301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

View Full Course Details including Latest Schedule Online

CERTNEXUS

CFR (CyberSec First Responder)

BONUS! Cyber Phoenix Subscription Included: All Phoenix TS students receive complimentary ninety (90) day access to the Cyber Phoenix learning platform, which hosts hundreds of expert asynchronous training courses in Cybersecurity, IT, Soft Skills, and Management and more!

Course Overview

Phoenix TS' CyberSec First Responder (CFR) course covers network defense and incident response methods, tactics, and procedures.

This course also covers network defense and incident response methods, tactics, and procedures are taught in alignment with industry frameworks such as NIST 800-61 r.2 (Computer Security Incident Handling), US-CERT's NCISP (National Cyber Incident Response Plan), and Presidential Policy Directive (PPD) 41 on Cyber Incident Coordination Policy. It is ideal for candidates who have been tasked with the responsibility of monitoring and detecting security incidents in information systems and networks, and for executing standardized responses to such incidents. The course introduces tools, tactics, and procedures to manage cybersecurity risks, identify various types of common threats, evaluate the organization's security, collect and analyze cybersecurity intelligence and remediation/report incidents as they occur. This course provides a comprehensive methodology for individuals responsible for defending the cybersecurity of their organization.

Schedule

DATE	LOCATION	
8/04/25 - 8/08/25 (5 days)	**Online/Virtual** Open	Contact Us
11/10/25 - 11/14/25 (5 days)	**Online/Virtual** Open	Contact Us
1/26/26 - 1/30/26 (5 days)	**Online/Virtual** Open	Contact Us

301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

DATE	LOCATION	
4/06/26 - 4/10/26 (5 days)	**Online/Virtual** Open	Contact Us
8/03/26 - 8/07/26 (5 days)	**Online/Virtual** Open	Contact Us
12/14/26 - 12/18/26 (5 days)	**Online/Virtual** Open	Contact Us

Course Objectives

- Compare and contrast various threats and classify threat profile
- Explain the purpose and use of attack tools and technique
- Explain the purpose and use of post exploitation tools and tactic
- Explain the purpose and use of social engineering tactic
- Given a scenario, perform ongoing threat landscape research and use data to prepare for incident
- Explain the purpose and characteristics of various data source
- Given a scenario, use appropriate tools to analyze log
- Given a scenario, use regular expressions to parse log files and locate meaningful data
- Given a scenario, use Windows tools to analyze incidents
- Given a scenario, use Linux-based tools to analyze incidents
- Summarize methods and tools used for malware analysis
- Given a scenario, analyze common indicators of potential compromise
- Explain the importance of best practices in preparation for incident response
- Given a scenario, execute incident response process
- Explain the importance of concepts that are unique to forensic analysis
- Explain general mitigation methods and devices

Program Level

Advanced

Training Delivery Methods

Group Live

Duration

5 Days / 32 hours Training

CPE credits

26 NASBA CPE Credits

Field of Study

Information Technology

Advanced Prep

N/A

Course Registration

Candidates can choose to register for the course by via any of the below methods:

- Email: Sales@phoenixts.wpenginepowered.com
- Phone: 301-582-8200
- Website: www.phoenixts.wpenginepowered.com

Upon registration completion candidates are sent an automated course registration email that includes attachments with specific information on the class and location as well as pre-course study and test preparation material approved by the course vendor. The text of the email contains a registration confirmation as well as the location, date, time and contact person of the class.

Online enrolment closes three days before course start date.

On the first day of class, candidates are provided with instructions to register with the exam provider before the exam date.

