Quality Thought®

Transforming Dreams! Redefining Future!

CELEBRATING 15 YEARS

Cyber Security

Cyber Security Fundamentals

Objective: To build a strong foundation in IT, networking, operating systems, cloud computing, and cybersecurity.

Phase 1: IT & Networking Fundamentals

◆ **Module 1: IT Fundamentals**

- Introduction to Computer Systems (Hardware & Software)
- Operating Systems Overview (Windows, Linux, macOS)
- Basics of Virtualization (VMware, VirtualBox, Cloud Instances)

◆ **Module 2: Networking Basics**

- OSI & TCP/IP Model, IP Addressing & Subnetting
- Common Network Devices (Router, Switch, Firewall)
- Essential Protocols: HTTP, DNS, SSH, VPN, RDP

◆ **Module 3: Network Security Essentials**

- Basics of Firewalls, IDS/IPS, and VPNs
- Hands-on: Setting Up a Basic Firewall (pfSense)
- Traffic Analysis with Wireshark

Phase 2: OS & Cloud Fundamentals

◆ **Module 4: Linux Basics for Security**

- Linux File System & Directory Structure
- Basic Linux Commands & Bash Scripting
- Linux Security Features (Firewall, Permissions, Process Management)

◆ **Module 5: Windows Basics for Security**

- Windows System Architecture & File Structure
- User & Group Management (Active Directory Basics)
- Windows Event Logs & Security Policies

◆ **Module 6: Cloud Security Fundamentals**

- Introduction to Cloud Computing (AWS, Azure, Google Cloud)
- Identity & Access Management (IAM), Security Groups & Firewalls
- Hands-on: Deploying & Securing an AWS EC2 Instance

Phase 3: Cybersecurity Foundations

◆ Module 7: Cybersecurity Fundamentals

- Cyber Threats: Malware, Phishing, Ransomware, Social Engineering
- Introduction to MITRE ATT&CK Framework & Cyber Kill Chain
- Basic Security Controls & System Hardening

◆ Module 8: Security Operations & Monitoring

- Introduction to Log Analysis
- Windows Event Logs for Security Monitoring
- Linux Syslog & Security Monitoring
- SIEM (Security Information & Event Management) Basics
- Cloud Security Logs

Course Outcome:

Strong **IT, Networking, Linux, Windows, and Cloud Security** knowledge
Hands-on skills in **firewall setup, cloud security, and system monitoring**

SOC Analyst Training Program

- **Target Audience:** Beginners aspiring to become SOC Analysts
- **Outcome:** Students will be job-ready for SOC Analyst (L1) roles, mastering SIEM, log analysis, threat detection, and incident response.
- **Hands-On Labs:** Implementing security monitoring, analysing real-world attacks, and responding to incidents using **open-source tools**.

PHASE 1: Security Operations & Monitoring

Objective: Learn the fundamentals of SOC operations, log analysis, and security monitoring.

◆ Module 1: Introduction to Security Operations

- What are a Security Operations Center (SOC)?
- SOC Roles & Responsibilities (Tier 1, Tier 2, Tier 3)
- Security Incident Lifecycle (NIST & SANS Models)
- Introduction to SIEM (Security Information and Event Management)

◆ Module 2: Understanding Log Sources

- Types of logs (Firewall, IDS/IPS, Windows, Linux, Web, Cloud)
- Syslog, Event Logs, and JSON Parsing
- Log Aggregation & Correlation
- Hands-on Lab: Collecting & Analysing Logs using **Wazuh & ELK**

◆ **Module 3: Network Security Monitoring**

- Packet Capture & Deep Packet Inspection (DPI)
- IDS vs. IPS (Suricata vs. Snort)
- Analysing PCAP files using **Wireshark**
- Hands-on Lab: Detecting Network Intrusions with **Suricata & Zeek**

◆ **Module 4: Endpoint Security & Threat Detection**

- Windows Event Logs & Sysmon Analysis
- Linux Syslog & Audit Monitoring
- Endpoint Detection & Response (EDR) Basics
- Hands-on Lab: Investigating Endpoint Attacks with **Wazuh EDR**

PHASE 2: Threat Intelligence & Detection

Objective: Learn how to detect, analyse, and respond to threats using real-world attack scenarios.

