CYBERSECURITY COURSE SYLLABUS

Module 1 — Introduction to Cyber Security

- What is Cyber Security?
- Different types of Cyber Security
- Types of Hackers
- Common Motives of a Hacker
- Different Roles in the Cyber Security Domain

Module 2 — Introduction to SOC Analyst

- What is a SOC?
- Who is a SOC Analyst?
- SOC Models (Dedicated, Co-managed, Virtual, etc.)
- SOC Team Architecture / Hierarchy
- Importance of SOC – Explained Using a Network Diagram
- Why Organizations Need a SOC Team
- Roles and Responsibilities of SOC Team Members

Module 3 — Security Operations Center Concepts

- Types of Computer Networks
- IP Addressing and Its Versions (IPv4, IPv6)
- Difference Between Private and Public IP Addressing
- OSI & TCP/IP Models
- TCP vs UDP Protocols
- TCP Handshake Process
- TCP Flags
- OSI Layer-wise Devices and Attacks
- AAA & Non-repudiation (Authentication, Authorization, Accountability)
- Encryption, Encoding, Hashing – Concepts and Types
- Principles of Information Security (CIA Triad, etc.)
- Basic Security Definitions
- Common Port Numbers
- Cyber Kill Chain Model
- MITRE ATT&CK Framework

Module 4 — Network and Security Devices

- Introduction to Network & Security Devices
- Firewalls (Types & Functions)
- Web Application Firewall (WAF)
- Intrusion Detection & Prevention Systems (IDS/IPS)
- Antivirus Solutions
- Endpoint Detection & Response (EDR)
- Web Proxy
- Email Gateway
- DHCP
- DNS
- Active Directory Basics

Module 5 — SIEM (Security Information & Event Management)

- Introduction to SIEM
- SIEM Workflow
- Concepts: Aggregation, Normalization, Correlation, Parsing
- Event vs Alert vs Incident
- SIEM Architecture Overview: QRadar, Splunk, Microsoft Sentinel
- SIEM Installation Overview
- Writing and Understanding SIEM Rules

SkillsITera
Break Limits. Build Skill. Rewrite Your Story
www.SkillsITera.com
+91 8639039660

CYBERSECURITY COURSE SYLLABUS

Module 6 — Incident Management

- Event Classification
- Incident Response Lifecycle (Preparation → Recovery)
- Incident Management Tools Overview
- Common SOC Use Cases / Alerts
- Incident Playbooks
- Service Level Agreements (SLAs)
- Handling Incidents Using SIEM and EDR
- Use Case Fine-Tuning
- Open Source Intelligence (OSINT) Tools
- EDR Alert Analysis
- SOC Shift Handover Procedures
- SOC Reporting Methods
- Basics of Malware Analysis

Module 7 — Cyber Threat Intelligence

- Introduction to Threat Intelligence & Threat Hunting
- Threat Intelligence Sources (OSINT, Commercial, etc.)
- Indicators of Compromise (IOC) and Indicators of Attack (IOA)
- Importance of IOCs in Detection
- IOC-based Threat Hunting in SIEM

Module 8 — Email Analysis

- Email Services & Protocols (IMAP, POP3, SMTP)
- Email Workflow (Sender → Receiver)
- Types of Phishing Emails
- Step-by-Step Email Analysis
- Email Header Analysis
- Email Authentication Protocols (SPF, DKIM, DMARC)
- SOC Actions in Response to Phishing Emails

Module 9 — Cyber Attacks

- DoS and DDoS Attacks
- DNS Attacks: Spoofing, Poisoning, Tunneling
- Brute Force Attack
- Password Spraying Attack
- Dictionary Attack
- SQL Injection
- Cross-Site Scripting (XSS) Injection
- Watering Hole Attack
- Supply Chain Attack
- Man-in-the-Middle (MITM) Attack
- Ransomware
- Session Hijacking
- Eavesdropping Attacks
- Business Email Compromise (BEC)
- Fileless Malware
- Living Off the Land Binaries (LOLBins)

Module 10 — Miscellaneous

- Kerberos Authentication Process
- Types of Malwares
- CVE and CVSS Scoring
- Zero-Day Vulnerability and Attacks
- OWASP Top 10 Vulnerabilities
- Windows Event IDs and Logon Types
- Data Exfiltration Techniques
- Data Loss Prevention (DLP) Overview

www.SkillsITera.com
+91 6300926962