INFOSOFT IT SOLUTIONS

Training | Projects | Placements

Revathi Apartments, Ameerpet, 1st Floor, Opposite Annapurna Block,

Infosoft It solutions, Software Training & Development Institute, 9059683947|9182540872

Cyber Security

Introduction to Cyber Security

- Overview of Cyber Security: Importance, evolution, and current landscape
- Cyber Threats and Attack Vectors: Types of threats (malware, phishing, etc.) and attack methodologies
- Cyber Security Frameworks and Standards: NIST Cybersecurity Framework, ISO/IEC 27001, GDPR

Information Security Fundamentals

- Confidentiality, Integrity, and Availability (CIA Triad): Principles of information security
- Risk Management in Cyber Security: Risk assessment, risk mitigation strategies
- Security Controls: Preventive, detective, and corrective controls

Network Security

- Network Security Principles: Securing network infrastructure and protocols
- Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS)
- Virtual Private Networks (VPNs) and Secure Sockets Layer (SSL) / Transport Layer Security (TLS)

Operating System Security

- Securing Operating Systems: Hardening OS configurations (Windows, Linux, macOS)

- Patch Management: Keeping systems up-to-date with security patches
- Endpoint Security: Antivirus, anti-malware, and endpoint protection strategies

Cryptography

- Cryptographic Basics: Symmetric and asymmetric encryption, hashing algorithms
- Digital Signatures and Certificates: Public key infrastructure (PKI)
- Cryptographic Protocols: SSL/TLS, IPsec, SSH

Web Security

- Web Application Security: OWASP Top Ten vulnerabilities (SQL injection, XSS, CSRF)
- Secure Coding Practices: Writing secure code, input validation, and output encoding
- Web Security Tools: Vulnerability scanners, web application firewalls (WAF)

Cloud Security

- Cloud Computing Fundamentals: IaaS, PaaS, SaaS models
- Securing Cloud Infrastructure: Shared responsibility model, cloud security best practices
- Identity and Access Management (IAM) in the Cloud

Incident Response and Management

- Incident Response Lifecycle: Preparation, detection, containment, eradication, recovery, and lessons learned
- Incident Response Team Roles and Responsibilities
- Forensics and Investigations: Digital forensics tools and techniques

Cyber Security Operations and Monitoring

- Security Operations Center (SOC): Role and functions
- Security Information and Event Management (SIEM): Log management, correlation, and analysis
- Threat Intelligence: Sources of threat intelligence, threat feeds, and threat hunting

Legal and Ethical Aspects of Cyber Security

- Cyber Security Laws and Regulations: GDPR, CCPA, HIPAA, etc.
- Ethics in Cyber Security: Professional codes of conduct, ethical hacking
- Privacy and Data Protection: Data breach notification laws, privacy-enhancing technologies

Cyber Security Governance and Compliance

- Cyber Security Governance Frameworks: COBIT, ITIL, etc.
- Compliance Management: Regulatory compliance, audits, and certifications (e.g., ISO 27001)

Emerging Trends in Cyber Security

- Artificial Intelligence and Machine Learning in Cyber Security
- IoT Security: Securing Internet of Things devices and networks
- Blockchain Security: Cryptocurrency security and smart contract vulnerabilities

Cyber Security Career Development

- Cyber Security Certifications: CISSP, CEH, CompTIA Security+, etc.
- Career Paths in Cyber Security: Roles and responsibilities (security analyst, penetration tester, etc.)
- Building a Cyber Security Career: Skills development and continuous learning