CyberSec First Responder: Threat Detection and Response (CFR)

Today's security professional needs to be able to proactively access an organization's security posture through vulnerability assessment and penetration testing, in addition to threat detection and response. CFR is different because it teaches a response plan. It goes beyond vulnerability analysis and testing, enforcing a more holistic approach to network security. CFR develops the skills needed to proactively defend against cyber attacks, in addition to the knowledge gained from each incident so that it never happens again.

CyberSec First Responders are just that – the first line of response against cyber attacks that cost your organization valuable time and money. The CyberSec First Responder: Threat Detection and Response (CFR) course trains the candidate in cyber security at the ground level.

This training course takes a holistic approach to prepare security professionals to analyze threats, secure networks, handle incidents, and utilize other critical security skills.

The course combines lecture materials and hands-on labs throughout, to make sure that you are able to successfully understand cyber security concepts and to recognize specific threats and attacks on your network.
This course is a great choice for information assurance (IA) personnel who need to develop, operate and maintain secure environments.

The CFR master class will develop the skills professionals need in the real world. Delivered over five days, CFR utilizes an immersive lab environment, hands-on activities and a digital learning platform with curriculum-rich content to ensure every student is equipped with the skills necessary to immediately strengthen their organizations' cybersecurity defences.

CyberSec training is designed to:

- Develop security threat intelligence skills
- Emphasize penetration testing
- Tie together different security tactics
- Allow the organization to secure its networks without having to invest in additional security infrastructure

Doelstellingen training:

– Assess information security risk in computing and network environments
– Create an information assurance lifecycle process
– Analyze threats to computing and networks
– Design and operate secure environments
– Assess security posture within a risk management framework
– Collect cyber security intelligence
– Respond and investigate cyber security incidents
– Audit secure environments

Cursusoutline:

1. Assessing Information Security Risk

- Identify the Importance of Risk Management
- Assess Risk
- Mitigate Risk
- Integrate Documentation into Risk Management

2. Creating an Information Assurance Lifecycle Process

- Evaluate Information Assurance Lifecycle Models
- Align Information Security Operations to the Information Assurance Lifecycle
- Align Information Assurance and Compliance Regulations

3. Analyzing Threats to Computing and Network Environments

- Identify Threat Analysis Models
- Assess the Impact of Reconnaissance Incidents
- Assess the Impact of Systems Hacking Attacks
- Assess the Impact of Malware
- Assess the Impact of Hijacking and Impersonation Attacks
- Assess the Impact of DoS Incidents
- Assess the Impact of Threats to Mobile Security
- Assess the Impact of Threats to Cloud Security

4. Designing Secure Computing and Network Environments

- Information Security Architecture Design Principles
- Design Access Control Mechanisms
- Design Cryptographic Security Controls
- Design Application Security
- Design Computing Systems Security
- Design Network Security

5. Operating Secure Computing and Network Environments

- Implement Change Management in Security Operations
- Implement Monitoring in Security Operations

6. Assessing the Security Posture Within a Risk Management Framework

- Deploy a Vulnerability Management Platform
- Conduct Vulnerability Assessments
- Conduct Penetration Tests on Network Assets
- Follow Up on Penetration Testing

7. Collecting Cybersecurity Intelligence Information

- Deploy a Security Intelligence Collection and Analysis Platform
- Collect Data from Security Intelligence Sources

8. Analyzing Cybersecurity Intelligence Information

- Analyze Security Intelligence to Address Incidents
- Use SIEM Tools for Analysis

9. Responding to Cybersecurity Incidents

- Deploy an Incident Handling and Response Architecture
- Perform Real-Time Incident Handling Tasks
- Prepare for Forensic Investigation

10. Investigating Cybersecurity Incidents

- Create a Forensic Investigation Plan
- Securely Collect Electronic Evidence
- Identify the Who, Why, and How of an Incident
- Follow Up on the Results of an Investigation

11. Auditing Secure Computing and Network Environments

- Deploy a Systems and Processes Auditing Architecture
- Prepare for Audits
- Perform Audits Geared Toward the Information Assurance Lifecycle

Labs:

Lab 1: Implementing a Threat Assessment Model
Lab 2: Examining Reconnaissance Incidents
Lab 3: Assessing the Impact of System Hijacking Attempts
Lab 4: Assessing the Impact of Malware
Lab 5: Assessing the Impact of Hijacking and Impersonation attacks
Lab 6: Assessing the Impact of DoS Incidents
Lab 7: Assessing the Impact of Threats to Mobile Devices
Lab 8: Designing Cryptographic Security Controls
Lab 9: Designing Application Security
Lab 10: Implementing Monitoring in Security Operations
Lab 11: Deploying a Vulnerability Management Platform
Lab 12: Conducting Vulnerability Assessments
Lab 13: Conducting Penetration Testing on Network Assets
Lab 14: Collecting and Analyzing Security Intelligence
Lab 15: Collecting Security Intelligence Data
Lab 16: Capturing and Analyzing Baseline Data
Lab 17: Analyzing Security Intelligence
Lab 18: Incorporating SIEMS into Security Intelligence Analysis
Lab 19: Developing an Incidence Response System
Lab 20: Securely Collecting Electronic Evidence
Lab 21: Analyzing Forensic Evidence
Lab 22: Preparing for an Audit
Lab 23: Performing Audits

Doelgroep:

CyberSec First Responder: Threat Detection and Response, or CFR, is a course designed for information assurance professionals who perform job functions related to the development, operation, management, and enforcement of security capabilities for systems and networks
Ideal for those with 2+ years of experience in IT or information security, CFR prepares cybersecurity professionals for performing numerous tasks within an organization. From developing secure networks to identifying breaches in real time, CFR equips professionals with the skills they need to keep the hackers out.

Examen:

This course prepares students to take the CyberSec First Responder certification exam. This exam consists of 135 multiple choice questions and can be taken directly after the five-day training.