CertNexus CyberSec First Responder Course Description: Exam CFR-310

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)