SERVICE DESCRIPTION

Incident Response Training and Exercises

Overview

Trustwave's Incident Response Training and Exercises ("**Service**") constitutes Trustwave's digital forensics and incident response (DFIR) training and exercise offerings. The Service is available to Client as a proactive service under the Advanced or Premium Digital Forensics Incident Response Retainers or as an a la carte service. The following descriptions sets out the parameters of the Service, as may be further modified by an applicable SOW or Order Confirmation between Trustwave and Client.

Service Features

Trustwave will provide one or both of the following (as indicated in the applicable SOW or Order Confirmation between Trustwave and Client):

- Incident Response (IR) Training Courses
- Tabletop Exercises

Incident Response Training Courses

Trustwave will provide one or both of the following IR training courses (as indicated in the applicable SOW or Order Confirmation):

- Fundamentals of Incident Response (FIRE)
- Incident Response Management and Investigation (IRMI)

FIRE Course

Trustwave will first discuss what attackers may see and do when attempting to gain access to a system. Trustwave will offer course participants the opportunity to perform basic attack techniques to gain unauthorized access to a system. Trustwave will also review the identification and capture of evidence relating to an attack.

Next, Trustwave will discuss the investigation process for a compromised system. Course participants will analyze the various forensic artifacts of a compromised system that indicate how an attack occurred.

IRMI Course

Trustwave bases this course on the "Incident Response Lifecycle". The course is designed to help course participants identify the six categories of IR roles and responsibilities. Course participants will learn to define and assign these roles and responsibilities prior to a cybersecurity incident. The six categories form a framework which can be adjusted to fit many business models or environments and is not specific to any one type of cybersecurity incident.

Tabletop Exercises

Overview

Trustwave will orchestrate interactive exercises for Client's personnel aimed at testing Client's in-house ability to react to and deal with cybersecurity incidents and its processes to resolve them. Trustwave will adjust the exercises to better meet Client's unique cybersecurity posture as Trustwave deems appropriate. The following are examples of the types of exercises that may be included in the Service. Trustwave will provide full details regarding each exercise in the applicable SOW, Order Confirmation, or separately.

<u>Technical Tabletop Exercise</u>

This exercise is best suited for Client's technical security team. During the exercise, Client's team will identify actions it takes within certain breach scenarios and how those actions can, where necessary, be modified to better respond to security incidents. The exercise may help Client identify gaps in Client's IR plans and processes and assist with the improvement of programs.

<u>Executive Tabletop Exercise</u>

This exercise is best suited for Client's executive-level staff. During the exercise, Client's team will look at the overarching decisions made during cybersecurity incidents, and how the executive-level staff may leverage their position to assist cybersecurity teams during or outside a cybersecurity incident.

Obligations

Trustwave Obligations

Trustwave will deliver training course or tabletop exercise either onsite at Client's place of business or remotely, as agreed between Trustwave and the Client. Trustwave will provision appropriate access to Service materials before or during the course or exercise.

Client Obligations

For Trustwave to provide the Service, Client will

- provide the following details for all participants in the training courses or exercises: names, function, specific IR role, and contact details;
- provide suitable on premises training facilities or appropriate remote communication mechanisms, together with appropriate levels of IT systems and connectivity (internet) as required by the course or exercise;
- as directed by Trustwave, distribute materials and information to participants and provide necessary levels of access to IT systems, documentation, and information to Trustwave;
- ensure participants can join a remote session hosted by Trustwave, including the use of webcam, microphone, and audio; and
- include no more than fifteen (15) participants in each training course or tabletop exercise.

Retainer Hours Consumption

If Trustwave provides the Service as a proactive service under the Advanced or Premium Digital Forensics Incident Response Retainer, each separate training course or tabletop exercise consumes forty (40) retainer hours.

Definitions

All capitalized terms not defined in this document have the meanings ascribed to them in Trustwave's Master Terms and Conditions available at https://www.trustwave.com/en-us/legal-documents/contract-documents/ or in the applicable SOW or Order Confirmation between Trustwave and Client.