BOOST
THE LEADING TRAINING PROVIDER

Information Technology

Cybersecurity Fundamentals Specialist Course

Course Introduction

This training program is designed to develop participants' abilities to design a secure system, touching on all the cyber roles needed to provide a cohesive security solution. Through different learning solutions and practical application activities, participants will learn about current threat trends across the Internet and their impact on organizational security. The training program will cover topics on standard cybersecurity terminology and compliance requirements, examine sample exploits, and gain hands-on experience by mitigating controls.

Target Audience

- IT Professionals Transitioning to Security Roles – IT staff (network admins, system admins, developers) who want to expand their skillset to include cybersecurity practices.
- Junior to Mid-Level Security Analysts – Security team members looking to broaden their understanding of holistic system security and hands-on mitigation strategies.
- Compliance and Risk Officers – Professionals who need to understand cybersecurity threats and controls in order to assess organizational risks and ensure regulatory compliance.
- Technical Managers and Team Leads – Leaders responsible for designing, managing, or overseeing secure systems, who need a comprehensive understanding of security components and coordination across roles.
- Students and Graduates in IT or Computer Science Fields

Learning Objectives

- Understand and apply different data protection strategies.
- Master Interpreting and analyzing tool output for network mapping/foot printing.

- Master reducing attack surface of systems and network devices.
- Understand how to examine the role of PKI/certificates in building trusted relationships between devices in a network.
- Master Implementing login security and other identity management solutions.
- Identify current malware threats, anti-malware solutions, social engineering threats, methods, and techniques.
- Master Analyzing software vulnerabilities and security solutions for reducing the risk of exploitation.
- Identify physical security controls and the relationship between physical and IT security.
- Understand 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

SECURITY ARCHITECTURE

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

- **Day 02**

DATA SECURITY

  - Cryptography
  - Principles of permissions
  - Steganography
  - Module review

PUBLIC KEY INFRASTRUCTURE

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

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 03**

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 04**

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
- **Day 05**

  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
June 16, 2025	June 20, 2025	5 days	4250.00 $	UAE - Dubai