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

This service description describes Endpoint 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 deploy an endpoint console (powered by Tanium), on an Amazon Web Services (AWS) instance in the Verizon intelligence lab, and will utilize it for Customer's endpoints. Customer will order annual license coverage for up to 5,000 Customer endpoints, and in increments of 1,000 Customer endpoints over 5,000 as specified on the SOF. Verizon will work with Customer to gather all necessary information required to deploy the Tanium agents on Customer endpoints, and confirm whether or not Customer has purchased enough licenses to cover Customer's entire endpoint environment. When ordered as an Add-on capability to the Rapid Response Retainer, and once licenses have been enabled, Endpoint Telemetry Analysis will allow Verizon to perform the following services:

1.1 **Monthly Endpoint Analysis.** Leveraging the Tanium agents and the data retrieved from Customer endpoints, Verizon will conduct a monthly endpoint analysis. 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 potentially identify other suspicious or malicious activity based on periodic checks for indicators of compromise and threat actor tactics, techniques, and procedures. 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.

1.2 **Reactive Analysis.** In the event Verizon is engaged pursuant to the Rapid Response Retainer to provide Emergency Services, Verizon can leverage the endpoint console to remotely conduct forensic investigations on suspicious machines by reviewing historical and current state data. Verizon can utilize the Tanium agents, to scope a suspected incident by performing searches of the Customer's endpoints. Verizon can also remotely quarantine compromised Customer machines or take targeted remediation actions, such as: kill malicious processes, capture files, deploy patches, repair registry keys, apply configuration updates, uninstall applications, close unauthorized connections, and more.

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).

1.4 **Endpoint Telemetry Analysis SLA.** Verizon will begin remote forensic investigative support leveraging data retrieved from Customer endpoints, within six hours of receipt of a Customer signed Engagement Letter (pursuant to the SOW section 1.2.3 Project Initiation Process) requesting assistance. This SLA will only apply in the event Customer has ordered enough licenses to cover Customer's entire endpoint environment, and all assets have been installed on Customer's entire endpoint environment. This reduced response times will not apply, in the event Customer has not met the requirements contained in this section.

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 solely responsible for providing the operating systems (Windows, *nix, Mac, etc.) in the target environment, and to be responsible for pushing and installing the client.

- Customer is responsible for purchasing enough licenses to cover Customer’s full endpoint estate in order for the Endpoint Telemetry Analysis SLA to be valid.
- Additional support beyond reasonable installation and maintenance of the deployed instances of Tanium on Customer's endpoints may require additional hours, which can be ordered by an Engagement Letter at the hourly rate identified in the SOF.