CertNexus®

CyberSec First Responder® – Advanced (CFR-A) Exam CFA-110 Blueprint

Date Issued: 9/30/2024
Date Modified: 9/30/2024
Version: 1.0

CFR Advanced

Introduction to CertNexus

CertNexus is a vendor-neutral certification body, providing emerging technology certifications and micro-credentials for business, data, developer, IT, and security professionals. CertNexus' mission is to assist closing the emerging tech global skills gap while providing individuals with a path towards rewarding careers in Cybersecurity, Data Science, Data Ethics, Internet of Things, and Artificial Intelligence (AI)/ Machine Learning (ML).

Acknowledgements

CertNexus was honored to have the following Subject Matter Experts contribute to the development of this exam blueprint.

Brian S. Wilson

CyberSec First Responder® – Advanced (CFR-A) Exam CFA-110

Exam Information

Candidate Eligibility

The CFR-A assessment requires no application fee, supporting documentation, or other eligibility verification measures for you to be eligible to take it. Simply purchase an access key for the *CyberSec First Responder® – Advanced (CFR-A): Applying Your Security Expertise (Exam CFA-110)* course from the CertNexus Store here. This course includes access to the credential process directly through the CHOICE platform.

Exam Prerequisites

Successful candidates should have knowledge of advanced cybersecurity concepts and possess practical skills from both a red-team (offensive) and blue-team (defensive) perspective. It is recommended that candidates acquire this level of knowledge and skills by attending the CertNexus® *CyberSec First Responder® – Advanced (CFR-A): Applying Your Security Expertise (Exam CFA-110)* course prior to taking the assessment.

Exam Specifications

Number of Items: 25

Passing Score: 80% or 20/25 items

Duration: Estimated 20–45 minutes; candidates may retake as many times as desired

Exam Options: Online through the CHOICE platform

Item Formats: Multiple Choice/Multiple Response

Upon successful completion, candidates will earn the CertNexus CFR-A credential.

Exam Description

Target Audience:
The CFR-A assessment is primarily designed for cybersecurity practitioners in various red-team or blue-team roles who wish to validate their knowledge of advanced techniques for securing the organization and its assets. Other individuals who wish to validate advanced cybersecurity knowledge are also candidates for this assessment.

Exam Objective:
Upon successful completion of the CFR-A assessment, cybersecurity professionals will demonstrate an understanding of advanced cybersecurity techniques, how they can be used to simulate attacks on organizational environments for the purposes of testing security, how to analyze attacks to learn more about their operation and impact, and how to implement protections that minimize the effects of those attacks.

To ensure that candidates possess the aforementioned knowledge, skills, and abilities, the CFR-A assessment will test them on the following domains with the following weightings:

Domain	% of Examination
1.0 Attack Computing Environments to Test Cybersecurity	52%
2.0 Analyze Attacks on Computing Environments	20%
3.0 Address the Security Concerns of Computing Environments	28%
Total	**100%**

The information that follows is meant to help you prepare for your credential assessment. This information does not represent an exhaustive list of all the concepts and skills that you may be tested on during your assessment. The domains, identified previously and included in the objectives listing, represent the large content areas covered in the assessment. 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 this information represents the industry-expert analysis of the job role(s) related to the credential and does not necessarily correlate one-to-one with the content covered in your training program or on your assessment. We strongly recommend that you study independently to familiarize yourself with any concept identified here that was not explicitly covered in your training program or products.

Domains and Objectives

Domain 1.0 Attack Computing Environments to Test Cybersecurity [52%]

Objective 1.1 Perform reconnaissance on target systems and networks.

- Recon subtasks
  - Footprinting
  - Fingerprinting
  - Scanning
  - Enumeration
- Recon tools
  - Nmap
  - Burp Suite
  - OWASP ZAP
  - Dirbuster/Gobuster
  - Spreadsheet/database to store findings
- Nmap scan modes
  - Port scan
  - Service scan
  - OS scan
- Nmap results interpretation
- Traffic interception and interpretation with web proxies

Objective 1.2 **Select and launch exploits using Metasploit.**

- Metasploit Framework
- Module types
  - exploits
  - payloads
  - auxiliary
- Module search
- Module options
- Exploitation shell methods
  - Bind
  - Reverse
- Exploitation shell types
  - Ruby
  - Perl
  - Meterpreter

