

EXPECT THE
UNEXPECTED

Cyber Defence Challenge

Training Schedule

Training ID 197



Copyright

All information contained herein is copyrighted information that is proprietary, privileged, or confidential. It is intended only for the purpose specific, and directed to the recipients specifically identified by CyberGym Ltd. Any unauthorised review, disclosure, reproduction, distribution, copying of, or reliance upon this document, and any included exhibits is strictly prohibited. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, for purposes other than intended, without prior written permission of 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	<ul style="list-style-type: none"> • 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	<i>Coffee Break</i>	
10:45 – 12:45	Active Defence Concept	<ul style="list-style-type: none"> • Information security concepts • Seven layers of security systems • Security systems benefits
12:45 – 13:45	<i>Lunch Break</i>	
13:45 – 15:00	Sysinternals Overview (Hands-on)	<ul style="list-style-type: none"> • Tools overview • Malware analysis
15:00 – 15:15	<i>Coffee Break</i>	
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	<ul style="list-style-type: none"> • APT model phases • Malware types • Detection Techniques
11:00 – 11:15	<i>Coffee Break</i>	
11:15 – 12:45	Malware (Hands-on)	<ul style="list-style-type: none"> • The trainees will analyse an infected workstation independently, analyse the collected data and determine suspicious activity.
12:45 – 13:45	<i>Lunch Break</i>	
13:45 – 16:00	Advanced Persistent Threat (APT) (Hands-on)	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Debriefing • Feedback