CyberSec First Responder: Threat Detection and Response Training

Duration: **5 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

Overview

Gain a broad view of how to respond to a cybersecurity incident while preparing for the CyberSec First Responder certification.

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, 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 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 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-410) 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-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

This course includes an exam voucher.

Is This The Right Course?

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

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

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.

Who Should Attend?

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.

CyberSec First Responder: Threat Detection and Response Training

Duration: **5 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

In this 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.

Outline

Lesson 1: Assessing Cybersecurity Risk

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

Lesson 2: Analyzing the Threat Landscape

- Topic A: Classify Threats
- Topic B: Analyze Trends Affecting Security Posture

Lesson 3: Analyzing Reconnaissance Threats to Computing and Network Environments

- Topic A: Implement Threat Modeling
- Topic B: Assess the Impact of Reconnaissance
- Topic C: Assess the Impact of Social Engineering

Lesson 4: Analyzing Attacks on Computing and Network Environments

- Topic A: Assess the Impact of System Hacking Attacks
- Topic B: Assess the Impact of Web-Based Attacks
- Topic C: Assess the Impact of Malware
- Topic D: Assess the Impact of Hijacking and Impersonation Attacks
- Topic E: Assess the Impact of DoS Incidents Topic F: Assess the Impact of Threats to Mobile Security
- Topic G: Assess the Impact of Threats to Cloud Security

Lesson 5: Analyzing Post-Attack Techniques

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Topic A: Assess Command and Control Techniques
- Topic B: Assess Persistence Techniques
- Topic C: Assess Lateral Movement and Pivoting Techniques
- Topic D: Assess Data Exfiltration Techniques
- Topic E: Assess Anti-Forensics Techniques

Lesson 6: Assessing the Organization's Security Posture

- Topic A: Implement Cybersecurity Auditing
- Topic B: Implement a Vulnerability Management Plan
- Topic C: Assess Vulnerabilities
- Topic D: Conduct Penetration Testing

Lesson 7: Collecting Cybersecurity Intelligence

- Topic A: Deploy a Security Intelligence Collection and Analysis Platform
- Topic B: Collect Data from Network-Based Intelligence Sources
- Topic C: Collect Data from Host-Based Intelligence Sources

Lesson 8: Analyzing Log Data

- Topic A: Use Common Tools to Analyze Logs
- Topic B: Use SIEM Tools for Analysis

Lesson 9: Performing Active Asset and Network Analysis

- Topic A: Analyze Incidents with Windows-Based Tools
- Topic B: Analyze Incidents with Linux-Based Tools
- Topic C: Analyze Indicators of Compromise

Lesson 10: Responding to Cybersecurity Incidents

- Topic A: Deploy an Incident Handling and Response Architecture
- Topic B: Mitigate Incidents
- Topic C: Hand Over Incident Information to a Forensic Investigation

Lesson 11: Investigating Cybersecurity Incidents

- Topic A: Apply a Forensic Investigation Plan
- Topic B: Securely Collect and Analyze Electronic Evidence
- Topic C: Follow Up on the Results of an Investigation

Appendix A: Mapping Course Content to CyberSec First Responder® (Exam CFR-410)
Appendix B: Regular Expressions