Logical Operations™

# CYBERSEC FIRST RESPONDER: THREAT DETECTION & RESPONSE

CYBERSEC FIRST RESPONDER

## CORPORATE BENEFIT

CFR takes a holistic approach to preparing employees to analyze threats, secure networks, handle incidents, and utilize other critical security skills to protect your organization with a single course.

## STUDENT PROFILE

Designed for information assurance professionals whose job functions include development, operations, management, and enforcement of secure systems and networks.

## COURSE OBJECTIVES

This course focuses on developing a systematic process for securing an organization's network by implementing an incidence handling and response plan through threat detection and analysis.

## LABS

At Logical Operations we feel there is no substitute for practice. Hands-on practical activities, written in Open Source Software, can be recreated or rented to provide this experience.

www.logicaloperations.com/cfr

# CYBERSEC FIRST RESPONDER

## LESSON OBJECTIVES

1. Assessing Information Security Risk
2. Creating an Information Assurance Lifecycle Process
3. Analyzing Threats to Computing and Network Environments
4. Designing Secure Computing and Network Environments
5. Operating Secure Computing and Network Environments
6. Assessing the Security Posture Within a Risk Management Framework
7. Collecting Cybersecurity Intelligence Information
8. Analyzing Cybersecurity Intelligence Information
9. Responding to Cybersecurity Incidents
10. Investigating Cybersecurity Incidents
11. Auditing Secure Computing and Network Environments

## WHO SHOULD ATTEND?

This course 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.

## PREREQUISITES

- Recommended at least 2 years of experience in computer network security technology or a related field.
- Recognize information security vulnerabilities and threats in the context of risk management.
- Operate at a foundational level some of the common operating systems for computing environments.
- Foundational 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.
- Operate at a foundational level some of common concepts for network environments, such as routing and switching.
- 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 (virtual private networks).

## DAYS OF TRAINING

5 days/approximately 35 contact hours/
1 semester/5 days boot camp

## CERTIFICATION / EXAM

Certified CyberSec First Responder/
3 - 4 hours (150+ questions)