Logical Operations CyberSec First Responder (CFR) Exam CFR-210

Exam Information

Candidate Eligibility:
The Logical Operations CyberSec First Responder (CFR-210) exam requires no application fee, supporting documentation, or other eligibility verification measures for you to be eligible to take the exam. Simply purchase an exam voucher here, then Logical Operations will send you an email containing the information you need to register to take the exam through Pearson VUE. You can also purchase a voucher directly through Pearson VUE. If your voucher came bundled with your CFR training program, you will receive registration information from your training provider. Once you have obtained your voucher information, you can register for an exam time here. By redeeming your exam voucher, you agree to our Candidate Agreement.

Exam Prerequisites
While there are no formal prerequisites to register for and schedule a CFR-210 exam time, Logical Operations strongly recommends you first possess the knowledge, skills, and abilities to do the following:

- Assess information security risk in computing and network environments
- Analyze the cybersecurity 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
- Evaluate an organization’s security posture within a risk management framework
- 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

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

Number of Items: 100

Passing Score: Between 62% and 69% depending on the exam form. Forms have been statistically equated based on question difficulty levels.

Duration: 120 minutes (Note: Published exam times include the 5 minutes you are allotted for reading and signing the Candidate Agreement and the 5 minutes you are allotted for the Pearson VUE testing system tutorial.)

Exam Options: In person at Pearson VUE test centers

Item Formats: Multiple Choice/Multiple Response/Drag-and-Drop

Exam Description

Target Candidate:

The Logical Operations CyberSec First Responder (CFR-210) exam target audience should have at least 2-5 years of experience working in a networking environment as a first responder. The successful candidate will have the knowledge and skills required to effectively detect, identify, and respond to malicious activities involving data systems. Additionally, the candidate will have the foundational knowledge to deal with a changing threat landscape and will be able to perform root cause analysis, determine scope, accurately report results, and recommend remediation actions.

To ensure exam candidates possess the aforementioned knowledge, skills, and abilities, the CFR-210 exam will test them on the following objective domains with the following weightings:

<table>
<thead>
<tr>
<th>Domain</th>
<th>% of Examination</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 Threat Landscape</td>
<td>25%</td>
</tr>
<tr>
<td>2.0 Passive Data-Driven Analysis</td>
<td>27%</td>
</tr>
<tr>
<td>3.0 Active Asset and Network Analysis</td>
<td>28%</td>
</tr>
<tr>
<td>4.0 Incident Response Lifecycle</td>
<td>20%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>
Objectives:

Domain 1.0  Threat Landscape
Objective 1.1  Compare and contrast various threats and classify threat profiles
  • Threat actors
    o Script kiddies
    o Recreational hackers
    o Professional hackers
    o Hacktivists
    o Cyber criminals
    o State sponsored hackers
    o Terrorists
    o Insider
  • Threat motives
    o Desire for money
    o Desire for power
    o Fun/thrill/exploration
    o Reputation/recognition
    o Association/affiliation
  • Threat intent
    o Blackmail
    o Theft
    o Espionage
    o Revenge
    o Hacktivism/political
    o Defamation of character
• Attack vector
  o Vulnerabilities
  o Exploits
  o Techniques

• Technique criteria
  o Targeted/non-targeted
  o Direct/indirect
  o Stealth/non-stealth
  o Client-side/server-side

• Understanding qualitative risk and impact

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

• Footprinting
  o Open source intelligence
  o Closed source intelligence

• Scanning
  o Port scanning
  o Vulnerability scanning
    ▪ Targeted vulnerability scanners vs. general vulnerability scanners
  o Network scanning
  o Web app scanning

• Enumeration
  o User enumeration
  o Application enumeration
  o Email enumeration
  o War dialing

• Gaining access
  o Exploitation frameworks
  o Client-side attacks
    ▪ Application exploits
    ▪ Browser exploits
  o Server-side attacks
  o Mobile
    ▪ Malicious apps
    ▪ Malicious texts
    ▪ Hijacking/rooting
  o 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
    - Man-in-the-middle
      - ARP spoofing
      - ICMP redirect
      - DHCP spoofing
      - NBNS spoofing
      - Session hijacking
      - DNS poisoning
  - Malware
    - Trojan
    - Malvertisement
    - Virus
    - Worm
  - Out of band
    - OEM supply chain
    - Watering hole
- Denial of Service
  - 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

