Cyber Academy

LEVEL 1: Foundation in Cybersecurity & Networking

Duration: 3 Months

Module 1: Introduction to Cybersecurity

1.1 Understanding Cybersecurity

- Definition and scope of cybersecurity
- Cybersecurity vs Information Technology
- Evolution of cyber threats
- Cyber threats vs vulnerabilities
- Why cybersecurity is critical for modern organizations

Cyber Threat Actors (Introduction):

- Hacktivists
- Cybercriminals
- Nation-state actors
- Insiders (malicious & accidental)
- Script kiddies
- Organized crime groups
- Advanced Persistent Threats (APTs)
- Malware authors
- Phishers

1.2 CIA Triad

- Confidentiality
  - Data privacy
  - Access control concepts
- Integrity
  - Data accuracy
  - Hashing and validation (conceptual)
- Availability
  - System uptime
  - Redundancy and fault tolerance

Module 2: Networking Fundamentals & Communication Basics

2.1 Fundamentals of Communication

- OSI Model (7 layers – purpose and functions)
- Basics of data communication
- How data travels across networks
- Types of networks:
  - LAN

    - WAN
    - MAN
    - PAN
- Network topologies (star, bus, ring, mesh)
- TCP/IP Model and comparison with OSI

2.2 Core Networking Concepts

- IP addressing:
    - IPv4 and IPv6 overview
- Subnetting basics (conceptual understanding)
- DNS – name resolution
- DHCP – automatic IP assignment
- ARP – MAC to IP mapping
- Common ports and protocols:
    - HTTP / HTTPS
    - FTP
    - SMTP
    - POP3 / IMAP

Module 3: Cyber Threat Landscape

3.1 Common Cyber Attacks (Introduction)

- Malware:
    - Virus
    - Worm
    - Trojan
    - Ransomware
- Phishing and spear phishing
- Denial of Service (DoS)
- Distributed Denial of Service (DDoS)
- Man-in-the-Middle (MITM) attacks
- SQL Injection (conceptual)
- Social engineering attacks

3.2 Attack Vectors

- Email-based attacks
- Web-based attacks
- Network-based attacks
- Human-based attacks

Module 4: Cybersecurity Best Practices

- Password management and password policies
- Multi-Factor Authentication (MFA)
- Encryption basics (data at rest & in transit)
- Patch and update management
- Backup concepts and importance
- Safe email practices
- Secure web browsing habits
-

Module 5: Cloud Security Fundamentals (Awareness Level)

- What is cloud security
- Shared Responsibility Model (conceptual)
- Common cloud security risks:
    - Misconfiguration
    - Weak access controls
    - Data exposure
- Identity and access management in the cloud (basic concepts)
- Importance of cloud logging and monitoring

Module 5: Introduction to Cybersecurity Tools & SOC

- What are cybersecurity tools
- Overview of common security tools:
    - Antivirus / Endpoint Protection
    - Firewalls
    - Web security tools
- Introduction to:
    - SOC (Security Operations Center)
    - SIEM (what it is and why it is used)
- Roles in a SOC (high-level overview)

Module 6: Global Regulatory Compliance & Data Privacy (Awareness Level)

6.1 Data Protection Regulations (Introduction for Beginners)

- What is compliance and why it matters
- Overview of major regulations:
    - GDPR
    - HIPAA
    - SOC 2
    - CCPA
    - PDPL / DPDPA

- ISO 27001:2022
- Role of compliance in cybersecurity
- Introduction to the Data Protection Officer (DPO) role

LEVEL 2: Advanced Cybersecurity & SOC Operations

Duration: 6 Months

Module 1: Introduction to Cybersecurity

1.1. Understanding Cybersecurity

- Defining Cybersecurity
- The Evolution of Cyber Threats
- Cyber threats and vulnerabilities
- Requirement of Cyber Security (Cyber Threat Actors)
    - Hacktivists
    - Cybercriminals
    - Nation-State Actors
    - Insiders
    - Script Kiddies
    - Organized Crime Groups
    - Advanced Persistent Threats (APTs)
    - Malware Authors
    - Phishers

The importance of cybersecurity

1.2. CIA Triad (Confidentiality, Integrity, Availability)

- Understanding the CIA Triad
- Confidentiality: Protecting Data Privacy
- Integrity: Ensuring Data Accuracy and Trustworthiness
- Availability: Data Accessibility and System Uptime

Module 2: Global Regulatory Compliances and Data Protection and Data Privacy

2.1 Data Protection Regulations

- GDPR, HIPAA, SOC 2, CCPA, PDPL, DPDPA, ISO 27001:2022
- Compliance requirements and importance
- Importance of Data Protection and data privacy requirements

2.2 Privacy Practices

- Data handling and consent
- Privacy impact assessments

Module 3: Cyber Threat Landscape

3.1 Types of Cyber Attacks Common Types of Cyber Attacks

- Malware Attacks (Viruses, Trojans, Worms)
- Phishing Attacks
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks
- Man-in-the-Middle (MitM) Attacks
- SQL Injection Attacks
- Social Engineering Attacks

