SERVICE DESCRIPTION

Incident Response Readiness Assessment (IRRA)

SpiderLabs DFIR

Trustwave SpiderLabs is an industry leader in responding to and providing incident response to customers who have suffered data compromises or security breaches involving credit card fraud, unauthorized access, data theft, insider threat, malware outbreaks or other security incidents.

Alone, most organizations are not adequately protected and are poorly prepared to detect, respond to and investigate such security incidents. Together, Trustwave SpiderLabs and Client can better prepare Client's systems to prevent and respond to such security incidents.

Trustwave SpiderLabs provide Client with Digital Forensics and Incident Response ("**DFIR**") consulting services, which are based on the following engagement principles:

- Work product that is built on the foundation of Trustwave's leading industry expertise.
- A well-defined engagement model that helps to ensure a premium and consistent client experience.
- Clarity in communications to improve Client's understanding of complex technical findings.
- A rigorous quality assurance process to standardize deliverables on a global scale.
- Prompt notification procedures for alerting Client to any material, high, or critical risk issues affecting Client's environment.
- Continual innovation based on people, process, and technology.

Overview

This service description outlines the Incident Response Readiness Assessment service (the "**IRRA**"). The IRRA is available to Client as a part of certain DFIR retainers or as an ad hoc service. The IRRA assists Client in assessing its ability to detect, react to, and resolve security incidents.

Incident Response Readiness Assessment

Assessment Process

Trustwave will assess Client's ability to respond to security incidents based on the following metrics:

- Personnel to be engaged in incident handling
  - Such as management, technical teams, HR, legal, 3rd parties
- High level IR plan review

    - This is intended to identify any significant problems or omissions with the existing plan. It is not a deep dive review
- Incident identification and escalation process
- Ticketing and case management
- Alerting technologies available – including any perceived gaps
- Investigation technologies available – including any perceived gaps
- Logging and audit facilities that are:
    - Available
    - Active
- Third party engagements
    - IR providers
    - IT services
    - Other – Legal, HR etc.

Deliverables

Trustwave will provide a report detailing the results of the assessment such as: Client's current state of preparedness for responding to incidents, any perceived gaps in forensic/incident response capability and recommendations for addressing those gaps.

Service Level Agreements

Incident Response Readiness Assessment

An experienced consultant from Trustwave SpiderLabs will deliver the IRRA either onsite at Client's place of business or remotely, as agreed between Trustwave and the Client. As directed by Trustwave, Client will distribute materials and information as needed and provide requested documentation and information to Trustwave.

Client Requirements

Client will make available certain key stakeholders identified by Trustwave (such as IR team managers and IT administrators) for remote interviews during an agreed period. Client acknowledges that Trustwave cannot perform the IRRA unless these key stakeholders are agreed upon and made available.

Client will provide Trustwave with the following documentation:

- Client's computer security incident response plan
- Client's high-level network diagram
- Asset list and locations

Retainer Hours Consumption

The IRRA consumes 40 hours of any available DFIR retainer hours under the Standard DFIR Retainer or the Comprehensive DFIR Retainer.