SQL SCHOOL
Premium Quality Training

CYBER SECURITY

100% Job Oriented Trainings & Projects
Handled by 10+ Years Experienced Cyber Security Experts

This Practical, Highly Technical Cyber Security Training Program is handled by Realtime On-Job Experts to make you a TRUE Cyber Security Professional.

This Cyber Security Training includes:

- **Module 1: Cyber Security – Ethical Hacking**
- **Module 2: Defensive Security (Blue Team) @ SOC / SIEM / EDR**
- **Module 3: GRC**

Applicable Job Roles:

1. **Cyber Security Professional**
2. **Cyber Security Specialist**
3. **SOC Analyst**
4. **SIEM Analyst**

DETAILED COURSE CONTENT

Module 1: Cyber Security – Ethical Hacking

Ch 1: Introduction to Cybersecurity

- The evolution of Cybersecurity
- What is Information Security & Cybersecurity
- Cybersecurity objectives
- Cybersecurity Roles
- Domain of cyber security
- Cybersecurity objectives
- The Cybersecurity skills gap
- Cybersecurity & situational awareness

Ch 2: Operating Systems in Cyber Security

- Intro to operating systems
- Different types of Operating Systems
- What is Virtual Machine
- What is Virtualization
- Intro to Kali Linux
- Installation of Kali Linux

Ch 3: Ethical Hacking in Cyber Security

- Introduction to Ethical hacking
- What is hacking
- Types of Hackers
- World Top 10 hackers and their HATs
- 5 Phases of Hacking
- FootPrint/Information Gathering

Ch 4: Ethical Hacking Tools

- Tools: Maltego, Recon-ng, whois, Shodan, Google Dorks.

- Scanning
- Tools: Nmap, Angry IP Scanner, Nessus

Ch 5: Ethical Hacking Access

- Gaining Access
- Maintaining Access
- Clearing Tracks
- Types of Attacks - Active / Passive Attacks
- Penetration Testing
- Offensive and defensive security
- Teams in cyber security - Red/Blue/Purple

Ch 6: Networking Essentials in Cyber Security - 1

- Infrastructure Terminology
- Designing with Security in Mind
- Network Diagrams
- Network Topology
- OSI Layers & TCP/IP Model
- IPv4 & Ipv6
- Ports & protocols
- Port numbers

Ch 7: Networking Essentials in Cyber Security - 2

- Wireless Attacks
- Firewalls
- IDS/IPS
- Honeypots
- Cloud Computing
- VPNs and VPN Concentrators

Ch 8: Networking Essentials in Cyber Security - 3

- Intrusion Detection Systems
- Router
- Switch
- Proxy
- Network Access Control (NAC)
- Different Types of networks

Ch 9: Cryptography & Data Protection - 1

- Introduction to Cryptography

- **Purpose and role in cybersecurity**
- **Key terminology (plaintext, ciphertext, key, algorithm)**
- **Types of Cryptography**
- **Symmetric Encryption (AES, DES, 3DES, Blowfish)**
- **Asymmetric Encryption (RSA, ECC)**
- **Hybrid encryption models**

Ch 10: Cryptography & Data Protection - 2

- **Hashing & Integrity**
- **Hash functions (MD5, SHA-1, SHA-256, SHA-3)**
- **Digital fingerprints and integrity verification**
- **Common hashing use cases (password storage, file verification)**
- **Digital Signatures & Certificates**
- **Signing process and verification**
- **Role of PKI (Public Key Infrastructure)**
- **X.509 certificates**
- **Key Management**
- **Key generation, distribution, storage, and rotation**
- **Hardware Security Modules (HSMs)**
- **Key escrow and recovery procedures**

Ch 11: Data Protection & Encryption - 1

- **Cryptographic Protocols**
- **SSL/TLS basics**
- **IPsec and VPN encryption**
- **Secure Email protocols (S/MIME, PGP)**
- **Common Cryptographic Attacks**
- **Brute force & dictionary attacks**
- **Hash collision attacks**
- **Data Encryption at Rest & In Transit**
- **Disk encryption (BitLocker, VeraCrypt)**
- **Database encryption methods**

Ch 12: Data Protection & Encryption - 2

- **Network encryption (HTTPS, SSH, VPN)**
- **Compliance & Best Practices**
- **Cryptography in ISO 27001, PCI DSS, HIPAA**
- **Strong encryption standards & key length recommendations**
- **Avoiding deprecated algorithms**
- **Tools for Cryptography**
    A. OpenSSL
    B. hashcat

Ch 13: Advanced Pentesting in Cyber Security

- Introduction to Bug Bounty
- Basic Terminology on Bug Bounty
- Bug Bounty Platforms
- Lab setup for Pentesting
- Installation of Burp Suite Tool
- Bug Bounty Platforms
- Reporting of the bugs
- Vulnerability Scanner Tools
- Web Application Vulnerabilities
- Cross Site Scripting
- Host Header Injection
- URL Redirection Attack
- Parameter Tampering
- SQL Injection
- Bypass Authentication
- Sensitive Information

