

## CyberSec First Responder - CFR-310

---

### Course Summary

#### 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. 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, 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-310) 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-310) meet all requirements for personnel requiring DoD directive 8570.01-M position certification baselines:

- CSSP Analyst
- CSSP Infrastructure Support
- CSSP Incident Responder

#### Topics

In this course, you will understand, assess, and respond to security threats and operate a system and network security analysis platform. You will:

- Compare and contrast various threats and classify threat profiles.
- Explain the purpose and use of attack methods and techniques.
- Explain the purpose and use of post-exploitation tools and tactics.
- Given a scenario, perform ongoing threat landscape research and use data to prepare for incidents.
- Explain the purpose and characteristics of various data sources.
- Given a scenario, use real-time data analysis to detect anomalies.
- Given a scenario, analyze common indicators of potential compromise.
- Given a scenario, use appropriate tools to analyze logs.
- Given a scenario, use appropriate containment methods or tools.
- Given a scenario, use appropriate asset discovery methods or tools.
- Given a scenario, use Windows tools to analyze incidents.
- Given a scenario, use Linux-based tools to analyze incidents.
- Given a scenario, execute the incident response process.
- Explain the importance of best practices in preparation for incident response.
- Identify applicable compliance, standards, frameworks, and best practices.
- Explain the importance of concepts that are unique to forensic analysis.
- Identify the common areas of vulnerability.
- Identify the steps of the vulnerability process.

#### Audience

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.

### Duration

5 Days