



EC-Council Certified Incident Handler (ECIH)

Training Brochure

Noida Address: B 77-78 2nd Floor Sec. 6 Noida 201301

Noida Address: B 106 2nd Floor Sec. 6 Noida 201301

Karol Bagh Address: 16/8 3rd Floor Karol Bagh New Delhi 110005

For queries on Training, please contact the undersigned:-

Nikita Bhasin 9310719612

**Silicon Univ EC-Council Accredited Training Centre- Training Arm of
Silicon Comnet Pvt. Ltd.**

EC-Council Certified Incident Handler (ECIH) Training Details:-

- **Duration: 30 Hours**
- **Mode: Hybrid (Online/Classroom)**
- **Classes: Weekdays/Weekends**

Silicon Univ

Silicon Univ EC-Council Accredited Training Centre- Training Arm of
Silicon Comnet Pvt. Ltd.

COURSE CONTENTS

EC-COUNCIL CERTIFIED INCIDENT HANDLER (ECIH)



Modules	Topics
Module 1	Introduction to Incident Handling and Response
	Understand Information Security Threats and Attack Vectors
	Explain Various Attack and Defense Framework
	Understand Information Security Concepts
	Understand Information Security Incidents
	Understand the Incident Management Process
	Understand Incident Response Automation and Orchestration
	Describe Various Incident Handling and Response Best Practices
	Explain Various Standards Related to Incident Handling and Response
	Explain Various Cybersecurity Frameworks
	Understand Incident Handling Laws and Legal Compliance
Module 2	Incident Handling and Response Process
	Understand Incident Handling and Response (IH & R) Process
	Explain preparation steps for Incident Handling and Response
	Understand Incident Recording and Assignment
	Understand Incident Triage
	Explain the Process of Notification
	Understand the process of containment
	Describe Evidence Gathering and Forensics Analysis
	Understand the Process of Recovery
	Describe Various Post-Incident Activities
	Explain the Importance of Information Sharing Activities
Module 3	First Response
	Explain the concept of First Response
	Understand the process of Securing and Documenting the Crime Scene
	Understand the process of Collecting Evidence at the Crime Scene
	Explain the Process of Preserving, Packaging and Transporting Evidence
Module 4	Handling and Responding to Malware Incidents

Silicon Univ EC-Council Accredited Training Centre- Training Arm of
Silicon Comnet Pvt. Ltd.

	Understand the Handling of Malware Incidents
	Explain Preparation for Handling Malware Incidents
	Understand Detection of Malware Incidents
	Explain Containment of Malware Incidents
	Describe How to Perform Malware Analysis
	Understand Eradication of Malware Incidents
	Explain Recovery after Malware Incidents
	Understand the Handling of Malware Incidents- Case Study
	Describe Best Practices against Malware Incidents
Module 5	Handling and Responding to Email Security Incidents
	Understand Email Security Incidents
	Explain Preparation Steps for Handling Email Security Incidents
	Understand Detection and Containment of Email Security Incidents
	Understand Analysis of Email Security Incidents
	Explain Eradication of Email Security Incidents
	Understand the Process of Recovery after Email Security Incidents
	Understand the handling of Email Security Incidents- Case Study
	Explain Best Practices against Email Security Incidents
Module 6	Handling and Responding to Network Security Incidents
	Understand the Handling of Network Security Incidents
	Prepare to Handle Network Security Incidents
	Understand Detection and Validation of Network Security Incidents
	Understand the Handling of Unauthorized Access Incidents
	Understand the Handling of Inappropriate Access Incidents
	Understand the Handling of Denial-of-Service Incidents
	Understand the Handling of Wireless Network Security Incidents
	Understand the Handling of Network Security Incidents- Case Study
	Describe Best Practices against Network Security Incidents
Module 7	Handling and Responding to Web Application Security Incidents
	Understand the Handling of Web Application Incidents
	Explain Preparation for Handling Web Application Security Incidents
	Understand Detection and Containment of Web Application Security Incidents
	Explain Analysis of Web Application Security Incidents
	Understand Eradication of Web Application Security Incidents
	Explain Recovery after Web Application Security Incidents
	Understand the Handling of Web Application Security Incidents- Case Study
	Describe Best Practices for Securing Web Applications
Module 8	Handling and Responding to Cloud Security Incidents

Silicon Univ EC-Council Accredited Training Centre- Training Arm of
Silicon Comnet Pvt. Ltd.

	Understand the Handling of Cloud Security Incidents
	Explain Various Steps Involved in Handling Cloud Service Incidents
	Understand How to Handle Azure Security Incidents
	Understand How to Handle AWS Security Incidents
	Understand How to Handle Google Cloud Security Incidents
	Understand the Handling of Cloud Security Incidents-Case Study
	Explain Best Practices against Cloud Security Incidents
Module 9	Handling and Responding to Insider Threats
	Understand the Handling of Insider Threats
	Explain Preparation Steps for Handling Insider Threats
	Understand Detection and Containment of Insider Threats
	Explain Analysis of Insider Threats
	Understand Eradication of Insider Threats
	Understand the Process of Recovery after Insider Attacks
	Understand the Handling of Insider Threats- Case Study
	Describe Best Practices against Insider Threats
Module 10	Handling and Responding to Endpoint Security Incidents
	Understand the Handling of Endpoint Security Incidents
	Explain the Handling of Mobile-based Security Incidents
	Explain the Handling of IoT-based Security Incidents
	Explain the Handling of OT-based Security Incidents
	Understanding the Handling of Endpoint Security Incidents- Case Study