APPLIED TECHNOLOGY ACADEMY

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

OffSec Foundational Incident Response (IR-200) Training

OffSec Authorized Training · Applied Technology Academy

IR-200 is a foundational incident response course designed to equip learners with essential skills to manage and mitigate cyber threats, preparing them for roles in Security Operations Centers (SOCs) and incident response teams. The course covers the incident response lifecycle, including developing detection and identification strategies, applying digital forensics, analyzing attack techniques with mitigation strategies, and developing communication plans for crises. Upon passing the exam, learners can earn the OffSec Incident Responder (OSIR) certification.

LEVEL	DURATION	EXPERIENCE	AVERAGE SALARY	LABS
Beginner	**5 Days**	**None (TCP/IP, Linux & Windows, security basics recommended)**	**$129,180**	**Yes**

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.

Course Outline

- **Module 1: Incident Response Overview**
- **Module 2: Fundamentals of Incident Response**
- **Module 3: Phases of Incident Response**

- **Module 4: Incident Response Communication Plans**
- **Module 5: Common Attack Techniques**
- **Module 6: Incident Detection and Identification**
- **Module 7: Initial Impact Assessment**
- **Module 8: Digital Forensics for Incident Responders**
- **Module 9: Incident Response Case Management**
- **Module 10: Active Incident Containment**
- **Module 11: Incident Eradication and Recovery**
- **Module 12: Post-Mortem Reporting**
- **Module 13: Challenge Lab**

Intended Audience

The IR-200 course is designed for individuals seeking to build a strong foundation in incident response.

It's ideal for:

- Aspiring incident responders
- Security Operations Center (SOC) analysts
- IT security specialists
- Professionals aiming to transition into specialized cybersecurity roles focused on incident management

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.

Follow-On Courses

- SOC-200- Foundational Security Operations and Defensive Analysis
- TH-200- Foundational Threat Hunting

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.