Certnexus - Incident Response for Business Professionals

Kód kurzu: IRBIZ

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.

Pro koho je kurz určen

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.

Co Vás naučíme

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.

Požadované vstupní znalosti

General understanding of cybersecurity concepts

Studijní materiály

Official guide book for this course

Osnova kurzu

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 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?

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

Copyright © 2020 GOPAS, a.s.,
All rights reserved