PROFESSIONAL SERVICES
RAPID RESPONSE RETAINER
STATEMENT OF WORK
TO VERIZON PROFESSIONAL SERVICES SERVICE ATTACHMENT

This Statement of Work (SOW) is entered into between the entities identified as, respectively, Verizon and Customer in the related Service Order (SOF).

1. PROJECT DESCRIPTION

1.1 **General Scope of Work.** Verizon's Rapid Response Retainer service helps prepare for, reduce the response time of, reduce the impact of, and respond more effectively to a cybersecurity incident. The core of the Rapid Response Retainer provides response capabilities, including retained hours to use on assessments, health checks or incident response planning. The Rapid Response Retainer core service can be enhanced with Add-on capabilities which provide investigators with tools and means for even more effective and immediate access to data when an incident occurs. Verizon will provide Customer with the Rapid Response Retainer core services, and any of the Add-on capabilities indicated on the SOF.

1.2 **Rapid Response Retainer – Core Service.** The Rapid Response Retainer core service includes certain activities that utilize security consulting support hours (Hours) as requested by Customer using the Engagement Letter process, each described below.

1.2.1 **Onboarding.** Within 10 days of the commencement of a Service Commitment, Verizon will send an email to Customer's point of contact (POC) requesting a date and time for a Rapid Response Retainer onboarding discussion. Onboarding will take place either in person, or via a conference call between Customer and Verizon. During the Onboarding session, Verizon will: (i) collect Customer contact information, (ii) collect the list of countries where Customer may need Services (as provided in the Project Delivery Countries section below) (the Country List); and (iii) collect any information required from Customer for registration into the Services which will include information required by any core services or Add-on capabilities ordered. Onboarding also includes:

- Review of Service components and the Engagement Letter process for requesting Services for a Project.
- Name of the Verizon designated investigative liaison contact, each as further described below.
- Escalation processes for Emergency Services.
- Customer selection of one Cyber Incident Capability Assessment (Annual Assessment) per twelve month period during the Service Commitment from the four available Annual Assessment options and requested schedule for delivery of the Annual Assessment. Verizon and Customer will agree on a time and location for the Annual Assessment. Following Onboarding, Verizon will forward Customer an Engagement Letter for Customer's execution containing the name of the Annual Assessment selected and agreed upon schedule.
- Network Sensor(s) deployment instructions.

Once the Onboarding process is complete, Customer will be able to order additional Services in addition to the Annual Assessment via the Project initiation process described below.

1.2.2 **Security Consulting Support.** Following Onboarding, Customer may order any of the Services described in this SOW or as described at the link shown below (the Professional Services Terms Link). The ordered Services will be provided with the number of Hours stated in an Engagement Letter. Customer may pre-purchase Hours at a discounted rate. Pre-purchased Hours must be used during the Service Commitment and will expire at the end of the Service Commitment term. The hourly rates for the Hours are shown in the SOF.

- Professional Services Terms Link:

https://enterprise.verizon.com/service_guide/reg/ps-plus-toc-2021MAR01.htm

1.2.3 **Project Initiation Process (Engagement Letters).** After the Onboarding process is complete, when Customer wishes to request additional Services, Customer will contact the Verizon by calling the Hotline, and initiate the Service via an Engagement Letter. The scope of each Engagement Letter will be agreed upon on a case-by-case basis. When Customer orders a Project, Verizon will provide an Engagement Letter that describes the Project requested, methodologies to be used in performance of the requested Project, the hourly rate to be used from the Customer SOF, and for non-Emergency Services, the number of Hours required to complete the requested Project that is developed on a call with Customer. All Engagement Letters will be in writing and follow the template shown at the Professional Services Terms Link. Customer must sign the Engagement Letter prior to any Project being performed. The signed Engagement Letter will become part of the Agreement. Any changes to an Engagement Letter require an amended and executed Engagement Letter. In the event of a conflict between the terms and conditions of the Agreement, the order of precedence shall be: the SOF, the Master Terms, the PSA, the SOW, and then the Engagement Letter.

1.2.4 **Cyber Incident Capability Assessments.** An Engagement Letter is required for an Annual Assessment. Rapid Response Retainer core service includes a choice of one of the Annual Assessments listed below, to be delivered during each twelve month period (Contract Year) of the Service Commitment, which Customer may choose during the Onboarding session or during subsequent discussions, as part of the Rapid Response Retainer core service. Customer may choose additional assessments using Hours as required by such assessment. If Customer does not want one of the four available Annual Assessments as part of the core service, Customer may request an alternate Service (as offered pursuant to this SOW), equivalent to no more than 40 Hours of support. The Annual Assessment choice is available for selection during the relevant Contract Year and must be ordered by Customer within 90 days of the end of the Service Commitment term. Annual Assessments expire at the end of the Service Commitment term. The Annual Assessment may be rescheduled or delayed for Emergency Services. The Engagement Letter will describe the specific scope and Deliverables for each of the Annual Assessment options below. The Annual Assessments choices below are described at the Professional Services Terms Link.

