CyberSec First Responder

Course ID #: 7000-118-ZZ-Z

Hours: 35

Course Content

Course Description:

This course covers network defense 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, identify various types of common threats, evaluate the organization's security, collect and analyze 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.

At Course Completion:

After competing this course, student will be able to:

Compare and contrast various threats and classify threat profiles.

- Explain the purpose and use of attack methods and techniques.
- Explain the purpose and use of post-exploitation tools and tactics.
- Explain the purpose and characteristics of various data sources.
- Explain the importance of best practices in preparation for incident response.
- Identify applicable compliance, standards, frameworks, and best practices.
- Explain the importance of concepts that are unique to forensic analysis.
- Identify the common areas of vulnerability.
- Identify the steps of the vulnerability process.

Target Student:

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.

CyberSec First Responder

Course ID #: 7000-118-ZZ-Z

Hours: 35

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.

Topics:

Lesson 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

Lesson 2: Analyzing the Threat Landscape

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

Lesson 3: Analyzing 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

CyberSec First Responder

Course ID #: 7000-118-ZZ-Z

Hours: 35

Lesson 4: Analyzing 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: Analyzing 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: Managing Vulnerabilities in the Organization

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

Lesson 7: Implementing Penetration Testing to Evaluate Security

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

Lesson 8: 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 9: Analyzing Log Data

- Topic A: Use Common Tools to Analyze Logs
- Topic B: Use SIEM Tools for Analysis
- Lesson 10: Performing Active Asset and Network Analysis
- Topic A: Analyze Incidents with Windows-Based Tools
- Topic B: Analyze Incidents with Linux-Based Tools
- Topic C: Analyze Malware
- Topic D: Analyze Indicators of Compromise
- Lesson 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

Lesson 12: Investigating Cybersecurity Incidents

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