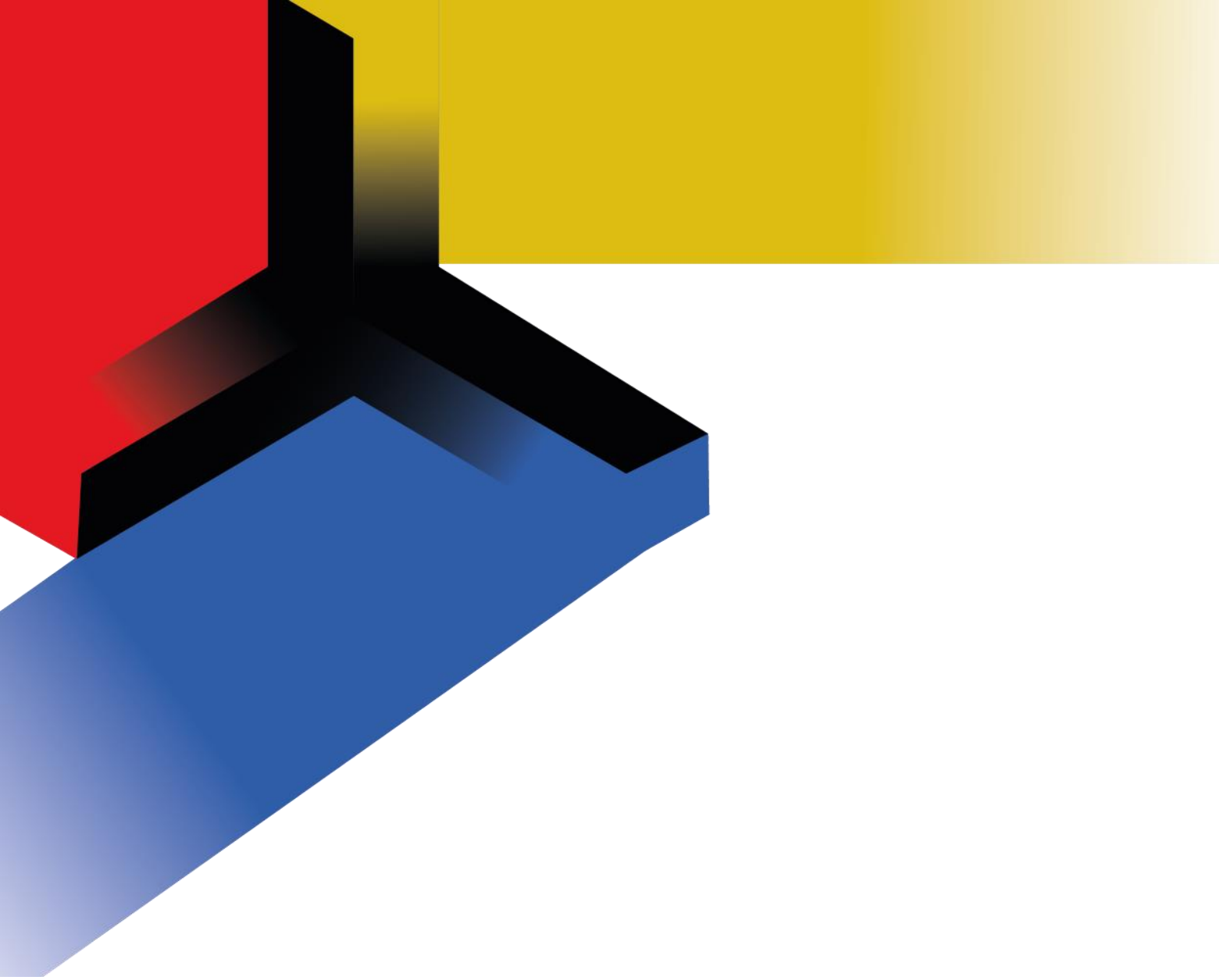

Incident Response - Advanced Tactics

Certification

CybergymIEC

Incident Response - Advanced Tactics

Hours: 34 | Credits: 34 | Days: 8 | Trainings: 8

DESCRIPTION

The Incident Response training program immerses trainees in the tools, skills, and methods used by an enterprise Incident Response team, offering hands-on practice in the Cyber Arena environment during a simulated cyber attack.

This is the 2nd and advanced part of the training program.

Trainees will master managing corporate security policies and compliance, developing and updating organizational procedures, evaluating damage and managing responsibilities, detecting and mitigating ongoing cyber-attacks under real-life APT conditions.

This training is modified to the academic sector.

TARGET AUDIENCE

- BA Technological BA Students
- Ma Technological BA Students
- Executives

LEARNING OBJECTIVES

- Ability to debrief the attack scenario
- Ability to detect, analyze and mitigate advanced and complex cyber attacks

CERTIFICATION

1

IR - Advanced Tactics (Theory - Fileless)

Main Goals:

Trainees will provide detailed explanations of Fileless detection tools.

Learning Objectives:

Familiarity with Fileless detection tools and concept

2

IR - Advanced Tactics (Malware 3)

Main Goals:

The trainees will detect, analyze and mitigate a malware in the system on a controlled environment

Learning Objectives:

Ability to analyze malwares in a system

3

IR - Advanced Tactics (Malware 4)

Main Goals:

The trainees will detect and mitigate a malware in the system on a controlled environment

Learning Objectives:

Ability to analyze malwares in a system

4

IR - Case Study - Technion

Main Goals:

Trainees will highlight three positive and three negative aspects of the organization's incident handling

Learning Objectives:

Ability to analyze a cyber incident conduct - Debriefing

5

IR - Advanced Tactics (Malware 5)

Main Goals:

The trainees will detect and mitigate a malware in the system on a controlled environment

Learning Objectives:

Ability to analyze malwares in a system

6

IR - Advanced Tactics (Malware 6)

Main Goals:

The trainees will detect and mitigate a malware in the system on a controlled environment

Learning Objectives:

Ability to analyze malwares in a system

7

IR - Advanced Tactics (APT 1)

Main Goals:

The trainees will mitigate a cyber attack in the arena
The trainees will debrief their action in the arena during the cyber attack

Learning Objectives:

- Ability to analyze a cyber incident conduct - Debriefing
- Ability to analyze and investigate and mitigate a hacked system

8

IR - Advanced Tactics (APT 2)

Main Goals:

The trainees will mitigate a cyber attack in the arena
The trainees will debrief their action in the arena during the cyber attack

Learning Objectives:

- Ability to analyze a cyber incident conduct - Debriefing
- Ability to analyze and investigate and mitigate a hacked system