Incident Response

Training Outline

Training ID 163

Powered by Wolfpack Information Risk (Pty) Ltd

CYBERGYM SA

WOLF PACK

Training Description

Main Training Goal

The main training goal is to provide the 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

- Information Security personnel
- IT Operations
- Incident Response teams
- Threat Hunters
- SOC Analysts

Mandatory prerequisites

- Good understanding of data communication concepts and the TCP/IP protocol suite
- Basic knowledge SIEM and other security monitoring solutions
- Good understanding of configuring and running Linux and Windows operating systems
- Familiarity with tools such as Wireshark and the Sysinternals Suite
- Basic knowledge of web application architecture
- Basic knowledge of information security principles

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 minimize the potential damage
- **Decide** which recovery steps should be taken in order to restore normal operation in the organization
- **Understand** the hacker point of view through real-live cyber-attacks

Training Schedule

Day 1

Time	Session	Description
08:30-8:45	Opening session	▰ CyberGym introduction ▰ Course overview ▰ Tools overview
08:45 – 9:15	Hacker Point of View	▰ Hacker profile, APT method and stages from the hacker's perspective
9:15 – 10:00	Malware Overview	▰ APT model phases ▰ Malware types & Detection Techniques
10:00- – 10:15	***Coffee Break***	
10:15 – 12:00	Sysinternals Overview **(Hands-on)**	▰ Tool overview ▰ Hands-on (malware analysis)
12:00 – 13:00	**Lunch Break**	
13:00 – 14:15	Malware Analysis Workshop 1 **(Hands-on - DarkComet)**	▰ Analyse an infected workstation independently, review collected data and confirm attack. ▰ Identify infection vectors, attack artefacts, persistence mechanisms and attacker objectives. ▰ Propose remediation measures
14:15 – 14:30	***Coffee Break***	
14:30 – 15:30	Malware Analysis Workshop 2 **(Hands-on - NJRAT)**	▰ As above.
15:30 – 16:00	Daily Summary	▰ Debriefing & feedback

Day 2

Time	Session	Description
8:30 – 09:00	Morning Session	▰ Recap of tools used
09:00 – 10:00	The First Responder	▰ Role and responsibilities during the overall process of handling a cyber event
10:00 – 10:15	***Coffee Break***	
10:15 – 11:00	Digital Evidence Collection	▰ Methods and tools that are used to perform evidence collection overview
11:00 – 12:00	Digital Evidence Collection Workshop – *Export Data*	▰ The trainees will use the methods and tools learned before to export data from an infected machine
12:00 – 13:00	**Lunch Break**	
13:00 – 14:00	Cyber Attack Case Study	▰ Lockheed Martin Attack
14:00 – 15:00	Arena Introduction **(Hands-on)**	▰ The trainees will learn about the following security systems: McAfee, Snort & Check-Point FWs and more
15:45 – 16:00	Daily Summary	▰ Debriefing & Feedback

Day 3

Time	Session	Description
08:30	Morning Session	▰ A short recap and daily schedule review
08:30 – 9:45	APT - ILT (Instructor Led Training) Incident Response Training **(Hands-on)**	▰ The trainees will be led by the White team to analyse attacks. According to the level of the trainees, the White Team will adjust the intensity of the attacks.
9:45 – 10:00	***Coffee Break***	
10:00 – 12:00	APT with ILT (Instructor Led Training) Incident Response Training **(Hands-on)**	▰ Continue with various APT attacks launched by actual Israeli red team hackers & defender scenarios
12:00 – 13:00	**Lunch Break**	
13:00 – 15:30	ILT (Instructor Led Training) Incident Response Training **(Hands-on)**	▰ Continue with various APT attacks launched by actual Israeli red team hackers & defender scenarios
15:30 – 16:00	Training Summary	▰ Debriefing & Feedback