Date Issued: 3/5/2018
Date Modified: 4/11/2019
Version: 1.5
Approved by: Scheme Committee

CertNexus CyberSec First Responder™ (CFR) Exam CFR-310

Exam Information

Candidate Eligibility:

The *CyberSec First Responder™ (CFR)* exam requires no application fee, supporting documentation, or other eligibility verification measures for you to be eligible to take the exam. An exam voucher will come bundled with your training program or can be purchased separately here. Once purchased, you will receive more information about how to register for and schedule your exam Pearson Vue. You can also purchase a voucher directly through Pearson Vue. Once you have obtained your voucher information, you can register for an exam time here. By registering, you agree to our Candidate Agreement included here.

Exam Prerequisites

While there are no formal prerequisites to register for and schedule an exam, we strongly recommend you first possess the knowledge, skills, and abilities to do the following:

- Assess cybersecurity risk in computing environments within a risk management framework.
- Evaluate an organization's cybersecurity posture.
- Identify that a cybersecurity incident has occurred.
- Collect cybersecurity intelligence.
- Analyze data collected from security and event logs using both Windows and Linux tools.
- Analyze threats to computing environments.
- Analyze attacks on computing environments.
- Analyze post-attack techniques on computing environments.
- Perform analysis on network assets.
- Investigate cybersecurity incidents.
- Provide remediation and containment suggestions in response to cybersecurity incidents.
- Assess and apply cybersecurity policies and procedures.
- Understand the cybersecurity threat landscape.
- Review vulnerability assessments performed on computing environments.
- Identify cybersecurity compliance, standards, frameworks, and best practices.
- Identify and describe basic concepts of forensics.
- Utilize log sources for continuous monitoring and detection of potential anomalies.

- Prepare for incident response and execute the incident response process when an incident has occurred.

You can obtain this level of skill and knowledge by taking the following courseware, which is available through training providers located around the world, or by attending an equivalent third-party training program:

- *Logical Operations CyberSec First Responder™ (Exam CFR-310)*

Exam Specifications

Number of Items: 100

Passing Score: 70% or 71%, depending on exam form. Forms have been statistically equated.

Duration: 120 minutes

Exam Options: In person at Pearson VUE test centers

Item Formats: Multiple Choice/Multiple Response

Exam Description

Target Candidate:

The C*yberSec First Responder™ (CFR)* exam is designed for individuals with between 3 and 5 years of experience working in a computing environment as part of a CERT/CSIRT/SOC who desire or are required to protect critical information systems before, during, and after an incident which may be a cybersecurity attack.

Exam Objective Statement:

The exam will certify that the successful candidate has the knowledge, skills, and abilities required to effectively identify, respond to, protect against, and remediate malicious activities involving computing systems. Additionally, the candidate has the foundational knowledge to deal with a changing threat landscape and will be able to assess risk and vulnerabilities, acquire data, perform analysis, continuously communicate, determine scope, recommend remediation actions, and accurately report results.

To ensure exam candidates possess the aforementioned knowledge, skills, and abilities, the C*yberSec First Responder™ (CFR)* exam will test them on the following domains with the following weightings:

Domain	% of Examination
1.0 Threats and Attacks	24%
2.0 Data Collection and Analysis	23%
3.0 Incident Response Methods, Tools, and Techniques	22%
4.0 The Incident Response Process	18%
5.0 Vulnerability Assessment	13%
Total	**100%**

The information that follows is meant to help you prepare for your certification exam. This information does not represent an exhaustive list of all the concepts and skills that you may be tested on during your exam. The exam domains, identified previously and included in the objectives listing, represent the large content areas covered in the exam. The objectives within those domains represent the specific tasks associated with the job role(s) being tested. The information beyond the domains and objectives is meant to provide examples of the types of concepts, tools, skills, and abilities that relate to the corresponding domains and objectives. All of this information represents the industry-expert analysis of the job role(s) related to the certification and does not necessarily correlate one-to-one with the content covered in your training program or on your exam. We strongly recommend that you independently study to familiarize yourself with any concept identified here that was not explicitly covered in your training program or products.