- Executive Breach Simulation;
- Cybersecurity First Responders Training Course;
- Incident Response Plan Assessment; or
- Network Health Checks.

1.2.5 **Network Sensors.** Verizon will work with Customer to deploy up to two lightweight software sensors (Network Sensors) in Customer's environment. These Network Sensors can be deployed on existing Customer hardware or as a virtual machine that is running a supported Linux-based operating system. Verizon does not supply hardware as part of this service. The Network Sensors are configurable to enable Verizon to collect, filter, and analyze network data. During Onboarding, Verizon will work with Customer to select the areas where the Network Sensor(s) will be deployed in the Customer environment and will be configured to capture a set amount of traffic based on the company size, after which the Network Sensors will be put into a passive mode until required for use during an Project pursuant to an Engagement Letter. Additional support beyond reasonable installation and maintenance of the deployed instances of the Network Sensor(s) on Customer's network may require the use of Hours, which can be ordered pursuant to an Engagement Letter at the hourly rate identified in the SOF (rate for VTRAC Services). In the event Verizon is engaged to provide Emergency Services, Verizon will leverage network data captured by the Network Sensor(s) to perform deep packet inspection locally, applying a capture policy to the traffic, and then encrypting, compressing and streaming it back to the Verizon's cloud platform for analysis. The Verizon cloud platform does not perform SSL (Secure Sockets Layer) decryption. Network Sensors capture network packet data transmitted on a network with no encryption. Customer may also request Verizon conduct unique, periodic, or one-off analysis leveraging the Network Sensor(s). Scope and pricing for analysis requests will be outlined in an Engagement Letter and provided pursuant to the hourly rates identified in the SOF (rate for VTRAC Services).

1.2.6 **Incident Response Hotline Access.** Verizon will provide a toll-free telephonic support number that is available 24x7x365 (Hotline). The Hotline is to be used by Customer when Customer has a security incident and requires Rapid Response Retainer support. Upon calling the Hotline, a Verizon representative will log the Customer's information and reason for the call, and will engage the next level of phone support.

1.2.7 **Investigative Team Phone Support / Remote Support.** When Customer calls the Hotline, with a suspected security incident, a member of Verizon's investigative team will return the Customer's call within the three hour SLA to get more information related to the security incident. If the call requires a Project to be initiated, the investigative response team member will define the scope of the Project in an Engagement Letter and schedule the Project for delivery as required.

1.2.8 **Investigative Liaison.** Verizon will provide an investigative liaison (Liaison) who will provide Customer with a consistent interface to Verizon's investigative response team. The Liaison will serve as a contact point for non-emergency response questions or issues regarding the Rapid Response Retainer service, and in some cases may directly contribute to the delivery of Services for Customer's reactive emergency response and proactive incident response consulting engagements.

1.2.9 **Intelligence Summaries.** Verizon will email Customer POCs with Verizon's research, investigations, solutions, and knowledge intelligence, which may include communications, such as weekly intelligence summaries and monthly intelligence briefings (phone and web conference).

1.2.10 **Project Management.** Verizon will be responsible for managing the Project change control process. Should the Project's requirements change during the course of a Project, Verizon will ensure that any modifications to scope, budgeted number of Hours and schedule are appropriately documented in an amended Engagement Letter.

1.3 **Rapid Response Retainer – Emergency Services**

1.3.1 **Emergency Services.** An Engagement Letter is required for Emergency Services and uses Hours as applicable.

1.3.1.1 **On Site Response with In-Transit SLA.** When the Parties agree that a member of Verizon's investigative response team must travel to a Customer Site, the Verizon investigative response team member will be "in-transit" to the Customer Site within 24 hours of (a) Customer's execution of the Engagement Letter and (b) Verizon's procurement of all required travel documentation and Customer's approval if required. "In-transit" means the investigative response team member is traveling to the Customer Site. The in-transit SLA clock begins when (a) and (b) are both complete and stops when the investigative response team member is in-transit. Verizon's investigative response phone support is available while the investigative response team member is in-transit.

1.3.1.2 **Emergency Services Phases.** Emergency Services are provided in 2 phases, Incident Response and Forensic Analysis, as described in more detail at the Professional Services Terms Link. Customer and Verizon will determine which of the phases are required for an Emergency Services Project.

1.3.2 **Malcode Analysis.** An Engagement Letter is required for Malcode Analysis and uses Hours as applicable. Malcode Analysis provides analysis of files that Customer suspects might be malicious. Malcode Analysis is described in more detail at the Professional Services Terms Link.

