CyberSec First Responder™ (CFR) Certification

Duration: 5 Days **Course Code: CFR**

Overview:

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 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.
This course is designed to assist students in preparing for the CertNexus CyberSec First Responder (Exam CFR-310) 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-310) meets all requirements for personnel requiring DoD directive 8570.01-M position certification baselines:
• CSSP Analyst
• CSSP Infrastructure Support
• CSSP Incident Responder
• CSSP Auditor

Target Audience:

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 who 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.

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

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

Content:

Lesson 1: Assessment of Information Security Risks

Topic A: The Importance of Risk Management

Topic B: Assess Risk

Topic C: Mitigate Risk

Topic D: Integrating Documentation into Risk Management

Lesson 2: Analyzing the Threat Landscape

Topic A: Classify Threats and Threat Profiles

Topic B: Perform Ongoing Threat Research

Lesson 3: Computing and Network Environments: Analyzing Reconnaissance Threats

Topic A: Implementation of Threat Modeling

Topic B: Reconnaissance: Assessing the Impact

Topic C: Social Engineering: Assessing the Impact

Lesson 4: Analyzing Attacks on Computing and Network Environments

Topic A: System Hacking Attacks: Assessing the Impact

Topic B: Web-Based Attacks: Assessing the Impact

Topic C: Malware: Assessing the Impact

Topic D: Hijacking and Impersonation Attacks: Assessing the Impact

Topic E: DoS Incidents: Assessing the Impact

Topic G: Threats to Cloud Security: Assessing the Impact

Lesson 5: Examining Post-Attack Techniques

Topic A: Examine Command and Control Techniques

Topic B: Examine Persistence Techniques

Topic C: Examine Lateral Movement and Pivoting Techniques

Topic D: Examine Data Exfiltration Techniques

Topic E: Examine Anti-Forensics Techniques

Lesson 6: Manage Vulnerabilities in the Organization

Topic A: Implement a Vulnerability Management Plan

Topic B: Examine Common Vulnerabilities

Topic C: Conduct Vulnerability Scans

Lesson 7: Evaluate Security by Implementing Penetration Testing

TopicA: Conduct Penetration Tests on Network Assets

Topic B: Follow Up on Penetration Testing

Lesson 8: Collecting Cybersecurity Intelligence

Topic A: Deployment of a Security Intelligence Collection and Analysis Platform

Topic B: Data Collection from Network-Based Intelligence Sources

Topic C: Data Collection from Host-Based Intelligence Sources

Topic A: Common Tools to Analyze Logs

Topic B: SIEM Tools for Analysis

Lesson 10: Performing Active Asset and Network Analysis

Topic A: Analyze Incidents using Windows-Based Tools

Topic B: Analyze Incidents using Linux-Based Tools

Topic C: Analyze Malware

Topic D: Analyze Indicators of Compromise

Lesson 11: Response to Cybersecurity Incidents

Topic A: Deployment of Incident Handling and Response Architecture

Topic B: Containment and Mitigation of Incidents

Topic C: Preparation for Forensic Investigation as a CSIRT

Lesson 12: Investigating Cybersecurity Incidents

Topic A: Use 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-310)

Appendix B: Regular Expressions

Appendix C: Security Resources

Further Information:

For More information, or to book your course, please call us on 00 20 (0) 2 2269 1982 or 16142

training@globalknowledge.com.eg

www.globalknowledge.com/en-eg/

Global Knowledge, 16 Moustafa Refaat St. Block 1137, Sheraton Buildings, Heliopolis, Cairo