INFOSOFT IT SOLUTIONS

Training | Projects | Placements

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

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

HACKING INCIDENT RESPONSE TRAINING

1: Introduction to Hacking Incidents

- Overview of hacking incidents
- Common types of cyber attacks (e.g., phishing, malware, DDoS)
- Case studies of notable hacking incidents

2: Incident Response Fundamentals

- Incident response lifecycle
- Incident response roles and responsibilities
- Legal and regulatory considerations in incident response

3: Preparation and Planning

- Developing an incident response plan
- Establishing incident response team and communication channels
- Conducting risk assessments and threat modeling

4: Detection and Analysis

- Identifying indicators of compromise (IOCs)
- Logging and monitoring for suspicious activities
- Conducting forensics analysis

5: Containment and Eradication

- Containing the impact of a hacking incident
- Removing malicious actors from the network
- Restoring affected systems to a secure state

6: Recovery and Lessons Learned

- Restoring operations after a hacking incident
- Conducting post-incident reviews and analysis
- Documenting lessons learned and updating incident response plans

7: Hands-on Exercises

- Simulated hacking incidents
- Role-playing exercises for incident response teams
- Using incident response tools and technologies

8: Advanced Threat Landscape

- Advanced persistent threats (APTs) and targeted attacks
- Nation-state cyber espionage
- Insider threats and internal sabotage

9: Advanced Incident Response Methodologies

- Threat hunting and proactive detection
- Agile incident response frameworks
- Adaptive incident response strategies

10: Advanced Forensics Analysis

- Memory forensics and volatile data analysis
- Network forensics and packet analysis
- File system forensics and disk imaging

11: Advanced Malware Analysis

- Dynamic malware analysis techniques
- Sandbox evasion and anti-forensics techniques
- Advanced malware reverse engineering

12: Advanced Digital Forensics

- Anti-forensics techniques and countermeasures
- Data recovery and reconstruction
- Steganography and covert channels

13: Advanced Incident Response Tools

- Automated incident response orchestration
- Threat intelligence platforms and feeds

- Security information and event management (SIEM) optimization

14: Advanced Incident Response Simulations

- Complex hacking incident simulations
- Red team vs. blue team exercises
- Live-fire incident response scenarios

15 : Emerging Trends and Future Challenges

- Artificial intelligence and machine learning in incident response
- Internet of Things (IoT) security and incident response challenges
- Quantum computing implications for cryptography and incident response