customer must obtain prior evaluation and approval from the relevant telecom authority.

2.3.9 **Translations.** Any translation of any part of the services provided hereunder such as reports and escalations into a language other than English will be provided by Verizon using a third party product and may not be accurately translated due to limitations of such translation software. Some translated words may be incorrect and any inconsistencies or differences in the translations will not be legally binding and will have no legal effect for compliance or enforcement purposes. Some content such as images may not translate accurately. Such translations will be sent together with the original English reports or escalations and the English versions shall prevail in the event of any inconsistencies. Verizon provides no warranty and will have no responsibility or liability for incorrect, inconsistent, incorrect or missed translations.

3. **SERVICE LEVEL AGREEMENT (SLA).** The SLA for VSOS may be found by clicking on the following URL: www.verizon.com/business/service_guide/reg/cp-vsos-sla.pdf.

4. **FINANCIAL TERMS**

4.1 **Service Commitment.** The VSOS Service Commitment is for a one year, two year or, three year Service Commitment as shown on the Order. The billing period for VSOS will commence on the Ready For Operations date. At the end of a Service Commitment, this Service Attachment and the Agreement will continue until either Party terminates upon 60 days' prior written notice.

4.2 **Rates and Charges.** Customer will pay the non-recurring charges (NRCs) and monthly recurring charges (MRCs) as set forth in an Order. Unless expressly indicated otherwise, the initial MRCs will be invoiced upon the Ready For Operations date. Unless expressly indicated otherwise, all NRCs will be invoiced upon the Commencement Date.

5. **DEFINITIONS.** The following definitions apply to VSOS, in addition to those identified in the Master Terms of your Agreement.

Terms	Definitions
8x5	8 hours a day, 5 days a week, Monday through Friday in the time zone of the Verizon resource and excluding public holidays.
24x7	24 hours a day, 7 days a week, 365 or 366 days a year, independent of time zones and local or international public holidays.
Applicable Rates	The rates that apply for work not covered under this Service Attachment. All such work is subject to the execution of a separate written agreement that describes the activities and the Applicable Rates for performing such work.
CMDB	A configuration management database is an ITIL term for a database used by an organization to store information about hardware and software assets.
Contextual Information	Customer provided additional information that, where available, originates from sources in the IT environment, inside or outside the Customer other than the event data itself and enriches the information contained in the event data that is added to transform "raw" Data into actionable information. Examples include: DNS: Map addresses to names IAM: Map user names to user identities Geo-location: Show the physical location of the system

	Vulnerability assessment information CMDB
Correlation Rule	The actual technical implementation of Use Case Scenarios on the Security AP.
Customer Context	A set of background, framework and situational information regarding a customer such as asset details, asset owner/custodian, asset criticality, Vulnerability details and business impact tolerance that Verizon will use to enhance Detection Content, alerting and analytics.
Daily Ingested Security Incident Volume	The total cumulative Security Incidents generated per day (24-hour period measured from 00:00 to 23:59 UTC for Global SOC model and for the relevant time zone for regional SOC models in USA, Australia, EU) from Security AP and ingested into Verizon's SOAR that require triage by Verizon.
Data Source	A source of Security Events sent to the Security AP from a variety of inputs such as security infrastructure, IT infrastructure, business applications, and other sources from Customer's business.
Detection Content	Content created on the Security AP that generates alerts based upon logic and the correlation of Security Events.
Detection Content Development Process	Process for how Detection Content will be developed as such process is agreed in writing by Customer and Verizon during onboarding and may be revised in writing by the Parties.
Detection Content Tuning	Process of working to reduce False Positives, correlating Security Events and trends and working with Security Alerts to enhance accuracy.
Escalated Security Incident	An occurrence of a Security Incident within the Security AP that has been subjected to an investigation and triage process by Verizon security analysts and has been determined to require further action to be taken and involvement from Customer.
Escalation Matrix	A table that intersects operational and logistical components with a set of escalation levels and time limits and provides a mutually established process for Security Incident escalations and illustrates key points of contacts for each escalation level.
Exploit	A method for using a Vulnerability to gain unauthorized access to functions, data, or privileges with malicious intent that can include a script, virus, trojan, or a worm.

