Course Outline

ProTech Professional Technical Services, Inc.

CompTIA Cybersecurity Analyst+ (CySA+)

Course Summary

Description

This course covers the duties of cybersecurity analysts 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 cybersecurity incident response team (CSIRT). The course introduces tools and tactics to manage cybersecurity risks, identify various types of common threats, evaluate the organization's security, collect and analyze cybersecurity intelligence, and handle incidents as they occur. Ultimately, the course promotes a comprehensive approach to security aimed toward those on the front lines of defense.

Objectives

CompTIA Cybersecurity Analyst+ candidates will be able to:

- Perform data analysis and interpret the results to identify vulnerabilities, threats, and risks to an organization.
- Configure and use threat detection tools.
- Secure and protect applications and systems within an organization.

Topics

- Explaining the Importance of Security Controls and Security Intelligence
- Utilizing Threat Data and Intelligence
- Analyze Network Monitoring Output
- Collecting Querying Security Monitoring Data
- Utilizing Digital Forensics and Indicator Analysis Techniques
- Applying Incident Response Processes
- Applying Risk Mitigation and Security Frameworks
- Performing Vulnerability Management
- Managing Post-Installation Adminstrative Tasks
- Understanding Data Privacay and Protection
- Applying Security Solutions for Software Assurance
- Applying Security Solutions for Cloud and Automation

Audience

This course is designed for cybersecurity practicioners who perform job functions related to protecting information systems by ensuring their availability, integrity, authentication ,confidentiality, and non-repudiation. This course ensures that all members of an IT team – everyone from help desk staff to the Chief Information Officer – understand their role in these security processes.

Prerequisites

Attendees should have Network+, Security+, or equivalent knowledge, as well as a minimum of 3-4 years of hands-on information security or related experience.

Duration

Five days

Course Outline

CompTIA Cybersecurity Analyst+ (CySA+)

Course Outline

I. Explaining the Importance of Security Controls and Security Intelligence
- A. Identify Security Control Types
- B. Explain the Importance of Threat Data and Intelligence

II. Utilizing Threat Data and Intelligence
- A. Classify Threats and Threat Actor Types
- B. Utilize Attack Frameworks and Indicator Management
- C. Utilize Threat Modeling and Hunting Methodologies

III. Analyze Network Monitoring Output
- A. Analyze Network Monitoring Output
- B. Analyze Appliance Monitoring Output
- C. Analyze Endpoint Monitoring Output
- D. Analyze Email Monitoring Output

IV. Collecting and Querying Security Monitoring Data
- A. Configure Log Review and SIEM Tools
- B. Analyze and Query Logs and SIEM Data

V. Utilizing Digital Forensics and Indicator Analysis Techniques
- A. Identify Digital Forensics Techniques
- B. Analyze Network-related IOCs
- C. Analyze Host-related IOCs
- D. Analyze Application-related IOCs
- E. Analyze Lateral Movement and Pivot IOCs

VI. Applying Incident Response Procedures
- A. Explain Incident Reponse Processes
- B. Apply Detection and Containment Processes
- C. Apply Eradication, Recovery, and Post-incident Processes

VII. Applying Risk Mitigation and Security Frameworks
- A. Apply Risk Identification, Calculation, and Prioritization Processes
- B. Explain Frameworks, Policies, and Procedures

VIII. Performing Vulnerability Management
- A. Analyze Output from Enumeration Tools
- B. Configure Infrastructure Vulnerability Scanning Parameters
- C. Analyze Output from Infrastructure Vulnerability Scanners
- D. Mitigate Vulnerability Issues

IX. Managing Post-Installation Administrative Tasks
- A. Apply Identity and Access Management Security Solutions
- B. Apply Network Architecture and Segmentation Security Solutions
- C. Explain Hardware Assurance Best Practices
- D. Explain Vulnerabilities Associated with Specialized Technology

X. Understanding Data Privacy and Protection
- A. Identify Non-Technical Data and Privacy Controls
- B. Identify Technical Data and Privacy Controls

XI. Applying Security Solutions for Software Assurance
- A. Mitigate Software Vulnerabilities and Attacks
- B. Mitigate Web Application Vulnerabilities and Attacks
- C. Analyze Output from Application Assessments

XII. Applying Security Solutions for Cloud and Automation
- A. Identify Cloud Service and Deployment Model Vulnerabilities
- B. Explain Service-Oriented Architecture
- C. Analyze Output from Cloud Infrastructure Assessment Tools
- D. Compare Automation Concepts and Technologies