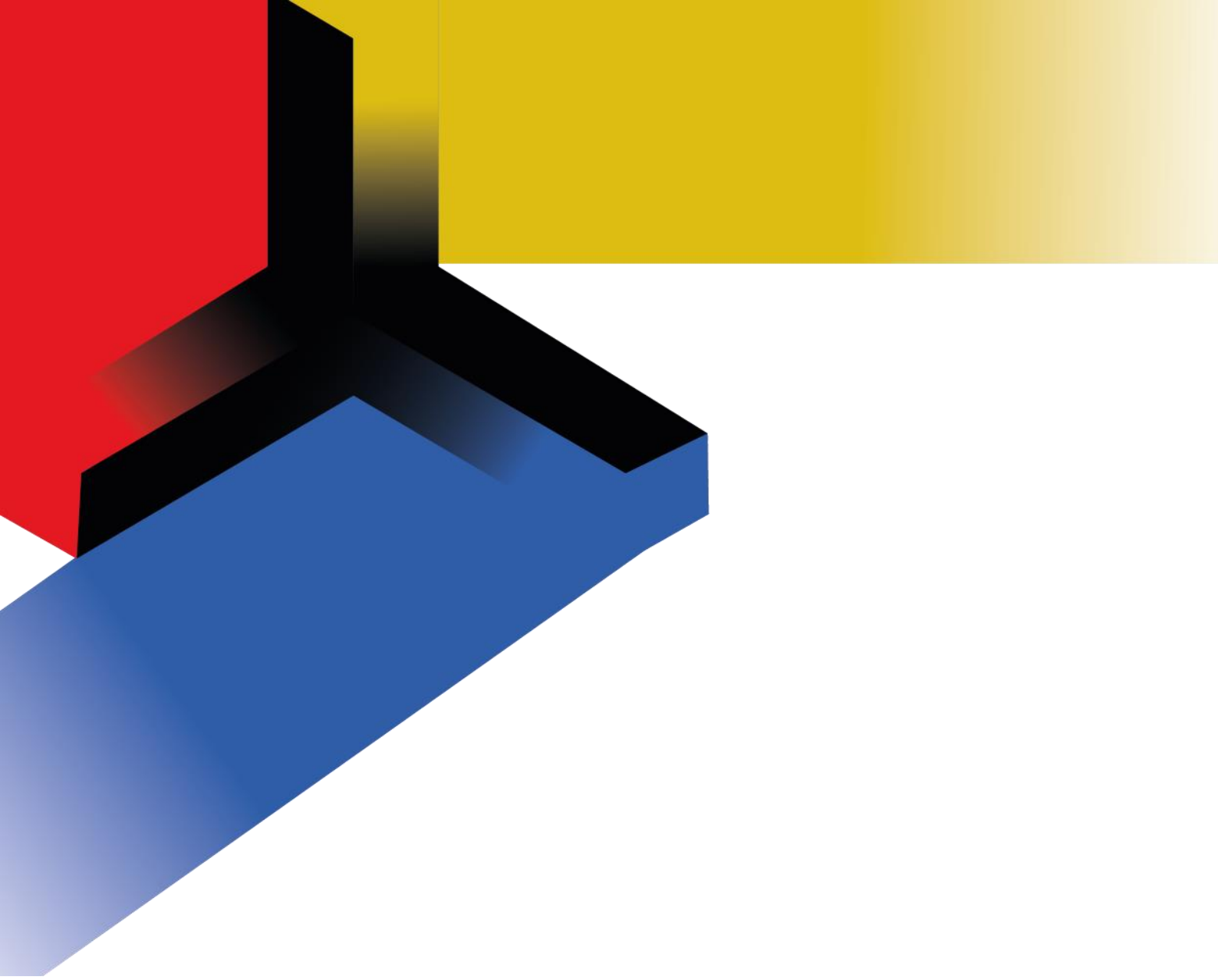

Incident Response - Principal Tactics

Certification

CybergymIEC

Incident Response - Principal 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.

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

CERTIFICATION

1

IR - Principal Tactics (1/2 Theory)

Main Goals:

The trainees will describe the roles of the IR team
The trainees will describe the hacker point of view

Learning Objectives:

Understand the basic roles of the IR team

2

IR - Principal Tactics (2/2 Theory)

Main Goals:

The trainees will describe different malwares and the methodology of an APT
The trainees will describe the use of Sysinternals suite

Learning Objectives:

- Ability to use cyber tools in the arena
- Understanding cyber security basic terms and concepts

3

IR - Principal Tactics (malwares 1+2)

Main Goals:

The trainees will detect, analyze and mitigate malwares in a controlled environment

Learning Objectives:

Ability to analyze malwares in a system

4

IR - Principal Tactics (1/2 DEC)

Main Goals:

The trainees will describe the Digital Evidence Collection process.
The trainees will experience in DEC process of data export.

Learning Objectives:

Ability to collect digital evidence for a cyber incident investigation

5

IR - Principal Tactics (2/2 DEC)

Main Goals:

The trainees will experience in DEC process of collecting timeline.

Learning Objectives:

Ability to collect digital evidence for a cyber incident investigation

6

IR - Case Study - Lockheed Martin

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

7

IR - Principal 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 - Principal 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