- Anti-forensics
  - Golden ticket
  - Buffer overflows against forensics tools
  - Packers
  - Virtual machine detection
  - Sandbox detection
  - ADS
  - Shredding
  - Memory residents

- Covering your tracks
  - Log wipers

**Objective 1.4  Explain the purpose and use of social engineering tactics**

- Phishing
  - Phishing variations
    - Spear phishing
    - Whaling
    - Vishing
  - Delivery mediums
• Email
• IM
• Post card
• Text
• QR code
• Social networking sites
  o Common components
    ▪ Spoofing messages
    ▪ Rogue domains
    ▪ Malicious links
    ▪ Malicious attachments
• Shoulder surfing
• Tailgating
• Face-to-face interactions
• Fake portals/malicious websites

Objective 1.5 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
    o Journals
    o Vulnerability databases
    o Books
    o Blogs
    o Intelligence feeds
    o Security advisories
    o Social network sites
• Common targeted assets
  o Financial information
  o Credit card numbers
  o Account information
  o Intellectual property
  o PHI
  o PII

Domain 2.0 Passive Data-Driven Analysis
Objective 2.1 Explain the purpose and characteristics of various data sources
  • Network-based
    o Device configuration file(s)
    o 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
      - 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
    - AV logs
    - Integrity checker
- Vulnerability testing data
  - Third party data
  - Automated/software testing programs

**Objective 2.2 Given a scenario, use appropriate tools to analyze logs**
- Log analytics tools
- Linux tools
  - grep
  - cut
  - diff
- Windows tools
  - Find
  - WMIC
  - Event Viewer
- Scripting languages
  - Bash
  - PowerShell
- Log correlation
  - SIEMs

**Objective 2.3 Given a scenario, use regular expressions to parse log files and locate meaningful data**
- Search types
  - Keyword searches
  - IP address searches
  - Special character searches
  - Port number searches
- Search operators
  - &
  - |
Special operators
- \W
- \w
- \s
- \D
- \d
- \b
- \c

Domain 3.0  Active Asset and Network Analysis
Objective 3.1  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
  - nbstat
- File system
  - dir
  - pe explorer
  - disk utilization tool
• Processes
  o TLIST
  o PROCMON
  o Process explorer
• Services
  o Services.msc
  o Msconfig
  o Net start
  o Task scheduler
• Volatile memory analysis
• Active Directory tools

Objective 3.2 Given a scenario, use Linux-based tools to analyze incidents

• Network
  o nmap
  o netstat
  o wireshark
  o tcpdump
  o traceroute
  o arp
  o ifconfig
• File system
  o lsof
  o iperf
  o dd
  o disk utilization tool
• Processes
  o htop
  o top
  o ps
• Volatile memory
  o free
• Session management
  o w, who
  o rwho
  o lastlog

Objective 3.3 Summarize methods and tools used for malware analysis

• Methods
  o Sandboxing
    ▪ Virtualization
  o Threat intelligence websites
- Crowd source signature detection
- Virus total

- Reverse engineering tools
  - IDA
  - Ollydbg

- General tools
  - strings
  - Antivirus
  - Malware scanners

**Objective 3.4 Given a scenario, analyze common indicators of potential compromise**

- Unauthorized programs in startup menu
- Malicious software
  - Presence of attack tools
- Registry entries
- Excessive bandwidth usage
- 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
- Recipient of suspicious emails
- Unauthorized sessions
- Failed logins
- Rogue hardware

**Domain 4.0 Incident Response Lifecycle**

**Objective 4.1 Explain the importance of best practices in preparation for incident response**

- Preparation and planning
  - Up-to-date contact lists
  - Up-to-date toolkit

- Ongoing training
  - Incident responder
  - Incident response team
  - Management
  - Tabletop (theoretical) exercises

- Communication methods
- Secure channels
- Out of band communications
- Organizational documentation
  - Policies
  - Procedures
  - Incident response plan
- Escalation procedures
  - Chain of command
- Industry standards for incident response