Ch 14: Vulnerability Attacks in Cyber Security

- File Upload Vulnerability
- Disclosure Vulnerability
- CSRF Attack Vulnerability
- information disclosure
- XML Vulnerability
- Missing SPF Records vulnerability
- OTP Bypass Technique Vulnerability
- IDOR Vulnerability
- No rate Limit Vulnerability
- Session Hijacking Vulnerability
- Long Password Attack Vulnerability

Ch 15: Cloud Security - 1

- Cloud Security Fundamentals
- Shared Responsibility Model
- Cloud Infrastructure Threats
- AWS Cloud Security fundamentals
- AWS Cloud Security Tools and usages
- Azure Cloud Security fundamentals
- Azure Cloud Security Tools and usages
- GCP Cloud Security fundamentals

Ch 16: Cloud Security - 2

- Cloud Resource Exploitation
- Unmonitored API Calls and Access Keys
- Credential Theft from Repositories
- Cloud Identity Attacks
- Lateral Movement in Cloud Environments
- Lack of Visibility and Logging

Module 2: Defensive Security (Blue Team) @ SOC / SIEM / EDR

Ch 17: SOC Fundamentals

- SOC Overview
- SOC Team Structure
- Tier 1 Responsibilities
- Tier 2 Responsibilities
- Tier 3 Responsibilities
- SOC Workflow and Escalation Path

Ch 18: Alert System

- Alert Lifecycle Stages
- Incident Response Phases
- Types of Alerts Handled in SOC
- Daily SOC Monitoring Activities
- KPIs and Metrics for SOC
- Incident Response Phases
- Types of Alerts Handled in SOC
- Daily SOC Monitoring Activities
- KPIs and Metrics for SOC

Ch 19: Log Mechanism & Audits

- Log Collection Strategy
- Log Parsing and Normalization
- Key SOC Log Sources
- Firewall Logs
- IDS/IPS Logs
- DNS Logs
- Endpoint Logs (Sysmon/EDR)
- Active Directory Logs
- Cloud Logs (CloudTrail, Azure Activity)

Ch 20: Cyber Security : SIEM (Splunk)

- Introduction to SIEM

- Use Case Design in SIEM
- Overview of Splunk Architecture

Ch 21: Splunk Operations

- Splunk Ingestion and Indexing
- Writing SPL Queries
- Splunk Dashboards and Alerts
- QRadar Architecture and Flow Collection
- QRadar Rule Creation using CRE
- Rule Writing – SPL (Splunk), AQL (Qradar)
- MITRE ATT\&CK Mapping to Alerts

Ch 22: Threat Hunting & Splunk

- Threat Hunting Basics
- Alert Enrichment Techniques
- Alert Suppression & False Positive Handling
- Ticketing Systems (ServiceNow, JIRA) Integration
- Shift Handover Protocols

Ch 23: QRadar

- AQL Querying in Qradar
- Introduction to EDR
- SentinelOne Architecture
- SentinelOne Agent Capabilities
- Remote Response Actions
- (Kill, Quarantine, Rollback)

Ch 24: Mobile Security

- Introduction to Mobile Security
- Threats via Malicious Applications
- App Cloning and Impersonation
- Jailbreaking and Rooting Risks
- Insecure App Communication
- Phishing via SMS or Messaging Apps
- Wi-Fi-based Attacks (MITM)
- Mobile Email Account Compromise
- Keylogging via Spyware Apps
- Mobile Device as
- Entry Point into Corporate Networks

Ch 25: Malware Analysis

- **Introduction to Malware Analysis**
- **Malware Categories**
  a. Virus
  b. Worm
  c. Trojan
  d. Ransomware
  e. Spyware
  f. Rootkit
  g. Fileless Malware
- **Malware Behavior and Infection Chain**
- **Static Analysis Fundamentals**

Ch 26: Metadata Security

- **File Header and Metadata Check**
- **String Extraction (strings, FLOSS)**
- **PE Header Inspection**
- **Hashing (MD5, SHA256) and Use Cases**
- **Dynamic Analysis Overview**
- **Sandbox Analysis (Any.run, Cuckoo)**
- **Tools for Monitoring Behavior**
  a. ProcMon
  b. RegShot
  c. Wireshark
  d. TCPView

Ch 27: IOC & Cyber Security

- **Reverse Engineering Introduction**
- **Disassemblers (Ghidra, IDA Free)**
- **Debuggers (x64dbg, OllyDbg)**
- **Packers and Obfuscation**
- **IOC Extraction Process**
- **Types of IOCs**
- **File Hashes**
- **Registry Keys**
- **IPs and Domains**
- **Filenames**

