Foundational Incident Response (OSIR) Syllabus

Course Summary, Methodology, and Organization of Content	
Course Summary	IR-200: Foundational Incident Response is a course designed to teach you the essential skills for effective incident response. You'll learn methodologies and tools for detecting, analyzing, and responding to cybersecurity incidents. Through hands-on labs and online content, you'll gain practical experience in incident analysis and recovery processes. IR-200 prepares you for the OffSec Incident Responder (OSIR) exam and positions you for a junior-level role in cybersecurity incident response.
Learning Methodology	IR-200 utilizes a blended learning approach that combines interactive online instruction with hands-on labs. Learners engage with comprehensive course materials, including readings and practical exercises, while applying their knowledge in simulated environments to develop practical skills. Completing the course and successfully passing the associated exam awards the OffSec Incident Responder (OSIR) certification.

The following section contains the various Learning Modules and Learning Units.

Learning Module	Learning Units
Incident Response Overview	What is a Cyber Incident?
	Cybersecurity within an IT Incident
	Common Types of Incidents
	Case Studies
	Wrapping Up

Fundamentals of Incident Response	Incident Response Frameworks
	Roles and Responsibilities of Incident Response Teams
	Wrapping Up
Phases of Incident Response	The Preparation Stage
	Managing an Incident Response
	Post-Response Activities
	Wrapping Up
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
	Wrapping Up

Common Attack Techniques	Indicators of Compromise (IOC) and Cybersecurity Frameworks
	Opportunistic Attacks
	Targeted Attacks
	Wrapping Up
Incident Detection and Identification	Passive Incident Alerting
	Active Incident Discovery
	Identifying False Positives
	Identifying Attack Chains
	Wrapping Up
Initial Impact Assessment	Impact Categories, Recoverability, and Incident Prioritization
	Creating an Initial Impact Assessment
	Wrapping Up

Digital Forensics for Incident Responders	Fundamentals of Digital Evidence Handling
	Forensic Tools and Techniques
	Malware Analysis
	Wrapping Up
Incident Response Case Management	Creating and Managing Incident Cases
	Creating a Case Based on Our Lab Incident
	Wrapping Up
Active Incident Containment	Isolation Techniques
	Containment Strategies
	Wrapping Up
Incident Eradication and Recovery	Eradication
	Recovery

	Wrapping Up
Post-Mortem Reporting	The Post-mortem Report
	Root Cause Analysis
	Impact and Damage Assessment
	Lessons Learned
	Bringing It Together
	Wrapping Up
Challenge Lab	IR-200: Foundational Incident Response Challenge Lab