PURPLE GRIFFON
The IT Service Management Training & Consultancy Specialists

Course Title: CyberSec First Responder	**Course Duration**: 5.0 Days
Exam: Not Included	**Exam Type**: Proctored Exam
Qualification: CyberSec First Responder Certificate	

Course Syllabus

Our CyberSec First Responder training course contains the following modules:

Module 1: Assessing Information Security Risk

- Topic A: Identify the Importance of Risk Management
- Topic B: Assess Risk
- Topic C: Mitigate Risk
- Topic D: Integrate Documentation into Risk Management

Module 2: Analysing the Threat Landscape

- Topic A: Classify Threats and Threat Profiles
- Topic B: Perform Ongoing Threat Research

Module 3: Analysing Reconnaissance Threats to Computing and Network Environments

- Topic A: Implement Threat Modeling
- Topic B: Assess the Impact of Reconnaissance
- Topic C: Assess the Impact of Social Engineering

Module 4: Analysing Attacks on Computing and Network Environments

- Topic A: Assess the Impact of System Hacking Attacks
- Topic B: Assess the Impact of Web-Based Attacks
- Topic C: Assess the Impact of Malware
- Topic D: Assess the Impact of Hijacking and Impersonation Attacks
- Topic E: Assess the Impact of DoS Incidents
- Topic F: Assess the Impact of Threats to Mobile Security
- Topic G: Assess the Impact of Threats to Cloud Security

Module 5: Analysing Post-Attack Techniques

- Topic A: Assess Command and Control Techniques
- Topic B: Assess Persistence Techniques
- Topic C: Assess Lateral Movement and Pivoting Techniques
- Topic D: Assess Data Exfiltration Techniques
- Topic E: Assess Anti-Forensics Techniques

Module 6: Managing Vulnerabilities in the Organisation

- Topic A: Implement a Vulnerability Management Plan
- Topic B: Assess Common Vulnerabilities
- Topic C: Conduct Vulnerability Scans

Module 7: Implementing Penetration Testing to Evaluate Security

- Topic A: Conduct Penetration Tests on Network Assets
- Topic B: Follow Up on Penetration Testing

Module 8: Collecting Cyberecurity Intelligence

- Topic A: Deploy a Security Intelligence Collection and Analysis Platform
- Topic B: Collect Data from Network-Based Intelligence Sources
- Topic C: Collect Data from Host-Based Intelligence Sources

Module 9: Analysing Log Data

- Topic A: Use Common Tools to Analyse Logs
- Topic B: Use SIEM Tools for Analysis

Module 10: Performing Active Asset and Network Analysis

- Topic A: Analyse Incidents with Windows-Based Tools
- Topic B: Analyse Incidents with Linux-Based Tools
- Topic C: Analyse Malware
- Topic D: Analyse Indicators of Compromise

Module 11: Responding to Cybersecurity Incidents

- Topic A: Deploy an Incident Handling and Response Architecture
- Topic B: Contain and Mitigate Incidents
- Topic C: Prepare for Forensic Investigation as a CSIRT

Module 12: Investigating Cybersecurity Incidents

- Topic A: Apply a Forensic Investigation Plan
- Topic B: Securely Collect and Analyse Electronic Evidence
- Topic C: Follow Up on the Results of an Investigation

Appendix A: Mapping Course Content to CyberSec First Responder™ (Exam CFR-410)

Appendix B: Regular Expressions

Appendix C: Security Resources

Appendix D: U.S. Department of Defense Operational Security Practices

Course Overview

Our five-day CyberSec First Responder training course takes a holistic approach to prepare IT Professionals to analyse threats, secure networks, and utilise critical problem-solving skillsets to protect an organisation from threats. Following the principles of **Detect**, **Analyse** and **Respond,** attendees will gain the knowledge and practical skills needed to recover from attacks and thwart potential future threats.

Course Learning Outcomes

Our CyberSec First Responder training course will yield the following benefits:

- Effectively identify malicious activities involving computing systems.
- Assess information security risks in network environments.
- Collect cyberSecurity intelligence to prepare for assessments.
- Develop the skills needed to cut the lag time between when a breach occurs and when it is detected.
- Assess the risks and vulnerabilities to analyse and determine the scope in an immersive, hands-on environment.
- Effectively protect critical information systems before, during, and after an attack.
- Analyse post-attack techniques and apply skills to respond proactively.

Audience

Our CyberSec First Responder training course is available for individuals with backgrounds including but not limited to:

- Cybersecurity Analysts
- Network Administrators
- Incident Response Specialists
- Security Operations Center (SOC) Analysts
- IT Security Professionals

Entry-Level Requirements

The entry-level requirements for our CyberSec First Responder training course are as follows:

At least 3-5 years of experience working in an IT environment and familiarity with networks, systems, administration, etc.

Recommended Reading

There is no recommended reading for our CyberSec First Responder training course.

What's Included

Our CyberSec First Responder training course includes the following:

- Pre-reading
- Course Manual
- Quizzes
- Exercises

Exam Information

CyberSec First Responder Certificate Exam:

This CyberSec First Responder Certification course prepares you for the new CFR-410 exam and is accredited by ANSI, a requirement for DoD 8570.

- **Questions:** 80
- **Passing Score:** 70% or 73% Depending On Exam Form.
- **Duration:** 120 Minutes
- **Exam Options:** Online Via Pearson OnVUE
- **Format:** Multiple Choice

What's Next

Our Certified Cyber Security Foundation & Practitioner training course will give you the skills required to deliver infrastructure, application, information and operational cyber security by implementing appropriate technical and organisational controls. It also prepares you to pass the internationally recognised IBITGQ (C CS F) and (C CS P) examinations on the first attempt.

Additional Information

Becoming a CyberSec First Responder can offer several benefits, both professionally and personally. Here are some key advantages:

- **High Demand and Career Opportunities**: The field of cybersecurity is growing rapidly, and there is a significant demand for skilled professionals who can effectively respond to cyber threats. As a CyberSec First Responder, you will have access to a wide range of career opportunities in industries such as finance, healthcare, government, and technology.
- **Job Security**: With the increasing frequency and complexity of cyber threats, organizations place a high value on professionals who can promptly respond to incidents and protect their systems and data.
- **Competitive Salary**: Due to the specialized nature of the role and the demand for cybersecurity expertise, CyberSec First Responders often receive competitive salaries.
- **Continuous Learning and Skill Development**: The cybersecurity landscape evolves rapidly, with new threats and attack techniques emerging regularly. As a CyberSec First Responder, you will have opportunities for continuous learning and skill development to stay updated with the latest trends, technologies, and countermeasures.
- **Contribution to Organizational Security**: CyberSec First Responders play a crucial role in protecting organizations from cyber threats and minimizing the impact of security incidents.