CYBERSEC FIRST RESPONDER™

CyberSec First Responder (CFR-310)

This document includes instructor led class overview and objectives, identifies target student and prerequisites, course outline, and course specific software and hardware requirements.

Course Length:

5 days

Overview:

This course covers the duties of those who are responsible for monitoring and detecting security incidents in information systems and networks, and for executing a proper response to such incidents. Depending on the size of the organization, this individual may act alone or may be a member of a cybersecurity incident response team (CSIRT). The course introduces tools and tactics to manage cybersecurity risks, identify various types of common threats, evaluate the organization's security, collect and analyze cybersecurity intelligence, and handle incidents as they occur. Ultimately, the course promotes a comprehensive approach to security aimed toward those on the front lines of defense.

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 can help students who are looking to fulfill DoD directive 8570.01 for information assurance (IA) training. This program is designed for personnel performing IA functions, establishing IA policies, and implementing security measures and procedures for the Department of Defense and affiliated information systems and networks.

Course Objectives:

In this course, you will assess and respond to security threats and operate a system and network security analysis platform.

You will:

- Assess information security risk in computing and network environments.
- Analyze the cybersecurity threat landscape.
- Analyze reconnaissance threats to computing and network environments.
- Analyze attacks on computing and network environments.
- Analyze post-attack techniques on computing and network environments.
- Implement a vulnerability management program.
- Evaluate the organization's security through penetration testing.
- Collect cybersecurity intelligence.
- Analyze data collected from security and event logs.
- Perform active analysis on assets and networks.
- Respond to cybersecurity incidents.
- Investigate cybersecurity incidents.

Target Student:

This course is designed primarily for cybersecurity practitioners who perform job functions related to protecting information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. 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—everyone from help desk staff to the Chief Information Officer—understand their role in these security processes.

Prerequisites:

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

- At least two years (recommended) of experience in computer network security technology or a related field.
- The ability to recognize information security vulnerabilities and threats in the context of risk management.
- Foundation-level operational skills with some of the common operating systems for computing environments.
- Foundational 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 understanding of some of the common concepts for network environments, such as routing and switching.
- Foundational knowledge of major TCP/IP networking protocols, including, but not limited to, TCP, IP, UDP, DNS, HTTP, ARP, ICMP, and DHCP
- 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.

Course Content

Lesson 1: Assessing Information Security Risk

Topic A: Identify the Importance of Risk Management
- Cybersecurity
- The Risk Equation
- Risk Management
- The Importance of Risk Management in Information Security
- ERM
- Reasons to Implement ERM
- Risk Exposure
- Risk Analysis Methods
- The Impact of Risks on the Enterprise
- Identifying the Importance of Risk Management

Topic B: Assess Risk
- ESA Frameworks
- ESA Framework Assessment Process

- The NIST Framework and Models
- The COBIT Frameworks
- The ITIL Model
- The ISO Model
- The SABSA Framework
- TOGAF
- Additional Frameworks and Standards
- Example Laws and Regulations
- New and Changing Business Strategies
- De-perimeterization
- User Behaviors
- New Products and Technologies
- New Threats
- Internal and External Influences
- System-Specific Risk Analysis
- Risk Determinations
- Documentation of Assessment Results
- Guidelines for Assessing Risk
- Assessing Risk

Topic C: Mitigate Risk

- Classes of Information
- Classification of Information Types into CIA Levels
- Security Control Categories
- Select Controls Based on CIA Requirements
- Aggregate CIA Score
- CVSS
- CVE
- Extreme Scenario Planning and Worst Case Scenarios
- Risk Response Techniques
- Additional Risk Management Strategies
- Continuous Monitoring and Improvement
- IT Governance
- Verification and Quality Control
- Defense in Depth
- Guidelines for Mitigating Risk
- Mitigating Risk

Topic D: Integrate Documentation into Risk Management

- From Policies to Procedures
- Policy Life Cycle
- Process and Procedure Life Cycle
- Topics to Include in Security Policies and Procedures
- Best Practices to Incorporate in Security Policies and Procedures
- Types of Policies
- Types of Procedures
- Business Documents That Support Security Initiatives
- Guidelines for Integrating Documentation into Risk Management

- Integrating Documentation into Risk Management

Lesson 2: Analyzing the Threat Landscape

Topic A: Classify Threats and Threat Profiles

- Threat Actors
- Threat Motives
- Threat Intentions
- Threat Targets
- Attack Vectors
- Attack Technique Criteria
- Qualitative Threat and Impact Analysis
- Guidelines for Classifying Threats and Threat Profiles
- Constructing Threat Profiles

