NS3EDU – Cyber Security Curriculum

Industry-Oriented | Job-Focused | Hands-On Training

LEVEL 1: Cyber Security Fundamentals (Beginner Level)

Part 1: Introduction to Cyber Security

- What is Cyber Security - Need for Cyber Security in Modern IT - Cyber Threat Landscape - Cyber Security Domains - Career Opportunities in Cyber Security

Part 2: Networking Basics for Security

- NetworkingOverview (LAN,WAN,Internet)
- OSI & TCP/IP Models (Security View)
- IP Addressing, Ports & Protocols
- Firewalls & Routers Basics
- Network Traffic Flow

Part 3: Operating System Fundamentals

- Windows OS Architecture
- Linux OS Architecture
- User & Permission Management
- File Systems & Processes
- System Logs

Part 4: Cyber Threats & Attacks

- Malware Types - Phishing & Social Engineering - DoS & DDoS Attacks - Man-in-the-Middle Attacks - Password Attacks

Part 5: Security Principles & Controls

- CIA Triad - Authentication vs Authorization - Access Control Models - Security Policies - Risk Management Basics

LEVEL 2: Cyber Security Analyst (Intermediate Level)

Part 6: Network Security

- Firewall Types & Configuration
- IDS & IPS - VPN & Secure Communication - Network Segmentation - Network Hardening

Part 7: Web Application Security

- OWASP Top 10 - SQL Injection - Cross-Site Scripting (XSS) - CSRF Attacks - Authentication Vulnerabilities

Part 8: Endpoint & System Security

- Endpoint Protection - Antivirus & EDR - Patch Management - System Hardening - Secure Configuration

Part 9: Security Monitoring & SOC

- SOC Overview - SIEM Tools - Log Collection & Analysis - Alert Handling - Incident Identification

Part 10: Incident Response & Digital Forensics

- Incident Response Lifecycle - Threat Containment - Evidence Collection - Forensic Analysis - Reporting

LEVEL 3: Advanced Cyber Security (Professional Level)

Part 11: Ethical Hacking Fundamentals

- Ethical Hacking Methodology - Reconnaissance Techniques - Scanning & Enumeration - Vulnerability Assessment - Legal & Ethical Guidelines

Part 12: Cloud & Cyber Security

- Cloud Security Fundamentals - IAM & Access Control - Cloud Network Security - Data Protection - Shared Responsibility Model

Part 13: Governance, Risk & Compliance (GRC)

- Security Governance - Risk Assessment
- ISO 27001, GDPR, PCI-DSS - Security Audits

Part 14: Advanced Threats & Defense

- Advanced Persistent Threats - Threat Intelligence - Malware Analysis Basics - Blue Team Operations

Part 15: Real-World Cyber Security Projects

- Network Security Implementation - SOC Monitoring Project - Web Application Security Testing - Incident Response Simulation - Cloud Security Deployment

Part 16: Career & Certification Preparation

- Cyber Security Job Roles
- SOC Analyst Career Path
- CEH, Security+, ISO 27001 Overview
- Interview Preparation
- Resume & Project Guidance

Outcome

Learners become job-ready cyber security professionals capable of securing systems, monitoring threats, responding to incidents, and working in SOC and enterprise environments.