False Positive	A Security Incident triggered by legitimate Detection Content but deemed to be a benign event. Detection Content Tuning may be required to reduce the number of benign events.
HMM1	Hunting Maturity Model is a model for evaluating an organization's cyber threat hunting capability. HMM1, or HMM1 – Minimal, means basic threat intelligence capability is integrated into automated alerting, basic data collection from key infrastructure points, and identification of the simplest indicators of compromise (IOCs) such as domains, hashes, and URLs.
Information Technology Infrastructure Library (ITIL)	A set of practices and a framework for IT activities such as IT service management (ITSM) and IT asset management that focus on aligning IT services with the needs of the business, was designed to allow organizations to establish a baseline, and is used to demonstrate compliance and measure improvements. ITIL describes processes, procedures, tasks, and checklists which are neither organization-specific nor technology-specific.
Response Action	An action initiated by the SOC analyst, Security AP or SOAR based upon the investigation of a Security Incident.
Response Action Content	Automations, scripts and playbooks to effect a Response Action.
Ready For Operations	The date provided by Verizon for each Security AP when the earlier of either: (i) Verizon has notified Customer that it has completed onboarding Customer to the Verizon Security Operations Service, or (ii) Verizon begins to provide VSOS to Customer. The SLA is effective as of this date.
Security Alert	The correlation of Security Events by a security system that may result in a potential impact to the confidentiality, availability or integrity of an information system.
Security AP	Supported security analytics platforms provided by Customer that have been approved by Verizon for security monitoring, which includes Splunk Enterprise Security, IBM QRadar, Microsoft Sentinel or other security analytics platforms approved in writing by Verizon.
Security Event	Any observable occurrence within an information system that is captured and has a potential bearing on the confidentiality, availability or integrity of such system.
Security Incident	An occurrence within a customer security analytics platform that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or

	transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies, requiring Verizon security analysts to investigate, triage and derive a determination as to the validity and criticality of the occurrence. Security Alerts and Security Events are usually correlated to generate such an incident.
Security Incident Flood	The occurrence of 30 or more Security Incidents within a 60-minute period.
Security Incident Ticket	A ticket raised to Customer by a Verizon security analyst to alert Customer of a Security Incident that requires Customer's attention or a ticket raised by Verizon to escalate a Security Incident to Customer.
Service Context	A set of documents with version control, collected by Verizon from Customer during onboarding, retained by Verizon, and updated from time to time upon prior written notice (email is acceptable) to Verizon that contains information about Customer that Verizon will use to provide the Verizon Security Operations Service.
SLA (Service Level Agreement)	The specific service levels and terms and conditions for Verizon's performance of the Verizon Security Operations Service, and Customer's receipt of service credits if Verizon fails to meet a SLA as set forth in such agreement.
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system Vulnerability.
Threat Content	Content such as a Threat feed, responses from a sandbox, etc. and that is consumed by either Detection Content or Response Content.
Threat Intelligence	Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes.
Ticketing System	Customer's IT service management platform to track Security Events and Security Incidents with 24x7x366 accessibility provided by Customer to Verizon to access and use for automating ticket interactions in performance of the Verizon Security Operation Services.
Use Case	Functional description of the activities to be monitored, the systems and actors involved and the Use Case Scenarios required to perform an action on monitored behavior (alerting and/or reporting), such as user behavior monitoring, malware detection, confidential data monitoring.

Use Case Scenario	A technical description of the interaction activities to be monitored between systems and actors, including the conditions that an event or Correlation Rule(s) result must match to generate a Security Alert, indicating a potential security risk or Threat to the systems such as 5 failed logins followed by a successful login.
UTC	Coordinated Universal Time: Universal time indication standardized by the Bureau International des Poids et Measures (BIPM) and defined in CCIR Recommendation 460-4. The UTC is the time indicated on atomic clocks. Verizon consults and uses it for its Sacs via the Internet protocol NTP. The UTC code uses the 24-hour clock (e.g., 4 pm (afternoon) is equal to 16:00 UTC).
Verizon Detection Content Library	Detection Content curated by Verizon as part of the standard VSOS offering and leveraged by VSOS customers during the provision of the Verizon services hereunder as relevant and required by the Verizon Security Operations Service.
Vulnerability	A weakness or defect that can be exploited to gain access to data, functions, or privileges violating the intended authorization and can range from defects in: (i) an application or system software such as bugs; (ii) the user administration such as non-protected user accounts, (iii) the configuration including unintended network or file access, or (iv) the policy and rule set definition such as unrestricted open ports or exposed Internet Protocol addresses.