3.2. Cyber Attack Vectors

- Types of Email Attack
    - Phishing, Spear Phishing
    - Business Email Compromise (BEC) or CEO Fraud
    - Ransomware, Malware Delivery
    - Email Spoofing
    - Attachment-Based Attack
    - Email Bombs and DDoS Attacks
    - Credential Stuffing
- Email security
- Web security
- Network security

3.3 Cloud Security

- Cloud security considerations
- Securing cloud-based data and applications
- Understanding cloud network security management

Module 4: Cybersecurity Implementation

4.1 Cyber Security Technical, Physical & Administrative Safeguards

- Password Management, Creating strong passwords, Password policies and practices
- Data Protection Encryption
- Security Patch management

- Regular Backups
- Regular Security Assessments
- Data Loss Prevention (DLP)
- Behaviour Analytics
- Access Controls
- Security Information and Event Management (SIEM)
- Security Orchestration, Automation, and Response (SOAR)
  SIEM & SOAR two critical components of a modern Cyber Security Strategy

4.2 Cybersecurity Roles and Responsibilities

- Introduction to Cybersecurity Roles and Teams
- Key Responsibilities in Cybersecurity
- Security Analysts: Monitoring and Incident Response
- Network Security Engineers: Protecting Network Infrastructure
- Ethical Hackers and Penetration Testers: Identifying Vulnerabilities
- Compliance and Risk Managers: Ensuring Regulatory Compliance

Module 5: Email, Web & Cloud Security

- Email security architecture
- Phishing defence mechanisms
- Web security

- Cloud security basics:
  - Shared responsibility model
  - Cloud network security
  - Securing cloud workloads

Module 6: Secure Network Practices

5.1 Network Security

- Firewalls and intrusion detection & Prevention
- Introduction to VAPT
- scanning networks
- vulnerability analysis
- Secure Browsing (Web Content Gateway)
- Safe email practices
- Avoiding malicious websites

5.2 Wireless Network Security

- Securing Wi-Fi networks
- Encryption WPA3/WPA2 & AES Encryption
- Guest network management

Module 6: Endpoint Security EDR/ XDR/ MDR

- Endpoint Protection
- Antivirus and antimalware software
- Patch management
- End point security- Servers/windows/Linux

Module 7: Incident Response and Management

- Incident Identification and Classification
- Recognizing security incidents
- Incident reporting
- Incident Response Plan
- Developing an incident response plan
- Roles and responsibilities during an incident

LEVEL 3: Cybersecurity Expertise & Enterprise Defense

Duration: 8 Months

Target Audience: Experienced SOC analysts, security engineers

Cyber Academy – Advanced Cybersecurity Expertise Program

Duration: 8 Months (32 Weeks)

Delivery Model: Theory (40%) | Hands-On Labs (40%) | Projects & Case Studies (20%)

MODULE 1: Advanced Introduction to Cybersecurity (2 Weeks)

1.1 Understanding Cybersecurity (Advanced Perspective)

- Enterprise definition of cybersecurity
- Cybersecurity vs Information Security vs Risk Management
- Evolution of cyber threats (from script attacks to APT campaigns)
- Modern attack lifecycle (Kill Chain & ATT&CK overview)
- Business impact of cyber incidents

Cyber Threat Actors (Deep Dive):

- Hacktivists – motivations & techniques
- Cybercriminal ecosystems & dark web economy
- Nation-state actors & cyber warfare

- Insider threats (malicious & negligent)
- Organized cybercrime & ransomware cartels
- Advanced Persistent Threats (APT groups)
- Malware authors & exploit developers
- Phishing-as-a-Service (PhaaS)

1.2 CIA Triad in Enterprise Environments

- Confidentiality – IAM, encryption, zero trust
- Integrity – hashing, code signing, database integrity
- Availability – DR, BCP, redundancy, DDoS protection

MODULE 2: Global Regulatory Compliance, Data Protection & Privacy (3 Weeks)

2.1 Data Protection Regulations & Cyber Security Framework

NEW 2.3 NIST Cybersecurity & Risk Frameworks

- NIST Cybersecurity Framework (CSF 2.0) Purpose and structure of NIST CSF Five core functions:
    - Identify
    - Protect
    - Detect
    - Respond
    - Recover
  - Mapping NIST CSF to:
    - ISO 27001:2022
    - SOC 2
    - Enterprise security controls
- GDPR – lawful processing, DPIA, breach notification
- HIPAA – healthcare data protection
- SOC 2 – Trust Service Criteria
- CCPA / CPRA – consumer data rights
- PDPL / DPDPA – regional compliance
- ISO 27001:2022 – ISMS framework

Compliance in Real Organizations

- Mapping technical controls to compliance
- Security vs compliance gap analysis
- Audit evidence & documentation

