IR-200: Foundational Incident Response Certification

Duration: 90 Days

Course Description:

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.

Course Outlines:

Incident Response Overview

- This module introduces the concepts of incident response with the main focus being NIST Special Publication 800-61.

Fundamentals of Incident Response

- This module covers the roles and responsibilities of incident response teams, and the main frameworks used by incident responders (CREST, SANS, NIST).

Phases of Incident Response

- NIST SP800-61 provides a four-phase model of Incident Response. This module describes what each phase of an incident response plan comprises.

Incident Response Communication Plans

Learn about the value and contents of incident response communications plans, and review examples of good and bad external communications.

Common Attack Techniques

- This module covers opportunistic and targeted attacks.

Incident Detection and Identification

- This module covers the detection and analysis of malicious activities.

Initial Impact Assessment

- The first thing we need to do when a security incident occurs is an initial assessment of the scope and impact of the incident. This module covers the way in which this is accomplished.

Digital Forensics for Incident Responders

- This Module covers forensic measures and evidence handling considerations.

Incident Response Case Management

- This module covers case management theory with an IRIS lab.

Active Incident Containment

- This module covers how to isolate and neutralize detected threats. It explores techniques such as design-led isolation, dynamic containment during incidents, and addresses topics like isolation techniques, containment strategies, and their implications for businesses.