EC-Council

ECIH™

EC-Council | Certified Incident Handler

ECIH Exam Blueprint v1

S. No.	Domain	Sub Domains	Weightage
1	**Incident Response and Handling**	• Information Security • Computer Security • Threat intelligence • Risk Management • Incident Handling • Security Policies	16%
2	**Process Handling**	• Incident Handling and Response • Incident Readiness • Security Auditing • Security Incidents • Forensic Investigation • Eradication and Recovery	14%
3	**Forensic Readiness and First Response**	• Computer Forensics • Digital Evidence • Forensic Readiness • Preservation of Electronic Evidence • Volatile Evidence • Static Evidence • Anti-forensics	13%
4	**Email Security Incidents**	• Email Security • Deceptive and Suspicious Email • Email Incidents • Phishing email	10%
5	**Application Level Incidents**	• Web Application Threats & Vulnerabilities • Web Attack • Eradication of Web Applications	8%
6	**Network & Mobile Incidents**	• Network Attacks • Unauthorized Access • Inappropriate Usage • Denial-of-Service • Wireless Network • Mobile Platform Vulnerabilities and Risks • Eradication of Mobile Incidents & Recovery	16%
7	**Insider Threats**	• Insider Threats • Eradication • Detecting and Preventing Insider Threats • Employee Monitoring Tools	7%

8	**Malware Incidents**	• Malware • Malware Incident Triage • Malicious Code	8%
9	**Incidents Occurred in a Cloud Environment**	• Cloud Computing Threats • Security in Cloud Computing • Eradication • Recovery in Cloud	8%