◆ **Module 5: Cyber Threat Intelligence (CTI)**

- Threat Intelligence Sources (MITRE ATT&CK, AlienVault OTX, MISP)
- IOC (Indicators of Compromise) & IOA (Indicators of Attack)
- Hands-on Lab: Automating Threat Intelligence Feeds with **MISP**

◆ **Module 6: Malware Analysis & Detection**

- Static vs. Dynamic Malware Analysis
- Analysing Suspicious Files with **YARA**
- Hands-on Lab: Investigating Malware using **Cuckoo Sandbox**

◆ **Module 7: Threat Hunting Fundamentals**

- Proactive vs. Reactive Security Monitoring
- Hypothesis-Driven Threat Hunting
- Hands-on Lab: Detecting APTs using **Sigma & KQL**

◆ **Module 8: Cloud Security Monitoring**

- AWS, Azure, & Google Cloud Security Logging
- Analysing Cloud Logs using **ELK & Wazuh**
- Hands-on Lab: Detecting Cloud Threats using **AWS Guard Duty**

PHASE 3: Incident Response & Automation

Objective: Learn how to respond to security incidents and automate detection workflows.

◆ **Module 9: Incident Handling & Response**

- Incident Handling Process (Preparation, Detection, Containment, Eradication, Recovery)
- Hands-on Lab: Simulating an Incident Response Scenario

◆ **Module 10: Digital Forensics & Investigation**

- Disk & Memory Forensics Basics
- Hands-on Lab: Analysing a Compromised System using **Autopsy & Volatility**

◆ **Module 11: Security Automation & SOAR**

- Automating Security Operations with SOAR
- Hands-on Lab: Creating Automated Playbooks using **The Hive & Cortex XSOAR**

PHASE 4: Advanced SOC Techniques

Objective: Learn advanced SOC techniques and prepare for real-world job scenarios.

◆ **Module 12: Red Team vs. Blue Team**

- Understanding Adversarial Techniques (TTPs)
- Hands-on Lab: Simulating a Red Team Attack & Blue Team Response

◆ **Module 13: SIEM Customization & Correlation Rules**

- Writing Custom SIEM Rules (Sigma, ELK, Wazuh Rules)
- Hands-on Lab: Creating SIEM Correlation Rules for Threat Detection

◆ **Module 14: SOC Job Preparation & Certification Guidance**

- SOC Analyst Job Responsibilities & Resume Building
- Mock Interviews & Certification Prep (SOC Analyst+, CompTIA Cy SA+, Splunk Core Certified User)

Final Project: SOC Attack Simulation & Response (Extra Cost) – One Month

🔻 Simulate a real-world cyber attack
🔻 Detect, analyse, and respond using SIEM, EDR, and Threat Intelligence
🔻 Present findings in an Incident Report

Security Operations & Monitoring (SOC Analyst, Blue Team)

Objective:
This course will train students in **security operations, threat detection, log analysis, incident response, threat intelligence, and SIEM tools**. By the end of the course, students will be **job-ready for SOC Analyst (Tier 1 & 2), Blue Team, and Threat Hunting roles**.

PHASE 1: Security Operations Fundamentals (Days 1-15)

Objective: Understand SOC structure, security monitoring, log analysis, and fundamental tools.

◆ **Module 1: Introduction to Security Operations & SOC (Day 1-3)**

- What is a Security Operations Center (SOC)?
- SOC Team Structure (Tier 1, Tier 2, Tier 3, Threat Intel, Incident Response)
- SOC Processes & Workflows (NIST, MITRE ATT&CK)

◆ **Module 2: Log Analysis & Security Monitoring Basics (Day 4-7)**

- Understanding Logs (Windows, Linux, Firewall, IDS/IPS, EDR, Cloud)
- Hands-on Lab: **Log Analysis using ELK & Wazuh**
- Log Retention & Compliance (ISO 27001, PCI DSS, GDPR)

◆ **Module 3: SIEM Fundamentals & Log Correlation (Day 8-12)**

- Introduction to **Security Information & Event Management (SIEM)**
- Deploying **SIEM tools (Splunk, Wazuh, ELK Stack)**
- Hands-on Lab: **Log Correlation & Custom SIEM Dashboards**

◆ **Module 4: Incident Handling Process & Threat Intelligence (Day 13-15)**

- Incident Response Frameworks (NIST, SANS)
- Threat Intelligence Platforms (MISP, AlienVault OTX)
- Hands-on Lab: **Analyzing Threat Intelligence Feeds**

PHASE 2: Threat Detection & Intrusion Monitoring (Days 16-30)

Objective: Learn network security monitoring, intrusion detection, and endpoint security.

