Document Generated: 04/02/2026

Learning Style: Virtual Classroom

Technology:

Difficulty: Intermediate

Course Duration: 5 Days

CyberSec First Responder (Exam CFR-310)

About This Course:

The CyberSec First Responder (CFR) course from CertNexus equips practitioners with the skills to assess risk, monitor for intrusions, analyze threats, and respond to incidents in real time. Built around leading frameworks like NIST 800-61r2 and PPD-41, this 5-day course prepares learners to protect information systems and

carry out Defensive Cyber Operations (DCO) effectively.

This course also prepares candidates for the CFR-410 certification exam, validating their ability to detect, contain, analyze, and recover from cybersecurity incidents across modern network environments.

Course Objectives:

- Assess cybersecurity risks and analyze threat landscapes
- Identify and respond to reconnaissance, malware, and network-based attacks
- Conduct vulnerability assessments and penetration testing
- Collect and analyze log data using SIEM and forensic tools
- Execute structured incident response and recovery procedures

Audience:

- Cybersecurity analysts and first responders
- Security Operations Center (SOC) personnel
- IT professionals responsible for security and incident response

Prerequisites:

- 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.

Course Outline:

1 – Assessing Cybersecurity Risk

- Identify the importance of risk management
- Assess and mitigate risk
- Integrate documentation into risk processes

2 – Analyzing the Threat Landscape

- Classify threats and threat profiles
- Analyze trends affecting security posture

3 – Analyzing Reconnaissance Threats to Computing and Network Environments

- Implement threat modeling
- Assess the impact of reconnaissance and social engineering

4 – Analyzing System Hacking Attacks

- Assess the impact of system, web-based, and malware attacks
- Evaluate threats like hijacking, impersonation, DoS, mobile and cloud vulnerabilities

5 – Analyzing Post-Attack Techniques

- Assess techniques including command & control, lateral movement, exfiltration, and anti-forensics

6 – Assessing the Organization's Security Posture

- Perform cybersecurity audits
- Conduct vulnerability assessments and penetration testing

7 – Collecting Cybersecurity Intelligence

- Set up intelligence platforms
- Collect data from host-based and network-based sources

8 – Analyzing Log Data

- Use SIEM tools and log analysis for threat detection

9 – Performing Active Asset and Network Analysis

- Investigate incidents using Windows and Linux tools
- Analyze indicators of compromise

10 – Responding to Cybersecurity Incidents

- Deploy incident handling architecture
- Mitigate incidents and support forensic handoff

11 – Investigating Cybersecurity Incidents

- Apply forensic investigation methods
- Collect, analyze, and follow up on digital evidence