Objective 4.2 Given a scenario, execute incident response process
- Preparation
- Identification
  - Detection/analysis
  - Collection
- Containment
- Eradication
- Recovery
- Post incident
  - Lessons learned
    - Root cause analysis
  - Reporting & documentation

Objective 4.3 Explain the importance of concepts that are unique to forensic analysis
- Authorization to collect information
- Legal defensibility
  - Chain of custody
  - Legally compliant tools
    - Encase
    - FTK
    - Forensics explorer
- Confidentiality
- Evidence preservation and evidence security
  - Digital
    - Imaging
    - Hashing
  - Physical
    - Secure rooms and facilities
    - Evidence bags
    - Lock boxes
- Law enforcement involvement

Objective 4.4 Explain general mitigation methods and devices
• Methods
  o System hardening
    ▪ Deactivate unnecessary services
    ▪ Patching
  o Updating internal security devices
    ▪ Report malware signatures
    ▪ Custom signatures
  o Block external sources of malware
  o DNS filtering
  o Blackhole routing
  o System and application isolation
  o Mobile device management
  o Application whitelist

• Devices
  o Firewall
  o WAF
  o Switch
  o Routers
  o Proxy
  o Virtual Machine
  o Mobile
  o Desktop
  o Server

Recertification Requirements
The Logical Operations CyberSec First Responder (CFR-210) 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. Find out more about the CFR Continuing Education Program [here](#).
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Expanded Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADS</td>
<td>Alternate Data Stream</td>
</tr>
<tr>
<td>ARP</td>
<td>Address Resolution Protocol</td>
</tr>
<tr>
<td>AV</td>
<td>Antivirus</td>
</tr>
<tr>
<td>BASH</td>
<td>Bourne Again Shell</td>
</tr>
<tr>
<td>CAM</td>
<td>Content Addressable Memory</td>
</tr>
<tr>
<td>CSRF</td>
<td>Cross-site Request Forgery</td>
</tr>
<tr>
<td>DDoS</td>
<td>Distributed Denial of Service</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>FTK</td>
<td>Forensic Tool Kit</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>GREP</td>
<td>Global Regular Expression Print</td>
</tr>
<tr>
<td>HIPS</td>
<td>Host Intrusion Prevention System</td>
</tr>
<tr>
<td>HKCU</td>
<td>Host Key Current User</td>
</tr>
<tr>
<td>HKLM</td>
<td>Host Key Local Machine</td>
</tr>
<tr>
<td>HOIC</td>
<td>High Orbit Ion Cannon</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hyper Text Transfer Protocol</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hyper Text Transfer Protocol Secure</td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Message Protocol</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>IM</td>
<td>Instant Message</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPS</td>
<td>Intrusion Prevention System</td>
</tr>
<tr>
<td>IRC</td>
<td>Internet Relay Chat</td>
</tr>
<tr>
<td>LFI</td>
<td>Local File Inclusion</td>
</tr>
<tr>
<td>LOIC</td>
<td>Low Orbit Ion Cannon</td>
</tr>
<tr>
<td>LSOF</td>
<td>List Open Files</td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
</tr>
<tr>
<td>NBNS</td>
<td>NetBIOS Name Service</td>
</tr>
<tr>
<td>NIPS</td>
<td>Network Intrusion Prevention System</td>
</tr>
<tr>
<td>OEM</td>
<td>Original Equipment Manufacturer</td>
</tr>
<tr>
<td>PE</td>
<td>Portable Executable</td>
</tr>
<tr>
<td>PHI</td>
<td>Protected Health Information</td>
</tr>
<tr>
<td>PII</td>
<td>Personally Identifiable Information</td>
</tr>
<tr>
<td>QR</td>
<td>Quick Response</td>
</tr>
<tr>
<td>RFI</td>
<td>Remote File Inclusion</td>
</tr>
<tr>
<td>SIEM</td>
<td>Security Information Event Management</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>WAF</td>
<td>Web Application Firewall</td>
</tr>
<tr>
<td>WAP</td>
<td>Wireless Access Point</td>
</tr>
<tr>
<td>WIPS</td>
<td>Wireless Intrusion Prevention System</td>
</tr>
<tr>
<td>WMIC</td>
<td>Windows Management Instrumentation Command Line</td>
</tr>
</tbody>
</table>