IntelliQ IT Trainings

Cyber Security Course Content

Date: ……. Timings: …….

Duration: ……. Fee: …….

Faculty: ……..

Course Topics at a Glance

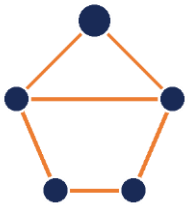
- ✓ **Networking & Security Fundamentals**
- ✓ **Cryptography & PKI**
- ✓ **Operating System Security (Windows & Linux)**
- ✓ **Web Application Security (OWASP Top 10)**
- ✓ **Ethical Hacking & Penetration Testing**
- ✓ **Vulnerability Assessment & Management**
- ✓ **Malware Analysis Basics**
- ✓ **Identity & Access Management (IAM)**
- ✓ **Firewalls, IDS/IPS & VPN**
- ✓ **Security Information & Event Management (SIEM)**
- ✓ **Security Operations Center (SOC) Operations**
- ✓ **Incident Response & Digital Forensics**
- ✓ **Cloud Security (AWS/Azure/GCP)**
- ✓ **Endpoint Detection & Response (EDR)**
- ✓ **Governance, Risk & Compliance (GRC)**
- ✓ **Security Standards: ISO 27001, NIST, PCI-DSS, GDPR, HIPAA**
- ✓ **Kali Linux & Security Tools**
- ✓ **Wireshark & Network Traffic Analysis**

→ Introduction to Cyber Security

- ✓ What Is Cyber Security & Why It Matters
- ✓ The CIA Triad – Confidentiality, Integrity, Availability
- ✓ Types of Cyber Threats & Threat Actors
- ✓ Common Attack Vectors & Attack Lifecycle (Cyber Kill Chain)
- ✓ Careers in Cyber Security – SOC, GRC, Pentest, Cloud Security

→ Networking Fundamentals for Security

- ✓ OSI & TCP/IP Models
- ✓ IP Addressing, Subnetting & Routing Basics
- ✓ Ports, Protocols & Services (HTTP/S, DNS, FTP, SSH, SMTP)
- ✓ Network Devices – Routers, Switches, Firewalls
- ✓ Introduction to Wireshark – Packet Capture & Analysis



→ Cryptography & PKI

- ✓ Symmetric vs Asymmetric Encryption
- ✓ Hashing Algorithms – MD5, SHA-256
- ✓ Digital Signatures & Certificates
- ✓ Public Key Infrastructure (PKI) Overview
- ✓ SSL/TLS – How Secure Communication Works

→ Operating System Security

Windows Security

- ✓ User Account Control & Group Policy
- ✓ Windows Event Logs & Auditing
- ✓ Registry & Services Hardening

Linux Security

- ✓ File Permissions & Ownership
- ✓ User & Sudo Privilege Management
- ✓ Log Files & System Hardening (SSH, iptables)

→ Identity & Access Management (IAM)

- ✓ Authentication vs Authorization
- ✓ Multi-Factor Authentication (MFA)
- ✓ Role-Based Access Control (RBAC)

- ✓ Single Sign-On (SSO) & Federation Basics
- ✓ Privileged Access Management (PAM) Concepts

→ Firewalls, IDS/IPS & VPN

- ✓ Firewall Types & Rule Configuration
- ✓ Intrusion Detection vs Prevention Systems
- ✓ Setting up and Configuring a VPN
- ✓ Network Segmentation & DMZ Design
- ✓ Proxy Servers & Web Filtering

→ Web Application Security

- ✓ OWASP Top 10 Vulnerabilities Overview
- ✓ SQL Injection – Detection & Prevention
- ✓ Cross-Site Scripting (XSS) & CSRF
- ✓ Broken Authentication & Session Management
- ✓ Secure Coding Practices
- ✓ Hands-on with Burp Suite / OWASP ZAP

→ Ethical Hacking & Penetration Testing

- ✓ Phases of Penetration Testing
- ✓ Reconnaissance & Footprinting Techniques
- ✓ Scanning & Enumeration with Nmap
- ✓ Exploitation Basics & Metasploit Framework
- ✓ Password Cracking Concepts
- ✓ Reporting & Responsible Disclosure

→ Vulnerability Assessment & Management

- ✓ Vulnerability Scanning with Nessus/OpenVAS
- ✓ CVSS Scoring & Risk Prioritization
- ✓ Patch Management Lifecycle
- ✓ Remediation Tracking & Reporting

→ Malware Analysis Basics

- ✓ Types of Malware – Virus, Worm, Trojan, Ransomware
- ✓ Static vs Dynamic Analysis Overview
- ✓ Sandboxing Tools & Techniques
- ✓ Indicators of Compromise (IOCs)

→ Security Information & Event Management (SIEM)

- ✓ What Is SIEM & Why It Is Used
- ✓ Log Collection, Normalization & Correlation
- ✓ Working with Splunk / IBM QRadar / ELK Stack

- ✓ Creating Alerts, Dashboards & Reports
- ✓ Use Case Development for Threat Detection

→ Security Operations Center (SOC)

- ✓ SOC Roles – L1, L2, L3 Analyst Responsibilities
- ✓ Alert Triage & Escalation Workflow
- ✓ Threat Intelligence Feeds & IOC Enrichment
- ✓ SOAR – Security Orchestration, Automation & Response

→ Incident Response & Digital Forensics

- ✓ Incident Response Lifecycle (NIST Framework)
- ✓ Evidence Collection & Chain of Custody
- ✓ Memory & Disk Forensics Basics
- ✓ Post-Incident Review & Lessons Learned

→ Endpoint Detection & Response (EDR)

- ✓ EDR vs Traditional Antivirus
- ✓ Deploying & Managing EDR Agents
- ✓ Threat Hunting Fundamentals
- ✓ Isolating & Remediating Infected Endpoints

→ Cloud Security

- ✓ Shared Responsibility Model (AWS/Azure/GCP)
- ✓ Identity & Access Management in the Cloud
- ✓ Securing Storage – S3 Bucket Policies & Encryption
- ✓ Cloud Security Posture Management (CSPM) Basics
- ✓ Cloud Logging & Monitoring – CloudTrail, CloudWatch

→ Governance, Risk & Compliance (GRC)

- ✓ Risk Assessment & Risk Management Frameworks
- ✓ ISO 27001 – Information Security Management System
- ✓ NIST Cybersecurity Framework
- ✓ PCI-DSS, GDPR & HIPAA Essentials
- ✓ Security Policies, Audits & Awareness Training

→ Security Tools Lab

- ✓ Kali Linux Setup & Toolkit Overview
- ✓ Nmap – Network Scanning
- ✓ Wireshark – Packet Analysis
- ✓ Metasploit – Exploitation Framework
- ✓ Burp Suite – Web App Testing
- ✓ John the Ripper / Hydra – Password Auditing