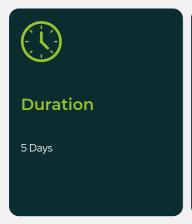


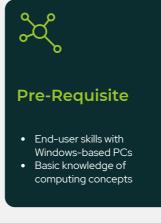
INTRODUCTION TO CYBERSECURITY TOOLS & CYBER ATTACKS

This course gives you the background needed to understand basic Cybersecurity. You will learn the history of Cybersecurity, types and motives of cyber attacks to further your knowledge of current threats to organizations and individuals. Key terminology, basic system concepts and tools will be examined as an introduction to the Cybersecurity field

Course Details









Course Objectives

After completing this course, participants are expected to be able to:

- Discuss the evolution of security based on historical events.
- List various types of malicious software.
- Describe key cybersecurity concepts including the CIA Triad, access management, incident response, and common cybersecurity best practices.
- Identify key cybersecurity tools which include the following: firewall, anti-virus, cryptography, penetration testing, and digital forensics.



Course Outline

Lesson 1 - History of Cybersecurity

- History of Cybersecurity
- Cybersecurity Definition
- Security Threats
- Vulnerability Assessments
- Roles in Security
- Cybersecurity Today
- Things to consider when starting a Cybersecurity program
- What is Security?
- Additional Security Challenges
- Beyond Technology: Critical Thinking in Cybersecurity
- Critical Thinking: A Model
- · Critical Thinking 5 Key Skills

Lesson 2 - Types of attacks and impact

- Hacking organizations
- Major different types of cyber attacks•
- Security Attack Definition
- Security services
- Security Mechanisms
- Network Security Model
- Security Architecture Attacks
- Malware and Ransomware
- Threat Protection Defined
- Internet Security Threats Mapping
- Internet Security Threats Packet Sniffing
- Security Threat IP Spoofing
- Security Threats Denial of service
- Security Attacks Host insertions
- The Cyber Kill Chain
- Social Engineering Phishing and Vishing
- Cyberwarfare
- Cybercrime Resources

Lesson 3 - An overview of key security concepts

- CIA Triad Confidentiality
- CIA Triad Integrity
- CIA Triad Availability
- Non Repudiation How does it apply to CIA?
- Access Management
- Incident Response
- Key Concepts Incident Response
- Incident Response Process
- Introduction to Frameworks and Best Practices
- IT Governance Process
- Cybersecurity Compliance and Audit Overview

Lesson 4 - An overview of key security tools

- Introduction to Firewalls
- Firewalls Packet Filtering
- Using Your Windows Lab Workspace
- Firewalls Application Gateway
- Firewalls XML Gateway
- Firewalls Stateless and Stateful
- Antivirus/Antimalware
- An introduction of Cryptography
- Types of Cryptography
- Cryptographic Attacks
- Cryptography a different perspective from a Security architect
- Penetration Testing Introduction
- Pentest Methodologies
- Vulnerability Tests
- What is Digital Forensics?



