TECHNOCATION FREELANCING TRAINING INSTITUTE & SOFTWARE HOUSE

Professional Cyber Security Course Outline

Module 1: Introduction to Cybersecurity

- What is Cybersecurity? (Importance & Scope)
- Types of Cyber Threats & Attacks
- Cybersecurity Domains (Network, Application, Cloud, IoT)
- Understanding Cyber Laws & Compliance (GDPR, HIPAA, ISO 27001)
- Career Paths in Cybersecurity

Module 2: Networking & Security Fundamentals

- Understanding Network Protocols (TCP/IP, HTTP, FTP, DNS)
- OSI Model & Network Layers
- Firewalls, IDS, & IPS (Security Mechanisms)
- VPNs & Encryption in Network Security
- Wireless Network Security & Common Vulnerabilities

Module 3: Ethical Hacking & Penetration Testing

- What is Ethical Hacking? (White Hat vs. Black Hat)
- Kali Linux & Ethical Hacking Tools
- Footprinting & Reconnaissance
- Scanning Networks (Nmap, Netcat)
- Vulnerability Assessment & Exploitation Techniques

Module 4: Web Application Security

- Common Web Vulnerabilities (OWASP Top 10)
- SQL Injection & Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Security Misconfigurations & Exploiting Weak Authentication
- Secure Coding Practices & Web Application Firewalls (WAF)

Module 5: Cryptography & Data Protection

- Basics of Cryptography (Symmetric & Asymmetric Encryption)
- Hashing Algorithms (MD5, SHA-256, bcrypt)
- Digital Signatures & Certificates
- Public Key Infrastructure (PKI)
- Securing Data at Rest & In Transit

Module 6: Malware Analysis & Threat Intelligence

- Types of Malware (Viruses, Worms, Ransomware, Trojans)
- Understanding Advanced Persistent Threats (APT)
- Threat Intelligence & Dark Web Monitoring
- Analyzing & Containing Malware (Sandboxing, Behavior Analysis)
- Endpoint Security Solutions (Antivirus, EDR, XDR)

Module 7: Cloud Security & Virtualization

- Security Challenges in Cloud Computing
- AWS, Azure & Google Cloud Security Best Practices
- Identity & Access Management (IAM)
- Secure Cloud Storage & Encryption
- Virtual Machines & Container Security (Docker, Kubernetes)

Module 8: Incident Response & Cyber Forensics

- Understanding Cyber Incident Response
- Digital Forensics & Evidence Collection
- Security Information & Event Management (SIEM)
- Log Analysis & Threat Hunting

- Disaster Recovery & Business Continuity Planning

Module 9: Social Engineering & Phishing Attacks

- What is Social Engineering? (Psychological Manipulation)
- Types of Social Engineering Attacks (Phishing, Baiting, Pretexting)
- Email Security & Anti-Phishing Techniques
- Security Awareness Training & Human Firewall
- Real-World Case Studies on Social Engineering

Module 10: Cybersecurity Compliance & Risk Management

- Understanding Risk Management Frameworks (NIST, ISO 27001)
- Cybersecurity Audits & Governance
- Security Policies & Best Practices
- Legal & Regulatory Compliance (GDPR, HIPAA, CCPA)
- Creating a Cybersecurity Strategy for Organizations

Module 11: Security Automation & AI in Cybersecurity

- Introduction to Security Automation Tools (SOAR, SIEM)
- AI & Machine Learning in Cybersecurity
- Automating Threat Detection & Response
- Using Python for Security Automation
- Case Studies on AI-Driven Security Attacks & Defenses

Module 12: Final Project & Certification Preparation

- Conducting a Penetration Test on a Simulated Network
- Cybersecurity Best Practices & Future Trends
- Preparing for Security Certifications (CEH, CISSP, CompTIA Security+)
- Resume Building & Job Interview Preparation