1.3.2.1 **Malcode Analysis SLA.** Within 24 hours of receipt of a signed Engagement Letter and Customer's suspect files received at the Verizon server, Verizon will perform an analysis of the files and provide Customer with the Malcode Analysis Report. If additional analysis is required after the first 24 hours, Verizon will continue with the service as described in the Engagement Letter.

1.4 **Rapid Response Retainer – Add-on Capability.** As an enhancement to the Rapid Response Retainer core services, Customer may order any of the following Add-on capabilities in the SOF. Each Add-on capability below is described at the Professional Services Terms Link.

- Network Telemetry Analysis;
- Dark Web Hunting;
- Endpoint Telemetry Analysis;
- Backbone NetFlow Collection.

2. SUPPLEMENTAL TERMS

2.1 **Service Commitment.** The Service Commitment is for a 12 month term, 24 month term, or, 36 month term, as identified on the SOF.

2.2 **Service Level Agreement Terms.** The Services listed below have SLAs. If Verizon fails to meet the respective SLA, Customer's sole and exclusive remedy shall be a credit of an additional five Hours of security consulting support, which may be used within Service Commitment term. An SLA remedy will be documented in an Engagement Letter showing the increase in the Hours at no additional cost to Customer. The SLAs are described above for the following Services:

- Investigative Team Phone Support / Remote Support;
- Emergency Services On Site In-Transit SLA;
- Malcode Analysis SLA.

2.2.1 **SLA Conditions.** The following conditions apply to SLAs:

- No SLA remedy will be due to the extent the SLA is not met because of any act or omission on the part of Customer, its contractors or vendors, or any other entity over which Customer exercises control or has the right to exercise control.
- No SLA remedy will be due to the extent the SLA is not met because of a Force Majeure Event, as defined in the Agreement.
- No SLA remedy will be due to the extent the SLA is not met because of the amount of time delays caused by incorrect or incomplete information provided by Customer.

2.3 **Customer Obligations**

2.3.1 **Customer IP Consents, Representations and Warranties.** Customer consents to Verizon's scanning and monitoring of Customer IP (CIP) and associated network components, the collection, use, processing, analysis and disclosure to Customer POCs Customer's Internet traffic data, and the use of threat intelligence pertaining to CIP in an aggregated and anonymized form with Verizon's portfolio of security services. Customer represents and warrants that: (i) the Customer provided list of CIP addresses contains only IP addresses assigned or allocated for the exclusive use of Customer and/or Customer Affiliates over which Customer has control; and (ii) Customer has all legally required consents/permissions from CIP users for Verizon's performance of the Service. For Services that include a network sensor, Customer understands that the network sensor will collect, analyze and provide reporting on data packets, traversing Customer's network to which such network sensor is attached.

2.3.2 **Project Delivery Countries.** Verizon will only perform Services in the countries listed in the Country List provided by Customer during initial Onboarding.

2.3.3 **Projects Delivered in India.** Professional Services performed for Customer locations in India shall be ordered separately with Verizon Communications India Private Limited. All Hours incurred in India shall be invoiced by Verizon Communications India Private Limited directly to Customer, pursuant to the terms of a Rapid Response Retainer India Service Order Form, which can be found at the Professional Services Terms Link. Any Hours, or SLA Hours, included in this SOW, if any, will not be available for use in India.

2.3.4 **Customer Notices.** Unless otherwise required (e.g., by Payment Card Industry requirements), Customer is responsible for the collection and dissemination of all information regarding an incident and

Rapid Response Retainer service does not include nor provide notification services.

2.3.5 **Payment Card Industry Project.** If a Service involves data that is subject to the Payment Card Industry (PCI) Security Standards Council (the PCI Council) requirements, Verizon shall have the right to disclose the results of the Services (including any report of compliance, working papers, notes and other information) to the PCI Council and other parties as required under the PCI Forensic Investigator (PFI) Program Guide and the qualified security assessor (QSA) Validation Requirements (Supplement for PCI Forensic Investigators) promulgated by the PCI Council. Copies of the PCI Council's current standard PCI Forensic Investigator Program Guide and QSA Validation Requirements (Supplement for PCI Forensic Investigators) are available on the PCI Council's website (see www.pcisecuritystandards.org).

2.3.6 **Recommendations.** Customer is responsible for the decision to implement (or not to implement) any recommendations. Verizon is not responsible for the results achieved from any Customer implementation.

3. FINANCIAL TERMS

3.1. **Rates and Charges.** Customer will pay an annual recurring charge as set forth in the SOF. Travel and expenses will be billed as provided in the PSSA, this SOW, and the SOF.

3.2. **Project Charges.** For additional Projects or Services provisioned under this SOW, Customer will be invoiced on a time and material basis at the rate identified on the Engagement Letter, and at the rates listed in the SOF.