Objectives:

Domain 1.0 Threats and Attacks

Objective 1.1 Compare and contrast various threats and classify threat profiles

- Threat targets
  - Individuals
  - Non-profit associations
  - Corporations
  - Governments
  - Critical Infrastructure
  - Systems
    - Mobile
    - IoT
    - SCADA
    - ICS
    - PLC
- Threat actors
  - Script kiddies
  - Recreational hackers
  - Professional hackers
  - Hacktivists
  - Cyber criminals
  - State sponsored hackers
  - Terrorists
  - Insider
- Threat motives/reasons
  - Desire for financial gain

        - Desire for power
        - Fun/thrill/exploration
        - Reputation/recognition
        - Association/affiliation
        - Revenge
        - Human error
    - Threat intent
        - Blackmail
        - Theft
        - Espionage
        - Hacktivism/political
        - Terrorism
        - Defamation of character
    - Attack phases
        - Reconnaissance
        - Scanning
        - Gaining access
        - Persistence/Maintaining access
        - Expanding access
        - Covering tracks
    - Attack vectors
    - Technique criteria
        - Targeted/non-targeted
        - Direct/indirect
        - Stealth/non-stealth
        - Client-side/server-side
    - Impact of the attack on the organization
        - Financial loss
            - Direct
            - Indirect
        - Data exfiltration
        - Customer relationship
        - Business reputation
        - Capacity
        - Time
        - Compliance/notification
        - Litigation
        - Insurance costs
        - Customer protection
        - Cybersecurity improvements required

        - Legal fees
        - Public relationship management

Objective 1.2 Explain the purpose and use of attack methods and techniques

- Footprinting
    - Open-source intelligence
    - Closed-source intelligence
- Scanning
    - Active vs. passive scanning
    - Port scanning
    - Vulnerability scanning
        - Targeted vulnerability scanners vs. general vulnerability scanners
    - Network scanning
    - Web app scanning
- Enumeration
    - User enumeration
    - Application enumeration
    - Email enumeration
    - Network enumeration
    - Wardriving
- Gaining access
    - Exploitation frameworks
    - Client-side attacks
        - Application exploits
        - Browser exploits
    - Server-side attacks
    - Mobile
        - Malicious apps
        - Malicious texts
        - Hijacking/rooting
    - Web attacks
        - CSRF
        - SQL injection
        - Directory traversal
        - LFI/RFI
        - Command injection
    - Password attacks
        - Password cracking
            - Brute forcing
            - Password guessing

            - Password dictionary
            - Rainbow tables
        - Password sniffing
    - Wireless attacks
        - Wireless cracking
        - Wireless client attacks
        - Infrastructure attacks
    - Social engineering
        - Phishing
        - Spear phishing
        - Quid pro quo
        - Baiting
        - Shoulder surfing
        - Tailgating
    - Man-in-the-middle
        - ARP spoofing/cache poisoning
        - ICMP redirect
        - DHCP spoofing
        - NBNS spoofing
        - Session hijacking
        - DNS poisoning
        - WPAD
    - Malware
        - Trojan
        - Malvertisement
        - Virus
        - Worm
        - Ransomware
        - Rootkit
    - Out of band
        - OEM supply chain
        - Watering hole
- DoS
    - DDoS
        - LOIC/HOIC
    - Resource exhaustion
    - Forced system outage
    - Packet generators

Objective 1.3 Explain the purpose and use of post exploitation tools and tactics

- Command and control

    - IRC
    - HTTP/S
    - DNS
    - Custom channels
    - ICMP
- Data exfiltration
    - Covert channels
    - File sharing services
- Pivoting
    - VPN
    - SSH tunnels
    - Routing tables
- Lateral movement
    - Pass the hash
    - Golden ticket
    - psexec
    - wmic
    - Remote access services
- Persistence/maintaining access
    - Rootkits
    - Backdoors
    - Hardware backdoor
    - Rogue accounts
    - Logic bombs
- Keylogging
    - Software-based
    - Hardware-based
- Anti-forensics
    - Buffer overflows
    - Virtual machine detection
    - Sandbox detection
    - Shredding
- Covering your tracks
    - Log wipers

