COURSE OVERVIEW

Course Name:
(CN-CFR+)
CertNexus CyberSec
First Responder

COURSE DURATION: 5 Days

Gauteng:
3rd Floor, 34 Whitely Road
Melrose Arch
Johannesburg
2196

Gauteng:
192 on Bram
192 Bram Fischer Drive
Ferndale, Randburg
Johannesburg
2160

Cape Town:
3rd Floor, Thomas Pattullo Building
19 Jan Smuts St
Cape Town
8000

Durban:
9 Mountview Close
Broadlands
Mount Edgecombe
Durban
4302

☎ 087 941 5764
✉ sales@impactful.co.za
🌐 impactful.co.za

INTRODUCTION

This course covers network defence 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. 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, defend cybersecurity assets, identify various types of common threats, evaluate the organization's security, collect and analyse cybersecurity intelligence, and remediate and report incidents as they occur. This course provides a comprehensive methodology for individuals responsible for defending the cybersecurity of their organization. This course is designed to assist students in preparing for the CertNexus CyberSec First Responder (Exam CFR-410) certification examination. What you learn and practice in this course can be a significant part of your preparation.

IMPACTFUL
Powered by LRMG

DELIVERY METHOD

Our courses have flexible delivery options:

- In-person classroom training at the Impactful training facilities
  - Johannesburg, Durban, Cape Town
- Virtual instructor-led training
- Nationally: on-site at the client

TARGET AUDIENCE

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 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 defence 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 defence, incident response, and incident handling process.

PREREQUISITES

To ensure your success in this course, you should meet the following requirements:

- At least two years (recommended) of experience or education in computer network security technology or a related field.
- The ability or curiosity to recognize information security vulnerabilities and threats in the context of risk management.
- Foundational knowledge of the concepts and operational framework of common assurance safeguards in network environments. Safeguards include, but are not limited to, firewalls, intrusion prevention systems, and VPNs.
- General knowledge of the concepts and operational framework of common assurance safeguards in computing environments. Safeguards include, but are not limited to, basic authentication and authorization, resource permissions, and anti-malware mechanisms.
- Foundation-level skills with some of the common operating systems for computing environments.
- Entry-level understanding of some of the common concepts for network environments, such as routing and switching.
- General or practical knowledge of major TCP/IP networking protocols, including, but not limited to, TCP, IP, UDP, DNS, HTTP, ARP, ICMP, and DHCP.

COURSE OBJECTIVES

In this course, you will identify, assess, respond to, and protect against security threats and operate a system and network security analysis platform.

You will:

- Assess cybersecurity risks to the organization.
- Analyse the threat landscape.
- Analyse various reconnaissance threats to computing and network environments.
- Analyse various attacks on computing and network environments
- Analyse various post-attack techniques.
- Assess the organization's security posture through auditing, vulnerability management, and penetration testing.
- Collect cybersecurity intelligence from various network-based and host-based sources.
- Analyse log data to reveal evidence of threats and incidents.
- Perform active asset and network analysis to detect incidents.
- Respond to cybersecurity incidents using containment, mitigation, and recovery tactics.
- Investigate cybersecurity incidents using forensic analysis techniques

COURSE CONTENT

Lesson 1: Assessing Cybersecurity Risk

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

Lesson 2: Analysing the Threat Landscape

- Topic A: Classify Threats
- Topic B: Analyse Trends Affecting Security Posture

Lesson 3: Analysing Reconnaissance Threats to Computing and Network Environments

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

Lesson 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

Lesson 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

Lesson 6: Assessing the Organization's Security Posture

- Topic A: Implement Cybersecurity Auditing
- Topic B: Implement a Vulnerability Management Plan
- Topic C: Assess Vulnerabilities
- Topic D: Conduct Penetration Testing

Lesson 7: Collecting Cybersecurity 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

Lesson 8: Analysing Log Data

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

Lesson 9: 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 Indicators of Compromise

Lesson 10: Responding to Cybersecurity Incidents

- Topic A: Deploy an Incident Handling and Response Architecture
- Topic B: Mitigate Incidents
- Topic C: Hand Over Incident Information to a Forensic Investigation

Lesson 11: 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