SOC (Security Operations Center) Analyst

1. Module: Basics of Cyber Security

- Information Security
- CIA Triad
- Common Network Security Terms
- Vulnerability, Exploit, Threat, Risk
- Malware
- Types of Malware
- Cyber Attack
- Types of Attack
- APT

2. Module: Introduction to SOC

- SOC Roles & Responsibilities
- SOC Levels (L1, L2, L3)
- SOC Workflow & Escalation Matrix
- Blue Team vs Red Team

3. Module: Networking Fundamentals

- OSI Model & TCP/IP Model
- IP Addressing & Subnetting
- Routing & Switching Basics
- DNS, DHCP, NAT
- Common Protocols
- HTTP/HTTPS
- FTP
- SSH
- SMTP
- SNMP
- Packet Analysis Basics
- VPN & Remote Access

4. Module: Firewall & Security Devices Technologies

- Introduction of Firewall
- Types of Firewall
- Stateful vs Stateless
- IDS and IPS
- Traditional vs Next-Generation Firewall
- Trust Zone, Untrust Zone , DMZ Zone
- WAF
- Antivirus/Endpoint Security
- Email Security
- NAC Basics
- VPN Security
- Configure Software Firewall
- Configure Firewall on Linux System

5. Module: SIEM

- Introduction to SIEM
- Log Collection & Correlation
- SIEM Architecture
- Alert Monitoring
- Use Cases
- Dashboard Creation
- Incident Investigation
- SIEM Platforms:
- Splunk
- WAZUH
- ELK Stack

6. Module: Endpoint Detection & Response (EDR)

- Introduction to EDR
- Endpoint Monitoring
- Threat Detection
- Malware Investigation
- IOC Analysis

7. Module: Threat Intelligence

- IOC & IOA
- MITRE ATT&CK Framework
- Cyber Kill Chain
- Threat Hunting Basics
- Open-Source Intelligence (OSINT)
- Threat Feeds

8. Module: Vulnerability Scanning

- Introduction of Vulnerability ,Bug and Payload
- Vulnerability Scoring System
- Tool for Vulnerability Scanning
- CVE & CVSS
- Patch Management
- Nessus Basics
- OpenVAS Basics
- Risk Prioritization
- WPScan , Nessus
- Acunetix, Qualys, Crashtest, Nikto, MSF-Pro, NSE Script, Pentest toolbox etc.

9. Module: Digital Forensics Basics

- Memory Forensics
- Disk Forensics
- Log Analysis
- Evidence Collection
- Chain of Custody
- Tools:
- Volatility
- FTK Imager
- Autopsy
- OS Forensic

10. Module: Email Security & Phishing Analysis

- Email Headers

- SPF, DKIM, DMARC
- Phishing Investigation
- URL Analysis
- Attachment Analysis
- Sandbox Basics

11. Module: Malware Analysis Basics

- Introduction to Malware
- Malware Concepts
- Types of Trojans
- VIRUS , Worms
- RAT's and Rootkits
- Malware Analysis
- Static vs Dynamic Analysis
- Hash Analysis
- Sandbox Analysis
- YARA Basics

12. Module: Cloud Security Basics

- Introduction of Cloud
- AWS Security Basics
- Azure Security Basics
- Cloud Logs
- IAM Basics
- Cloud Threats

13. Module: AI and ML in Cyber Security

- Introduction of AI and ML
- Role of AI and ML in Cyber Security
- AI and ML Prevent Cyber Attack
- AI-based Security
- 30+ AI tool used in Cyber Security
- AI for Defensive and Offensive Mode