IRBIZ (Exam IRZ-110) Incident Response for Business Professionals

This document includes instructor led class overview and objectives, identifies target student and prerequisites, course outline, and course specific software and hardware requirements.

Course Length:

1 day

Overview:

This course covers incident response methods and procedures are taught in alignment with industry frameworks such as US-CERT's NCISP (National Cyber Incident Response Plan), and Presidential Policy Directive (PPD) 41 on Cyber Incident Coordination Policy. It is ideal for candidates who have been tasked with managing compliance with state legislation and other regulatory requirements regarding incident response, and for executing standardized responses to such incidents. The course introduces procedures and resources to comply with legislative requirements regarding incident response.

This course is designed to assist students in preparing for the CertNexus Incident Responder Credential (CIR-110). What you learn and practice in this course can be a significant part of your preparation.

Course Objectives:

In this course, you will understand, assess and respond to security threats and operate a system and network security analysis platform.
You will:

- Explain the importance of best practices in preparation for incident response
- Given a scenario, execute incident response process
- Explain general mitigation methods and devices
- Assess and comply with current incident response requirements.

Target Student:

This course is designed primarily for IT leaders and company executives who are responsible for complying with incident response legislation.   This course focuses on the knowledge, resources, and skills necessary to comply with incident response, and incident handling process requirements.

Prerequisites:

General understanding of cybersecurity concepts.

Course Content

Lesson 1: Assessment of Information Security Risks

Topic A: The Importance of Risk Management

Topic D: Integrating Documentation into Risk Management

Lesson 2: Response to Cybersecurity Incidents

Topic A: Deployment of Incident Handling and Response Architecture

Topic B: Containment and Mitigation of Incidents

Topic C: Preparation for Forensic Investigation as a CSIRT

Lesson 3: Investigating Cybersecurity Incidents

Topic A: Use a Forensic Investigation Plan

Topic B: Securely Collect and Analyze Electronic Evidence

Topic C: Follow Up on the Results of an Investigation

Lesson 4: Complying with Legislation

- Examples of Legislation (if this is covered in above topics, no need to include here) GDPR, HIPPA, Elections
- Case study: Incident Response and GDPR (Using GDPR legislation, create a response that is compliant with it – this could be discussion-based activity as well.)
- State Legislation Resources and Example – Search terms to find state legislation
  - Using NYS as example use the NYS Privacy Response act or other legislation to create a similar case study as previous.
  - Provide answers on when to use federal versus state and do you have to follow both?

Appendix C: Security Resources