Verizon Threat Intelligence Platform Service (VTIPS) Professional Service Description

Incident Analytics

1. Scope of Work.

1.1 **Incident Analytics Service.** Verizon will assist Customer with Customer's collection, classification and analysis of Customer's security incidents ("Incident Data") in accordance with the vocabulary for event recording and incident sharing ("VERIS") framework. VERIS is an industry standard framework designed to provide a common language for describing security incidents in a structured and repeatable manner. More information can be found at http://veriscommunity.net/index.html.

Verizon will provide support to Customer as follows:

1.1.1 Verizon VERIS Framework Implementation Support and Training

1.1.1.1. Verizon will assist with the development of Customer's plan to implement the VERIS framework so that Customer can gather and analyze Incident Data collected from Customer's security incidents. Verizon will subsequently assist Customer with incorporating VERIS into Customer's existing investigative response ("IR") tools and processes. To achieve this, Verizon will meet with Customer stakeholders to:

1.1.1.1.1 obtain an overview of Customer's current IR tracking process;

1.1.1.1.2 understand Customer Incident Data points that are currently being tracked;

1.1.1.1.3 gather information on how the VERIS framework might be incorporated;

1.1.1.1.4 identify potential roadblocks that may be encountered and identify where Customer Incident Data will be collected from;

1.1.1.1.5 determine the number of Customer business groups or departments that will need to be included in the classifications; and

1.1.1.1.6 determine how many Customer Incident Data sources or processes there are within Customer's organization.

1.1.1.2 Following collection of the information, Verizon will then provide training to Customer to aid understanding of how to implement the VERIS framework into Customer's organization. The training will provide an overview of the VERIS framework, both conceptually and in practice. Verizon will deliver this training to Customer's employees only.

1.1.1.3 The total maximum hours for the services described in this section "Verizon VERIS Framework Implementation Support and Training" will be no more than the number of hours specified in the Engagement Letter.

1.1.2 Incident Classification (if specified in the Engagement Letter)

1.1.2.1 Verizon will support Customer with incident classification by providing Customer with detailed information regarding the VERIS framework, recording Customer's in-scope Incident Data in the "VERIS language," and assisting Customer with performing the classifications correctly and uniformly in accordance with the VERIS framework across Incident Data as further detailed in the sub sections below. In order to provide this service, Customer shall present Verizon with access to the in-scope Incident Data that Customer requires to classify according to the VERIS framework. Verizon will assist Customer on the transfer and preparation of the Incident Data.

1.1.2.1.1 Understanding the VERIS framework. Verizon will provide training to Customer on utilization of the VERIS framework. The training will be on the four sections of the VERIS framework, each of which captures a different aspect of a security incident. The sections are: a) "demographics," such as the date of the incident, how serious it was, the region in which it occurred and Customer's vertical industry; b) "incident classifications" using metrics to detail the series of events that an incident comprises, who was affected and what was done, using the VERIS A4 model (Actors, Action, Asset, and Attribute); c) "discovery and mitigation" analyzes the events immediately following an incident and the lessons learned. Metrics include

a timeline, how the incident was discovered, the resources used, the controls used and whether they were adequate; and d) “impact analysis” which categorizes the varieties of losses experienced; estimate their magnitude; and captures a qualitative assessment of the overall effect on the organization.

1.1.2.1.2 Recording the In-Scope Incident Data and Validation. At Customer’s option and where specified in the Engagement Letter:

1.1.2.1.2.1 If Customer has performed Incident Classification, Verizon will assist Customer to record the Incident Data in the VERIS language. Verizon will also assist Customer in its classification of backlogged Incident Data that Customer provides to Verizon. Verizon will review Customer’s classifications of incidents up to the number specified in the Engagement Letter and provide feedback to Customer on classification. Once Customer has demonstrated that Customer understands how to classify the test incidents, Verizon will give Customer time to complete Customer’s in-scope Incident Data. Once the classifications have been completed on the in-scope Incident Data, Verizon will assist Customer to review random validations of the incidents that were classified to understand if the classifications were done pursuant to the VERIS framework; or

1.1.2.1.2.2 If Verizon has performed Incident Classification, Verizon will take Customer’s in-scope Incident Data and record it in the VERIS language. Verizon will assist Customer in classification of backlogged Incident Data that Customer provides to Verizon. Once Verizon has completed classification of the in-scope Incident Data, Verizon will demonstrate to Customer that the classifications were done pursuant to the VERIS framework by performing several random validations of the incidents that were classified.