Complaint Resolution Policy

To view our complete Complaint Resolution Policy policy please click here: Complaint Resolution Policy

Refunds and Cancellations

To view our complete Refund and Cancellation policy please click here: Refund and Cancellation Policy

PhoenixTS

301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

Course Outline

Assessment of Information Security Risks

- The importance of risk management
- Assess risk
- Mitigate risk
- Integrating documentation into risk management

Analyzing the Threat Landscape

- Classify threats and threat profiles
- Perform ongoing threat research

Computing and Network Environments: Analyzing Reconnaissance Threats

- Implementation of threat modeling
- Reconnaissance: assessing the impact
- Social engineering: assessing the impact

Analyzing Attacks on Computing and Network Environments

- System hacking attacks: assessing the impact
- Web-based attacks: assessing the impact
- Malware: assessing the impact
- Hijacking and impersonation attacks: assessing the impact
- DoS incidents: assessing the impact
- Threats to mobile security: assessing the impact
- Threats to cloud security: assessing the impact

Examining Post-Attack Techniques

- Examine command and control techniques
- Examine persistence techniques
- Examine lateral movement and pivoting techniques
- Examine data ex-filtration techniques

- Examine anti-forensics techniques

Manage Vulnerabilities in the Organization

- Implement a vulnerability management plan
- Examine common vulnerabilities
- Conduct vulnerability scans

Evaluate Security by Implementing Penetration Testing

- Conduct penetration tests on network assets
- Follow up on penetration testing

Collecting Cybersecurity Intelligence

- Deployment of a security intelligence collection and analysis platform
- Data collection from network-based intelligence sources
- Data collection from host-based intelligence sources

Analyze Log Data

- Common tools to analyze logs
- Course content (cont.)
- SIEM tools for analysis

Performing Active Asset and Network Analysis

- Analyze incidents using Windows-based tools
- Analyze incidents using Linux-based tools
- Analyze malware
- Analyze indicators of compromise

Response to Cybersecurity Incidents

- Deployment of incident handling and response architecture
- Containment and mitigation of incidents
- Preparation for forensic investigation as a CSIRT

Investigating Cybersecurity Incidents

- Use a forensic investigation plan
- Securely collect and analyze electronic evidence
- Follow up on the results of an investigation
- Appendix A: mapping course content to CyberSec First Responder (Exam CFR-310)
- Appendix B: regular expressions
- Appendix C: security resources
- Appendix D: U.S. Department of Defense operational security practices

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

Exam Details

- Exam: CFR-310
- Up to 100 Questions
- Types of Questions: Multiple choice and multiple response
- Passing Score: 70% or 71%, depending on exam form. Forms have been statistically equated.
- Test Duration: 120 minutes
- Test Delivery: Pearson VUE

Domain	% of Exam
Threats and Attacks	24%
Data Collection and Analysis	23%
Incident Response Methods, Tools, and Techniques	22%
The Incident Response Process	18%
Vulnerability Assessment	13%

CFR Certification Training FAQs

Who should attend this training?

This course is designed primarily for cybersecurity practitioners preparing for or who currently perform job functions related to protecting information systems by ensuring their availability, integrity, authentication,

confidentiality, and non-repudiation.

It is ideal for those roles within federal contracting companies, and private sector firms who whose mission or strategic objectives require the execution of Defensive Cyber Operations (DCO) or DoD Information Network (DODIN) operation and incident handling. This course focuses on the knowledge, ability, and skills necessary to provide for the defense of those information systems in a cybersecurity context, including protection, detection, analysis, investigation, and response processes.

In addition, the course ensures that all members of an IT team—regardless of size, rank or budget—understand their role in the cyber defense, incident response, and incident handling process.

BONUS! Cyber Phoenix Subscription Included: All Phoenix TS students receive complimentary ninety (90) day access to the Cyber Phoenix learning platform, which hosts hundreds of expert asynchronous training courses in Cybersecurity, IT, Soft Skills, and Management and more!

Phoenix TS is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints re-garding registered sponsors may be submitted to the National Registry of CPE Sponsors through its web site: www.nasbaregistry.org

Starting at **$2,395**

Price Match Guarantee

We'll match any competitor's price quote. Call 301-258-8200 Option 4.

301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

Included in this **CFR (CyberSec First Responder)**

- 5 days instructor-led training
- CFR (CyberSec First Responder) training book
- Notepad, pen and highlighter
- Variety of bagels, fruits, doughnuts and cereal available at the start of class*
- Tea, coffee and soda available throughout the day*
- Freshly baked cookies every afternoon*