PROFESSIONAL SERVICES
DARK WEB HUNTING
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 Form (SOF).

1. **PROJECT DESCRIPTION.** Verizon will provide Customer with the Dark Web Hunting Service at the level of service indicated on the SOF.

1.1 **General Scope of Work.** Verizon's Dark Web Hunting service provides proactive, investigative intelligence research, analysis, and reporting to help Customer manage security risks and situational awareness. Dark Web Hunting provides adversarial threat patterns and activities focused on Customer's business priorities. The Dark Web Hunting service provides 5 services level options with additional priority findings and service options available using the Engagement Letter process. Verizon will provide Customer with the Dark Web Hunting services at the level and options indicated on the SOF.

1.2 **Dark Web Hunting Service.** Dark Web Hunting includes the following services and options:

1.2.1 **Hunting**. Verizon will hunt the surface, deep, and dark web of the internet for the Keywords and indications of the theft or misuse of Customer information related to the Risk Areas selected by the Customer. Verizon uses advanced open source research techniques, extensive use of numerous search engines, foreign language capabilities, search engines, forums, and blogs, and dark web markets to provide detailed intelligence information produced from publicly available surface, deep and dark web information, to search for Keywords in the Risk Areas identified as priority for the Customer. Verizon will scan, and detect nefarious activity occurring outside Customer's infrastructure, to help identify and mitigate physical and cyber related adversarial activity against the Customer priorities determined during Onboarding.

1.2.2 **Alerts**. Verizon will collect alerts, analyze them, and then prioritize the alert by a community based risk/confidence score. A high priority finding/alert is a community based risk/confidence score of 70 or above, unless otherwise requested by Customer.

1.2.3 **Weekly Report**. Verizon will provide a weekly report including a summary of Keyword findings/alerts in the Risk Areas identified. The number of findings provided in the Report, and the level of complex reporting, will be dependent on the service level selected by Customer.

1.2.4 **Level 1.** Level 1 includes Hunting, Alerts, and Weekly Reports over a period of 13 weeks, utilizing narrowly focused Risk Areas and Keywords. The weekly Report will summarize up to 15 highest priority findings in the Customer selected Risk Area.

1.2.5 **Level 2.** Level 2 includes Hunting, Alerts, and Weekly Reports on an annual basis. The Weekly Reports will summarize the 15 highest priority findings based on Customer selected Keywords and Risk Areas.

1.2.6 **Level 3.** Level 3 includes Hunting, Alerts, and Weekly Reports on an annual basis. The Weekly Report will summarize the 30 highest priority findings based on Customer selected Keywords and Risk Areas. Level 3 also includes contextualized analysis of the findings to better understand the risk associated with the finding.

1.2.7 **Level 4.** Level 4 includes Hunting, Alerts, and Weekly Reports on an annual basis. The Weekly Report will summarize the 30 highest priority findings based on Customer selected Keywords and Risk Areas. Level 4 includes contextualized analysis of findings to help Customer better understand the risk associated to the finding. Level 4 also includes correlation of data and link analysis.

1.2.8 **Level 5.** Level 5 includes 1 onsite surface, deep, and dark web threat hunter (Dark Web Hunter), where available, during Business Hours, for a minimum term of 12 months. Remote support will be provided in the first ninety days, while identifying an onsite Dark Web Hunter that meets the Customer's requirements. After the first ninety days, Customer is responsible for providing the onsite Dark Web Hunter with computer and network access for delivery of reports and communications, internet access (for proprietary dark web hunting hardware), office space, desk, chair, telephone access, and access to Customer facilities and personnel to speak with and integrate into Customer offices which he/she supports. The Dark Web Hunter will perform the following work:

- provide surface, deep, and dark web hunting support during Normal Business Hours;
- support the Customer identified Risk Areas;
- perform requested surface, deep, and dark web searches and associated analysis in support of weekly deliverable requirements, such as domain name, IP address, email address, file hash, malware name, URL, bad actor name, and/or campaign name;
- prepare intelligence analysis:
- provide operationalized dark web cyber intelligence analytical deliverables;
- leverage tools, techniques and technologies to collect and structure open source data from the surface, deep, and dark web sources and deliver intelligence information from those platforms;
- facilitate Change Order and Engagement Letter processing;
- interact with Customer regarding the Deliverables to discuss and refine, as needed, the quality of the information and analysis; and,
- interact with Customer IT and security teams.

