# CyberSec First Responder® (CFR-410)

Duration 5 days

## COURSE DESCRIPTION

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

## COURSE OBJECTIVES

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.

## COURSE OUTLINE

**Lesson 1: Assessing Cybersecurity Risk**
- Identify the Importance of Risk Management
- Assess Risk
- Mitigate Risk
- Integrate Documentation into Risk Management

**Lesson 2: Analyzing the Threat Landscape**
- Classify Threats
- Analyze Trends Affecting Security Posture

**Lesson 3: Analyzing Reconnaissance Threats to Computing and Network Environments**
- Implement Threat Modeling
- Assess the Impact of Reconnaissance
- Assess the Impact of Social Engineering

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

**Lesson 5: Analyzing Post-Attack Techniques**
- Assess Command and Control Techniques
- Assess Persistence Techniques
- Assess Lateral Movement and Pivoting Techniques
- Assess Data Exfiltration Techniques
- Assess Anti-Forensics Techniques

**Lesson 6: Assessing the Organization's Security Posture**
- Implement Cybersecurity Auditing
- Implement a Vulnerability Management Plan
- Assess Vulnerabilities
- Conduct Penetration Testing

**Lesson 7: Collecting Cybersecurity Intelligence**
- Deploy a Security Intelligence Collection and Analysis Platform
- Collect Data from Network-Based Intelligence Sources
- Collect Data from Host-Based Intelligence Sources

**Lesson 8: Analyzing Log Data**
- Use Common Tools to Analyze Logs
- Use SIEM Tools for Analysis

**Lesson 9: Performing Active Asset and Network Analysis**
- Analyze Incidents with Windows-Based Tools
- Analyze Incidents with Linux-Based Tools
- Analyze Indicators of Compromise

**Lesson 10: Responding to Cybersecurity Incidents**
- Deploy an Incident Handling and Response Architecture
- Mitigate Incidents
- Hand Over Incident Information to a Forensic Investigation

**Lesson 11: Investigating Cybersecurity Incidents**
- Apply a Forensic Investigation Plan
- Securely Collect and Analyze Electronic Evidence
- Follow Up on the Results of an Investigation

## 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.

## 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.

## COURSE-SPECIFIC TECHNICAL REQUIREMENTS

### Hardware
For this course, you will need one Microsoft® Windows Server® 2019 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 2019**
2 gigahertz (GHz) 64-bit (x64) 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.

**NETWORK TRAINING CENTER CO.,LTD. (NTC)** | www.trainingcenter.co.th

**Call us today 0-2634-7993-4**

177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th

### Both Computers

80 GB storage device or larger.

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.

Fast Ethernet (100 Mb/s) adapter or faster 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 2019 Standard Edition with sufficient licenses.**

**Microsoft Windows 10 Professional 64-bit with sufficient licenses.**

Windows Server 2019 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.

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 2021.2.**

The Kali Linux operating system is already installed on a VM that will be loaded in VirtualBox.

**Miscellaneous software that is not included in the course data files due to licensing restrictions:**

Java Runtime Environment (JRE) version 8u291 (JavaSetup8u291.exe).

Npcap version 1.50 (npcap-1.50.exe).

Process Explorer version 16.42 (procexp.exe).

Splunk® Enterprise version 8.2.1 (splunk-8.2.1-ddff1c41e5cf-x64-release.msi).

Log Parser version 2.2 (LogParser.msi).

Log Parser Studio version 2.0 (LPSV2.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 is included in the course data files:**

Oracle® VM VirtualBox version 6.1.16 (VirtualBox-6.1.16-140961-Win.exe).

Wireshark version 3.4.6 (Wireshark-win64-3.4.6.exe).

Snort® version 2.9.18 (Snort_2_9_18_Installer.x64.exe).

icmpsh (icmpsh.zip).

XAMPP version 7.3.28 (xampp-windows-x64-7.3.28-1-VC15-installer.exe).

OpenSSH for Windows version 7.1 (setupssh-7.1p2-1.exe).

PuTTY version 0.76 (putty.exe).

LibreOffice Portable version 7.1.4 (LibreOfficePortable_7.1.4_MultilingualStandard.paf.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. 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. LibreOffice is distributed with the course data files under version 2 of the Mozilla Public License (MPL). If you prefer, you can install a version of Microsoft Office instead of using LibreOffice.

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