CN-IRBIZ

INCIDENT RESPONSE FOR BUSINESS PROFESSIONALS

DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
1 Day	Fundamentals	Cyber Security	Classroom or Virtual	NA

INTRODUCTION

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.

AUDIENCE PROFILE

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.
- Students 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.

PREREQUISITES

General understanding of cybersecurity concepts.

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.

COURSE TOPICS

Lesson 1: Assessment of Information Security Risks

- The Importance of Risk Management
- Integrating Documentation into Risk Management

Lesson 2: Response to Cybersecurity Incidents

- Deployment of Incident Handling and Response Architecture
- Containment and Mitigation of Incidents
- Preparation for Forensic Investigation as a CSIRT

Lesson 3: Investigating Cybersecurity Incidents

- Use a Forensic Investigation Plan

- Securely Collect and Analyze Electronic Evidence
- Follow Up on the Results of an Investigation

Lesson 4: Complying with Legislation

- Examples of Legislation (GDPR,HIPPA, Elections)
- Case study: Incident Response and GDPR (Using GDPR legislation, create a response that is compliant with it

ASSOCIATED CERTIFICATIONS & EXAM

The Incident Response for Business Professionals exam (#IRZ-110) will certify that the candidate can assess and respond to security threats and operate a system and network security analysis platform.

Upon completion of this course, delegates will receive a MIE attendance certificate.