



## ERIC REED

**CYBERSECURITY TRAINING**

PASS ON THE FIRST ATTEMPT!™



### COMPANY OVERVIEW

For over 25 years, Eric Reed Cybersecurity Training has been a trusted leader in cybersecurity education, equipping more than 60,000 professionals with the skills needed to defend against emerging cyber threats. Our mission is to empower individuals and organizations with comprehensive, hands-on training that translates directly to real-world success. Recognized with multiple industry awards—including an unprecedented 10-time EC Council Instructor of the Year and 7-time Circle of Excellence honoree—we combine innovative delivery methods with a passion for excellence to ensure our students achieve certification success on the first attempt



### EC-COUNCIL E|CIH V3

The EC-Council Certified Incident Handler (ECIH) certification focuses on incident detection, response, and recovery strategies to mitigate cybersecurity threats.



**ONLINE LIVE LEARNING**



**ON-DEMAND LIVE LEARNING**

### ONLINE LIVE & ON-DEMAND LIVE

All the benefits of live, instructor-led training with the convenience of on-demand.

- **Online Live:** Attend our scheduled sessions in real time (Monday–Friday). Get immediate interaction with the instructor and fellow students.
- **On-Demand Live:** Access recordings of the most recent live sessions on your own schedule, while still having direct instructor support.
- **Flexible Scheduling:** Choose a structured approach—one-week bootcamp (M–F), two nights a week for five weeks, or every Saturday for five weeks. Need more wiggle room? Adjust any schedule to fit your lifestyle!



### COURSE OBJECTIVES

- Develop and implement incident response plans.
- Detect, contain, and remediate cyber incidents.
- Utilize forensic tools for threat analysis and mitigation.
- Apply best practices for threat intelligence and recovery.
- Ensure compliance with security policies and regulations.



### SALARY RANGE

**E|CIH → \$85,000 - \$125,000**

*These figures are approximate and depend on location, experience, and job role. Higher salaries are usually seen in major tech hubs and with significant experience.*



### JOB ROLES

- **Incident Response Analyst**



*"It's was a great class that covered all aspects of security. Most importantly, I appreciate the fact that you are giving up your own time to assist us and maintain a sharedrive with the latest security tools and informative papers even after the class is over. I was able to pass the test after one week of attending the training."*

*-Shadi Ehalabi*

### Contact Us

- 📞 (707) 722-7333
- ✉ info@ericreedlive.com
- 📍 1401 61st St S  
Gulfport, FL 33707



[WWW.LINKEDIN.COM/IN/ERICREEDLIVE/](http://WWW.LINKEDIN.COM/IN/ERICREEDLIVE/)



## EC-COUNCIL E | CIH OVERVIEW

### 1 - Introduction to Incident Handling and Response

Understand Information Security Threats and Attack Vectors  
Explain Various Attack and Defense Frameworks  
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



### 2 - Incident Handling and Response Process

Understand Incident Handling and Response (IH&R) Process  
Step 1: Preparation for Incident Handling and Response  
Step 2: Incident Recording and Assignment  
Step 3: Incident Triage  
Step 4: Notification  
Step 5: Containment  
Step 6: Evidence Gathering and Forensic Analysis  
Step 7: Eradication  
Step 8: Recovery  
Step 9: Post-Incident Activities  
Information Sharing Activities



### 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 for Preserving, Packaging, and Transporting Evidence



### 4 - Handling and Responding to Malware Incidents

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



## 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



## 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 Usage 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



## 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



## 8 - Handling and Responding to Cloud Security Incidents

Understand the Handling of Cloud Security Incidents

Explain Various Steps Involved in Handling Cloud Security 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



## **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



## **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
- Understand the Handling of Endpoint Security Incidents - Case Study