Incident Response

Training Outline – 2 Days

Training ID 163

CYBERGYM®

Training Description

Main Training Goal

The main training goal is to provide trainees the opportunity to **experience** and handle a wide range of cyber attacks, while providing the trainees with the ability to sharpen their skills in **detecting**, **investigating**, **mitigating** and **recovering** from cyber events.

Target Audience

- IT Personnel
- Information Security Personnel
- SOC Analysts
- Incident Response Teams.

Mandatory prerequisites

- Deep understanding of data communication
- Good knowledge of security and SIEM systems.

Training Outcomes

- **Identify** cyber incidents using indicators provided by the SIEM and security systems.
- **Analyse** the incident with various security and investigation tools.
- **Contain** cyber-incidents in real time to minimise the potential damage.
- **Decide** which recovery steps should be taken in order to restore normal operation in the organisation.
- **Understand** the hacker point of view through real-life cyber-attacks.

Training Schedule

Day 1

Time	Session	Description
09:00 – 09:30	Opening session	• Company Presentation • Schedule Overview.
09:30 – 10:15	The First Responder	Role and responsibilities during the overall process of handling a cyber event.
10:15 – 10:45	Hacker Point of View	Hacker profile, APT method and stages from the hacker's perspective.
10:45 – 11:00	***Coffee Break***	
11:00 – 11:45	Malware Overview	• APT Model Phases • Malware Types • Detection Techniques.
11:45 – 12:30	Sysinternals Overview	• Tools Overview • Hands-on (Malware Analysis).
12:30 – 13:30	**Lunch Break**	
13:30 – 15:00	Malware Workshop	The trainees will have to analyse an infected workstation independently, analyse the collected data and determine if and which workstation is suspicious as the infected one.
15:00 – 15:15	***Coffee Break***	
15:15 – 16:30	Malware Workshop	Continuation.
16:30 – 17:00	Daily Summary	Debriefing and Feedback.

Day 2

Time	Session	Description
09:00 – 09:30	Morning Session	A short recap and daily schedule review.
09:30 – 10:30	Active Defence Concept	• Information Security Concept • Seven Layers of Security Systems • Security Systems Benefits.
10:30 – 10:45	***Coffee Break***	
10:45 – 11:30	Digital Evidence Collection	Methods and tools that are used to perform evidence collection overview.
11:30 – 12:30	Digital Evidence Collection Workshop – *Export Data*	The trainees will use the methods and tools learned before to export data from an infected machine.
12:30 – 13:30	**Lunch Break**	
13:30 – 14:15	Cyber Attack Case Study	Lockheed Martin Attack.
14:15 – 16:30	Cyber Crisis Management *(Desktop Simulation)*	• A cyber incident has occurred – Things go from bad to worse • Trainees are divided into Management and Technical teams and need to make decisions as the pressure is turned up
16:30 – 17:00	Daily Summary	• Debriefing • Feedback.