SERVICE DESCRIPTION

Fundamentals of Incident Response (FIRE) 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 Fundamentals of Incident Response (FIRE) training course (part of the First Responder Training series). The FIRE 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. The course addresses how an attacker can compromise a system and how evidence of that compromise can be gathered and analyzed so as to understand the nature and impact of the attack.

Service Details

Course Outline

Day one will focus on what attackers see and do when attempting to gain access to a system. Participants are offered the opportunity to perform basic attack techniques to gain unauthorized access to a system. Day one will also cover the identification and capture of evidence relating to an attack.

Day two will walk participants through the investigation process for a compromised system. Participants will analyze the various forensic artifacts of a compromised system that indicate how an attack occurred.

Course Syllabus:

Day One: Part 1 - Anatomy of A Breach

Topics covered include:

- Target identification and exploitation
- Lateral movement inside the network
- Post-exploitation and maintaining access
- Data exfiltration

Day One: Part 2 - Identification and Acquisition of Digital Evidence

Topics covered include:

- Windows RAM and hard drive forensic imaging
- Network traffic capture
- Network logs

Day Two: Analysis of Digital Evidence

Topics covered include:

- Building an incident timeline
- Firewall logs
- Network traffic
- Operating system forensic artifacts
- Using the Indicators of Compromise identified during analysis to “tell the story” of what happened during the attack

Service Level Agreements

An experienced consultant from Trustwave SpiderLabs will deliver the FIRE 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 FIRE training course: names, function, specific IR role, and contact details. Client will provide suitable onsite premises training facilities or appropriate remote communication mechanisms.

Materials

Participants attending the course shall bring their own computers which run VMWare Workstation 15 Pro or Player on a Windows operating system with 8GB of RAM minimum (the “**Software**”). If participants do not own a copy of the Software, participants may download and use an evaluation version only for the purposes of this course.

Trustwave will provide participants with an external USB3 hard drive for use only during the course. Participants will return the external USB3 hard drives at the conclusion of the course. Participants

should bring their own external drive with approximately 150GB of space if they wish to keep a copy of the material.

Course Size

Client may include up to 15 participants in the course.

Retainer Hours Consumption

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