SERVICE DESCRIPTION

Incident Response Management and Investigation (IRMI) Course

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 Management and Investigation (IRMI) training course (part of the First Responder Training series). The IRMI training course is available to Client as a part of certain DFIR retainers or as an ad hoc service. Trustwave SpiderLabs provides this course over two days. This course aims to define and offer guidance on the proactive, reactive and reflective activities that should occur before, during and after security incidents. The target audience for this course includes anyone who assists with security incidents, not only IT security staff.

Service Details

Course Outline

The course is based on the "Incident Response Lifecycle" and helps participants identify the related roles and responsibilities, which fall into six categories. Participants will learn to define and assign these roles and responsibilities prior to a security incident. The six categories form a framework which can be adjusted to fit any business model or environment and is not specific to any one type of security incident.

Course Syllabus

Day One: The Cyber Kill Chain and the Incident Response Lifecycle

- Discussion on how the “Cyber Kill Chain” can be used to understand an attacker’s actions in a compromised environment.
- Discussion on how the “Incident Response Lifecycle” can be used to assist incident response and other security teams before, during, and after a security incident.

Day Two: The Six Categories

- Identification and explanation of the six-category framework and how the framework incorporates more teams than just security or technical.
- Open discussion around Client’s environment and how (i) the six categories can be applied, (ii) pre-emptive information may be gathered and catalogued, and (iii) staff from various groups can contribute during an incident.

Service Level Agreements

An experienced consultant from Trustwave SpiderLabs will deliver the IRMI training course 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 to participants and provide requested documentation and information to Trustwave.

Client Requirements

Client will provide the following details for all participants in the IRMI training course: names, function, specific IR role, and contact details. Client will provide suitable on premises training facilities or appropriate remote communication mechanisms.

Access

Client shall ensure participants can join a remote session hosted by Trustwave, including the use of webcam, microphone and audio.

Course Size

Client may include up to 15 participants in the course.

Retainer Hours Consumption

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