◆ **Module 5: Intrusion Detection & Prevention Systems (IDS/IPS) (Day 16-19)**

- Network-based IDS/IPS (Snort, Suricata)
- Hands-on Lab: **Deploying Snort/Suricata for Threat Detection**
- Creating **Custom IDS/IPS Rules**

◆ **Module 6: Endpoint Detection & Response (EDR) (Day 20-24)**

- Introduction to **EDR/XDR Solutions (CrowdStrike, Wazuh, Osquery)**
- Hands-on Lab: **Monitoring Windows & Linux endpoints using Wazuh**
- Investigating **Suspicious Endpoint Behavior**

◆ **Module 7: Cloud Security Monitoring (Day 25-30)**

- Security Monitoring in AWS, Azure, GCP
- Hands-on Lab: **Configuring AWS GuardDuty, Azure Sentinel**
- Cloud Log Analysis (CloudTrail, Flow Logs, Security Logs)

PHASE 3: Threat Hunting & Advanced Security Monitoring (Days 31-45)

Objective: Learn proactive defense techniques using threat hunting and malware analysis.

◆ **Module 8: Proactive Threat Hunting (Day 31-35)**

- MITRE ATT&CK Framework for Threat Hunting
- Hands-on Lab: **Threat Hunting using Sigma Rules & YARA**
- Detecting Advanced Persistent Threats (APT)

◆ **Module 9: Malware Analysis & Reverse Engineering (Day 36-40)**

- Static vs. Dynamic Malware Analysis
- Hands-on Lab: **Analyzing Malware using Cuckoo Sandbox**
- Extracting **Indicators of Compromise (IoCs)**

◆ **Module 10: SOC Use Cases & Real-World Attack Scenarios (Day 41-45)**

- Detecting **Brute Force Attacks, Phishing, Insider Threats**
- Hands-on Lab: **Simulating and Detecting Cyber Attacks in SIEM**
- Creating **SOC Playbooks for Threat Response**

PHASE 4: Incident Response & SOAR Automation (Days 46-60)

Objective: Learn incident handling, forensics, and automation using SOAR.

◆ **Module 11: Incident Response & Digital Forensics (Day 46-50)**

- Hands-on Lab: **Incident Triage & Investigation**
- Memory Forensics (Volatility)
- File System & Network Forensics

◆ **Module 12: Automating SOC Workflows with SOAR (Day 51-55)**

- Introduction to **Security Orchestration, Automation, and Response (SOAR)**
- Hands-on Lab: **Automating Incident Response using TheHive & Cortex XSOAR**
- Writing **Custom SOAR Playbooks for Automated Threat Remediation**

◆ **Module 13: SOC Final Assessment & Career Readiness (Day 56-60)**

- Hands-on Lab: **Final SOC Attack Simulation & Report Writing**
- Resume Building & SOC Job Interview Preparation
- SOC Career Path (Tier 1 to Tier 3, Threat Intel, Red Teaming)

Final Project: Real-World SOC Investigation & Threat Hunting Report (One Month Extra Cost)

✓ Analyze a **real-world attack scenario** (Ransomware, APT, Phishing)
✓ Investigate logs, correlate alerts, and identify **Indicators of Compromise (IoCs)**
✓ Create a **Threat Report & Incident Response Plan**

◆ Network Security Specialist

PHASE 1: Network Security Foundations

Objective: Understand core network security concepts, protocols, and fundamental defences.

◆ Module 1: Network Security Basics

-OSI & TCP/IP Model from a Security Perspective
-Common Network Attacks (MITM, DoS, Spoofing, DNS Poisoning)
-Introduction to Network Security Tools (Wireshark, Tcpdump, Nmap)

◆ Module 2: Firewall Security & Packet Filtering

-Types of Firewalls (Packet Filtering, Stateful, Application Layer)
-Hands-on Lab: **Deploying & Configuring pfSense & SonicWall Firewalls**
-Creating Secure Firewall Rules & Access Control Lists (ACLs)

◆ Module 3: Virtual Private Networks (VPNs) & Secure Remote Access

-VPN Types (IPSec, SSL, L2TP, Wire Guard)
-Hands-on Lab: **Setting up OpenVPN & IPSec VPNs**
-Implementing Zero Trust Network Access (ZTNA)

◆ Module 4: Network Segmentation & Secure Architecture

-VLANs, DMZs, Micro segmentation for Security
-Hands-on Lab: **Configuring VLANs & Network Isolation**
-Implementing Least Privilege Network Access

📌 PHASE 2: Advanced Threat Protection & Monitoring

Objective: Learn advanced perimeter security, intrusion detection, and network monitoring.

