BOOST
THE LEADING TRAINING PROVIDER

Information Technology

Cybersecurity Foundations

Course Introduction

Businesses and organizations have been spending a lot for cybersecurity. As our society is more technologically reliant than ever before, there is no sign that this trend will stop. Personal data that could result in identity theft is now posted to the public on our social media accounts. Sensitive information like social security numbers, credit card information and bank account details are now stored in cloud storage services like Dropbox or Google Drive.

This training course is designed to provide participants with a global perspective of the challenges of designing a secure system, touching on all the cyber roles needed to provide a cohesive security solution. Through lecture, labs, and breakout discussion groups, they learn about current threat trends across the Internet and their impact on organizational security. The course will cover topics on standard cybersecurity terminology and compliance requirements, examine sample exploits, and gain hands-on experience mitigating controls.

Target Audience

This training course is designed for network professionals seeking to advance their knowledge and explore cybersecurity as a career path, and executives and managers seeking to improve their ability to communicate with security professionals and implement a robust security solution at the organizational level.

Learning Objectives

- Gain a comprehensive understanding and awareness of security
- Identify different data protection principles
- Interpret and analyze tool output for network mapping/footprinting
- Reduce attack surface of systems and network devices
- Review networking as it applies to security controls

- Examine the role of PKI/certificates in building trusted relationships between devices in a network
- Implement login security and other identity management solutions
- Explore current malware threats, anti-malware solutions, social engineering threats, methods, and techniques
- Analyze software vulnerabilities and security solutions for reducing the risk of exploitation
- Identify physical security controls and the relationship between physical and IT security
- Learn legal considerations and investigative techniques when it comes to cybersecurity

Course Outline

- **Day 01**

CYBERSECURITY AWARENESS

  - What is security?
  - Confidentiality, integrity, and availability
  - Security baselining
  - Security concerns: Humans
  - Types of threats
  - Security controls
  - What is hacking?
  - Risk management
  - Data in motion vs. data at rest
  - Module review

NETWORK DISCOVERY

  - Networking review
  - Discovery, footprinting, and scanning

- Common vulnerabilities and exposures
- Security policies
- Vulnerabilities
- Module review

SYSTEMS HARDENING

- What is hardening?
- Types of systems that can be hardened
- Security baselines
- How to harden systems
- Hardening systems by role
- Mobile devices
- Hardening on the network
- Analysis tools
- Authentication, authorization, and accounting
- Physical security
- Module review

- **Day 02**

SECURITY ARCHITECTURE

- Security architecture
- Network devices
- Network zones
- Network segmentation
- Network Address Translation
- Network Access Control
- Module review

DATA SECURITY

- Cryptography
- Principles of permissions

- Steganography
- Module review

PUBLIC KEY INFRASTRUCTURE

- Public key infrastructure
- Certification authorities
- Enabling trust
- Certificates
- CA management
- Module review

- **Day 03**

IDENTITY MANAGEMENT

- What is identity management?
- Personally identifiable information
- Authentication factors
- Directory services
- Kerberos
- Windows NT LAN Manager
- Password policies
- Cracking passwords
- Password assessment tools
- Password managers
- Group accounts
- Service accounts
- Federated identities
- Identity as a Service
- Module review

NETWORK HARDENING

- Limiting remote admin access

- AAA: Administrative access
- Simple Network Management Protocol
- Network segmentation
- Limiting physical access
- Establishing secure access
- Network devices
- Fundamental device protection summary
- Traffic filtering best practices
- Module review

MALWARE

- What is malware?
- Infection methods
- Types of malware
- Backdoors
- Countermeasures
- Protection tools
- Module review

• **Day 04**

SOCIAL ENGINEERING

- What is social engineering?
- Social engineering targets
- Social engineering attacks
- Statistical data
- Information harvesting
- Preventing social engineering
- Cyber awareness: Policies and procedures
- Social media
- Module review

SOFTWARE SECURITY

- Software engineering
- Security guidelines
- Software vulnerabilities
- Module review

ENVIRONMENT MONITORING

- Monitoring
- Monitoring vs. logging
- Monitoring/logging benefits
- Logging
- Metrics
- Module review

PHYSICAL SECURITY

- What is physical security?
- Defense in depth
- Types of physical security controls
- Device security
- Human security
- Security policies
- Equipment tracking
- Module review

- **Day 05**

INCIDENT RESPONSE

- Disaster types
- Incident investigation tips
- Business continuity planning
- Disaster recovery plan
- Forensic incident response

- Module review

LEGAL CONSIDERATIONS

- Regulatory compliance
- Cybercrime
- Module review

TRENDS IN CYBERSECURITY

- Cybersecurity design constraints
- Cyber driving forces
- How connected are you?
- How reliant on connectivity are you?
- Identity management
- Cybersecurity standards
- Cybersecurity training

Confirmed Sessions

FROM	TO	DURATION	FEES	LOCATION
May 26, 2025	May 30, 2025	5 days	4250.00 $	UAE - Dubai
July 13, 2025	July 17, 2025	5 days	2150.00 $	Virtual - Online
Aug. 4, 2025	Aug. 8, 2025	5 days	5950.00 $	switzerland - Geneva
Dec. 22, 2025	Dec. 26, 2025	5 days	4250.00 $	UAE - Dubai