5 Days

CyberSec First Responder® (CFR)

Upcoming Sessions

22-26 Jul 2024	Dubai - UAE	$5,950
16-20 Dec 2024	Dubai - UAE	$5,950
21-25 Apr 2025	Dubai - UAE	$5,950

Training Details

Training Course Overview

This Anderson training 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 training 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 training course provides a comprehensive methodology for individuals responsible for defending the cybersecurity of their organization.

This training 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 training course can be a significant part of your preparation.

To ensure your success in this course, specific prerequisites are mandatory to take. The program prerequisites can be accessed and viewed by visiting the following hyperlinked file: CFR Prerequisites***, and*** CertNexus Exam Blueprints***.***

Training Course Objectives

In this training 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.

Designed For

This Anderson training 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 training 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 training 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.

This training 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*

Training Details

Day One:

Assessing Cybersecurity Risk

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

Analyzing the Threat Landscape

- Classify Threats
- Analyze Trends Affecting Security Posture

Day Two:

Analyzing Reconnaissance Threats to Computing and Network Environments

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

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

Day Three:

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

Assessing the Organization's Security Posture

- Implement Cybersecurity Auditing
- Implement a Vulnerability Management Plan
- Assess Vulnerabilities
- Conduct Penetration Testing

Day Four:

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

Analyzing Log Data

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

Performing Active Asset and Network Analysis

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

Day Five:

Responding to Cybersecurity Incidents

- Deploy an Incident Handling and Response Architecture
- Mitigate Incidents
- Hand Over Incident Information to a Forensic Investigation

Investigating Cybersecurity Incidents

- Apply a Forensic Investigation Plan
- Securely Collect and Analyze Electronic Evidence
- Follow Up on the Results of an Investigation

Preview

- Anderson Certificate of Completion will be provided to delegates who attend and complete the course
- CertNexus Certificate will be issued to those delegates who successfully pass Exam CFR-410

Accreditation

INFO & IN-HOUSE SOLUTION

For more information about this course, call or email us at:

Call us: +971 4 365 8363

Email: info@anderson.ae

Request for a Tailor-made training and educational experience for your organization now:

Email: inhouse@anderson.ae

Anderson
Executive Development Centre

P.O Box 74589, Dubai, United Arab Emirates
Web: www.anderson.ae
Email: info@anderson.ae
Phone: +971 4 365 8363
Fax: +971 4 360 4759