◆ Module 5: Intrusion Detection & Prevention Systems (IDS/IPS)

-Signature-based vs. Anomaly-based Detection
-Hands-on Lab: **Deploying Snort & Suricata for Threat Detection**
-Creating & Tuning Custom IDS/IPS Rules

◆ Module 6: Secure Wireless Networks

-Wireless Security Protocols (WPA2, WPA3, EAP)
-Hands-on Lab: **Hardening Wi-Fi Security & Detecting Rogue APs**
-Wireless Attack Techniques (Evil Twin, DE authentication, KRACK)

◆ **Module 7: Network Traffic Analysis & Threat Detection**

-Understanding Network Logs & Anomaly Detection
-Hands-on Lab: **Packet Analysis using Wireshark & Zeek (Bro IDS)**
-Detecting Malicious Traffic & IoCs in Network Logs

📌 **PHASE 3: Securing Enterprise & Cloud Networks**

Objective: Learn enterprise-grade network security strategies, DDoS mitigation, and cloud security.

◆ **Module 8: Secure Network Architecture & Zero Trust**

-Network Hardening Strategies (NIST, CIS Controls)
-Implementing Zero Trust Security Model
-Hands-on Lab: **Designing a Secure Network Topology**

◆ **Module 9: DDoS Protection & Network Forensics**

-Understanding DDoS Attack Techniques (Volumetric, Application Layer)
-Hands-on Lab: **Mitigating DDoS Attacks using Cloudflare & WAF**
-Conducting **Network Forensics & Incident Response**

◆ **Module 10: Cloud Network Security (AWS, Azure, GCP)**

-Cloud Networking & Security Groups
-Hands-on Lab: **Configuring AWS VPC Security & Network ACLs**
-Securing Cloud Traffic using VPNs & Firewalls

📌 **PHASE 4: Incident Response & Network Security Automation**

Objective: Learn network security automation, SIEM integration, and incident response.

◆ **Module 11: Security Operations & SIEM**

-Integrating Firewalls & IDS with SIEM (Splunk, Wazuh)
-Hands-on Lab: **Analysing Network Security Logs in SIEM**
-Creating **Custom Network Security Alerts & Dashboards**

◆ **Module 12: Network Security Automation & SOAR**

-Automating Threat Detection with SOAR (Cortex XSOAR, The Hive)
-Hands-on Lab: **Writing Network Security Playbooks for SOAR**
-Implementing Automated Threat Remediation

◆ **Module 13: Network Security Final Assessment & Career Readiness**

-Hands-on Lab: **Final Network Attack Simulation & Report Writing**
-Resume Building & Network Security Job Interview Preparation
-Career Path Guidance (Network Security Engineer, SOC, Red Team)

🚀 Final Project: Enterprise Network Security Assessment & Defense Strategy (One Month) Extra Cost

✓ Conduct a **comprehensive security assessment** of a simulated enterprise network
✓ Identify **vulnerabilities, threats, and misconfigurations**
✓ Design a **Network Security Hardening Plan & Incident Response Report**

🔴 Penetration Testing & Red Teaming

PHASE 1: Ethical Hacking & Penetration Testing Foundations

Objective: Understand the **penetration testing process, methodologies, and tools**.

◆ Module 1: Introduction to Ethical Hacking & Red Teaming

-Ethical Hacking vs. Red Teaming vs. Bug Bounties
-Penetration Testing Methodologies (OSSTMM, PTES, NIST)
-Legal & Ethical Considerations (Pentesting Contracts, Rules of Engagement)

◆ Module 2: Reconnaissance & Open Source Intelligence (OSINT)

-Passive & Active Reconnaissance Techniques
-Hands-on Lab: **Using OSINT Tools (Maltego, Shodan, FOCA, Recon-ng)**
-DNS Enumeration & Subdomain Takeover

◆ Module 3: Scanning & Enumeration

-Network Scanning (Nmap, Masscan, Netcat)
-Service & Port Enumeration (SMB, SNMP, FTP, SSH)
-Hands-on Lab: **Identifying Attack Surfaces & Vulnerabilities**

◆ Module 4: Exploitation Fundamentals

-Understanding Exploit Development & CVE Analysis
-Hands-on Lab: **Exploiting Vulnerable Services (Metasploit, Manual Exploits)**
-Privilege Escalation Basics (Windows & Linux)

📌 PHASE 2: Network, Web, & Wireless Penetration Testing

Objective: Learn **network, web, and wireless hacking techniques**.