Ch 28: Cyber Security - Emails

- **Overview of Email-Based Threats**
- **Anatomy of a Phishing Email**
- **Spear Phishing vs Generic Phishing**

- **Business Email Compromise (BEC)**
- **Malware Delivery via Email**
- **Email Header Components**
- **SPF Record Validation**
- **DKIM Signature Verification**
- **DMARC Policy Enforcement**
- **Email Flow and Received Headers**
- **Tools for Email Security**

  a. Microsoft Defender for O365
  b. Cisco ESA
  c. Proofpoint
  d. Mimecast
- **IOC Search in Mailboxes**
- **Quarantining and Purging Emails**

Ch 29: Data Security (DLP)

- **Intro to Data Security**
- **Intro to DLP**
- **DLP for Emails**
- **DLP for Files**
- **Writing and applying rules in DLP**
- **Proofpoint DLP**
- **User Awareness and Reporting Channels**

Ch 30: Threat Intelligence & Incident Response

- **Threat Intelligence Fundamentals**
- **Intelligence Lifecycle Stages**
- **Strategic vs Tactical vs**
- **Operational vs Technical TI**
- **IOC Formats (IP, Hash, URL, Domain)**
- **TI Sources and Feeds**

  a. VirusTotal
  b. AlienVault OTX
  c. Recorded Future
  d. Shodan
  e. URLScan.io
- **MITRE ATT&CK Overview**

Ch 31: IOC & SIEM

- **IOC Enrichment in SIEM**
- **Incident Response and Threat Factors**
- **Types Incident need to reported**

- Management of incidents
- Reporting and remediating Incidents
- Learning from Past incidents.

Module 3: GRC

Ch 32: Governance & Information Security Frameworks

- Overview of Governance in Cybersecurity
- Role of governance in InfoSec
- Key governance principles and policies
- Information Security Management Systems (ISMS)
- Purpose and structure of ISMS
- PDCA (Plan–Do–Check–Act) cycle
- Major Cybersecurity Frameworks

Ch 33: Governance & CIS

- ISO 27001/27002 Overview
- NIST Cybersecurity Framework (CSF)
- CIS Controls
- COBIT for Information Security Governance
- Security Policies & Standards
- Policy hierarchy (Policies → Standards → Procedures → Guidelines)
- Writing effective security policies
- Roles & Responsibilities in GRC
- Board, CISO, risk managers, compliance officers
- RACI matrix in security governance

Ch 34: Risk Management & Assessment

- Risk Management Fundamentals
- Risk terms (Threat, Vulnerability, Impact, Likelihood)
- Risk appetite & tolerance
- Risk Assessment Methodologies
- Qualitative vs Quantitative
- Common methods: ISO 27005, NIST SP 800-30
- Risk Identification

Ch 35: Risk Management & Assessment

- Asset identification & classification
- Threat and vulnerability mapping
- Risk Analysis & Evaluation
- Risk scoring & prioritization (Heatmaps, Risk Matrix)
- Business Impact Analysis (BIA)

- **Risk Treatment Strategies**
- **Accept, Avoid, Transfer, Mitigate**
- **Residual risk management**
- **Risk Register Management**
- **Structure and maintenance of a risk register**
- **Risk review frequency and reporting**

Ch 36: Compliance & Audit Management

- **Compliance Fundamentals**
- **Legal, regulatory, and contractual requirements**
- **Sector-specific regulations (GDPR, HIPAA, PCI DSS, SOX, etc.)**
- **Security Control Mapping**
- **Cross-mapping controls between frameworks (ISO, NIST, CIS)**
- **Maintaining a controls library**
- **Internal & External Audits**
- Audit lifecycle (Planning → Fieldwork → Reporting → Follow-up)
- **Evidence gathering and validation**
- **Continuous Compliance Monitoring**

Ch 37: Cyber Security Tools

- **Tools for compliance tracking (Archer, ServiceNow GRC, OneTrust)**
- **Key compliance metrics & dashboards**
- **Remediation & Gap Closure**
- **Corrective Action Plans (CAPs)**
- **Post-audit follow-up process**

Ch 38: Security Awareness, Exception

- **Security Awareness Programs**
- **Designing GRC-focused awareness campaigns**
- **Measuring awareness effectiveness**
- **Exception Management**
- **Types of security exceptions**
- **Approval workflow & documentation**
- **Monitoring and tracking approved exceptions**

Ch 39: Policy Management

- **Policy Lifecycle Management**
- **Drafting, reviewing, approving, and publishing policies**
- **Version control & review timelines**
- **GRC Reporting & Metrics**
- **Executive dashboards & board-level reporting**

- Key Risk Indicators (KRIs) & Key Performance Indicators (KPIs)
- Integration with Incident Response
- Using GRC data in IR investigations
- Lessons learned & continuous improvement in governance

- **Above course content includes total of THREE modules.**
- **Duration of each module: 30 Hours**
- **Total Course is planned for 3 Months**