2.2 Privacy Engineering & Practices

- Data classification & handling
- Consent management systems
- Privacy Impact Assessments (PIA/DPIA)
- Data retention & deletion policies

MODULE 3: Advanced Cyber Threat Landscape (4 Weeks)

3.1 Types of Cyber Attacks (Technical Analysis)

- Malware families (ransomware, spyware, RATs)
- Phishing campaigns & payload delivery
- DDoS attack types (Volumetric, Protocol, App-layer)
- MITM attacks (ARP poisoning, SSL stripping)
- SQL Injection & injection flaws
- Social engineering psychology

3.2 Attack Vectors (Hands-On Focus)

Email Attack Techniques

- Phishing & spear phishing
- Business Email Compromise (BEC)
- Malware & ransomware delivery
- Email spoofing & impersonation
- Attachment & macro-based attacks
- Credential harvesting

Web & Network Attack Vectors

- Web application exploitation
- Network lateral movement
- Credential abuse

3.3 Cloud Security Threats

- Cloud misconfigurations
- IAM abuse in cloud
- Cloud network exposure
- Securing cloud data & workloads

MODULE 4: Cybersecurity Implementation & Architecture (4 Weeks)

4.1 Technical, Administrative & Physical Controls

- Password policies, MFA & PAM
- Encryption (data at rest & in transit)
- Patch & vulnerability management
- Backup & disaster recovery strategies
- Data Loss Prevention (DLP)
- User & Entity Behavior Analytics (UEBA)

Security Platforms

- SIEM architecture & use cases
- SOAR workflows & automation
- Integrating SIEM, SOAR & EDR

4.2 Cybersecurity Roles in Enterprise

- SOC L1/L2/L3 responsibilities
- Security engineering vs operations
- Red Team vs Blue Team vs Purple Team
- GRC & Risk Management roles

MODULE 5: Email, Web & Cloud Security (3 Weeks)

Email Security

- Secure email gateways
- Anti-phishing technologies
- DMARC, SPF, DKIM
- BEC detection & response

Web Security

- Web application firewalls (WAF)
- OWASP Top 10 overview
- Secure browsing & proxy gateways

Cloud Security

- Shared responsibility model
- Cloud network segmentation
- Securing workloads & storage
- Cloud logging & monitoring

MODULE 6: Network & Infrastructure Security (4 Weeks)

Network Security

- Firewalls (Stateful, NGFW)
- IDS / IPS deployment & tuning
- Network segmentation & zero trust
- Secure remote access (VPNs)

Wireless Security

- Wi-Fi attack techniques
- WPA2/WPA3 security
- Rogue AP detection
- Guest network isolation

MODULE 7: Endpoint Security – EDR / XDR / MDR (3 Weeks)

- Endpoint protection architecture
- Antivirus vs EDR vs XDR
- Behavioral detection
- Endpoint threat hunting

- Windows & Linux server security
- Endpoint incident response

MODULE 8: Incident Response, DFIR & SOC Operations (4 Weeks)

- Incident identification & classification
- Alert triage & escalation
- Incident response lifecycle
- IR playbooks
- Ransomware response
- Digital forensics basics
- Log & evidence preservation

MODULE 9: VAPT & PENETRATION TESTING (FULL HANDS-ON) – 8 WEEKS

9.1 VAPT Fundamentals

- Vulnerability Assessment vs Penetration Testing
- Black box, Grey box, White box testing
- Kali & Parrot linux
- Rules of engagement
- Legal & ethical considerations

9.2 Reconnaissance & Enumeration

- Passive & active reconnaissance
- OSINT techniques
- DNS & subdomain enumeration
- Network discovery

Hands-On Tools

- Nmap
- Netcat
- Whois
- Shodan (theory + demo)

9.3 Network Penetration Testing

- Port scanning & service detection
- Exploiting weak services
- SMB, FTP, SSH attacks
- Lateral movement basics

Hands-On Labs

- Internal network exploitation
- Privilege escalation (Windows/Linux)

9.4 Web Application Penetration Testing

- OWASP Top 10 deep dive
- SQL Injection (manual & automated)
- XSS (stored, reflected, DOM)
- Authentication & session attacks
- File upload vulnerabilities

Hands-On Labs

- Vulnerable web apps testing
- Manual exploitation techniques

9.5 Email & Phishing Simulation Testing

- Phishing campaign planning
- Payload delivery methods
- Credential harvesting labs
- Security awareness testing

9.6 Exploitation, Post-Exploitation & Reporting

- Exploit frameworks (conceptual use)
- Persistence techniques
- Data exfiltration simulations
- Cleaning tracks (theory)

Professional VAPT Reporting

- Executive summary
- Risk ratings (CVSS)
- Proof of concept
- Remediation guidance

MODULE 10: Capstone Projects (Final 4 Weeks)

Students must complete:

- Full VAPT assessment (network + web)
- SOC incident handling simulation
- Compliance gap assessment
- Final presentation & defense