OffSec

IR-200

Foundational Incident Response

OSIR

IR-200 (Foundational Incident Response) focuses on core incident response concepts and explores how organizations manage and mitigate cyber threats in real-world situations. Upon completion of this course, learners will understand the incident response lifecycle, develop comprehensive incident response plans, and utilize tools and techniques for efficient detection and analysis of security events. Learners will gain expertise in foundational incident response practices, positioning them as a valuable asset to incident response teams, Security Operations Centers (SOCs), and organizations committed to strengthening their cybersecurity defenses.

Incident Response Overview	Introduces the core concepts of incident response, focusing on NIST Special Publication 800-61
Fundamentals of Incident Response	Learn about the roles and responsibilities of incident response teams and the frameworks they use (CREST, SANS, NIST)
Phases of Incident Response	Dive into NIST SP800-61's four phases of Incident Response
Incident Response Communication Plans	Review examples of good and bad external communications to learn the importance of incident response communication plans
Common Attack Techniques	Identify commonly used opportunistic and targeted attacks to improve your ability to respond and recover from security incidents
Incident Detection and Identification	Recognize and analyze malicious activities to decide which actions you should take to manage and mitigate them
Digital Forensics for Incident Responders	Identify, collect, analyze, and preserve digital evidence from cybersecurity attacks
Incident Response Case Management	Walk through the process of opening a case, adding assets, creating an event timeline, and identifying through an IRIS lab
Active Incident Containment	Isolate and neutralize detected threats using isolation techniques and containment strategies

OffSec

IR-200

Foundational Incident Response

OSIR

Incident Eradication and Recovery	Focus on identifying and eliminating threats quickly to restore normal operations
Initial Impact Assessment	Develop assessments to evaluate the effects an incident has or could have on an organization
Post-Mortem Reporting	Create technical records of incidents to improve responses to future incidents and reinforce the value of information security services