Topic B: Perform Ongoing Threat Research

- Ongoing Research
- Situational Awareness
- Commonly Targeted Assets
- The Latest Vulnerabilities
- The Latest Threats and Exploits
- The Latest Security Technologies
- Resources Aiding in Research
- The Global Cybersecurity Industry and Community
- Trend Data
- Trend Data and Qualifying Threats
- Guidelines for Performing Ongoing Threat Research
- Performing Ongoing Threat Landscape Research

Lesson 3: Analyzing Reconnaissance Threats to Computing and Network Environments

Topic A: Implement Threat Modeling

- The Diverse Nature of Threats
- The Anatomy of a Cyber Attack
- Threat Modeling
- Reasons to Implement Threat Modeling
- Approaches to Threat Modeling
- Attack Trees
- Threat Modeling Tools
- Threat Categories
- Implementing a Threat Model

Topic B: Assess the Impact of Reconnaissance

- Footprinting, Scanning, and Enumeration
- Footprinting Methods
- Network and System Scanning Methods
- Enumeration Methods
- Variables Affecting Reconnaissance
- Evasion Techniques for Reconnaissance
- Reconnaissance Tools
- Packet Trace Analysis

- Performing Reconnaissance on a Network
- Examining Reconnaissance Incidents
- Capturing and Analyzing Data with Wireshark

Topic C: Assess the Impact of Social Engineering

- Social Engineering
- Types of Social Engineering
- Phishing and Delivery Media
- Phishing and Common Components
- Social Engineering for Reconnaissance
- Assessing the Impact of Social Engineering

Lesson 4: Analyzing Attacks on Computing and Network Environments

Topic A: Assess the Impact of System Hacking Attacks

- System Hacking
- Password Sniffing
- Password Cracking
- Privilege Escalation
- Social Engineering for Systems Hacking
- System Hacking Tools and Exploitation Frameworks
- Assessing the Impact of Systems Hacking Attacks

Topic B: Assess the Impact of Web-Based Attacks

- Client-Side vs. Server-Side Attacks
- XSS
- XSRF
- Command Injection
- Directory Traversal
- File Inclusion
- Additional Web Application Vulnerabilities and Exploits
- Web Services Exploits
- Web-Based Attack Tools
- Assessing the Impact of Web-Based Threats

Topic C: Assess the Impact of Malware

- Malware Categories
- Trojan Techniques
- Virus and Worm Techniques
- Adware and Spyware Techniques
- Supply Chain Attack
- Malware Tools
- Assessing the Impact of Malware

Topic D: Assess the Impact of Hijacking and Impersonation Attacks

- Spoofing, Impersonation, and Hijacking
- ARP Spoofing
- DNS Poisoning
- ICMP Redirect
- DHCP Spoofing
- NBNS Spoofing

- WPAD Hijacking
- Session Hijacking
- Hijacking and Spoofing Tools
- Assessing the Impact of Hijacking and Impersonation Attacks

Topic E: Assess the Impact of DoS Incidents

- DoS Attack
- DoS Attack Techniques
- Botnets and DDoS
- Evasion Techniques for DDoS Incidents
- DoS Tools
- Assessing the Impact of DDoS Incidents

Topic F: Assess the Impact of Threats to Mobile Security

- Trends in Mobile Security
- Wireless Threats
- Threats in BYOD Environments
- Threats to Specific Mobile Platforms
- Mobile Infrastructure Hacking Tools
- Assessing the Impact of Threats to Mobile Devices

Topic G: Assess the Impact of Threats to Cloud Security

- Cloud Infrastructure Challenges
- Threats to Virtualized Environments
- Threats to Big Data
- Cloud Infrastructure Hacking Tools
- Cloud Platform Security
- Assessing the Impact of Threats to Cloud Infrastructures

Lesson 5: Analyzing Post-Attack Techniques

Topic A: Assess Command and Control Techniques

- Command and Control
- IRC
- HTTP/S
- DNS
- ICMP
- Additional Channels
- Assessing Command and Control Techniques

Topic B: Assess Persistence Techniques

- Advanced Persistent Threat
- Rootkits
- Backdoors
- Logic Bombs
- Rogue Accounts
- Detecting Rootkits

Topic C: Assess Lateral Movement and Pivoting Techniques

- Lateral Movement
- Pass the Hash
- Golden Ticket

- Remote Access Services
- WMIC
- PsExec
- Pivoting
- VPN Pivoting
- SSH Pivoting
- Routing Tables and Pivoting
- Assessing Lateral Movement and Pivoting Techniques

