Global Knowledge™

CyberSec First Responder: Threat Detection and Response

Duration: 5 Days **Course Code: GK2180**

Overview:

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 computer security incident response team (CSIRT). The course introduces strategies, frameworks, methodologies, and tools to manage cybersecurity risks, identify various types of common threats, design and operate secure computing and networking environments, assess and audit the organization's security, collect, and analyze cybersecurity intelligence, and handle incidents as they occur. The course also covers closely related information assurance topics such as auditing and forensics to provide a sound basis for a comprehensive approach to security aimed toward those on the front lines of defense. In addition, this course can help students who are looking to fulfill DoD directive 8570.01 for information assurance (IA) training. This program is designed for personnel performing IA functions, establishing IA policies and implementing security measures and procedures for the Department of Defense and affiliated information systems and networks.

Target Audience:

Cybersecurity practitioners who perform job functions related to protecting and defending information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation

Objectives:

- Assess information security risk in computing and network environments
- Create an information assurance lifecycle process
- Analyze threats to computing and network environments
- Design secure computing and network environments
- Operate secure computing and network environments
- Assess the security posture within a risk management framework
- Collect cybersecurity intelligence information
- Analyze collected intelligence to define actionable response
- Respond to cybersecurity incidents
- Investigate cybersecurity incidents
- Audit secure computing and network environments

Prerequisites:

- Cybersecurity Foundations
- Understanding Networking Fundamentals

Content:

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

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

- 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

Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.co.uk

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK