INFOSOFT IT SOLUTIONS

Training | Projects | Placements

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

Info soft it solutions ,Software Training& Development 905968394,918254087

INCIDENT RESPONSE PLANNING TRAINING

1: Introduction to Incident Response

- Overview of Incident Response
- Importance of Incident Response Planning
- Legal and Regulatory Requirements
- Incident Response Lifecycle

2: Preparing for Incident Response

- Building an Incident Response Team
- Roles and Responsibilities
- Incident Response Policies and Procedures
- Communication Plans

3: Threat Identification and Analysis

- Types of Security Incidents
- Indicators of Compromise (IoCs)
- Threat Intelligence
- Tools for Incident Detection

4: Incident Detection and Reporting

- Incident Detection Methods
- Initial Incident Reporting
- Triage and Prioritization of Incidents
- Documenting Incidents

5: Containment Strategies

- Immediate Actions
- Short-term vs. Long-term Containment
- Eradication of Threats
- Best Practices for Containment

6: Incident Eradication and Recovery

- Eradication Techniques
- System Restoration and Validation
- Recovery Planning
- Business Continuity Considerations

7: Post-Incident Activities

- Post-Incident Analysis
- Incident Reporting
- Lessons Learned
- Improving the Incident Response Plan

8: Legal and Ethical Considerations

- Legal Implications of Incident Response
- Ethical Issues in Incident Handling
- Privacy Considerations
- Working with Law Enforcement

9: Incident Response Tools and Technologies

- Overview of Incident Response Tools
- SIEM Systems
- Forensic Analysis Tools
- Automation in Incident Response

10: Developing an Incident Response Plan

- Components of an Incident Response Plan
- Creating Incident Response Playbooks
- Testing and Validating the Plan
- Training and Awareness Programs

ADVANCE TOPICS ;-

1: Advanced Incident Response Frameworks

- Review of Basic Incident Response Concepts
- Advanced Incident Response Models (NIST, SANS, ISO)
- Incident Response Maturity Models
- Integrating Incident Response with Business Continuity and Disaster Recovery

2: Advanced Threat Intelligence

- Threat Intelligence Lifecycle
- Advanced Techniques for Gathering and Analyzing Threat Intelligence
- Utilizing Threat Intelligence Platforms
- Operationalizing Threat Intelligence in Incident Response

3: Advanced Threat Detection Techniques

- Anomaly Detection and Behavioral Analysis
- Machine Learning and AI in Threat Detection
- Advanced Persistent Threats (APTs) and Detection Strategies
- Utilizing Advanced SIEM and IDS/IPS Systems

4: Incident Response in Cloud Environments

- Cloud Security Fundamentals
- Incident Response Strategies for Cloud Services (AWS, Azure, GCP)
- Forensics and Evidence Collection in Cloud Environments
- Legal and Compliance Issues in Cloud Incident Response

5: Advanced Digital Forensics

- Forensic Methodologies and Best Practices
- Network Forensics
- Memory and Malware Analysis
- Advanced Forensic Tools and Techniques

6: Incident Containment and Eradication

- Complex Containment Strategies
- Eradication of Sophisticated Threats
- Coordinated Response Across Multiple Locations
- Incident Containment in Industrial Control Systems (ICS) and IoT

7: Incident Response Automation and Orchestration

- Introduction to Security Orchestration, Automation, and Response (SOAR)
- Automating Incident Response Workflows
- Integration of SOAR with SIEM and Other Security Tools
- Case Studies of Successful Incident Response Automation

8: Advanced Incident Recovery

- Strategies for Complex System Recovery
- Data Recovery and Integrity Verification
- Incident Recovery in Hybrid and Multi-Cloud Environments
- Continuous Monitoring Post-Recovery

9: Legal and Ethical Considerations in Advanced Incident Response

- Advanced Legal Issues in Incident Response
- Global Compliance Requirements
- Ethical Hacking and Incident Response
- Working with International Law Enforcement Agencies

10: Post-Incident Analysis and Reporting

- Comprehensive Post-Incident Review Techniques
- Developing Detailed Incident Reports
- Communication Strategies for Stakeholders
- Continuous Improvement of the Incident Response Plan