Objective 1.4 Given a scenario, perform ongoing threat landscape research and use data to prepare for incidents

- Latest technologies, vulnerabilities, threats and exploits
- Utilize trend data to determine likelihood and threat attribution
- New tools/prevention techniques
- Data gathering/research tools/cybersecurity intelligence

        - Journals
        - Vulnerability databases
        - Books
        - Blogs
        - Intelligence feeds
        - Security advisories
        - Social network sites
        - Automated threat scoring
    - Common targeted assets
        - Financial information
        - Account information
        - Intellectual property
        - Trade secrets
        - PII/PHI
        - National security data and identities
        - Computing resources
        - Power resources

Domain 2.0 Data Collection and Analysis

Objective 2.1 Explain the purpose and characteristics of various data sources

- Network-based
    - Device configuration file(s)
    - Firewall logs
    - WAF logs
    - IDS/IPS logs
    - Switch logs
    - Router logs
    - Carrier provider logs
    - Proxy logs
    - Wireless
        - WAP logs
        - WIPS logs
        - Controller logs
    - Network sniffer
        - Packet capture
        - Traffic log
        - Flow data
    - Device state data
        - CAM tables
        - Routing tables
        - NAT tables

        - DNS cache
        - ARP cache
    - SDN
- Host-based
    - System logs
    - Service logs
        - SSH logs
            - Time
            - Crypto protocol
            - User
            - Success/failure
        - HTTP logs
            - HTTP methods (get, post)
            - Status codes
            - Headers
            - User agents
            - SSL debugging
        - SQL logs
            - Access logs
            - Query strings
        - SMTP logs
        - FTP logs
        - DNS logs
            - Suspicious lookups
            - Suspicious domains
            - Types of DNS queries
    - Windows Event Logs
        - App log
        - System log
        - Security log
    - Linux syslog
    - Application logs
        - Browser
        - HIPS logs
        - Antivirus logs
        - Integrity checker
- Cloud
    - Audit logs
    - Threat feeds
    - Security bulletins

- Vulnerability testing data
    - Third-party data
    - Automated/software testing programs

Objective 2.2 Given a scenario, use real-time data analysis to detect anomalies

- Log collection
    - Agent-based
    - Agentless
    - Syslog
- Log auditing
    - Source validation
    - Verification of log integrity
    - Evidence collection
- Log enrichment
    - IP address and host name resolution
    - Field name consistency
    - Time zones
- Alerts, reports, and event correlation
    - Threat hunting
    - Long tail analysis
    - Intrusion detection
    - Behavioral monitoring
- Log retention
    - Industry compliance/regulatory requirements
- Anomalies
    - False positives
    - Superhuman logins/geovelocity
    - APT activity
    - Botnets

Objective 2.3 Given a scenario, analyze common indicators of potential compromise

- Unauthorized programs in startup menu
- Malicious software
    - Presence of attack tools
- Registry entries
- Unusual network traffic
    - Bandwidth usage
    - Malicious network communication
- Off hours usage
- New administrator/user accounts
- Guest account usage
- Unknown open ports

- Unknown use of protocols
- Service disruption
- Website defacement
- Unauthorized changes/modifications
    - Suspicious files
    - Patches
- Recipient of suspicious emails
- Unauthorized sessions
- Failed logins
- Rogue hardware

Objective 2.4 Given a scenario, use appropriate tools to analyze logs

- Log aggregator and analytics tools
    - SIEM
- Linux tools
    - grep
    - cut
    - diff
- Windows tools
    - Find
    - WMIC
    - Event Viewer
- Scripting languages
    - Bash
    - PowerShell

