CyberSec First Responder: Threat Detection and Response (Exam CFR-210)

Modality: Self-Paced Learning

Duration: 12 Hours

About this course:

This series will help students to understand the anatomy of cyber-attacks. Individuals will gain the skills needed to serve their organizations before, during, and after a breach. A CyberSec First Responder is the first line of defense against cyber-attacks. Students will prepare to analyze threats, design secure computing and network environments, proactively defend networks, and respond/investigate cybersecurity incidents.

The average salary for a Cyber Security Professional is **$105,000** per year.

Course Objectives:

After completing this course, students will be able to:

- 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.
- Evaluate the organization's security posture within a risk management framework.
- 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.

Audience:

- This series is designed for information assurance professionals who perform job functions related to the development, operation, management, and enforcement of security capabilities for systems and networks. This certification could lead to a job as a security administrator, network administrator, or system administrator.

Prerequisites:

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

- At least two years (recommended) of experience in computer network security technology or a related field.

- Recognize information security vulnerabilities and threats in the context of risk management.
- Operate at a foundational level 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.
- Operate at a foundational level 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 virtual private networks (VPNs).

Sugessted Prerequisite Courses:

- CompTIA® A+®: A Comprehensive Approach (Exams 220-901 and 220-902)
- CompTIA® Network+® (Exam N10-006)
- CompTIA® Security+® (Exam SY0-401)

Course Outline:

- **Module 01 - Assessing Information Security Risk**
- **Module 02 - Analyzing the Threat Landscape**
- **Module 03 - Analyzing Reconnaissance Threats to Computing and Network Environments**
- **Module 04 - Analyzing Attacks on Computing and Network Environments**
- **Module 05 - Analyzing Post-Attack Techniques**
- **Module 06 - Evaluating the Organization?s Security Posture**
- **Module 07 - Collecting Cybersecurity Intelligence**
- **Module 08 - Analyzing Log Data**
- **Module 09 - Performing Active Asset and Network Analysis**
- **Module 10 - Responding to Cybersecurity Incidents**
- **Module 11 - Investigating Cybersecurity Incidents**