# CyberSec First Responder: Threat Detection and Response

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.

**Length Days: 5** | **Length Hours: 40**

## PREREQUISITES

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

• 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).

You can obtain this level of skills and knowledge by taking the following courses or by passing the relevant exams:
CompTIA A+
CompTIA Network+
CompTIA Security+

## TARGET AUDIENCE

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.

## COURSE OBJECTIVES

In this course, you will develop, operate, manage, and enforce security capabilities for systems and networks. You will:

- Assess information security risk in computing and network environments
- Create an information assurance lifecycle process
- Analyze threats to computing and network environments
- Design secure computing and network environments
- Operate secure computing and network environments
- Assess the security posture within a risk management framework
- Collect cybersecurity intelligence information
- Respond to cybersecurity incidents
- Investigate cybersecurity incidents
- Audit secure computing and network environments

## COURSE OUTLINE

### 1 - ASSESSING INFORMATION SECURITY RISK

Topic A: Identify the Importance of Risk Management
Topic B: Assess Risk
Topic C: Mitigate Risk
Topic D: Integrate Documentation into Risk Management

### 2 - CREATING AN INFORMATION ASSURANCE LIFECYCLE PROCESS

Topic A: Evaluate Information Assurance Lifecycle Models
Topic B: Align Information Security Operations to the Information Assurance Lifecycle
Topic C: Align Information Assurance and Compliance Regulations

### 3 - ANALYZING THREATS TO COMPUTING AND NETWORK ENVIRONMENTS

Topic A: Identify Threat Analysis Models
Topic B: Assess the Impact of Reconnaissance Incidents
Topic C: Assess the Impact of Systems Hacking Attacks
Topic D: Assess the Impact of Malware
Topic E: Assess the Impact of Hijacking and Impersonation Attacks
Topic F: Assess the Impact of Denial of Service Incidents
Topic G: Assess the Impact of Threats to Mobile Infrastructure
Topic H: Assess the Impact of Threats to Cloud Infrastructures

## 4 - DESIGNING SECURE COMPUTING AND NETWORK ENVIRONMENTS

Topic A: Information Security Architecture Design Principles
Topic B: Design Access Control Mechanisms
Topic C: Design Cryptographic Security Controls
Topic D: Design Application Security
Topic E: Design Computing Systems Security
Topic F: Design Network Security

## 5 - OPERATING SECURE COMPUTING AND NETWORK ENVIRONMENTS

Topic A: Implement Change Management in Security Operations
Topic B: Implement Monitoring in Security Operations
Topic C: Test and Evaluate Information Assurance Architectures

## 6 - ASSESSING THE SECURITY POSTURE WITHIN A RISK MANAGEMENT FRAMEWORK

Topic A: Deploy a Vulnerability Assessment and Management Platform
Topic B: Conduct Vulnerability Assessments
Topic C: Conduct Penetration Tests on Network Assets
Topic D: Analyze and Report Penetration Test Results

## 7 - COLLECTING CYBERSECURITY INTELLIGENCE INFORMATION

Topic A: Deploy a Security Intelligence Collection and Analysis Platform
Topic B: Sources

## 8 - ANALYZING CYBERSECURITY INTELLIGENCE INFORMATION

Topic A: Analyze Security Intelligence to Address Incidents
Topic B: Incorporate Security Intelligence and Event Management

## 9 - RESPONDING TO CYBERSECURITY INCIDENTS

Topic A: Deploy an Incident Handling and Response Architecture
Topic B: Perform Real-Time Incident Handling Tasks
Topic C: Prepare for Forensic Investigation

## 10 - INVESTIGATING CYBERSECURITY INCIDENTS

Topic A: Create a Forensics Investigation Plan
Topic B: Securely Collect Electronic Evidence
Topic C: Identify the Who, Why, and How of an Incident
Topic D: Follow Up on the Results of an Investigation

## 11 - COMPUTING AND NETWORK ENVIRONMENTS

Topic A: Deploy a Systems and Processes Auditing Architecture
Topic B: Maintain a Deployable Audit Toolkit
Topic C: Perform Audits Geared Toward the Information Assurance Lifecycle