GIAC Certified Incident Handler (GCIH) Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The modern cyber threat landscape is defined by the proliferation of sophisticated attacks, including Ransomware-as-a-Service (RaaS), advanced persistent threats (APTs), and supply chain compromises. As the average dwell time remains a critical risk factor, organizations urgently need Certified Incident Handlers capable of rapid threat detection, containment, and eradication. GIAC Certified Incident Handler (GCIH) Training Course is meticulously designed to transform security professionals into expert First Responders and Digital Forensics analysts, equipping them with the offensive knowledge to anticipate, analyze, and mitigate complex cyber-attacks. The training emphasizes practical, hands-on experience with industry-leading tools and techniques for cloud-centric incident response and post-exploitation analysis.

This comprehensive program is fully aligned with the PICERL Incident Handling Process (Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned) and the MITRE ATT&CK Framework, ensuring immediate, real-world applicability. By mastering essential skills in network forensics, malware analysis, and live system investigation, participants will gain the confidence to lead effective incident response teams and drastically reduce organizational cyber risk. Upon completion, trainees will be fully prepared to pass the GIAC Certified Incident Handler (GCIH) exam and elevate their career in the high-demand field of cyber resilience and proactive threat hunting.

Programme Curriculum

GIAC Certified Incident Handler (GCIH) Training Course

Introduction

The modern cyber threat landscape is defined by the proliferation of sophisticated attacks, including Ransomware-as-a-Service (RaaS), advanced persistent threats (APTs), and supply chain compromises. As the average dwell time remains a critical risk factor, organizations urgently need Certified Incident Handlers capable

of rapid threat detection, containment, and eradication. GIAC Certified Incident Handler (GCIH) Training Course is meticulously designed to transform security professionals into expert First Responders and Digital Forensics analysts, equipping them with the offensive knowledge to anticipate, analyze, and mitigate complex cyber-attacks. The training emphasizes practical, hands-on experience with industry-leading tools and techniques for cloud-centric incident response and post-exploitation analysis.

This comprehensive program is fully aligned with the PICERL Incident Handling Process (Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned) and the MITRE ATT&CK Framework, ensuring immediate, real-world applicability. By mastering essential skills in network forensics, malware analysis, and live system investigation, participants will gain the confidence to lead effective incident response teams and drastically reduce organizational cyber risk. Upon completion, trainees will be fully prepared to pass the GIAC Certified Incident Handler (GCIH) exam and elevate their career in the high-demand field of cyber resilience and proactive threat hunting.

Course Duration

5 days

Course Objectives with Strong Trending Keywords

1. Master the PICERL Incident Handling Process and implement a robust, Zero Trust-aligned Incident Response Plan (IRP).
2. Perform rapid Triage and Scoping using SIEM/SOAR platforms to minimize dwell time and organizational impact.
3. Utilize Proactive Threat Hunting techniques and the MITRE ATT&CK Framework for early threat anticipation and defense.
4. Conduct effective Network Forensics and Log Analysis to identify and trace covert C2 channels and data exfiltration.
5. Execute Live System Forensics and Memory Analysis for Endpoint Detection and Response (EDR) and artifact collection.
6. Analyze common Post-Exploitation Attacks, including Lateral Movement, Persistence mechanisms, and credential harvesting.
7. Apply practical Malware Analysis and sandbox techniques to understand Ransomware-as-a-Service and custom malware.
8. Implement strategic Containment and Eradication measures across cloud environments and traditional networks.
9. Investigate and defend against modern Web Application Attacks, including advanced injection, API abuse, and configuration flaws.
10. Identify and remediate initial access vectors like Stolen Credentials, phishing, and exploiting known vulnerabilities.
11. Produce legally sound Post-Incident Reports, manage Chain of Custody, and conduct thorough Lessons Learned reviews.
12. Leverage Hacker Tools to understand the Adversary Mindset and strengthen defensive postures.
13. Integrate Threat Intelligence (TI) feeds to enrich incident data and support data-driven decision-making during a breach.

Target Audience

1. Incident Handlers / SOC Analysts.
2. Cybersecurity Consultants.

3. System/Network Administrators.
4. Security Engineers
5. Threat Intelligence Analysts.
6. IT Auditors/Compliance Professionals.
7. Information Security Managers.
8. Professionals preparing to challenge the official GIAC GCIH Certification Exam.

