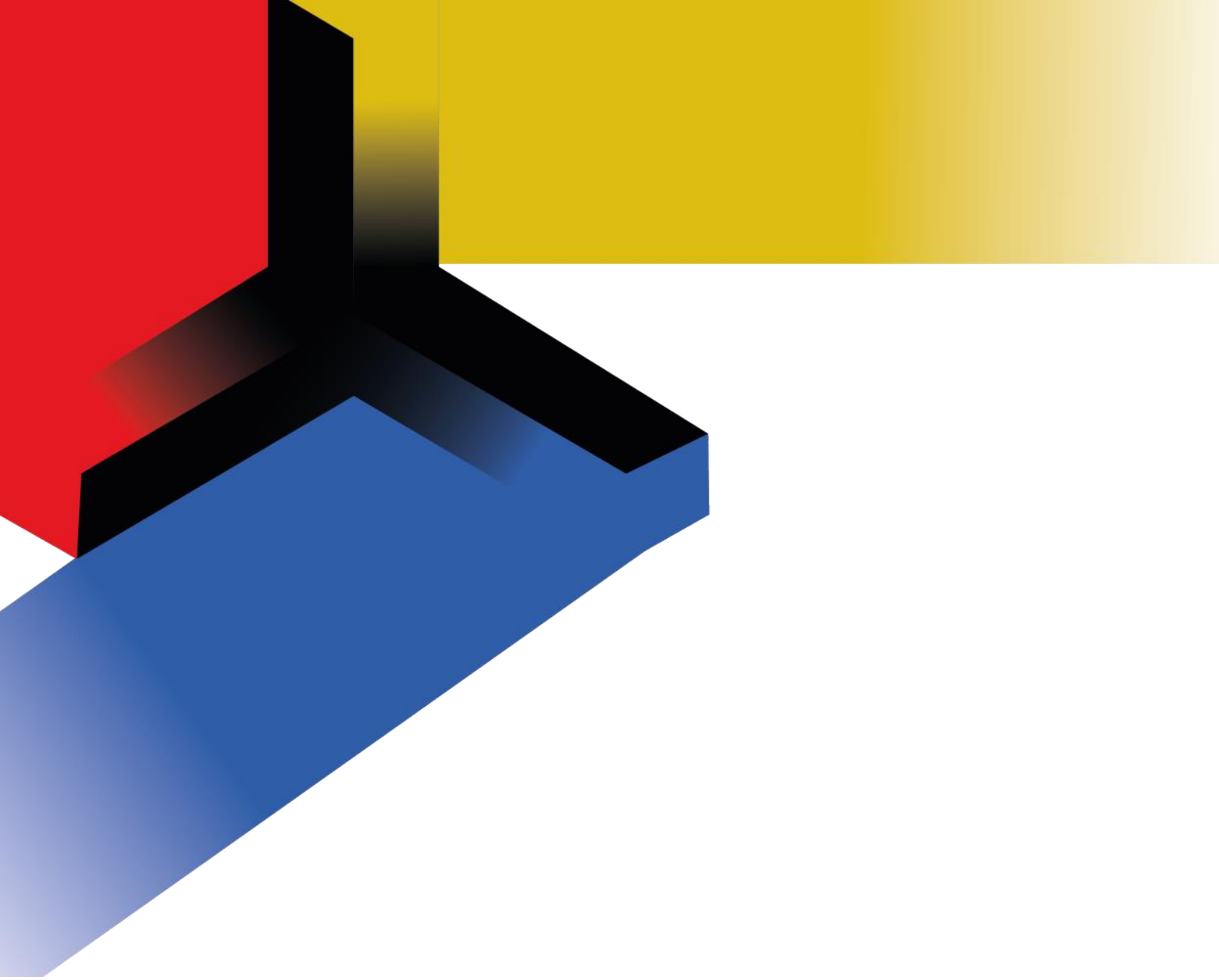

Basic Cyber Security for Technological BA

Certification

CybergymIEC

Basic Cyber Security for Technological BA

Hours: 30 | Credits: 30 | Days: 15 | Trainings: 15

DESCRIPTION

This 30-hour course is designed for BA students in technological fields such as computer science, information technology, mathematics, and physics. It begins with theoretical topics, advancing to hands-on exercises and practical experience. Students will learn about cyber tools for investigating incidents and engage in hands-on labs. The course culminates in a cyber warfare arena with real-life attacks, providing practical experience in mitigating these threats.

TARGET AUDIENCE

BA Technological BA Students

LEARNING OBJECTIVES

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

CERTIFICATION

1

Basic Cyber Security 1

Main Goals:

The trainees will explain cyber security concepts

Learning Objectives:

Understanding cyber security basic terms and concepts

2

Basic Cyber Security 2

Main Goals:

The trainees will mention the latest cyber attacks in the world
The trainees will explain the network layers

Learning Objectives:

Understanding cyber security basic terms and concepts

3

Basic Cyber Security 3

Main Goals:

The trainees will explain the use and operation of Sysinternals tools in Cybergym's arenas

Learning Objectives:

Ability to use Sysinternals tools as part of cyber incident process

4

Basic Cyber Security 4

Main Goals:

The trainees will explain the use and operation of Wireshark
The trainees will explain how to use MITRE ATT&CK framework

Learning Objectives:

Ability to use cyber tools in the arena

5

Basic Cyber Security 5

Main Goals:

The trainees will explain about SIEM platforms and their use

Learning Objectives:

Understand the use of SIEM in an organization

6

Basic Cyber Security 6

Main Goals:

The trainees will explain about SIEM platforms and their use

Learning Objectives:

Understand the use of SIEM in an organization

7

Basic Cyber Security 7

Main Goals:

The trainees will explain the different roles in the IR team
The trainees will explain the hacker point of view

Learning Objectives:

Understand the importance of and gain insights into managing a crisis with the relevant key players, both technical and managerial

8

Basic Cyber Security 8

Main Goals:

The trainees will describe the phases of a trojan horse attack and its behavior
The trainees will mention 2 positive and 2 negative points of conduct in the Norsk Hydro cyber incident

Learning Objectives:

Ability to analyze a cyber incident conduct - Debriefing

9

Basic Cyber Security 9

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

10

Basic Cyber Security 10

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

11

Basic Cyber Security 11

Main Goals:

The trainees will explain the digital evidence collection methodology
The trainees will use the methods and tools to export data from an infected machine on a controlled environment

Learning Objectives:

Ability to collect digital evidence for a cyber incident investigation

12

Basic Cyber Security 12

Main Goals:

The trainees will create a timeline of the attack using the evidence they have collected in the previous exercise on a controlled environment
The trainees will experience the use of Wireshark

Learning Objectives:

Ability to collect digital evidence for a cyber incident investigation

13

Basic Cyber Security 13

Main Goals:

The trainees will detect, analyze and handle a real-live APT

Learning Objectives:

Ability to analyze and investigate a hacked system

14

Basic Cyber Security14

Main Goals:

The trainees will detect, analyze and handle a real-live APT

Learning Objectives:

Ability to analyze and investigate a hacked system

15

Basic Cyber Security 15

Main Goals:

The trainees will detect, analyze and handle a real-live APT

Learning Objectives:

Ability to analyze and investigate a hacked system