



Logic Finder
Consulting, Development and Training

Introduction to Cybersecurity and Cyber Threat Landscape

Instructor Led Live Virtual Class

Duration: 6 Day (20-30 hours) | Course Number: LF-Introduction to Cybersecurity and Cyber Threat Landscape-200

Course Syllabus:

Duration: 12 Weeks

Week 1-2: Introduction to Cybersecurity and Cyber Threat Landscape

Objective: Understand the fundamentals of cybersecurity.

Topics:

- Basic concepts: confidentiality, integrity, availability
- Types of cyber threats and attacks (malware, phishing, etc.)
- Cyber threat actors and motivations

Practical: Introduction to cybersecurity tools, and setting up a secure workstation.

2. Week 3-4: Network Security Fundamentals

Objective: Grasp the basics of network security.

Topics:

- Networking concepts (TCP/IP, DNS, HTTP/HTTPS)
- Firewalls, VPNs, and intrusion detection systems
- Wireless network security

Practical: Basic network configuration and monitoring using tools like Wireshark and Nmap.

Week 5-6: System Security and Hardening

Objective: Learn how to secure operating systems and endpoints.

Topics:

- Operating system security features
- Endpoint protection and anti-virus software
- Patch management and system updates

Practical: Setting up and securing a Windows/Linux environment, implementing endpoint security measures.

Week 7-8: Cybersecurity Tools and Technologies

Objective: Explore various cybersecurity tools.

Topics:

- Introduction to ethical hacking and penetration testing tools
- Security information and event management (SIEM) tools
- Vulnerability assessment tools

Practical: Hands-on with tools like Metasploit, Burp Suite, and Splunk.

Week 9-10: Incident Response and Forensics

Objective: Learn to manage and respond to security incidents.

Topics:

- Incident response lifecycle
- Digital forensics basics
- Legal considerations in cyber investigations

Practical: Simulating a cyber incident and practicing incident response.

Week 11-12: Advanced Topics and Capstone Project

Objective: Apply learned skills in a real-world scenario.

Topics:

- Advanced persistent threats (APT)
- Cloud security and IoT considerations
- Emerging trends in cybersecurity

Practical: Capstone project involving a comprehensive security assessment or a simulated cyber attack and defense scenario.

Each week should include:

Lectures: Covering theoretical aspects.

Labs: Practical, hands-on exercises.

Assignments: To reinforce learning.

Quizzes/Tests: To assess understanding.