Topic D: Assess Data Exfiltration Techniques

- Data Exfiltration
- Covert Channels
- Steganography
- File Sharing Services
- Assessing Data Exfiltration

Topic E: Assess Anti-Forensics Techniques

- Anti-Forensics
- Golden Ticket and Anti-Forensics
- Buffer Overflows
- Memory Residents
- Program Packers
- VM and Sandbox Detection
- ADS
- Covering Tracks
- Assessing Anti-Forensics Techniques

Lesson 6: Managing Vulnerabilities in the Organization

Topic A: Implement a Vulnerability Management Plan

- Vulnerability Management
- Vulnerability Management Process
- Requirements Identification
- Execution and Report Generation
- Remediation
- Remediation Inhibitors
- Systemic Security Concerns
- Ongoing Scanning
- Scanning Frequency
- Guidelines for Implementing a Vulnerability Management Plan
- Implementing a Vulnerability Management Plan

Topic B: Assess Common Vulnerabilities

- Vulnerability Assessment
- Penetration Testing
- Vulnerability Assessment vs. Penetration Testing
- Vulnerability Assessment Implementation
- Tools Used in Vulnerability Assessment
- Port Scanning and Fingerprinting
- Networking Vulnerabilities

- Host Vulnerabilities
- Application Vulnerabilities
- Virtual Infrastructure Vulnerabilities
- ICS Vulnerabilities
- Guidelines for Assessing Common Vulnerabilities
- Assessing Virtual Infrastructure Vulnerabilities

Topic C: Conduct Vulnerability Scans

- Vulnerability Scans
- Specific Vulnerability Scanning Tools
- Vulnerability Report Analysis
- Results Validation and Correlation
- Guidelines for Conducting Vulnerability Scans
- Conducting Vulnerability Scans

Lesson 7: Implementing Penetration Testing to Evaluate Security

Topic A: Conduct Penetration Tests on Network Assets

- Vulnerability Scans
- Specific Vulnerability Scanning Tools
- Vulnerability Report Analysis
- Results Validation and Correlation
- Guidelines for Conducting Vulnerability Scans
- Conducting Vulnerability Scans

Topic B: Follow Up on Penetration Testing

- Effective Reporting and Documentation
- Target Audiences
- Information Collection
- Penetration Test Follow-Up
- Report Classification and Distribution
- Analyzing and Reporting Penetration Test Results

Lesson 8: Collecting Cybersecurity Intelligence

Topic A: Deploy a Security Intelligence Collection and Analysis Platform

- Security Intelligence
- The Challenge of Security Intelligence Collection
- Security Intelligence Collection Life Cycle
- Security Intelligence Collection Plan
- CSM
- What to Monitor
- Security Monitoring Tools
- Data Collection
- Guidelines for Selecting Security Data Sources
- Information Processing
- Log Enrichment
- Log Auditing
- External Data Sources
- Publicly Available Information
- Collection and Reporting Automation

- Data Retention
- Analysis Methods
- Deploying a Security Intelligence Collection and Analysis Platform

Topic B: Collect Data from Network-Based Intelligence Sources

- Network Device Configuration Files
- Network Device State Data
- Switch and Router Logs
- Wireless Device Logs
- Firewall Logs
- WAF Logs
- IDS/IPS Logs
- Proxy Logs
- Carrier Provider Logs
- Cloud Provider Logs
- Software-Defined Networking
- Network Traffic and Flow Data
- Log Tuning
- Collecting Network-Based Security Intelligence

Topic C: Collect Data from Host-Based Intelligence Sources

- Operating System Log Data
- Windows Event Logs
- Syslog Data
- Application Logs
- DNS Event Logs
- SMTP Logs
- HTTP Logs
- FTP Logs
- SSH Logs
- SQL Logs
- Collecting Host-Based Security Intelligence

Lesson 9: Analyzing Log Data

Topic A: Use Common Tools to Analyze Logs

- Preparation for Analysis
- Guidelines for Preparing Data for Analysis
- Log Analysis Tools
- The grep Command
- The cut Command
- The diff Command
- The find Command
- WMIC for Log Analysis
- Event Viewer
- Bash
- Windows PowerShell
- Additional Log Analysis Tools
- Long Tail Analysis

- Guidelines for Using Windows- and Linux-Based Tools for Log Analysis
- Analyzing Linux Logs for Security Intelligence

