COURSE OUTLINE

CN-CFR

CYBERSEC FIRST RESPONDER

DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
5 Days	Advanced	Cyber Security	Classroom or Virtual	NA

INTRODUCTION

This course covers network defense and incident response methods, tactics, and procedures are taught in alignment with industry frameworks such as NIST 800-61 r.2 (Computer Security Incident Handling), US-CERT's NCISP (National Cyber Incident Response Plan), and US Presidential Policy Directive (PPD) 41 on Cyber Incident Coordination Policy. 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.

In addition, this course and subsequent certification (CFR-410) meets all requirements for personnel requiring DoD directive 8570.01-M position certification baselines: CSSP Analyst, CSSP Infrastructure Support, CSSP Incident Responder, CSSP Auditor.

AUDIENCE PROFILE

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 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

COURSE OBJECTIVES

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 profile
- Explain the purpose and use of attack tools and technique
- Explain the purpose and use of post exploitation tools and tactic

- Explain the purpose and use of social engineering tactic
- Given a scenario, perform ongoing threat landscape research and use data to prepare for incident
- Explain the purpose and characteristics of various data source
- Given a scenario, use appropriate tools to analyze log
- Given a scenario, use regular expressions to parse log files and locate meaningful data
- Given a scenario, use Windows tools to analyze incidents
- Given a scenario, use Linux-based tools to analyze incidents
- Summarize methods and tools used for malware analysis
- Given a scenario, analyze common indicators of potential compromise
- Explain the importance of best practices in preparation for incident response
- Given a scenario, execute incident response process
- Explain the importance of concepts that are unique to forensic analysis
- Explain general mitigation methods and devices

COURSE TOPICS

Lesson 1: Assessment of Information Security Risks
- The Importance of Risk Management
- Assess Risk
- Mitigate Risk
- Integrating Documentation into Risk Management

Lesson 2: Analyzing the Threat Landscape
- Classify Threats and Threat Profiles
- Perform Ongoing Threat Research

Lesson 3: Computing and Network Environments: Analyzing Reconnaissance Threats
- Implementation of Threat Modeling
- Reconnaissance: Assessing the Impact
- Social Engineering: Assessing the Impact

Lesson 4: Analyzing Attacks on Computing and Network Environments
- System Hacking Attacks: Assessing the Impact
- Web-Based Attacks: Assessing the Impact
- Malware: Assessing the Impact
- Hijacking and Impersonation Attacks: Assessing the Impact
- DoS Incidents: Assessing the Impact
- Threats to Mobile Security: Assessing the Impact
- Threats to Cloud Security: Assessing the Impact

Lesson 5: Examining Post-Attack Techniques
- Examine Command and Control Techniques
- Examine Persistence Techniques
- Examine Lateral Movement and Pivoting Techniques
- Examine Data Exfiltration Techniques
- Examine Anti-Forensics Techniques

Lesson 6: Manage Vulnerabilities in the Organization
- Implement a Vulnerability Management Plan
- Examine Common Vulnerabilities
- Conduct Vulnerability Scans

Lesson 7: Evaluate Security by Implementing Penetration Testing
- Conduct Penetration Tests on Network Assets
- Follow Up on Penetration Testing

Lesson 8: Collecting Cybersecurity Intelligence
- Deployment of a Security Intelligence Collection and Analysis Platform
- Data Collection from Network-Based Intelligence Sources
- Data Collection from Host-Based Intelligence Sources

Lesson 9: Analyze Log Data
- Topic A: Common Tools to Analyze Logs
- SIEM Tools for Analysis

Lesson 10: Performing Active Asset and Network Analysis
- Analyze Incidents using Windows-Based Tools
- Analyze Incidents using Linux-Based Tools
- Analyze Malware Topic D: Analyze Indicators of Compromise

Lesson 11: Response to Cybersecurity Incidents
- Deployment of Incident Handling and Response Architecture
- Containment and Mitigation of Incidents
- Preparation for Forensic Investigation as a CSIRT

Lesson 12: Investigating Cybersecurity Incidents
- Use a Forensic Investigation Plan
- Securely Collect and Analyze Electronic Evidence
- Follow Up on the Results of an Investigation

ASSOCIATED CERTIFICATIONS & EXAM

The CyberSec First Responder exam (#CFR-410) will certify that the candidate can identify, assess, respond to, and protect against security threats and operate a system and network security analysis platform.

The CFR exam is accredited under the ANSI/ISO/IEC 17024 standard and is approved by the U.S. Department of Defense (DoD) to fulfill Directive 8570/8140 requirements.

Upon completion of this course, delegates will receive a MIE attendance certificate.