Rapid Response Retainer Professional Service Description
Attack Detection Assessment

1. **Scope of Work.**

1.1. **Attack Detection Assessment.** The attack detection assessment services ("Attack Detection Assessment") is intended to assist Customer in measuring its capability to recognize and react to cyber-attacks. Verizon will evaluate Customer's operational incident-handling procedures. Attack Detection Assessment includes six phases that are cumulative in nature, providing multiple overlapping analyses of the strengths and weaknesses of Customer's operational incident handling capabilities.

1.1.1. **Phase 1: Defensive Countermeasures.** During phase 1, Verizon will review the selection, positioning and configuration of Customer's in-place security technologies including but not limited to firewalls, host and network-based intrusion detection, beacon identification and anti-virus. Verizon will provide a profile of Customer's defensive and threat hunting capabilities. Verizon will review Customer's event logging and alerting technologies such as security event management ("SEM") tools and intelligence integration platforms. Verizon will perform an on-site physical security inspection at one Customer location as defined in the Engagement Letter under the supervision of a designated Customer point of contact.

1.1.2. **Phase 2: Cyber Security Event Visibility.** Verizon will identify gaps in Customer's cyber security event detection which enable such events to go undetected. Phase 2 involves the correlation of Verizon cyber intelligence sources against Customer internet communications (e.g., firewall logs, netflow, etc.) for a sample period of up to 30 days (retroactive). In Phase 2, Verizon will benchmark the effectiveness of Customer's cyber security event capture methods. Phase 2 will require the completion and execution of a Customer IP schedule ("CIP").

1.1.3. **Phase 3: Incident Classification.** Verizon will perform a review of Customer's incident classification process documentation and will perform in-person interviews with identified Customer personnel. Verizon will evaluate the effectiveness of these process to detect cyber threats faced by Customer. Verizon will perform phase 3 at Customer's location as defined in the Engagement Letter.

1.1.4. **Phase 4: Intel Fusion.** Verizon will measure the effectiveness of cyber intelligence contained in Customer's operational incident handling processes. Verizon will evaluate Customer's ability to correlate cyber intelligence artifacts against cyber security event log streams. Verizon will review Customer's intelligence sources, data collection mechanism(s), archive and retention platforms, vetting and overall intelligence integration across log streams. Verizon will provide recommendations, if required, for changes to the collection, handling and application of cyber intelligence artifacts (i) to enable earlier detection of attacks in motion, (ii) during pre-attack research and (iii) to provide early indication of a possible intrusion or data theft. Phase 4 will be conducted on Customer's premises as defined in the Engagement Letter and will involve review of documentation and one-on-one interviews with identified Customer personnel.

1.1.5. **Phase 5: Visualization and Situational Awareness.** Verizon will test Customer's selection, deployment, configuration and usage of visualization tools. Verizon will perform manual inspection of the visualization tools and platforms, walk through examples and interview identified Customer personnel. In phase 5, Verizon will evaluate Customer's application of these tools.

1.1.6. **Phase 6: Incident Triage.** Verizon will review the process utilized by Customer's operational incident handling personnel, or Computer emergency readiness team ("CERT"), in handling potential security incidents. Verizon will review how Customer's incident handling activities map to the existing Customer incident response plan. In phase 6, Verizon will evaluate Customer's staff's technical skillset, toolsets and familiarity with their role/function within documented policy. Verizon will review the quality and timeliness of cyber security incident information collection and documentation, as provided to CERT staff, to confirm the information is properly actionable. Verizon will evaluate the implementation and effectiveness of Customer's device tuning and optimization as a result of an incident. Verizon will conduct phase 6 at Customer's location as defined in the Engagement Letter and will involve a review of Customer's documentation as well as one-on-one interviews with identified Customer personnel.

During any phase, Verizon will communicate to Customer's point of contact significant weaknesses or points of security exposure as may be identified by Verizon.

1.2. **Project Management.** Verizon will work with Customer to schedule a kickoff conference call to initiate the Project. Verizon and Customer will collaborate to set the agenda and determine required stakeholders and other attendees. During or before the kickoff call, Customer will provide a list of appropriate contact personnel with "after hours" emergency contact numbers, and appropriate on-site authorization documentation (where applicable). The output of the kick off call will be an agreement on the resources, dates, times, and locations for the tasks described.

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. Upon completion of the Attack Detection Assessment, Verizon will furnish assessment findings and conclusions in the form of a "Management Report" including actionable recommendations to improve situational awareness related to cyber-attacks in motion and feedback on how Customer's current incident handling capabilities are appropriate to the size and business of the Customer.

3. **Documentation to be produced by Customer and Customer Obligations (if any).** Delivery of the Professional Services by Verizon is dependent on Customer's performance of the following:
   3.1. Customer will appoint a single point of contact for co-ordination of the Project activities for interaction with Verizon and ensuring smooth data flow and exchange of information required for execution of the Project within the agreed time-frame;
   3.2. Customer will be responsible for the actual content of any data file, selection, and implementation of controls on its access and use, and security of stored data; and
   3.3. Customer must complete and execute a CIP prior to the initiate of Attack Detection Assessment.

4. **Assumptions (if any).** Delivery of the Professional Services by Verizon is predicated on the following assumptions and conditions:
   4.1. Customer is responsible for the implementation of any changes under the applicable Engagement Letter to applications or devices managed by Customer or Customer's service providers; and
   4.2. Attack Detection Assessment will be performed during the hours defined in the Engagement Letter.