1.2.9 **Additional Priority Findings**: Customer can order additional priority findings to be included in the Weekly Report in packages of 5.

1.3 **Dark Web Hunting Service Options.** After the Onboarding process is complete, Customer may request additional Dark Web Hunting consulting support (each a Project) by contacting VTRAC-Intel@verizon.com or reaching out to the Verizon consultant assigned during Onboarding, and initiating the Project via an Engagement Letter as specified herein.

1.3.1 **Dark Web Hunting Consulting Support.** In the event Customer requires support in addition to the services being provided pursuant to the Service Level ordered, Customer may request support from Verizon within the categories listed below. Specific services available within each category that are applicable to the Customer's needs will be discussed during a scoping call. Scope and pricing will be outlined in an Engagement Letter and will be provided pursuant to the hourly rates identified in the SOF. Support categories are:

- Custom surface, deep, and dark web research;
- Custom tactical, operational, and strategic intelligence analysis; and,
- incident response investigative activities.

1.3.2 **Engagement Letter Process**. The scope of each Engagement Letter will be agreed upon on a case-by-case basis. Verizon and Customer will agree upon the Project objectives, scope of work, Customer sites, number of Hours, and expected Deliverables. When Customer orders a Project, Verizon will provide a written Engagement Letter that describes the Project requested, methodologies to be used in performance of the requested Project, and the number of Hours required to complete the requested Project. Additional or changed Project Hours will require an amended Engagement Letter.

1.4 **Onboarding.** Within 10 days following the Service Activation Date, Verizon will send an email to Customer's Point of Contact (POC) requesting a date and time for an onboarding discussion. Onboarding will take place via a conference call between Customer and Verizon. During the Onboarding session, Verizon will: (a) collect Customer contact information; (b) review the Service Level ordered; (c) exchange contact information for the assigned Verizon Dark Web Hunter, and Customer point of contact; and, (d) review the Engagement Letter process for requesting additional Dark Web Consulting Support.

1.4.1 **Keyword and Risk Areas.** During onboarding, Verizon will work with the Customer to determine Customer's monitoring and hunting priorities. The priorities will consist of a list of Customer keywords, and the risk areas the Customer would like Verizon to focus on during Hunting, Alerting, and Weekly Reporting. Customer keywords can encompass elements such as awareness of brand reputation, product reputation, personnel protection, physical infrastructure protection, supply chain risk management, and network architecture protection (Keywords). Verizon will search the surface, deep and dark web for Keywords identified and will focus on the risk areas that Customer identifies as its primary concern (Risk Areas). Risk Areas may include any of the following:

- Brand

- TypoSquatting Risk
- Domain/Sub-Domain Risk
- IP Range Risk
- Hash Value Risk
- Malware Risk
- Intellectual Property / Loss Risk
- Third Party Risk (Includes Supply Chain/Vendors/Contractors)
- Critical Infrastructure Risk
- Physical Security Risk
- Human Factor Risk (C-Suite/New Hire/Separations/Insider Threat)
- Travel Risk
- Social Engineering Risk
- Attack Patterns
- Vulnerability Management Risk
- Competitor Risk
- Fraud

2. SUPPLEMENTAL TERMS

2.1. Term and Termination

2.1.1 **Service Term**. The Service term will begin on the Activation Date, and run for the Service Commitment, each as stated on the SOF.

2.1.2 **Service Termination.** Termination of the Service prior to the Service Commitment term is subject to Early Termination Charges. Customer will pay the invoice for such charges in accordance with the terms of the Agreement. Non-recurring charges (NRC) are non-refundable.

2.2 **Deliverables**. The Weekly Report and deliverables as described in an Engagement Letter are considered Deliverables. 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.

2.3 **Customer Obligations.** Customer is solely responsible for identifying Keywords and Risk Areas.

3. Financial Terms

3.1. **Rates and Charges.** Customer will pay the Charge as detailed 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 rates listed in the SOF.