Domain 3.0 Incident Response Methods, Tools, and Techniques

Objective 3.1 Given a scenario, use appropriate containment methods or tools

- Methods
    - Whitelist/blacklist
    - IDS/IPS rules configuration
    - Network segmentation
    - Web content filtering
    - Port blocking
- Tools
    - Firewall
    - IDS/IPS
    - Web proxy
    - Anti-malware
    - Endpoint security solutions
    - DLP

Objective 3.2 Given a scenario, use appropriate asset discovery methods or tools

- Methods
  - Agent-based
  - Agentless
- Tools
  - Nmap
  - Wireshark
  - Zenmap
  - tcpdump
  - Qualys
  - Snort
  - OpenVAS
  - Nessus
  - Burp Suite
  - Nikto

Objective 3.3 Given a scenario, use Windows tools to analyze incidents

- Registry
  - Regedit
    - Key, hives, values, value types
    - HKLM, HKCU
  - REGDUMP
  - Autoruns
- Network
  - Wireshark
  - Fport
  - Netstat
  - IPConfig
  - Nmap
  - Tracert
  - Net
  - Nbtstat
- File system
  - Dir
  - PE Explorer
  - Disk utilization tool
  - md5sum
  - sha256sum
  - md5deep
- Malware
  - VirusTotal
  - IDA Pro

    - Cuckoo
- Processes
    - tasklist
    - Process Monitor
    - Process Explorer
- Services
    - Services.msc
    - MSConfig
    - Net start
    - Task Scheduler
- Volatile memory
    - Rekall
- Active Directory tools

Objective 3.4 Given a scenario, use Linux-based tools to analyze incidents

- Network
    - Nmap
    - Netstat
    - Wireshark
    - tcpdump
    - traceroute
    - ARP
    - ifconfig
- File system
    - lsof
    - dd
    - Disk utilization tool
    - md5sum
    - sha256sum
    - md5deep
    - strings
    - grep
- Malware
    - VirusTotal
    - IDA Pro
    - Cuckoo
- Processes
    - htop
    - top
    - ps
- Volatile memory

        - free
        - Volatility
        - Rekall
    - Session management
        - w/who
        - rwho
        - lastlog

Domain 4.0 The Incident Response Process

Objective 4.1 Given a scenario, execute the incident response process

- Preparation
- Identification
    - Detection/analysis
    - Collection
- Containment
- Eradication
- Recovery
- Post incident
    - Root cause analysis
    - Lessons learned
    - Reporting and documentation
        - Summary
        - Incident description
        - Initial investigation
        - Technical description of the attack
        - Impact of the attack
        - Incident response plan
        - Incident timeline log
        - Action plan/remediation plan
        - Attachments (logs)
- Communication (occurs throughout all phases)

Objective 4.2 Explain the importance of best practices in preparation for incident response

- Preparation and planning
    - Up-to-date contact lists
    - Up-to-date incident response toolkit
- Ongoing training
    - Incident responder
    - Incident response team
    - Management
    - Tabletop (theoretical) exercise
- Internal communication methods

    - Secure channels
    - Out-of-band communications
- External communication plan
    - Local law enforcement
    - Stockholders
    - Breach victims
    - Media
    - Other CERTs/CSIRTs
    - Vendors
- Organizational documentation
    - Policies
    - Procedures
    - Incident response plan
    - Security configuration controls
    - Baseline configurations
    - Hardening documentation
- Escalation procedures
    - Chain of command

Objective 4.3 Identify applicable compliance, standards, frameworks, and best practices

- Compliance
    - ISO 27001
    - PCI DSS
    - SOX
    - HIPAA
    - GLBA
    - GDPR
- Standards
    - ISO/IEC 27000 series
    - ANSI/ISA-62443
    - NIST Special Publication 800 Series
    - Standard of Good Practice from ISF
    - NERC 1300 and RFC 2196
- Frameworks
    - Cybersecurity Framework
    - CIS Critical Security Controls
    - COBIT
    - NIST Special Publication 800-61
    - RMF
- Best practices
    - OWASP

    - MITRE CAPEC

Objective 4.4 Explain the importance of concepts that are unique to forensic analysis

