TIER 1 – TR001

Duration: 16 hours: - 2 Days

Description

TIER 1 is an essential course that covers main topics from the cyber world and allows the participants to get a quick view of the complex world of digital crimes.

This training covers the core concepts of defense and understanding in the practical world using the CYBERIUM ARENA simulator. Students will learn about different domain structures and security technology products.

Target Audience

The course targets participants with basic knowledge in IT or networking and managers wanting to understand better the cyber world and corporate cybersecurity and cyber defense from an attacker's point of view.

- College Graduates
- IT Professionals
- Managers

Pre-requisites

- None

Objectives

- Acquiring the knowledge and tools to understand the corporate network
- Understanding cyber-attacks
- Being able to make better decisions in the corporate world
- Being able to protect your computer environment
- Becoming familiar with different attack scenarios

Day 1

Module 1: Introduction to TIER 1

During this module, students will study the fundamental concepts of the cyber world. The goal of this module is to allow students that don't have any background to understand the risks and be able to approach their digital environment better.

- **Fundamentals Concepts in Information & Cyber Security**
  - Definitions
  - Key Players
  - History and Future
  - Security Awareness
  - Type of Hackers
- **Cyber Basics**
  - Basic Networking
    - Network Attacks
    - Remote Access
  - Virtualization
  - Steganography and Ciphers
  - Hash Functions and Encodings

Module 2: Introduction to Linux

In this module, we will take a closer look at the advantages and disadvantages of the Linux operating system. We will get familiar with Linux fundamentals and the bash scripting language.

- **Introduction to Linux**
  - What is Linux
  - Linux Installation
- **Linux Terminal**
  - Basic Commands and Tools
  - File System Structure
  - System Administrator
  - Permissions in Linux
  - Text Manipulation
  - Bash Scripting

Day 2

Module 3: Cyber Defense

This module will dive deeper into the world of cybersecurity, the primary goal being to teach participants to embrace the attacker state-of-mind to recognize the necessary defense mechanisms. Participants will deal with several types of malware, spyware, and viruses, learn about hash functions, and basic web attacks.

- **Basic Networking**
  - OSI Model using Wireshark
  - DNS and DHCP - From an Attacker Point of View
- **Defense Concepts**
  - Security Products
    - Firewall
    - IPS and IDS
    - DLP
    - SIEM/SOC
  - Anonymity on the Network
  - Concepts of Wi-Fi Security
- **Cyber Attacks**
  - DDoS
  - MiTM Attacks
  - Brute Force and Mitigation Techniques
  - Trojan Methods: Reverse vs. Bind
  - Encryption and Decoding