CFR - CyberSec First Responder 310

5 days | Exam CFR-310

Overview

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. 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) meet all requirements for personnel requiring DoD directive 8570.01-M position certification baselines:

- CSSP Analyst
- CSSP Infrastructure Support
- CSSP Incident Responder
- CSSP Auditor

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 profiles.
- Explain the purpose and use of attack methods and techniques.
- Explain the purpose and use of post-exploitation tools and tactics.

- Given a scenario, perform ongoing threat landscape research and use data to prepare for incidents.
- Explain the purpose and characteristics of various data sources.
- Given a scenario, use real-time data analysis to detect anomalies.
- Given a scenario, analyze common indicators of potential compromise.
- Given a scenario, use appropriate tools to analyze logs.
- Given a scenario, use appropriate containment methods or tools.
- Given a scenario, use appropriate asset discovery methods or tools.
- Given a scenario, use Windows tools to analyze incidents.
- Given a scenario, use Linux-based tools to analyze incidents.
- Given a scenario, execute the incident response process.
- Explain the importance of best practices in preparation for incident response.
- Identify applicable compliance, standards, frameworks, and best practices.
- Explain the importance of concepts that are unique to forensic analysis.
- Identify the common areas of vulnerability.
- Identify the steps of the vulnerability process.

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 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-specific Technical Requirements

Hardware

For this course, you will need one Microsoft® Windows Server® 2016 computer and one Microsoft® Windows® 10 computer for each student and for the instructor. Make sure that each computer meets the classroom hardware specifications:

Windows Server 2016

• 2 gigahertz (GHz) 64-bit processor.
• 4 gigabytes (GB) of Random Access Memory (RAM).

Windows 10

• 2 GHz 64-bit processor that supports the VT-x or AMD-V virtualization instruction set and Second Level Address Translation (SLAT).
• 8 GB of RAM. This client will host a Linux® virtual machine.

Both Computers

• 80 GB storage device or larger.
• Super VGA (SVGA) or higher resolution monitor capable of a screen resolution of at least 1,024 × 768 pixels, at least a 256-color display, and a video adapter with at least 4 MB of memory.
• Bootable DVD-ROM or USB drive.
• Keyboard and mouse or a compatible pointing device.
• Gigabit Ethernet adapter (10/100/1000BaseT) and cabling to connect to the classroom network.
• IP addresses that do not conflict with other portions of your network.
• Internet access (contact your local network administrator).
• (Instructor computer only) A display system to project the instructor's computer screen.
• (Optional) A network printer for the class to share.

Software

• Microsoft Windows Server 2016 Standard Edition with sufficient licenses.
• Microsoft Windows 10 Professional 64-bit with sufficient licenses.
• Windows Server 2016 and Windows 10 require activation unless you have volume-licensing agreements. There is a grace period for activation. If the duration of your class will exceed the activation grace period (for example, if you are teaching the class over the course of an academic semester), you should activate the installations at some point before the grace period expires. Otherwise, the operating systems may stop working before the class ends.
• Microsoft® Office 2016 or an open source alternative such as LibreOffice or Apache OpenOffice™.

• Java Runtime Environment (JRE) version 8 or higher.
• If preferred, a third-party browser such as Google Chrome™ or Mozilla® Firefox®.
• If preferred, a third-party PDF reader such as Adobe® Acrobat® Reader.
• Kali Linux version 2018.2. The steps to download the Kali Linux system image are described in the course setup that follows. Note that the URL path to this download may have changed after this course was written.

• Miscellaneous software that is notincluded in the course data files due to licensing restrictions:

- Process Explorer version 16.21 (procexp.exe).
- Splunk® Enterprise version 7.0.2 (splunk-7.0.2-03bbabbd5c0f-x64-release.msi).
- Log Parser version 2.2 (LogParser.msi).
- Log Parser Studio version 2.0 (LPSDV2.D2.zip).

The steps to download these tools are described in the course setup that follows. Note that the URL paths to these downloads may have changed after this course was written. The activities in this course were written to the versions of the software noted previously. If new versions of these tools have been released when you present this course, make sure to test them with their corresponding activities to note any keying discrepancies.

• Miscellaneous software that isincluded in the course data files:
- Oracle® VM VirtualBox version 5.1.30 (VirtualBox-5.1.30-118389-Win.exe).
- Wireshark version 2.0.1 (Wireshark-win64-2.0.1.exe).
- Snort® version 2.9.8.0 (Snort_2_9_8_0_Installer.exe).
- icmpsh (icmpsh.zip).
- XAMPP version 5.6.15 (xampp-win32-5.6.15-1-VC11-installer.exe).
- SeaMonster version 5 (SeaMonster5_win32.x86.zip).
- OpenSSH for Windows version 7.1 (setupssh-7.1p2-1.exe).
- PuTTY version 0.67 (putty.exe).
- VirtualBox, Wireshark, Snort, and icmpsh are distributed with the course data files under version 2 of the GNU General Public License (GPL). XAMPP is distributed under

version 3 of the GNU GPL. SeaMonster is distributed under version 3 of the GNU Lesser General Public License (LGPL). OpenSSH for Windows is distributed with the course data files under a Berkeley Software Distribution (BSD) license. PuTTY is distributed with the course data files under the MIT License.

- If necessary, software for viewing the course slides (instructor machine only).

Course Content

Lesson 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

Lesson 2: Analyzing the Threat Landscape

- Topic A: Classify Threats and Threat Profiles
- Topic B: Perform Ongoing Threat Research

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

- 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: Managing Vulnerabilities in the Organization

- Topic A: Implement a Vulnerability Management Plan
- Topic B: Assess Common Vulnerabilities
- Topic C: Conduct Vulnerability Scans

Lesson 7: Implementing Penetration Testing to Evaluate Security

- Topic A: Conduct Penetration Tests on Network Assets
- Topic B: Follow Up on Penetration Testing

Lesson 8: 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 9: Analyzing Log Data

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

Lesson 10: 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 Malware
- Topic D: Analyze Indicators of Compromise

Lesson 11: Responding to Cybersecurity Incidents

- Topic A: Deploy an Incident Handling and Response Architecture
- Topic B: Contain and Mitigate Incidents
- Topic C: Prepare for Forensic Investigation as a CSIRT

Lesson 12: 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-310)

Appendix B: Regular Expressions

Appendix C: Security Resources

Appendix D: U.S. Department of Defense Operational Security Practices