Cyber Defence Challenge

Training Schedule

Training ID 197

CYBERGYM®

Training Description

Main Training Goal

The main training goal is to sharpen the trainee's skills of **detecting** and **performing first analysis** of cyber incidents using various detection and monitoring tools.

Target Audience

- IT Personnel
- Information Security Personnel
- Entry level SOC Analysts.

Mandatory prerequisites

- Knowledge of data communication
- Knowledge of different operating systems
- Knowledge of organisational management tools.

Training Outcomes

- **Identify** cyber incidents using indicators provided by the SIEM and security systems.
- Perform first analysis of the incident with various security and monitoring tools.
- Understand the organisational impact of the cyber incidents and how they should be handled.
- **Experience** real live cyber incidents.
- **Understand** the hacker point of view through real-life cyber attacks.

Training Schedule

Day 1

Time	Session	Description
09:00 – 09:30	Opening session	• Training & team introduction • Arena overview
09:30 – 10:30	Cyber Attacks in the World	Case studies of known attacks and what we can learn from them.
10:30 – 10:45	***Coffee Break***	
10:45 – 12:45	Active Defence Concept	• Information security concepts • Seven layers of security systems • Security systems benefits
12:45 – 13:45	***Lunch Break***	
13:45 – 15:00	Sysinternals Overview (Hands-on)	• Tools overview • Malware analysis
15:00 – 15:15	***Coffee Break***	
15:15 – 16:30	Wireshark Demonstration (Hands-on)	Slides and Demo
16:30 – 16:45	Daily Summary	Debriefing and feedback.

Day 2

Time	Session	Description
09:00 – 09:15	Morning Session	A short recap and daily schedule review.
09:15 – 11:00	Malware Overview	• APT model phases • Malware types Detection Techniques
11:00 – 11:15	***Coffee Break***	
11:15 – 12:45	Malware (Hands-on)	• The trainees will analyse an infected workstation independently, analyse the collected data and determine suspicious activity.
12:45 – 13:45	***Lunch Break***	
13:45 – 16:00	Advanced Persistent Threat (APT) (Hands-on)	• The Israeli Red Team launches an attack against the company website resulting in the compromise of sensitive assets. • Use your blue team skills to respond and defend.
16:00 – 16:30	Training Summary	• Debriefing • Feedback