



## Prerequisites:

# CyberSec First Responder (CFR) Exam CFR-410

### CFR Exam Details

This exam 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 ISO/IEC 17024:2012 standard and is approved by the U.S. Department of Defense (DoD) to fulfill Directive 8570/8140 requirements.

### Target Audience

Individuals with between 3 and 5 years of experience working in a computing environment as part of a CERT/CSIRT/SOC who protect critical information systems before, during, and after an incident.

### Prerequisites

To ensure your success in this course, you should meet the following requirements:

- 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.



## Training course-specific Technical Requirements

Technical requirements below are for **local class setup only**. Requirements for the **use of labs** can be found [here](#). For full lab support reference [click here](#).

### Hardware

For this training 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.

#### **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 training 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 training 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 training course setup that follows. Note that the URL paths to these downloads may have changed after this training course was written. The activities in this training course were written to the versions of the software noted previously. If new versions of these tools have been released when you present this training course, make sure to test them with their corresponding activities to note any keying discrepancies.
- Miscellaneous software that is included in the training 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 training 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 training course data files under a Berkeley Software Distribution (BSD) license. PuTTY is distributed with the training course data files under the MIT License. LibreOffice is distributed with the training 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 training course slides (instructor machine only).