SERVICE DESCRIPTION

Computer Security Incident Response Plan (CSIRP) Development

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 Computer Security Incident Response Plan (CSIRP) service. The CSIRP service is available to Client as a part of certain DFIR retainers or as an ad hoc service. The CSIRP service acts as an independent review of Client's current incident response plan (IRP). Trustwave will suggest amendments, improvements and identify gaps with in the IRP.

Service Details

Review Process

Client and Trustwave will review Client's existing IRP together. Client and Trustwave will work together to build on and further develop the IRP to reflect operational processes. Client and Trustwave will work together to outline playbooks for development.

Deliverables

Trustwave will provide a report detailing suggested additions, amendments and other improvements to the Client's IRP. Client will remain solely responsible for implementing any changes and ensuring the efficacy of the IRP.

Service Level Agreements

An experienced consultant from Trustwave SpiderLabs will deliver the CSIRP service 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 CSIRP service unless these key stakeholders are agreed upon and made available.

Client will provide Trustwave with the following documentation:

- Client's existing IRP
- Details of network and endpoint monitoring processes and technologies including SOC/SIEM implementation and operation in Client's environment
- Details of key stakeholders during incident response processes
- Details of any technologies deployed within Client's environment that may aid IR investigation (e.g. EDR toolsets, AV, full network packet capture capability, forensic software/staffing, file transfer capability (where data for analysis needs to be extracted from the environment for local analysis by Trustwave – for example SFTP servers)).

Retainer Hours Consumption

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