Objective 1.3 **Exploit vulnerabilities in software.**

- Attack types
  - Credential harvesting
  - Password cracking
  - Code execution/injection
  - Data exfiltration
  - Malware infection
- Post-exploitation behaviors
  - C&C
  - APTs
  - Privilege elevation/escalation
  - Lateral movement/pivoting
- Exploit/payload selection
  - Informed by active recon
  - Informed by general research (e.g., CVEs)
- Specific vulnerabilities in unpatched/outdated software

Objective 1.4 **Exploit web-application vulnerabilities.**

- Vulnerabilities and attacks
  - XSS
  - CSRF
  - SSRF
  - XXE
  - SQL injection
  - Path traversal
  - File inclusion
  - Unrestricted file uploads
- Information disclosure through web proxies
- Vulnerable forms and fields
- URL encoding
- Inadequate input validation
- Malicious code injection
- Web shells

Objective 1.5 **Exploiting vulnerabilities in systems.**

- Access vulnerabilities/attacks
  - Online password cracking
  - Offline password cracking
  - Credential sniffing
  - Backdoors
- Network vulnerabilities/attacks
  - ARP poisoning/spoofing
  - DNS poisoning/spoofing
  - Session hijacking
  - DDoS
- Data vulnerabilities
  - Lack of or weak encryption
  - Lack of or weak access control
- File-configuration vulnerabilities
  - Poorly configured permissions
  - Misconfigurations in system files
- C&C aspects
  - Bots
  - Beaconing
  - Controllers
- Automation scripts
  - Python
  - Bash
- Cracking utilities
  - Hydra
  - John the Ripper
  - Wordlists
- Sniffers/protocol analyzers
  - Wireshark
  - TShark
- Man-in-the-middle tools
  - Ettercap
  - bettercap
- Social engineering
  - Pharming
  - Phishing

Domain 2.0 Analyze Attacks on Computing Environments [20%]

Objective 2.1 Analyze logs for signs of attack.

- SIEMs and other log-analysis platforms
  - Wazuh
  - Graylog
  - ELK stack
  - Splunk
  - Datadog
- Log files of interest
  - System logs
  - Authentication logs
  - Kernel logs
  - Web-server logs
- Collection and aggregation of log data
- Analysis techniques and components
  - Log filtering and searching
  - Log-data visualization
  - Event context
  - Event severity/criticality
  - Noise reduction
  - Saved searches/queries
- Threat hunting
  - Event correlation
  - Patterns of suspicious events/behavior
  - Threat intelligence

Objective 2.2 Detect attacks using active monitoring systems.

- Active monitoring solutions
  - IDS/IPS
  - SIEM
  - EDR
  - XDR
  - TIP
  - SOAR
  - CASB
- File-integrity monitoring
  - Creation, modification, and deletion of files
  - Alerts and reports
  - Scan schedules

- Network-traffic monitoring
  - Detection rules
  - Rule scripting
  - Spoofing detection
  - Beaconing detection
  - Whitelisting
  - Traffic content/inspection
  - Detection logs
- IDS/IPS tools
  - Snort
  - Suricata
  - Zeek

Objective 2.3 Perform digital forensics.

- Process/phases
  - Pre-process
  - Acquisition/preservation
  - Analysis
  - Presentation
  - Post-process
- Volatile-memory capturing
  - Forensically sound tools (e.g., AVML)
  - Importance of capturing quickly
  - Importance of minimizing interaction with target system
  - Chain of custody
  - Virtual files representing physical memory
  - Compression
  - Symbol tables
- Memory-dump analysis
  - Forensically sound tools (e.g., Volatility)
  - Shell history
  - Environment variables
  - Kernel messages
  - Memory maps
  - Running processes/services
  - Socket status
- Reverse-engineering malware
  - Disassembly
  - Decompilation
  - Debugging
  - Opcodes
  - Compiled vs. interpreted languages

Domain 3.0 Address the Security Concerns of Computing Environments [28%]

Objective 3.1 Protect data.

- Data security
  - Authorized access only
  - Protect against corruption
  - Protect against theft
- Data lifecycle protections
  - At rest
  - In transit
  - In use
- Backup and recovery processes
  - Implementation
  - Partitioning
  - Strong encryption
  - Strong access control
  - Compliance with policies
- Encryption considerations
  - Symmetric vs. asymmetric
  - Key length
  - Key management/security
  - Block-cipher modes
- Protection of data-management interfaces
  - MySQL
  - phpMyAdmin

Objective 3.2 Protect access.