◆ **Module 5: Network Penetration Testing**

-Network Sniffing & Traffic Analysis (Wireshark, Tcpdump)
-Hands-on Lab: **MITM Attacks, ARP Spoofing, DNS Spoofing**
-Exploiting SMB, RDP, and SSH Misconfigurations

◆ **Module 6: Web Application Security & Pentesting**

-OWASP Top 10 Web Vulnerabilities (XSS, SQL i, CSRF, IDOR)
-Hands-on Lab: **Exploiting Web Apps using Burp Suite, SQL map, XSS Hunter**
-API Security Testing & Exploiting API Weaknesses

◆ **Module 7: Wireless & IoT Hacking**

-Wireless Security Protocols (WPA2, WPA3, WEP Cracking)
-Hands-on Lab: **Capturing & Cracking Wi-Fi Handshakes (Air crack-ng, Evil Twin)**
-IoT Device Exploitation & Smart Home Security Testing

📌 **PHASE 3: Advanced Exploitation & Red Teaming**

Objective: Learn **Active Directory attacks, privilege escalation, lateral movement, and persistence**.

◆ **Module 8: Privilege Escalation & Persistence**

-Linux & Windows Privilege Escalation Techniques
-Hands-on Lab: **Exploiting Weak Permissions, Scheduled Tasks, DLL Hijacking**
-Persistence Mechanisms (Registry, Start-up, Rootkits)

◆ **Module 9: Active Directory (AD) Penetration Testing**

-AD Enumeration (Bloodhound, Power View)
-Hands-on Lab: **Kerb roasting, Pass-the-Hash, Pass-the-Ticket Attacks**
-Lateral Movement using Mimi Katz & Rubeus

◆ **Module 10: Red Teaming Tactics & Adversary Simulation**

-Red Team vs. Blue Team vs. Purple Team
-Hands-on Lab: **Building Custom C2 Frameworks (Cobalt Strike, Empire, Sliver)**
-Evasion Techniques (Obfuscation, AMSI Bypass, Sandbox Evasion)

📌 **PHASE 4: Post-Exploitation, Reporting & Career Readiness**

Objective: Learn **post-exploitation techniques, attack reporting, and career preparation**.

◆ **Module 11: Post-Exploitation & Data Exfiltration**

-Hands-on Lab: **Extracting Sensitive Data, Password Hashes, Token Impersonation**
-Exfiltration Techniques (DNS Tunnelling, Steganography, Covert Channels)
-Covering Tracks (Log Manipulation, Anti-Forensics)

◆ **Module 12: Writing Penetration Testing Reports**

-Hands-on Lab: **Creating a Professional Pentest Report**
-CVSS Scoring & Risk Assessment
-Delivering Findings to Stakeholders

◆ **Module 13: Red Team Final Assessment & Career Guidance**

-**Final Exam: Simulated Red Team Engagement on an Enterprise Network**
-Resume Building & Ethical Hacking Job Interview Prep
-Career Paths: **Penetration Tester, Red Teamer, Bug Bounty Hunter, Security Consultant**

🚀 **Final Project: Full-Scale Red Team Assessment on a Simulated Enterprise Network (Extra Cost & One Month)**

✓ Conduct a **real-world penetration test & adversary simulation**
✓ Identify & exploit **vulnerabilities in network, web, AD, and cloud environments**
✓ Write a **comprehensive penetration testing report**

💼 **Career Opportunities after this Course**

🎯 **SOC Analyst (L1/L2)**
🎯 **Threat Intelligence Analyst**
🎯 **Incident Responder**
🎯 **Cybersecurity Analyst**
🎯 **SIEM Engineer**

🎯 **SOC Analyst (Tier 1, Tier 2, Tier 3)**
🎯 **Threat Hunter**
🎯 **Security Operations Engineer**
🎯 **Incident Responder**
🎯 **Cyber Threat Intelligence Analyst**

🎯 **Network Security Engineer**
🎯 **Firewall & Perimeter Security Administrator**
🎯 **SOC Analyst (Network Security Focus)**
🎯 **Threat Detection Engineer**
🎯 **Cloud Network Security Engineer**

- Penetration Tester (Web, Network, Wireless, Cloud)
- Red Team Operator / Adversary Emulation Specialist
- Bug Bounty Hunter & Security Researcher
- Offensive Security Consultant
- Exploit Developer & Malware Analyst