OffSec IR-200- Incident Response Essentials

Course Duration: 5 Days
Exam Reference: OffSec Incident Responder (OSIR)

Course Overview

OffSec's Incident Response Essentials (IR-200) course provides cybersecurity professionals with practical training to prepare for, identify, and handle security incidents effectively. The course focuses on core incident response concepts and explores how organizations manage and mitigate cyber threats in real-world situations. Participants will learn to understand the incident response lifecycle, develop comprehensive incident response plans, and utilize tools and techniques for efficient detection and analysis of security events.

Upon successfully completing the hands-on exam, Learners earn the OffSec Certified Incident Responder (OSIR) certification. This credential validates expertise in foundational incident response practices, positioning you as a valuable asset to incident response teams, Security Operations Centers (SOCs), and organizations committed to strengthening their cybersecurity defenses.

Prerequisites

While there are no formal prerequisites, it's strongly recommended that you have:

- A basic understanding of networking concepts
- Familiarity with Linux and Windows operating systems

Learners can also go through the OffSec Network Penetration Testing Essentials Learning Path to ensure they're ready for the course, included in Learn Fundamentals and Learn One subscription.

Course Objectives

Upon completing IR-200 and successfully passing the OSIR exam, you'll develop a strong foundation in:

- Incident response concepts and methodologies
- Preparation and planning for security incidents
- Detection and analysis of security events
- Containment, eradication, and recovery techniques
- Post-incident activities and reporting
- Practical skills applicable to roles in incident response, SOC analysis, and cybersecurity operations

APPLIED TECHNOLOGY ACADEMY

Contact Us

800.674.3550

2151 W. Hillsboro Blvd., Ste 210
Deerfield Beach, FL 33442

Connect With Us

OffSec IR-200- Incident Response Essentials

Course Outline

Module 1: Incident Response Overview

- What is a Cyber Incident?
- Cybersecurity within an IT Incident
- Common Types of Incidents
- Case Studies

Module 2: Fundamentals of Incident Response

- Incident Response Frameworks
- Roles and Responsibilities of Incident Response Teams

Module 3: Phases of Incident Response

- The Preparation Stage
- Managing an Incident Response
- Post-Response Activities

Module 4: Incident Response Communication Plans

- The Importance of a Communications Plan
- Communications Plan Before a Crisis
- Communications Plan During a Crisis
- Communications Plan After a Crisis

Module 5: Common Attack Techniques

- Indicators of Compromise (IOC) and Cybersecurity Frameworks
- Opportunistic Attacks
- Targeted Attacks

Module 6: Incident Detection and Identification

- Passive Incident Alerting
- Active Incident Discovery
- Identifying False Positives
- Identifying Attack Chains

Module 7: Initial Impact Assessment

- Impact Categories, Recoverability, and Incident Prioritization
- Creating an Initial Impact Assessment

OffSec IR-200- Incident Response Essentials

Module 8: Digital Forensics for Incident Responders

- Fundamentals of Digital Evidence Handling
- Forensic Tools and Techniques
- Malware Analysis

Module 9: Incident Response Case Management

- Creating and Managing Incident Cases
- Creating a Case Based on Our Lab Incident

Module 10: Active Incident Containment

- Isolation Techniques
- Containment Strategies

Module 11: Incident Eradication and Recovery

- Eradication
- Recovery

Module 12: Post-Mortem Reporting

- The Post-Mortem Report
- Root Cause Analysis
- Impact and Damage Assessment
- Lessons Learned
- Bringing It Together

Module 13: Challenge Lab