- Access security
  - IAM
  - Least privilege
  - Adequate file/directory permissions
  - Secure authentication/authorization methods/protocols (e.g., SSH)
  - MFA/2FA
  - Logging of authentication failures/successes
- Strong password policies
  - Complexity
  - Length
  - History
  - Expiration
- Protection against brute-force attacks
  - Account lockout
  - Ban durations
  - Max retries
  - Failure intervals

Objective 3.3 **Protect software.**

- Software security
  - Patching
  - Assessment/testing of updates
  - Static code analysis
  - Dynamic software analysis
  - Secure coding practices
- Protection against injection attacks
  - Static queries
  - Prepared statement/parameterized queries
  - Stored procedures
  - Input validation
- Protection against XSS attacks
  - Input sanitization
  - Use of modern sanitization functions
  - Consistent application of sanitization
- Protection against CSRF attacks
  - Anti-CSRF tokens
  - Server-side checking of tokens
- Protection against file-based attacks
  - Validation of file extensions
  - Validation of `Content-Type` headers
  - Scrubbing of metadata
  - Re-encoding of uploaded files

Objective 3.4 **Protect networks and systems.**

- Network/system security
  - Firewalls/IPSs
  - Network segmentation
  - Secure protocols (e.g., HTTPS and SFTP)
  - System audits
  - Hardening of services/software
  - Change management
- Hardening opportunities
  - Updating of outdated software
  - Strengthening of authentication mechanisms
  - Tightening of file/directory permissions
  - Limiting of exposed network information
  - Increasing restrictions on specific services
  - Installing security software (e.g., anti-malware)

CFR-A Acronyms

Acronym	Expanded Form
2FA	Two-factor authentication
AES	Advanced Encryption Standard
AOT	Ahead of time
APT	Advanced persistent threat
AVML	Acquire Volatile Memory for Linux
C&C/C2	Command and control
CASB	Cloud-access security broker
CBC	Cipher-block chaining
CGI	Common Gateway Interface
CSRF	Cross-site request forgery
CVE	Common Vulnerabilities and Exposures
DDoS	Distributed denial of service
DOM	Document Object Model
DQL	Dashboards Query Language
DTD	Document-type definition
DVWA	Damn Vulnerable Web App
ECB	Electronic codebook
EDR	Endpoint detection and response
ELF	Executable and Linkable Format
ELK	Elasticsearch, Logstash, Kibana
GCFIM	Generic Computer Forensic Investigation Model
HIDS	Host-based intrusion detection system
HIPS	Host-based intrusion prevention system
HSQLDB	Hyper SQL Database
IAM	Identity and access management
IDS	Intrusion detection system
IPC	Interprocess communication
IPS	Intrusion prevention system
ISF	Intermediate Symbol Format

IV	Initialization vector
JDBC	Java Database Connectivity
JSON	JavaScript Object Notation
LFI	Local file inclusion
LiME	Linux Memory Extractor
LSB	Linux Standard Base
LTS	Long-term support
MFA	Multi-factor authentication
MITM	Man in the middle
NIDS	Network-based intrusion detection system
NIPS	Network-based intrusion prevention system
NIST	National Institute of Standards and Technology
OSINT	Open-source intelligence
OST	Open Source Tripwire
OTP	One-time password
OWASP	Open Worldwide Application Security Project
PAM	Pluggable authentication module
RFI	Remote file inclusion
RSA	Rivest–Shamir–Adleman
SET	Social-Engineer Toolkit
SIEM	Security information and event management
SOAR	Security orchestration, automation, and response
SPAN	Switch Port Analyzer
SSRF	Server-side request forgery
TIP	Threat intelligence platform
XSS	Cross-site scripting
XDR	Extended detection and response
XOR	Exclusive OR
XXE	XML external entities
ZAP	Zed Attack Proxy

CertNexus offers personnel certifications and micro-credentials in a variety of emerging technology skills including Cybersecurity, Cyber Secure Coding, the Internet of Things (IoT), IoT Security, Data Science, Artificial Intelligence, and Data Ethics. For a complete list of our credentials visit https://certnexus.com/certification/.

CERTNEXUS®

1150 University Ave, Suite 20, Rochester, NY 14607
1-800-326-8724 | info@certnexus.com
certnexus.com