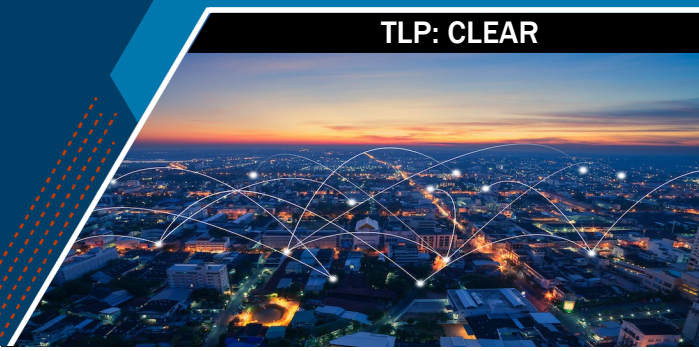
INCIDENT RESPONSE PATHWAY



INCIDENT RESPONSE PATHWAY

The **Incident Response Pathway** is a comprehensive 4-week, instructor-led cybersecurity training course designed to develop proficiency in managing the complete incident response lifecycle. Starting with foundational frameworks and methodologies, participants progress through advanced detection techniques, containment strategies, and recovery procedures. The course combines theoretical instruction with extensive hands-on labs, covering critical skills in malware detection, log analysis, network forensics, and SIEM tool usage. By completion, students are prepared to handle complex incidents across traditional and cloud environments, create professional documentation, and coordinate response efforts effectively. Whether beginning in incident response or enhancing existing expertise, participants gain both strategic and practical skills needed to address today's evolving threat landscape.

KEY LEARNING OUTCOMES

- Configure and maintain a basic incident response environment
- Configure and utilize SIEM tools for effective incident detection
- Implement effective containment strategies for various incident types
- Security Operations Engineer
- Utilize cloud-native security tools for incident handling

CAREER OPPORTUNITIES RELATED TO THIS SUBJECT

- Incident Response Analyst
- SOC Analyst
- Cybersecurity Analyst
- Security Operations Engineer
- Threat Response Engineer
- Digital Forensics Specialist
- Security Incident Handler
- IT Security Specialist

PATHWAY METRICS

- Course Duration: 4-Weeks (160 hours)
- CPE Credits: 160
- Certification: EC-Council Certified Incident Handler (ECIH)

This document is marked TLP: CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp.

PROFICIENCY LEVEL: INTERMEDIATE CYBERSECURITY PROFESSIONAL

Participants should have a more robust understanding of foundational IT and cybersecurity principles and some technical exposure to incident response tools and threat detection concepts. The course builds on core competencies and accelerates through complex scenarios and advanced topics involving both on-premises and cloud environments. A strong foundation in the fundamentals is essential for successfully navigating the course and engaging with the material. This course is not recommended for beginners.

TARGET AUDIENCE

This pathway is ideal for individuals seeking to build or enhance skills in responding to cybersecurity incidents. It is particularly suited for:

- Aspiring or early-career incident responders, SOC analysts, or cybersecurity operations personnel
- IT professionals transitioning into cybersecurity roles, especially in operations or compliance
- Government personnel supporting security operations centers (SOCs), IR teams, or forensic investigations
- Technical staff who need to understand IR procedures and reporting within a larger cyber defense strategy

RECOMMENDED PREREQUISITES

While the prerequisites are not mandatory, they are essential for successfully navigating this course. This program is designed for individuals with a more robust understanding of IT and cybersecurity fundamentals—it is not recommended for beginners. If you lack a solid foundation in these areas, the course material may prove too challenging. All Pathway courses are live instructor-led to help facilitate learning and skill development for participants across broad skill levels.

To ensure readiness for the hands-on and technical aspects of the course, participants should ideally have the following exposure and proficiencies prior to enrolling:

- Basic proficiency with computers and operating systems (Windows/Linux), command-line navigation, and general understanding of logging/system data collection, file systems, folders, and application usage.
- Basic understanding of IT systems, including patch management, software updates, and common misconfigurations. *No prior experience in system hardening, vulnerability scanning, or deep operating systems knowledge is needed.*
- Familiarity with basic cybersecurity concepts including the CIA triad (confidentiality, integrity, availability), basic threat types (i.e., malware, phishing), software patching, and high-level understanding on security vulnerabilities.
- Comfort using basic command-line, including directory navigation, file operations, user commands, and introductory scripting capabilities. *No automation or tool-specific experience is required; however, it may be advantageous during training in lab environments.*

INCIDENT RESPONSE COURSE OUTLINE

Week 1: Fundamentals of Incident Response: *Introduction to incident response fundamentals through theoretical instruction and hands-on labs, covering frameworks, methodologies, and basic incident handling procedures.*

Week 1 Learning Outcomes:

- Articulate the phases of the incident response lifecycle and their interconnections
- Configure and maintain a basic incident response environment
- Create professional incident documentation and reports
- Execute basic incident response procedures following standard protocols
- Identify and apply relevant legal and regulatory requirements
- Demonstrate understanding of incident response team roles and responsibilities
- Implement basic malware response procedures

Week 2: Incident Detection and Analysis: *Technical deep dive into incident detection and analysis, focusing on tools and techniques for security incident investigation and threat analysis.*

Week 2 Learning Outcomes:

- Configure and utilize SIEM tools for effective incident detection
- Perform network traffic analysis using professional tools like Wireshark
- Conduct basic malware analysis and understand malware behavior
- Identify and analyze multi-stage attacks
- Correlate security events from multiple data sources
- Create detailed technical analysis reports
- Implement effective detection strategies for various attack types

Week 3: Incident Containment, Eradication, and Recovery: *Practical application of response techniques focusing on containment, eradication, and recovery procedures through hands-on exercises and simulations.*

Week 3 Learning Outcomes:

- Implement effective containment strategies for various incident types
- Perform thorough root cause analysis of security incidents
- Execute system and data recovery procedures
- Develop and implement business continuity plans
- Coordinate comprehensive incident response activities
- Document containment and eradication procedures
- Validate recovery effectiveness and system integrity
- Create after-action reports and lessons learned documentation

Week 4: Cloud Incident Response and Certification Preparation: *Advanced exploration of cloud-specific incident response challenges combined with certification preparation and a comprehensive capstone project.*

Week 4 Learning Outcomes:

- Implement incident response procedures in cloud environments
- Utilize cloud-native security tools for incident handling
- Adapt traditional IR procedures for cloud environments
- Respond to advanced persistent threats (APTs)
- Design and execute hybrid environment response plans
- Prepare effectively for professional certification exams
- Present technical findings to various stakeholders
- Demonstrate comprehensive incident response capabilities