Rapid Response Retainer Professional Service Description
Add-on Capability: Network Telemetry Analysis

This service description describes Network Telemetry Analysis, which may be selected as an Add-on Capability pursuant to the Rapid Response Retainer base program (see Rapid Response Retainer Statement of Work), and included in a SOF.

1. **SERVICE DESCRIPTION.** Verizon will leverage tools that provide network threat detection, and full-packet forensics for enterprise, cloud, or industrial environments. The Network Telemetry Analysis tool enables retention of network packet data (Network Data) which can be analyzed using various detection techniques, including threat intelligence, signatures, and behavioral/anomaly classifiers. Network Data may include any technical data and related information about the Customer environment, including, but not limited to the operating system type and version; network host data; origin and nature of malware, endpoint GUID's (globally unique identifiers); Internet Protocol (IP) addresses; MAC addresses; log files; network configurations; network security policies; information related to the usage, origin of use, traffic patterns, and behavior of the users on a network; and any aggregate, demographic or network traffic data. Verizon will leverage Network Sensors installed locally on a Customer's network or cloud environment to passively capture Network Data and stream to the Verizon platform for analysis, threat detection, and correlation of threats, and to create a forensic memory of the Network Data for a thirty day retention period. Verizon will use this tool to have visibility into Network Data for impact analysis, investigation, and response. The Network Telemetry Analysis Add-on, is available in four sizes, and Customer will order the annual license coverage option, based on the number of employees in the Customer's company, as detailed on the SOF. Size options for license coverage include:
   - Option 1: Up to 2,500 employees (includes 2 sensors) / Up to 25 Mbps of network traffic;
   - Option 2: 2,501- 10,000 employees (includes 2 sensors) / Up to 50 Mbps of network traffic;
   - Option 3: 10,001-50,000 employees (includes 2 sensors) / Up to 100 Mbps of network traffic; or
   - Option 4: 50,001+ employees (includes 2 sensors) / Up to 500 Mbps of network traffic.

1.1 **Services.** When ordered as an Add-on capability to the Rapid Response Retainer, Network Telemetry Analysis will allow Verizon to perform the following services:

1.1.1 **Monthly Analysis.** Leveraging Customer's network traffic collected by the deployed Network Sensors, Verizon will conduct a monthly analysis of the captured packet data. Verizon's analysis will include high level operational and security observations designed to help Customer be more attuned to the organization's security posture, and identify potential C2 (command and control) communications, indicators of compromise, and other suspicious or potentially malicious activity. After performing the analysis, Verizon will email the Customer a written report of findings. Verizon will promptly report critical findings via the communication method established during Rapid Response Retainer Onboarding. All monthly analysis activities will be performed during Business Hours and on a schedule agreed to by Verizon and Customer.

1.1.2 **Reactive Analysis.** In the event Verizon is engaged pursuant to the Rapid Response Retainer to provide Emergency Services, Verizon will leverage Network Data captured by the Network Sensor, 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. If necessary, Verizon will work with Customer to place the Network Sensor, to update the capture profile, to capture additional data or additional network segments for up to 30 days, enabling rapid access to full packet forensics to aid in the investigation. Additional collection of Network Data beyond 30 days will result in additional fees. The platform does not perform SSL (Secure Sockets Layer) decryption. Sensors capture network packet data transmitted on a network with no encryption.

1.1.3 **Custom Analysis.** Customer may request Verizon conduct unique, periodic, or one-off analysis (custom engagement) leveraging the deployed sensor(s). Scope and pricing for custom analysis requests will be

outlined in an Engagement Letter and provided pursuant to the hourly rates identified in the Rapid Response Retainer SOF (rate for RISK Services).

1.2 **Network Sensors.** Up to two lightweight software sensors (Network Sensors) will be provided to Customer to deploy in the Customer environment. A Network Sensor is a Linux software package that captures Network Data from the Customer environment, optimizes, encrypts and transmits data back to the Verizon platform. Sensors are deployed passively off a SPAN/Tap or Mirror port from a network or tap aggregation device within the Customer environment. These sensors can be deployed on existing hardware or as a virtual machine that is running a support Linux based operating system. The Network Sensors are configurable appliances that enable Verizon to collect, filter, and analyze Network Data. Verizon will work with the Customer to select the areas that the Network Sensors will be installed in the Customer environment and will be configured to capture a set amount of traffic based on company size and package option determined on the SOF. Customer can order additional Network Sensors separately. Hardware is not included as part of this Service. Network Sensors can only be deployed in countries provided to Customer during Onboarding. Additional support beyond reasonable installation and maintenance of the deployed instances of the Network Sensor(s) on Customer's network may require additional hours, which can be ordered by an Engagement Letter at the hourly rate identified in the Rapid Response Retainer SOF (rate for RISK Services).

1.3 **Data and Data Retention.** Verizon will store collected Customer Network Data for a thirty (30) day retention period. Standard retention periods are on a rolling basis and the Customer Network Data stored is the most recently captured for the retention period selected. Customer Network Data is automatically deleted when it exceeds the thirty day data retention period.

2. **DELIVERABLES AND DOCUMENTATION.** Any Deliverables provided by Verizon are intended for Customer and Verizon use only. Customer may disclose a Deliverable to a third party pursuant to the confidentiality terms of the Agreement. Verizon will provide a Monthly Report and deliverables as described in an Engagement Letter.

3. **CONDITIONS.** Delivery of the Services by Verizon is predicated on the following conditions:
   - Customer is responsible for assisting Verizon in the deployment of the Network Sensor, by providing hardware or a virtual machine that is running a supported Linux based operating system, and ensuring Customer's local networking team is available.
   - **Interoperability.** Where applicable, Customer acknowledges that modifications or changes to the Customer environment may cause interoperability problems, inability to transmit Network Data to Verizon, or malfunctions of the Network Sensor. Customer will give Verizon written notice of any modifications or changes within five Business Days after making any such changes. Customer acknowledges that it is Customer's responsibility to maintain, at its sole cost and expense, the Customer environment to ensure that the Customer environment is interoperable with the Service.