Topic B: Use SIEM Tools for Analysis

- Security Intelligence Correlation
- SIEM
- The Realities of SIEM
- SIEM Analysis
- Guidelines for Using SIEMs for Security Intelligence Analysis
- Incorporating SIEMs into Security Intelligence Analysis

Lesson 10: Performing Active Asset and Network Analysis

Topic A: Analyze Incidents with Windows-Based Tools

- Registry Analysis Tools for Windows
- File System Analysis Tools for Windows
- Process Analysis Tools for Windows
- Service Analysis Tools for Windows
- Volatile Memory Analysis Tools for Windows
- Active Directory Analysis Tools
- Network Analysis Tools for Windows
- Analyzing Incidents with Windows-Based Tools

Topic B: Analyze Incidents with Linux-Based Tools

- File System Analysis Tools for Linux
- Process Analysis Tools for Linux
- Volatile Memory Analysis Tools for Linux
- Session Analysis Tools for Linux
- Network Analysis Tools for Linux
- Analyzing Incidents with Linux-Based Tools

Topic C: Analyze Malware

- Malware Sandboxing
- Crowd-Sourced Signature Detection
- Reverse Engineering
- Disassemblers
- Malware Strings
- Anti-Malware Solutions
- MAEC
- Guidelines for Analyzing Malware
- Analyzing Malware

Topic D: Analyze Indicators of Compromise

- IOCs
- Unauthorized Software and Files
- Suspicious Emails
- Suspicious Registry Entries
- Unknown Port and Protocol Usage
- Excessive Bandwidth Usage
- Service Disruption and Defacement
- Rogue Hardware

- Suspicious or Unauthorized Account Usage
- Additional IOCs
- Guidelines for Analyzing Indicators of Compromise
- Analyzing Indicators of Compromise

Lesson 11: Responding to Cybersecurity Incidents

Topic A: Deploy an Incident Handling and Response Architecture

- Incident Handling and Response Planning
- Disaster Recovery Planning
- Incident Response Process
- SOCs
- CSIRT
- A Day in the Life of a CSIRT
- Communication within the CSIRT
- Internal and External Communication Plans
- Incident Identification
- The Impact and Scope of Incidents
- Incident Evaluation and Analysis
- Incident Containment
- Incident Mitigation and Eradication
- Incident Recovery
- Post-Incident
- Questions to Answer in an AAR
- Incident Handling Tools
- Developing an Incident Response System

Topic B: Contain and Mitigate Incidents

- System Hardening
- Isolation
- Blacklisting
- Whitelisting
- DNS Filtering
- Black Hole Routing
- Mobile Device Management
- Secure Erasure and Disposal
- Devices and Tools Used in Containment and Mitigation
- The Importance of Updating Device Signatures
- Additional Containment and Mitigation Tactics
- Data Breach Incident Case Study
- DoS Incident Case Study
- APT Case Study
- Guidelines for Containing and Mitigating Incidents
- Identifying and Analyzing an Incident
- Containing, Mitigating, and Recovering from an Incident

Topic C: Prepare for Forensic Investigation as a CSIRT

- The Duties of a Forensic Analyst
- Communication of CSIRT Outcomes to Forensic Analysts

- Guidelines for Conducting Post-Incident Tasks
- Preparing for a Forensic Investigation

Lesson 12: Investigating Cybersecurity Incidents

Topic A: Apply a Forensic Investigation Plan

- A Day in the Life of a Forensic Analyst
- Forensic Investigation Models
- Forensic Investigation Preparation
- Investigation Scope
- Timeline Generation and Analysis
- Authentication of Evidence
- Chain of Custody
- Communication and Interaction with Third Parties
- Forensic Toolkit (Software)
- Forensic Toolkit (Physical)
- Guidelines for Preparing for a Forensic Investigation
- Applying a Forensic Investigation Plan

Topic B: Securely Collect and Analyze Electronic Evidence

- Order of Volatility
- File Systems
- File Carving and Data Extraction
- Data Preservation for Forensics
- Secure Storage of Physical Evidence
- Forensic Analysis of Compromised Systems
- Securely Collecting Electronic Evidence
- Analyzing Forensic Evidence

Topic C: Follow Up on the Results of an Investigation

- Cyberlaw
- Technical Experts and Law Enforcement Liaisons
- Documentation of Investigation Results
- Conducting Post-Mortem Activities

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

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 course, you will need one Windows Server® 2016 computer and one 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 not* included 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 *is* included 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**).
- Greenbone Security Manager Community Edition version 4.1.7 (**gsm_ce_4.1.7.iso**)
- 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, icmpsh, and Greenbone Security Manager 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).