Date Issued: 9-13-2016
Date Modified: 9-13-2016
Version: 1.0
Approved by: CFR Scheme Committee

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

Exam Information

Candidate Eligibility:

The *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 (LO) course, which is available through training providers located around the world, or by attending an equivalent third-party training program:

- *CyberSec First Responder: Threat Detection and Response (Exam CFR-210)*

Exam Specifications

Number of Items: 100

Duration: 120 minutes

Exam Options: In person at Pearson VUE testing centers

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

Exam Description

Target Candidate:

The *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 above mentioned knowledge, skills, and abilities, the *CFR-210* exam will test them on the following objective domains with the following weightings:

Domain	% of Examination
1.0 Threat Landscape	25%
2.0 Passive Data-Driven Analysis	27%
3.0 Active Asset and Network Analysis	28%
4.0 Incident Response Lifecycle	20%
Total	**100%**

**Note: The lists of examples provided in bulleted format below each objective are not exhaustive lists. Other technologies, processes, or tasks pertaining to each objective may also be included on the exam even if it is not listed or covered in this objectives document.

(A list of acronyms used in these objectives appears at the end of this document.)

Objectives:

Domain 1: Threat Landscape

1.1 Compare and contrast various threats and classify threat profiles

- Threat actors
  - Script kiddies
  - Recreational hackers
  - Professional hackers
  - Hacktivists
  - Cyber criminals
  - State sponsored hackers
  - Terrorists
  - Insider
- Threat motives
  - Desire for money
  - Desire for power
  - Fun/thrill/exploration
  - Reputation/recognition
  - Association/affiliation
- Threat intent
  - Blackmail
  - Theft
  - Espionage
  - Revenge
  - Hacktivism/political
  - Defamation of character
- Attack vector
  - Vulnerabilities
  - Exploits
  - Techniques
- Technique criteria
  - Targeted/non-targeted
  - Direct/indirect
  - Stealth/non-stealth
  - Client-side/server-side
- Understanding qualitative risk and impact

1.2 Explain the purpose and use of attack tools and techniques

- Footprinting
  - Open source intelligence
  - Closed source intelligence
- Scanning
  - Port scanning
  - Vulnerability scanning

        - Targeted vulnerability scanners vs. general vulnerability scanners
    - Network scanning
    - Web app scanning
- Enumeration
    - User enumeration
    - Application enumeration
    - Email enumeration
    - War dialing
- 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
    - 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

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

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
  - Common components
    - Spoofing messages
    - Rogue domains
    - Malicious links
    - Malicious attachments
- Shoulder surfing
- Tailgating
- Face-to-face interaction
- Fake portals/malicious websites

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
  - Journals
  - Vulnerability databases
  - Books
  - Blogs
  - Intelligence feeds
  - Security advisories
  - Social network sites
- Common targeted assets
  - Financial information
  - Credit card numbers
  - Account information
  - Intellectual Property
  - PHI
  - PII

Domain 2: Passive Data-Driven Analysis

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
    - 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

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
    - Power shell
- Log correlation
    - SIEMs

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
    - &
    - |
    - ~ or !
    - -
    - .
    - *
    - ?
    - +
    - ( )
    - [ ]
    - $
    - ^
    - \
- Special operators
    - \W
    - \w
    - \s
    - \D
    - \d
    - \b
    - \c

Domain 3: Active Asset and Network Analysis

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
  - nbtstat
- File system
  - dir
  - pe explorer
  - disk utilization tool
- Processes
  - TLIST
  - PROCMON
  - Process explorer
- Services
  - Services.msc
  - Msconfig
  - Net start
  - Task scheduler
- Volatile memory analysis
- Active Directory tools

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

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

3.3 Summarize methods and tools used for malware analysis

- Methods

    - Sandboxing
        - Virtualization
    - Threat intelligence websites
        - Crowd source signature detection
        - Virus total
- Reverse engineering tools
    - IDA
    - Ollydbg
- General tools
    - strings
    - Antivirus
    - Malware scanners

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: Incident Response Lifecycle

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

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

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

4.4 Explain general mitigation methods and devices

- Methods
    - System hardening
        - Deactivate unnecessary services
        - Patching
    - Updating internal security devices
        - Report malware signatures
        - Custom signatures
    - Block external sources of malware
    - DNS filtering
    - Blackhole routing
    - System and application isolation
    - Mobile device management

    - Application whitelist
- Devices
    - Firewall
    - WAF
    - Switch
    - Routers
    - Proxy
    - Virtual Machine
    - Mobile
    - Desktop
    - Server

Continuing Education Requirements

The *CyberSec First Responder* (CFR-210) certification is valid for 3 years from the time certification is granted. You must re-take the most up-to-date version of the exam prior to the 3-year period's end to maintain a continuously valid certification.

To view the Logical Operations Candidate Agreement, click here.

Then purchase a voucher to take the exam by clicking here.

CyberSec First Responder ACRONYMS

Acronym	Expanded Form
ADS	Alternate Data Stream
ARP	Address Resolution Protocol
AV	Antivirus
BASH	Bourne Again Shell
CAM	Content Addressable Memory
CSRF	Cross-site Request Forgery
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FTK	Forensic Tool Kit
FTP	File Transfer Protocol
GREP	Global Regular Expression Print
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
IDS	Intrusion Detection System
IM	Instant Message

IP	Internet Protocol
IPS	Intrusion Prevention System
IRC	Internet Relay Chat
LFI	Local File Inclusion
LOIC	Low Orbit Ion Cannon
LSOF	List Open Files
NAT	Network Address Translation
NBNS	NetBIOS Name Service
NIPS	Network Intrusion Prevention System
OEM	Original Equipment Manufacturer
PE	Portable Executable
PHI	Protected Health Information
PII	Personally Identifiable Information
QR	Quick Response
RFI	Remote File Inclusion
SIEM	Security Information Event Management
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SSH	Secure Shell
VPN	Virtual Private Network
WAF	Web Application Firewall
WAP	Wireless Access Point
WIPS	Wireless Intrusion Prevention System
WMIC	Windows Management Instrumentation Command Line