Course Modules

Module 1: Incident Response Foundations and Preparation

- The PICERL/DAIR frameworks and their application in enterprise IR.
- Developing and testing an Incident Response Plan and Cyber Resilience strategy.
- Establishing Jump Boxes and proper toolkits.
- Defining the Chain of Custody procedures for evidence collection.
- Case Study: Analyzing a major industry breach to critique the initial Preparation and Communication strategies utilized.

Module 2: Hacker Techniques and Reconnaissance

- Understanding the Adversary Mindset and the stages of a cyber-attack
- Performing deep Open-Source Intelligence and public reconnaissance.
- Utilizing Nmap for advanced scanning, service enumeration, and IDS/IPS Evasion techniques.
- Investigating Password Attacks and defenses.
- Case Study: Simulating an external reconnaissance phase against a target organization using OSINT and scanning to identify high-value targets.

Module 3: System Hacking and Exploitation

- The mechanics of system exploitation, including Buffer Overflows and shellcode.
- Hands-on practice with Metasploit to deploy exploits and manage payloads.
- Analyzing Client-Side Attacks and protecting endpoints.
- The concept of Order of Volatility and proper data acquisition from live systems.
- Case Study: Using a target machine to perform an authenticated exploitation via Metasploit, followed by initial evidence capture.

Module 4: Network and Web Application Attacks

- Common vulnerabilities and exploitation of network protocols
- Analyzing traffic to detect Covert Channels and tunnel creation using Wireshark.
- Investigating and defending against the OWASP Top 10.
- Implementing and bypassing network-level Containment measures
- Case Study: Responding to an active Web Shell deployment, identifying the initial SQL Injection vector, and implementing a quick-fix containment.

Module 5: Post-Exploitation and Maintaining Access

- Techniques used by attackers to maintain Persistence and achieve Privilege Escalation.
- Detecting and removing malicious software like Rootkits, Trojans, and backdoors on Windows and Linux.
- Deep-dive into Lateral Movement and Credential Harvesting using tools like Mimikatz and Pass-the-Hash.
- Monitoring for Living Off the Land binaries that attackers use to blend in.

- Case Study: Investigating a simulated internal breach where an attacker pivoted from one compromised system to an Active Directory controller.

Module 6: Digital Forensics and Live System Analysis

- Advanced techniques for Memory Forensics and disk analysis for artifact retrieval.
- Using tools for deep-dive analysis of system artifacts.
- Analyzing host logs for signs of compromise and Evasion Techniques.
- Documenting all forensic steps to ensure the integrity of the Chain of Custody for potential legal action.
- Case Study: Conducting a live memory dump and analysis to find hidden malware processes and command history, effectively uncovering the Indicator of Compromise

Module 7: Malware and Ransomware Incident Response

- The anatomy of Ransomware-as-a-Service and common malware delivery mechanisms.
- Performing Basic Malware Analysis in a secure sandbox environment.
- Containment: Implementing targeted Eradication and Recovery steps for a file-encrypting ransomware incident.
- Best practices for data backups, system hardening, and Application Whitelisting.
- Case Study: Leading a full ransomware incident response, from initial encryption notification to successful decryption/recovery of affected systems.

Module 8: Remediation, Recovery, and Lessons Learned

- The crucial final stages of incident response.
- Writing professional, detailed Post-Incident Reports for technical and executive audiences.
- Conducting a comprehensive Post-Mortem Review to identify systemic failures and improve security policy.
- Translating Lessons Learned into actionable improvements for Proactive Threat Hunting and security control updates.
- Case Study: Reviewing and presenting a final Incident Report to a simulated executive team, focusing on the root cause and strategic recommendations.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to FINESKILL TRAINING CENTER account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
07 Sep 2026	11 Sep 2026	Online	$1,100
14 Sep 2026	18 Sep 2026	Online	$1,100
21 Sep 2026	25 Sep 2026	Online	$1,100
28 Sep 2026	02 Oct 2026	Online	$1,100
05 Oct 2026	09 Oct 2026	Online	$1,100
12 Oct 2026	16 Oct 2026	Online	$1,100
19 Oct 2026	23 Oct 2026	Online	$1,100
26 Oct 2026	30 Oct 2026	Online	$1,100

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now