insureTech Skills

2025

CYBER SECURITY ANALYST TRAINING CURRICULUM

COURSE HIGHLIGHTS

Hands-on lab experience and real-world projects,

30 Hour Live Virtual Training

Industry-experienced instructors

Classes available on Weekend/Weekdays

COURSE OBJECTIVES

- IT Professionals
- Security Architect
- Network Administrator
- Ethical Hacker
- System Administrators
- Vulnerability Analysts
- Threat Intelligence Analysts
- Cybersecurity Consultant, and

MODULE 1:

Introduction to Cybersecurity and the Role of a Cybersecurity Analyst

Subtopics

- Understanding the Role of a Cybersecurity Analyst
- Importance of Cybersecurity in Modern Organizations

Key Concepts: Risk Management, Incident Response, Vulnerability Management
Cyber Threat Intelligence and its Importance

MODULE 2:

Introduction of Networking Concepts

Subtopics

- Understanding of basic networking
- Protocols and its type, TCP/IP Protocol Suit
- Different type of communication
- Client-server Architecture
- OSI Reference Model
- IP Addressing: IPv4 & Ipv6

MODULE 3:

Threat and Vulnerability Management

Subtopics

- Identifying and Evaluating Cyber Threats
  Vulnerability Scanning and Risk Assessment Techniques

- Exploitation of Vulnerabilities and Mitigation Strategies
- Continuous Monitoring for Threats and Vulnerabilities
- Cybersecurity Frameworks for Threat Management

LAB:

Tools: Nessus, BurpSuit, Owasp, Nikto, CMSeek
Exercise: Perform a vulnerability scan and report findings.

MODULE 4:

Network Security and Defensive Techniques

Subtopics

- Network Segmentation and Firewall Configuration
- IDS/IPS Implementation and Configuration
- Monitoring Network Traffic for Malicious Activity
- Defense Mechanisms Against Lateral Movement in Networks

LAB:

Tools: Wireshark, Nmap
Exercise: Analyze network traffic with Wireshark to identify potential threats

MODULE 5:

Cloud Concepts and Security

Subtopics

- Cloud Computing Models: IaaS, PaaS, SaaS
- Cloud Security Risks and Best Practices
- Compliance and Governance for Cloud Security

LAB:

Tools: Wireshark, Nmap
Exercise: Analyze network traffic with Wireshark to identify potential threats

MODULE 6:

Endpoint Security

Subtopics

- The Importance of Endpoint Protection in Organizational Security
- Antivirus, EDR (Endpoint Detection and Response), and PatchManagement
- Securing Remote Devices and Implementing BYOD Policies
- Mobile Device Management (MDM) and Endpoint Hardening

LAB:

Tools: Windows Firewall, Windows Defender
Exercise: Configure and manage endpoint protection on test systems.

MODULE 7:

Risk Management and Security Governance

Subtopics

- Risk Assessment Models and Frameworks
- Developing a Risk Management Strategy for Organizations
- Security Governance and Regulatory Compliance (NIST, PCI-DSS, HIPAA, GDPR)
- Effective Communication of Security Strategies with Stakeholders

Tools Used Throughout the Curriculum:

- Nessus: Vulnerability scanning and risk management tool.
- Splunk: SIEM tool for log aggregation and threat detection.
- Wireshark: Network traffic analysis tool.
- Nikto, CMSeek: Web Server testing
- OWASP ZAP/Burp Suite: Web application security testing tools.
- Windows Firewall/Windows Defender: Endpoint protection tools.