Verizon Threat Intelligence Platform Service (VTIPS) Professional Service Description
Malcode Analysis

1 Scope of Work.

1.1 **Malcode Analysis.** (Uses Hours as Required)

1.1.1 An Engagement Letter is required for malcode analysis.

1.1.2 Malcode analysis provides analysis of files that Customer suspects might be malicious. Malcode analysis is limited as described herein and does not replace an Emergency Services forensic analysis. All files uploaded for malcode analysis must be isolated as individual files and may not be uploaded as part of a memory dump or network capture. Verizon will analyze no more than one file per 24-hour period.

1.1.3 Customer will upload malicious or suspicious files to the Verizon server for analysis. Instructions on how to upload files to the Verizon server will be provided to the Customer during the Onboarding session.

1.1.4 **Analysis.** Malcode analysis will typically focus on the interactions of the malcode with Customer's system. Verizon will attempt to determine the functionalities of suspected malicious files. Depending on the nature of the suspected malware functionality, the analysis may include identification of communication channels, a listing of indicators of compromise, and malware response guidelines. Malcode analysis may include the following, as determined by Verizon:

1.1.4.1 Code anatomy, which provides an overview of the malware binary content;

1.1.4.2 Behavioral analysis, which is a high level overview of the malcode's functioning with the objective of assisting in identifying system changes caused by the malcode and/or communication channels (e.g., IP addresses and domain names) utilized by the malcode; and

1.1.4.3 Malware intelligence analysis, which leverages Verizon's intelligence datasets to determine if the malware is already known and/or affiliated with known incidents or actors.

1.1.5 **Report.** Verizon will issue a report at the end of the analysis of the submitted code sample ("Malcode Analysis Report"), which will contain any identified findings, indicators of compromise and recommendations for additional analysis.

1.1.6 **Malcode Analysis SLA.** Within 24 hours of receipt of a signed Engagement Letter and Customer's suspect files 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.

2. **Deliverables and Documentation to be produced by Verizon.** Any Deliverables are intended for Customer and Verizon use only. Customer may disclose a Deliverable to a third party pursuant to the Agreement's confidentiality terms. Verizon will provide:

2.1 Malcode Analysis Report