INFOSOFT IT SOLUTIONS

Training | Projects | Placements

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

soft it solutions Software Training& Development 905968394,918254087

ENDPOINT SECURITY

Introduction to Endpoint Security

- Overview of Endpoint Security
- Importance of Endpoint Security in today's IT landscape
- Common threats and vulnerabilities targeting endpoints

Endpoint Protection Platforms (EPP)

- Understanding Endpoint Protection Platforms
- Features and capabilities of EPP solutions
- Comparison of leading EPP vendors

Endpoint Detection and Response (EDR)

- Introduction to Endpoint Detection and Response (EDR)
- EDR capabilities and functionalities
- Real-time monitoring and threat detection on endpoints

Antivirus and Anti-malware Technologies

- Overview of traditional antivirus and anti-malware solutions
- Modern approaches to antivirus and anti-malware
- Integration with EPP and EDR solutions

Endpoint Hardening and Configuration Management

- Techniques for endpoint hardening
- Best practices in endpoint configuration management
- Role of Group Policies and Configuration Baselines

Patch Management for Endpoints

- Importance of patch management in endpoint security
- Patch management lifecycle
- Automated patch deployment strategies

Endpoint Encryption and Data Loss Prevention (DLP)

- Encryption technologies for endpoint protection
- Data Loss Prevention strategies and tools
- Endpoint backup and recovery solutions

Endpoint Security Policies and Compliance

- Developing effective endpoint security policies
- Compliance requirements and standards
- Monitoring and auditing endpoint security compliance

Incident Response and Endpoint Forensics

- Incident response planning and procedures
- Endpoint forensics techniques and tools
- Post-incident analysis and remediation

Advanced Threat Detection and Analysis

- Deep dive into advanced threat detection techniques
- Behavioral analysis and anomaly detection
- Threat intelligence integration and management

Endpoint Security Architecture and Design

- Design principles for scalable endpoint security architecture
- Micro-segmentation and network access control (NAC)
- Integration with cloud and hybrid environments

Advanced Endpoint Protection Platforms (EPP)

- Next-generation EPP features and capabilities
- Endpoint isolation and sandboxing techniques
- Advanced malware detection and mitigation strategies

Advanced Endpoint Detection and Response (EDR)

- Advanced EDR use cases and scenarios
- Threat hunting methodologies
- Automated response and remediation techniques

Zero Trust Architecture for Endpoints

- Zero Trust principles and implementation for endpoints
- Identity-based access controls
- Continuous authentication and authorization

Threat Hunting and Incident Response

- Threat hunting frameworks and methodologies
- Endpoint-centric incident response strategies
- Forensic analysis and evidence preservation

Endpoint Security Automation and Orchestration

- Automation frameworks for endpoint security operations
- Orchestration of security workflows
- Integration with Security Information and Event Management (SIEM) systems

Endpoint Forensics and Memory Analysis

- Memory forensics techniques for endpoint investigations
- Advanced malware analysis in memory
- Leveraging memory artifacts for incident response

Advanced Endpoint Compliance and Audit

- Advanced compliance monitoring and reporting
- Endpoint security auditing techniques
- Integration with governance, risk, and compliance (GRC) frameworks