EC-Council

ECIH™
EC-Council Certified Incident Handler

ECIH Exam Blueprint v2

S. No.	Domain	Sub Domains	Weightage
1	**Incident Response and Handling Process**	1.1 Information Security Incidents 1.2 Incident Management 1.3 Incident Response Automation and Orchestration 1.4 Incident Handling Standards and Frameworks 1.5 Incident Handling Laws and Acts 1.6 Incident Response and Handling Process a) Preparation b) Incident Recording and Assignment c) Incident Triage d) Notification e) Containment f) Evidence Gathering and Forensics Analysis g) Eradication h) Recovery i) Post-Incident Activities	11%
2	**First Response**	2.1 First Responder 2.2 Securing and Documenting the Crime Scene 2.3 Collecting Evidence at the Crime Scene 2.4 Preserving, Packaging, and Transporting the Evidence	11%
3	**Malware Incidents**	3.1 Malware Incidents Handling Preparation 3.2 Malware Incidents Detection 3.3 Malware Incidents Containment and Eradication	11%

		3.4 Recovery after Malware Incidents 3.5 Guidelines for Preventing Malware Incidents	
4	**Email Security Incidents**	4.1 Types of Email Security Incidents 4.2 Preparation for Handling Email Security Incidents 4.3 Detection and Containment of Email Security Incidents 4.4 Eradication of Email Security Incidents 4.5 Recovery after Email Security Incidents 4.6 Best Practices against Email Security Incidents	12%
5	**Network Level Incidents**	5.1 Preparation for Handling Network Security Incidents 5.2 Network Security Incidents Detection and Validation 5.3 Handling Unauthorized Access Incidents 5.4 Handling Inappropriate Usage Incidents 5.5 Handling Denial-of-Service Incidents 5.6 Handling Wireless Network Security Incidents	12%
6	**Application Level Incidents**	6.1 Preparation for Handling Web Application Security Incidents 6.2 Web Application Security Incidents Detection and Analysis 6.3 Containment and Eradication of Web Application Security Incidents 6.4 Recovery from Web Application Security Incidents 6.5 Best Practices for Securing Web Applications	11%
7	**Cloud Security Incidents**	7.1 Challenges in Cloud Incident Handling and Response	10%

		7.2 Handling Cloud Security Incidents 7.3 Handling Azure Security Incidents 7.4 Handling AWS Security Incidents 7.5 Handling Google Cloud Security Incidents 7.6 Best Practices Against Cloud Security Incidents	
8	**Insider Threats**	8.1 Types of Insider Threats 8.2 Preparation Steps for Handling Insider Threats 8.3 Detection, Containment, and Eradication of Insider Threats 8.4 Recovery After Insider Attacks 8.5 Best Practices against Insider Threats	11%
9	**Endpoint Security Incidents**	9.1 Need for Endpoint Security Incident Handling and Response 9.2 Preparation for Handling Endpoint Security Incidents 9.3 Detection and Validation of Endpoint Security Incidents 9.4 Handling Mobile-based Security Incidents 9.5 Handling IoT-based Security Incidents 9.6 Handling OT-based Security Incidents	11%