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

Modality: On Demand

Duration: 12 Hours

About this course:

This arrangement will assist understudies with understanding the life structures of cyber-attacks. Individuals will gain the aptitudes expected to serve their associations before, during, and after a rupture. CyberSec First Responder is the main line of protection against digital assaults. Understudies will get ready to analyze dangers, structure secure computing, and network conditions, proactively protect networks and react/investigate cybersecurity incidents.

The normal compensation for a Cyber Security Professional is $105,000 every year.

Course Objectives:

- Evaluate the risk of information security in computing and system situations.
- Investigate the cybersecurity danger landscape.
- Investigate observation dangers to computing and system situations.
- Investigate assaults on computing and network situations.
- Investigate post-assault methods in computing and system situations.
- Assess the association's security act within a hazard the board structure.
- Gather cybersecurity intelligence.
- Break down information gathered from security and event logs.
- Perform a dynamic examination of networks and assets.
- React to cybersecurity incidents.
- Investigate cybersecurity incidents.

Audience:

This arrangement is intended for information affirmation experts who perform work capacities identified with the improvement, activity, the executives, and implementation of security abilities for frameworks and networks. This credential could prompt an occupation as a network administrator, security administrator, or system administrator.

Prerequisites:

To guarantee your accomplishment in this course, you ought to have the following prerequisites:

- In any event, two years (suggested) of involvement with computer network security innovation or a related field.
- Perceive information security dangers and vulnerabilities with regard to risk administration.
- Work at a basic level common operating framework for computing conditions.

- Basic information on the ideas and operational system of common assurance safeguards in computing situations. Safeguards include, but are not restricted to, fundamental authorization and authentication, asset authorizations, and hostile to malware instruments.
- Work at a primary level basic ideas for network conditions, for example, routing and switching.
- Primary information on significant protocols of TCP/IP networking, including, but not constrained to, TCP, IP, HTTP, ARP, UDP, DNS, ICMP, and DHCP.

Suggested Prerequisite Courses:

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

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**