COURSE SYLLABUS

# CyberSec First Responder® (CFR) Certification Training Course (Self-Paced)

This self-study course includes the CFR eLearning, test prep guide, labs, and exam voucher. CFR covers network defense and incident response methods, tactics, and procedures that are in alignment with industry frameworks such as NIST 800-61r2 (Computer Security Incident Handling Guide), US-CERT's National Cyber Incident Response Plan (NCIRP), and Presidential Policy Directive (PPD)-41 on Cyber Incident Coordination, NIST 800.171r2 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations).

> Group classes in Live Online and onsite training is available for this course. For more information, email onsite@graduateschool.edu or visit: https://sdfm.graduateschool.edu/courses/cybersec-first-responder-cfr-certification-training

CustomerRelations@graduateschool.edu • (888) 744-4723

## Course Outline

### Module 1: Assessing Cybersecurity Risk

- Identify the importance of risk management
- Assess risk in the organization's environment
- Implement strategies to mitigate risks
- Integrate documentation into the risk management process

### Module 2: Analyzing the Threat Landscape

- Classify various cybersecurity threats
- Analyze trends that affect an organization’s security posture

### Module 3: Analyzing Reconnaissance Threats

- Implement threat modeling techniques
- Assess the impact of reconnaissance on the organization
- Understand the effects of social engineering attacks

### Module 4: Analyzing Attacks on Computing and Network Environments

- Assess system hacking and web-based attack impacts
- Evaluate the impact of malware, hijacking, and impersonation attacks
- Understand the implications of DoS incidents
- Analyze threats to mobile and cloud security

### Module 5: Analyzing Post-Attack Techniques

- Examine command and control techniques used by attackers
- Evaluate persistence, lateral movement, and pivoting techniques
- Analyze data exfiltration and anti-forensics techniques

### Module 6: Assessing the Organization's Security Posture

- Implement cybersecurity auditing practices
- Develop and execute a vulnerability management plan
- Conduct penetration testing

### Module 7: Collecting Cybersecurity Intelligence

- Deploy a security intelligence collection and analysis platform
- Collect data from network-based and host-based intelligence sources

### Module 8: Analyzing Log Data

- Use common tools to analyze log data
- Utilize SIEM tools for analysis

### Module 9: Performing Active Asset and Network Analysis

- Analyze incidents with Windows-based and Linux-based tools
- Investigate indicators of compromise

### Module 10: Responding to Cybersecurity Incidents

- Deploy incident handling and response architecture
- Mitigate cybersecurity incidents effectively
- Hand over incident information for forensic investigation

### Module 11: Investigating Cybersecurity Incidents

- Apply a forensic investigation plan
- Securely collect and analyze electronic evidence
- Follow up on investigation results