CYBERSEC FIRST RESPONDER: THREAT DETECTION AND RESPONSE

Course Code: 2180

Gain a broad view of how to respond to a cybersecurity incident while preparing for the CyberSec First Responder certification.

This course covers the duties of those who are responsible for monitoring and detecting security incidents in information systems and networks, and for executing a proper response to such incidents. Depending on the size of the organization, this individual may act alone or may be a member of a cybersecurity incident response team (CSIRT). The course introduces tools and tactics to manage cybersecurity risks, identify various types of common threats, evaluate the organization's security, collect and analyze cybersecurity intelligence, and handle incidents as they occur. Ultimately, the course promotes a comprehensive approach to security aimed toward those on the front lines of defense.

This course is designed to assist students in preparing for the CyberSec First Responder certification examination (exam CFR-310). What you learn and practice in this course can be a significant part of your preparation.

This course supports a certification that is a DoD Approved 8570 Baseline Certification and meets DoD 8140/8570 training requirements.

What You'll Learn

- Assess information security risk in computing and network environments.
- Analyze the cybersecurity threat landscape.
- Analyze reconnaissance threats to computing and network environments.
- Analyze attacks on computing and network environments.
- Analyze post-attack techniques on computing and network environments.
- Implement a vulnerability management program.
- Evaluate the organization's security through penetration testing.
- Collect cybersecurity intelligence.
- Analyze data collected from security and event logs.
- Perform active analysis on assets and networks.
- Respond to cybersecurity incidents.
- Investigate cybersecurity incidents.

Who Needs to Attend

This course is designed primarily for cybersecurity practitioners who perform job functions related to protecting information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

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—everyone from help desk staff to the Chief Information Officer - understand their role in these security processes.

Prerequisites

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

- At least two years (recommended) of experience in computer network security technology or a related field.
- The ability to recognize information security vulnerabilities and threats in the context of risk management.
- Foundation-level operational skills with some of the common operating systems for computing environments.
- Foundational 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 understanding of some of the common concepts for network environments, such as routing and switching.
- Foundational knowledge of major TCP/IP networking protocols, including, but not limited to, TCP, IP, UDP, DNS, HTTP, ARP, ICMP, and DHCP.
- 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.

CYBERSEC FIRST RESPONDER: THREAT DETECTION AND RESPONSE

Course Code: 2180

CLASSROOM LIVE	$3,495 CAD	5 days

Classroom Live Outline

Lesson 1: Assessing Information Security Risk

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

Lesson 2: Analyzing the Threat Landscape

- Classify Threats and Threat Profiles
- Perform Ongoing Threat Research

Lesson 3: Analyzing Reconnaissance Threats to Computing and Network Environments

- Implement Threat Modeling
- Assess the Impact of Reconnaissance
- Assess the Impact of Social Engineering

Lesson 4: Analyzing Attacks on Computing and Network Environments

- Assess the Impact of System Hacking Attacks
- Assess the Impact of Web-Based 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

Lesson 5: Analyzing Post-Attack Techniques

- Assess Command and Control Techniques
- Assess Persistence Techniques
- Assess Lateral Movement and Pivoting Techniques

- Assess Data Exfiltration Techniques
- Assess Anti-Forensics Techniques

Lesson 6: Managing Vulnerabilities in the Organization

- Implement a Vulnerability Management Plan
- Assess Common Vulnerabilities
- Conduct Vulnerability Scans

Lesson 7: Implementing Penetration Testing to Evaluate Security

- Conduct Penetration Tests on Network Assets
- Follow Up on Penetration Testing

Lesson 8: Collecting Cybersecurity Intelligence

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

Lesson 9: Analyzing Log Data

- Use Common Tools to Analyze Logs
- Use SIEM Tools for Analysis

Classroom Live 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

CYBERSEC FIRST RESPONDER: THREAT DETECTION AND RESPONSE

Course Code: 2180

VIRTUAL CLASSROOM LIVE	$3,495 CAD	5 days

Virtual Classroom Live Outline

Lesson 1: Assessing Information Security Risk

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

Lesson 2: Analyzing the Threat Landscape

- Classify Threats and Threat Profiles
- Perform Ongoing Threat Research

Lesson 3: Analyzing Reconnaissance Threats to Computing and Network Environments

- Implement Threat Modeling
- Assess the Impact of Reconnaissance
- Assess the Impact of Social Engineering

Lesson 4: Analyzing Attacks on Computing and Network Environments

- Assess the Impact of System Hacking Attacks
- Assess the Impact of Web-Based 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

Lesson 5: Analyzing Post-Attack Techniques

- Assess Command and Control Techniques
- Assess Persistence Techniques
- Assess Lateral Movement and Pivoting Techniques

- Assess Data Exfiltration Techniques
- Assess Anti-Forensics Techniques

Lesson 6: Managing Vulnerabilities in the Organization

- Implement a Vulnerability Management Plan
- Assess Common Vulnerabilities
- Conduct Vulnerability Scans

Lesson 7: Implementing Penetration Testing to Evaluate Security

- Conduct Penetration Tests on Network Assets
- Follow Up on Penetration Testing

Lesson 8: Collecting Cybersecurity Intelligence

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

Lesson 9: Analyzing Log Data

- Use Common Tools to Analyze Logs
- Use SIEM Tools for Analysis

Virtual Classroom Live 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

CYBERSEC FIRST RESPONDER: THREAT DETECTION AND RESPONSE

Course Code: 2180

PRIVATE GROUP TRAINING	5 days

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 9/16/2019 12:46:34 PM