CyberSec First Responder Certification Training

Course: **00073**
Filter: **Beginner**
Duration: **20 hours**
Category:: **Cyber Security**
Price: **2450,00 €**

About Course

This CyberSec First Responder Certification course from CertNexus takes a holistic approach to prepare IT Professionals to analyze threats, secure networks, and utilize critical problem-solving skillsets to protect an organization from threats. Focusing on the key areas of detect, analyze, and respond, attendees will gain the knowledge and practical skills needed to recover from attacks and thwart potential future threats. Passing the CFR Certification Exam meets U.S. DoD Directive 8140/8570.01 CSSP Analyst, CSSP Infrastructure Support, CSSP Incident Responder, and CSSP Auditor requirements.

What you'll learn

- Effectively identify malicious activities involving computing systems.
- Assess information security risks in network environments.
- Collect cybersecurity intelligence to prepare for assessments.
- Develop the skills needed to cut the lag time between when a breach occurs and when it is detected.
- Assess the risks and vulnerabilities to analyze and determine the scope in an immersive, hands-on environment.
- Effectively protect critical information systems before, during, and after an attack.
- Analyze post-attack techniques and apply skills to respond proactively

Pre-requisites

- 3-5 years of experience working in an IT environment and familiarity with networks, systems, administration, etc.

Curriculum

Module 1: Assessing Information Security Risk

- Identify the Importance of Risk Management
- Assess Risk
- Mitigate Risk
- Integrate Documentation into Risk Management

Module 2: Analyzing the Threat Landscape

- Classify Threats and Threat Profiles
- Perform Ongoing Threat Research

Module 3: Analyzing Reconnaissance Threats to Computing and Network Environments

- Implement Threat Modeling
- Assess the Impact of Reconnaissance
- Assess the Impact of Social Engineering

Module 4: Analyzing Attacks on Computing and Network Environments

- Assess the Impact of System Hacking Attacks
- Assess the Impact of Web-Based Attacks
- Assess the Impact of Malware
- Assess the Impact of Hijacking and Impersonation Attacks
- Assess the Impact of DoS Incidents
- Assess the Impact of Threats to Mobile Security
- Assess the Impact of Threats to Cloud Security

Module 5: Analyzing Post-Attack Techniques

- Assess Command and Control Techniques
- Assess Persistence Techniques

- Assess Lateral Movement and Pivoting Techniques
- Assess Data Exfiltration Techniques
- Assess Anti-Forensics Techniques

Module 6: Managing Vulnerabilities in the Organization

- Implement a Vulnerability Management Plan
- Assess Common Vulnerabilities
- Conduct Vulnerability Scans

Module 7: Implementing Penetration Testing to Evaluate Security

- Conduct Penetration Tests on Network Assets
- Follow Up on Penetration Testing

Module 8: Collecting Cybersecurity Intelligence

- Deploy a Security Intelligence Collection and Analysis Platform
- Collect Data from Network-Based Intelligence Sources
- Collect Data from Host-Based Intelligence Sources

Module 9: Analyzing Log Data

- Use Common Tools to Analyze Logs
- Use SIEM Tools for Analysis

Module 10: Performing Active Asset and Network Analysis

- Analyze Incidents with Windows-Based Tools
- Analyze Incidents with Linux-Based Tools
- Analyze Malware
- Analyze Indicators of Compromise

Module 11: Responding to Cybersecurity Incidents

- Deploy an Incident Handling and Response Architecture
- Contain and Mitigate Incidents

- Prepare for Forensic Investigation as a CSIRT

Module 12: Investigating Cybersecurity Incidents

- Apply a Forensic Investigation Plan
- Securely Collect and Analyze Electronic Evidence
- Follow Up on the Results of an Investigation
- Mapping Course Content to CyberSec First Responder™ (Exam CFR-410)
- Regular Expressions
- Security Resources
- U.S. Department of Defense Operational Security Practices