CYBERSEC FIRST RESPONDER™

ADASTANETWORK

CYBERSEC FIRST RESPONDER (CFR-410)

5 DAYS TRAINING

DATE: 08 - 12 JANUARY 2024

VENUE: BANGSAR SOUTH

Overview

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, NIST 800.171r2 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations).

Who Should Attend

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.

Pre-Requisite

A good knowledge in computer network security technology or a related field.

Course Objective

- Assess cybersecurity risks to the organization.
- Analyze the threat landscape.
- Analyze various reconnaissance threats to computing and network environments.
- Analyze various attacks on computing and network environments.
- Analyze various post-attack techniques.
- Assess the organization's security posture through auditing, vulnerability management, and penetration testing.
- Collect cybersecurity intelligence from various network-based and host-based sources.
- Analyze log data to reveal evidence of threats and incidents.
- Perform active asset and network analysis to detect incidents.
- Respond to cybersecurity incidents using containment, mitigation, and recovery tactics.
- Investigate cybersecurity incidents using forensic analysis techniques

HRDCORP CLAIMABLE

CERTNEXUS

SCAN FOR REGISTER

603 2242 0550 / 6011 2898 8992

inquiry@adastanetwork.asia

ADASTANETWORK SDN BHD
Unit 10-01,The Vertical II,Tower B,
Avenue 3,Bangsar South City,
No.8, Jalan Kerinchi,
59200 Kuala Lumpur.

COURSE CONTENT

CYBERSEC FIRST RESPONDER™

Lesson 1: Assessing Cybersecurity 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
Topic B: Analyze Trends Affecting Security Posture
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
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: Assessing the Organization's Security Posture
Topic A: Implement Cybersecurity Auditing
Topic B: Implement a Vulnerability Management Plan
Topic C: Assess Vulnerabilities
Topic D: Conduct Penetration Testing
Lesson 7: 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 8: Analyzing Log Data
Topic A: Use Common Tools to Analyze Logs
Topic B: Use SIEM Tools for Analysis
Lesson 9: 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 Indicators of Compromise
Lesson 10: Responding to Cybersecurity Incidents
Topic A: Deploy an Incident Handling and Response Architecture
Topic B: Mitigate Incidents
Topic C: Hand Over Incident Information to a Forensic Investigation
Lesson 11: 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

certified by: CertNexus Authorized Training Partner | Logical Operations