INFOSOFT IT SOLUTIONS

Training | Projects | Placements

Revathi Apartments, Ameerpet, 1st Floor, Opposite Annapurna Block, Infosoft It solutions,
Software Training & Development Institute, +91 - 9059683947 | +91 - 9182540872

Cyber Security And SIEM

Introduction to Cyber Security

- Need of Cybersecurity
- CIA Triad
- Security Architecture
- Security Governance
- Security Auditing
- Regulations & Frameworks
- Ethical Hacking
- Types of Hackers
- Phases of Ethical Hacking
- Penetration Testing
- Types of Penetration Testing
- Footprinting
- Objectives of Footprinting
- Types of Footprinting
- Footprinting Techniques

Cryptography

- Types of cryptography
- Symmetric cryptography
- Asymmetric cryptography
- Hash functions
- Digital signatures
- Public Key Infrastructure (PKI)
- Attacks on cryptosystems

Computer Networks & Security

- Introduction to Computer Network
- Computer Networks - Architecture
- Layered architecture
- Open Systems Interconnect (OSI) Model
- Transmission Control Protocol/Internet Protocol (TCP/IP)
- Network Scanning
- Enumeration
- Common Network Threats/Attacks

Application and Web Security

- Web server architecture
- Web server attacks
- Countermeasures and patch management
- Web application architecture
- Web application attacks

Identity and Access Management

- Authentication and authorization

- Authentication and authorization principles
- Regulation of access
- Access administration
- Password protection
- Identity theft

Vulnerability Analysis & System Hacking

- Vulnerability Analysis
- Types of Vulnerability Analysis
- Vulnerability Assessment Lifecycle
- Vulnerability Assessment Tools
- Vulnerability Scoring Systems
- Vulnerability Assessments Report
- System Hacking
- Password Cracking
- Privilege escalation
- Executing Applications
- Hiding Files
- Clearing Logs

Sniffing and SQL Injection

- Malware and its propagation ways
- Malware components
- Types of malware
- Concept of sniffing
- Types of sniffing
- Types of sniffing attacks
- SQL injection
- Types of SQL injection

- SQL injection Methodologies

DoS and Session Hijacking

- DoS attack
- DDoS attack
- Common symptoms of DoS/DDoS attack
- Categories of DoS/DDoS Attack Vectors
- DoS/DDoS detection techniques
- Session hijacking
- Application level session hijacking
- Network level session hijacking
- Intrusion Detection System (IDS)
- Types of Intrusion Detection System
- Introduction to Firewalls
- Types of Firewalls
- Introduction to Honeypots
- Evading IDS

Introduction to SIEM

Getting Started with ES

- Provide an overview of Splunk for Enterprise Security (ES)
- Identify the differences between traditional security threats and new adaptive threats
- Describe correlation searches, data models and notable events
- Describe user roles in ES
- Log on to ES

Security Monitoring and Incident Investigation

Use the Security Posture dashboard to monitor enterprise security status

- Use the Incident Review dashboard to investigate notable events
- Take ownership of an incident and move it through the investigation workflow
- Use adaptive response actions during incident investigation
- Create notable events
- Suppress notable events

Investigations

- Use ES investigation timelines to manage, visualize and coordinate incident investigations
- Use timelines and journals to document breach analysis and mitigation efforts

Forensic Investigation with ES

- Investigate access domain events
- Investigate endpoint domain events
- Investigate network domain events
- Investigate identity domain events

Risk and Network Analysis

- Understand and use Risk Analysis
- Use the Risk Analysis dashboard
- Manage risk scores for objects or users

Web Intelligence

- Use HTTP Category Analysis, HTTP User Agent Analysis, New Domain Analysis, and Traffic Size Analysis to spot new threats
- Filter and highlight events

User Intelligence

- Evaluate the level of insider threat with the user activity and access anomaly dashboards
- Understand asset and identity concepts
- Use the Asset Investigator to analyze events
- Use the Identity Investigator to analyze events
- Use the session center for identity resolution (UBA integration)

Threat Intelligence

- Use the Threat Activity dashboard to analyze traffic to or from known malicious sites
- Inspect the status of your threat intelligence content with the threat artifact dashboard

Protocol Intelligence

- Describe Stream events data is input into Splunk events
- Use ES predictive analytics to make forecasts and view trends

Glass Tables

- Build glass tables to display security status information
- Add glass table drilldown options
- Create new key indicators for metrics on glass tables