- Evidence collection, preservation, and security
    - Digital
        - Imaging
        - Hashing
    - Physical
        - Evidence bags
        - Evidence tags
- Chain of custody
- Forensic investigation
    - Static analysis
    - Dynamic analysis
- Forensic collection and analysis tools
    - FTK
    - EnCase
    - eDiscovery
    - Forensic Explorer
    - Kali Linux Forensic Mode
    - CAINE
    - SANS SIFT

Domain 5.0 Vulnerability Assessment

Objective 5.1 Identify common areas of vulnerability

- Users
- Operating system
- Applications
    - Networking software
        - Network operations and management
        - Firewall
        - Network security applications
    - Database software
- Network devices
    - Access points
    - Routers
    - Wireless routers
    - Switches
    - Firewall
- Network infrastructure
    - Network configurations
    - Network services

        - DSL
        - Wireless protocols
        - IP addressing
    - IoT
    - Configuration files

Objective 5.2 Identify the steps of the vulnerability assessment process

- Plan a vulnerability assessment
    - Identify critical assets and data
    - Establish scope
    - Determine scanning frequency
        - Regulatory requirements
        - Changes to the system
- Perform a vulnerability assessment
    - Determine scanning criteria
    - Utilize scanning tools
    - Identify and assess exposures
    - Generate reports
- Conduct post-assessment tasks
    - Remediate/mitigate vulnerabilities
        - Hardening
            - Patches
            - Configurations
        - Exceptions documented
    - Conduct audit/validate action was taken

Recertification Requirements

The *CyberSec First Responder™ (CFR)* certification is valid for 3 years from the date that it is initially granted. In order to maintain a continuously valid certification, candidates can recertify via one of the following options:

1. Retake the most recent version of the exam before their certification expires.
2. Earn and submit enough continuing education credits (CECs) to recertify without retaking the exam.

CyberSec First Responder™ (CFR) Acronyms

Acronym	Expanded Form
ANSI	American National Standards Institute
APT	advanced persistent threat
ARP	Address Resolution Protocol
CAM	content-addressable memory
CAPEC	Common Attack Pattern Enumeration and Classification
CERT	computer emergency response team
CIS	Center for Internet Security
COBIT	Control Objectives for Information and Related Technologies
CSIRT	computer security incident response team
CSRF	Cross-Site Request Forgery
DDoS	distributed denial of service
DHCP	Dynamic Host Configuration Protocol
DLP	data loss prevention
DNS	Domain Name System
DSL	digital subscriber line
FTP	File Transfer Protocol
GDPR	General Data Protection Regulation
GLBA	Gramm-Leach-Bliley Act
HIPAA	Health Insurance Portability and Accountability Act
HIPS	Host Intrusion Prevention System
HKCU	Host Key Current User
HKLM	Host Key Local Machine

HOIC	High Orbit Ion Cannon
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
ICMP	Internet Control Message Protocol
ICS	Incident Command System
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IRC	Internet Relay Chat
ISA	International Society for Automation
ISF	Information Security Forum
ISO	International Organization for Standardization
LFI	Local File Inclusion
LOIC	Low Orbit Ion Cannon
NAT	network address translation
NBNS	NetBIOS Name Service
NIPS	Network Intrusion Prevention System
NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
OWASP	Open Web Application Security Project
PCI DSS	Payment Card Industry Data Security Standard
PHI	protected health information

PII	personally identifiable information
PLC	programmable logic controller
RMF	Risk Management Framework
RFI	Remote File Inclusion
SCADA	supervisory control and data acquisition
SDN	software-defined networking
SIEM	Security Information Event Management
SMTP	Simple Mail Transfer Protocol
SOC	security operations center
SOX	Sarbanes-Oxley Act
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
VPN	virtual private network
WAF	web application firewall
WAP	wireless access point
WIPS	Wireless Intrusion Prevention System
WMIC	Windows Management Instrumentation Command-line
WPAD	Web Proxy Auto-Discovery