1.1.2.2 The total maximum hours for the services described in this section ”Incident Classification” will be no more than the number of hours specified in the Engagement Letter.

1.1.3 Data Analysis (if specified in the Engagement Letter).

1.1.3.1 Verizon will assist Customer with analyzing Incident Data. For the initial analysis, Customer shall provide Verizon with the in-scope incidents classified pursuant to the VERIS framework. (Note: Verizon may have performed the classifications). Once the statistical analysis of the Incident Data has been concluded, the resulting findings will be summarized. At this point, Verizon will perform an in-depth analysis of the classified dataset to identify trends, commonalities, and security weaknesses, common failures or root causes. By identifying the trends and patterns in the dataset, Verizon will assist Customer in identifying justified treatment options that may reduce similar incidents from occurring in the future. Verizon will summarize the result of its analysis in a report of findings (the “Data Analysis Report”).

1.1.3.2 The total maximum hours for the services described in this section ”Data Analysis” will be no more than the number of hours specified in the Engagement Letter.

1.1.4 Comparative Data (if specified in the Engagement Letter)

1.1.4.1 Utilizing the in-scope incidents classified pursuant to the VERIS framework, and any data analysis that may have been done, Verizon will provide Customer with data comparisons against those in the Verizon master database (the “Comparative Data Report”). The Verizon database has detailed security incidents which are collected in collaboration with global organizations and ongoing Incident Data collected within the VERIS framework globally. The Comparative Data Report will show where Customer stands in relation to other companies of a similar stature (i.e. same industry, and/or size, and/or location, etc.) and will allow Customer the ability to make decisions about the status and direction of Customer’s security program. (Note: Verizon may have performed the classifications).

1.1.4.2 The total maximum hours for the Comparative Data services described in this section ”Comparative Data” will be no more than the number of hours specified in the Engagement Letter.

1.2 Verizon will work with Customer to schedule a kickoff meeting to initiate the Project. Verizon and Customer will collaborate to determine required stakeholders and other attendees, agenda, and meeting location (i.e. on site or remote). At or before the kickoff meeting, Customer shall provide a list of contact personnel with "after hours" emergency contact numbers and on-site authorization documentation (where applicable). As an output of the meeting, Verizon will produce an agreed project plan, which specifies resources, dates, times, and locations for the Project tasks (the "Project Plan").

13 The Professional Services will be provided remotely unless otherwise agreed in the Engagement Letter.

2. Deliverables and Documentation to be Produced by Verizon. 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 the Project Plan;

2.2 the Data Analysis Report if applicable; and

2.3. the Comparative Data Report if applicable.

3. Documentation to be Produced by Customer and Customer Obligations. Delivery of the Professional Services by Verizon is dependent on Customer's performance of the following:

3.1 Customer will provide to Verizon addresses of networked devices to be tested within the scope of the Professional Services at least seventy-two (72) hours or more prior to the scheduled commencement of the Professional Services;

3.2 Customer will provide Verizon with copies of all configuration information, log files, intrusion detection events, and other data relevant to the in-scope Professional Services;

3.3 Customer will provide access to the in-scope Incident Data (classified in the VERIS format, if required) that Customer is wishing to classify, analyze, or conduct a comparative analysis on;

3.4 Customer will be responsible for the actual content of any data file, selection, and implementation of controls on its access and use, and back-up and security of stored data; and

3.5 Customer will be responsible for ensuring that the Incident Data does not contain any personally identifiable information.

4. ASSUMPTIONS Delivery of the Professional Services by Verizon is predicated on the following assumptions and conditions:

4.1 Access to the Customer contacts and resources are provided by Customer during designated time frames, which will be established during the Project kick-off meeting. The failure to provide this timely access could delay completion of the Professional Services.

4.2 The Incident Data does not contain any personally identifiable information.