CyberSECURE First Responder

Prepare for Certified CyberSECURE First Responder Exam

Duration: 5 Days

Overview:

CyberSec First Responders are just that: the first line of response against cyber-attacks that can cost your organization valuable time and money. The CyberSec First Responder: Threat Detection and Response course, or CFR, will prepare security professionals to become the first line of response against cyber-attacks by teaching students to analyze threats, design secure computing and network environments, proactively defend networks, and respond/investigate cybersecurity incidents. CFR is also designed for students who are seeking to fulfill DoD directive 8570.01 for information assurance training.

Target Student:

CyberSec First Responder: Threat Detection and Response is designed for information assurance professionals who perform job functions related to the development, operation, management, and enforcement of security capabilities for systems and networks. This course is also designed for students who are seeking to fulfill DoD directive 8570.01 for information assurance training.

At Course Completion:

In this course, you will develop, operate, manage, and enforce security capabilities for systems and networks.

You will:

- Assess information security risk in computing and network environments
- Create an information assurance lifecycle process
- Analyze threats to computing and network environments
- Design secure computing and network environments
- Operate secure computing and network environments
- Assess the security posture within a risk management framework
- Collect cybersecurity intelligence information
- Respond to cybersecurity incidents
- Investigate cybersecurity incidents
- Audit secure computing and network environments

Prerequisites:

Students taking this course should have the following skills:

- At least 2 years of experience in computer network security technology or a related field is recommended.

Course Outlines

Lesson 1: Assessing Information Security Risk

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

Lesson 2: Creating an Information Assurance Lifecycle Process

- Evaluate Information Assurance Lifecycle Models
- Align Information Security Operations to the Information Assurance Lifecycle
- Align Information Assurance and Compliance Regulations

Lesson 3: Analyzing Threats to Computing and Network Environments

- Identify Threat Analysis Models
- Assess the Impact of Reconnaissance Incidents
- Assess the Impact of Systems Hacking Attacks
- Assess the Impact of Malware
- Assess the Impact of Hijacking and Impersonation Attacks
- Assess the Impact of Denial of Service Incidents
- Assess the Impact of Threats to Mobile Infrastructure
- Assess the Impact of Threats to Cloud Infrastructures

Lesson 4: Designing Secure Computing and Network Environments

- Information Security Architecture Design Principles
- Design Access Control Mechanisms
- Design Cryptographic Security Controls
- Design Application Security
- Design Computing Systems Security
- Design Network Security

Lesson 5: Operating Secure Computing and Network Environments

- Implement Change Management in Security Operations
- Implement Monitoring in Security Operations
- Test and Evaluate Information Assurance Architectures

Lesson 6: Assessing the Security Posture Within a Risk Management Framework

- Deploy a Vulnerability Assessment and Management Platform
- Conduct Vulnerability Assessments
- Conduct Penetration Tests on Network Assets
- Analyze and Report Penetration Test Results

Lesson 7: Collecting Cybersecurity Intelligence Information

- Deploy a Security Intelligence Collection and Analysis Platform
- Sources

Lesson 8: Analyzing Cybersecurity Intelligence Information

- Analyze Security Intelligence to Address Incidents
- Incorporate Security Intelligence and Event Management

Lesson 9: Responding to Cybersecurity Incidents

- Deploy an Incident Handling and Response Architecture
- Perform Real-Time Incident Handling Tasks
- Prepare for Forensic Investigation

Lesson 10: Investigating Cybersecurity Incidents

- Create a Forensics Investigation Plan
- Securely Collect Electronic Evidence
- Identify the Who, Why, and How of an Incident
- Follow Up on the Results of an Investigation

Lesson 11: Computing and Network Environments

- Deploy a Systems and Processes Auditing Architecture
- Maintain a Deployable Audit Toolkit
- Perform Audits Geared Toward the Information Assurance Lifecycle