

CyberSec First Responder: Threat Detection and Response (CFR)

Download Whitepaper: Accelerate Your Modernization Efforts with a Cloud-Native Strategy
[Get Your Free Copy Now](#)

Course Number: 2180V

Duration: 5 days

Overview

Course Description

This course covers network defense and incident response methods, tactics, and procedures that are in alignment with industry frameworks such as NIST 800-61r2 (Computer Security Incident Handling Guide), US-CERT's National Cyber Incident Response Plan (NCIRP), and Presidential Policy Directive (PPD)-41 on Cyber Incident Coordination, NIST 800.171r2 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations). It is ideal for candidates who have been tasked with the responsibility of monitoring and detecting security incidents in information systems and networks, and for executing standardized responses to such incidents. The course introduces tools, tactics, and procedures to manage cybersecurity risks, defend cybersecurity assets, identify various types of common threats, evaluate the organization's security, collect and analyze cybersecurity intelligence, and remediate and report incidents as they occur. This course provides a comprehensive methodology for individuals responsible for defending the cybersecurity of their organization.

This course is designed to assist students in preparing for the CertNexus CyberSec First Responder (Exam CFR-410) certification examination. What you learn and practice in this course can be a significant part of your preparation.

In addition, this course and subsequent certification (CFR-410) meet all requirements for personnel requiring DoD directive 8570.01-M position certification baselines:

- CSSP Analyst
- CSSP Infrastructure Support
- CSSP Incident Responder
- CSSP Auditor

This course includes an exam voucher.

Skills Gained

In this course, you will identify, assess, respond to, and protect against security threats and operate a system and network security analysis platform.

You will:

- Assess cybersecurity risks to the organization.
- Analyze the threat landscape.
- Analyze various reconnaissance threats to computing and network environments.
- Analyze various attacks on computing and network environments.
- Analyze various post-attack techniques.
- Assess the organization's security posture through auditing, vulnerability management, and penetration testing.
- Collect cybersecurity intelligence from various network-based and host-based sources.
- Analyze log data to reveal evidence of threats and incidents.
- Perform active asset and network analysis to detect incidents.
- Respond to cybersecurity incidents using containment, mitigation, and recovery tactics.
- Investigate cybersecurity incidents using forensic analysis techniques.

Who Can Benefit

This course is designed primarily for cybersecurity practitioners preparing for or who currently perform job functions related to protecting information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. It is ideal for those roles within federal contracting companies and private sector firms whose mission or strategic objectives require the execution of Defensive Cyber Operations (DCO) or DoD Information Network (DoDIN) operation and incident handling. This course focuses on the knowledge, ability, and skills necessary to provide for the defense of those information

systems in a cybersecurity context, including protection, detection, analysis, investigation, and response processes.

In addition, the course ensures that all members of an IT team?regardless of size, rank, or budget? understand their role in the cyber defense, incident response, and incident handling process.

Prerequisites

To ensure your success in this course, you should meet the following requirements:

- At least two years (recommended) of experience or education in computer network security technology or a related field.
- The ability or curiosity to recognize information security vulnerabilities and threats in the context of risk management.
- Foundational knowledge of the concepts and operational framework of common assurance safeguards in network environments. Safeguards include, but are not limited to, firewalls, intrusion prevention systems, and VPNs.
- General knowledge of the concepts and operational framework of common assurance safeguards in computing environments. Safeguards include, but are not limited to, basic authentication and authorization, resource permissions, and anti-malware mechanisms.
- Foundation-level skills with some of the common operating systems for computing environments.
- Entry-level understanding of some of the common concepts for network environments, such as routing and switching.
- General or practical knowledge of major TCP/IP networking protocols, including, but not limited to, TCP, IP, UDP, DNS, HTTP, ARP, ICMP, and DHCP.

Audience

Course Details

Lab 1: Implementing a Threat Assessment Model

Lab 2: Examining Reconnaissance Incidents

Lab 3: Assessing the Impact of System Hijacking Attempts

Lab 4: Assessing the Impact of Malware

Lab 5: Assessing the Impact of Hijacking and Impersonation attacks

Lab 6: Assessing the Impact of DoS Incidents

Lab 7: Assessing the Impact of Threats to Mobile Devices

Lab 8: Designing Cryptographic Security Controls

Lab 9: Designing Application Security

Lab 10: Implementing Monitoring in Security Operations

Lab 11: Deploying a Vulnerability Management Platform

Lab 12: Conducting Vulnerability Assessments

Lab 13: Conducting Penetration Testing on Network Assets

Lab 14: Collecting and Analyzing Security Intelligence

Lab 15: Collecting Security Intelligence Data

Lab 16: Capturing and Analyzing Baseline Data

Lab 17: Analyzing Security Intelligence

Lab 18: Incorporating SIEMS into Security Intelligence Analysis

Lab 19: Developing an Incidence Response System

Lab 20: Securely Collecting Electronic Evidence

Lab 21: Analyzing Forensic Evidence

Lab 22: Preparing for an Audit

Lab 23: Performing Audits

2015-05-22 14:28:05.883000000

Lab 13: Conducting Penetration Testing on Network Assets

Lab 14: Collecting and Analyzing Security Intelligence

Lab 15: Collecting Security Intelligence Data

Lab 16: Capturing and Analyzing Baseline Data

Lab 17: Analyzing Security Intelligence

Lab 18: Incorporating SIEMS into Security Intelligence Analysis

Lab 19: Developing an Incidence Response System

Lab 20: Securely Collecting Electronic Evidence

Lab 21: Analyzing Forensic Evidence

Lab 22: Preparing for an Audit

Lab 23: Performing Audits