EC-Council Certified Incident Handler (ECIH) - Exam Topics (with Details)

Incident Response and Handling

- Fundamentals of incident management
- Phases of incident response (Preparation, Detection, Containment, Eradication, Recovery, Lessons Learned)

Incident Handling and Response Process

- Creating and managing incident response teams
- Establishing incident handling policies and procedures

Handling Different Types of Incidents

- Malware incidents
- Web application attacks
- Network security incidents
- Email security incidents
- Insider threats

Forensic Readiness and Evidence Collection

- Chain of custody procedures
- Evidence identification and preservation
- Basic forensic tools and techniques

Risk Assessment and Management in IR

- Assessing business impact of incidents
- Risk mitigation strategies
- Integration of IR into organizational risk management

Incident Recovery and Lessons Learned

- System recovery strategies
- Validating recovery success
- Documenting lessons learned and improving IR plans

Communication During Incidents

- Internal and external communication strategies
- Coordination with law enforcement and stakeholders

Regulatory and Legal Considerations

- Compliance with laws and regulations
- Understanding data protection and privacy obligations