CompTIA Cybersecurity Analyst+

Course CT-04B Five days Instructor-Led, Hands-on

Introduction

When attacks slip through unnoticed, the results are costly: data breaches, regulatory fines, downtime, and lost customer trust. And the demand for skilled defenders has never been higher, with the U.S. Bureau of Labor Statistics projecting a 33% growth in Information Security Analyst jobs from 2023 to 2033, far outpacing most careers. Without trained analysts, organizations are left vulnerable.

CompTIA Cybersecurity Analyst (CySA+) training equips you with the skills employers demand, including threat detection, log analysis, and incident response. This hands-on certification course prepares you to identify vulnerabilities, stop attacks before they spread, and keep critical systems secure.

This instructor-led course prepares you to proactively defend systems using behavioral analytics, threat intelligence, and hands-on investigation tools. You'll gain real-world experience managing vulnerabilities, analyzing SIEM output, investigating incidents, and preparing for forensic analysis—all while developing the knowledge needed to pass the CompTIA CySA+ certification exam (CS0-002 or CS0-003).

The CySA+ certification is also DoD 8570/8140 approved, making this course an excellent choice for military, civilian, and contractor personnel who require compliance with Department of Defense cybersecurity workforce standards.

At Course Completion

This course will teach you the fundamental principles of using threat and vulnerability analysis tools plus digital forensics tools. It will prepare you to take the CompTIA Cybersecurity Analyst+ CS0-002 exam by providing 100% coverage of the objectives and content examples listed on the syllabus. Study of the course can also help to build the prerequisites to study more advanced IT security qualifications.

Upon successful completion of this course, students will understand:

- Assess information security risk in computing and network environments.
- Analyze reconnaissance threats to computing and network environments.
- Analyze attacks on computing and network environments.
- Analyze post-attack techniques on computing and network environments.
- Implement a vulnerability management program.
- 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.

Contact ISInc for more information at 916.920.1700 or by visiting our website at http://www.isinc.com

- Address security issues with the organization's technology architecture

Prerequisites

Prior to attending this course, students should have the following experience:

Network+, Security+ or equivalent knowledge. Minimum of 4 years of hands-on experience as an incident response analyst or security operations center (SOC) analyst, or equivalent experience

Course Materials

The student kit includes a comprehensive workbook and other necessary materials for this class.

Course Outline

Module 1: Assessing Information Security Risk

- Understand the importance of risk management
- Perform risk assessments across systems and networks
- Apply risk mitigation strategies
- Integrate documentation into the risk management process

Module 2: Analyzing Reconnaissance Threats to Computing and Network Environments

- Evaluate the impact of reconnaissance activities
- Assess the risks posed by social engineering attacks

Module 3: Analyzing Attacks on Computing and Network Environments

- Analyze the impact of system hacking attempts
- Evaluate the effects of web-based attacks
- Assess malware threats and their consequences
- Understand hijacking and impersonation attacks
- Analyze Denial-of-Service (DoS) incidents
- Examine mobile security threats
- Explore cloud security risks

Module 4: Analyzing Post-Attack Techniques

- Identify command and control methods
- Assess techniques for maintaining persistence
- Analyze lateral movement and pivoting strategies
- Understand data exfiltration methods

Contact ISInc for more information at 916.920.1700 or by visiting our website at http://www.isinc.com

- Examine anti-forensics techniques

Module 5: Managing Vulnerabilities in the Organization

- Implement a comprehensive vulnerability management plan
- Identify and assess common system and application vulnerabilities
- Conduct vulnerability scans effectively
- Perform penetration testing on network assets

Module 6: Collecting Cybersecurity Intelligence

- Set up platforms for collecting and analyzing security intelligence
- Gather data from network-based intelligence sources
- Collect intelligence from host-based sources

Module 7: Analyzing Log Data

- Utilize common tools to analyze log files
- Leverage SIEM (Security Information and Event Management) tools for deeper analysis

Module 8: Performing Active Asset and Network Analysis

- Investigate incidents using Windows-based tools
- Analyze events using Linux-based tools
- Perform basic malware analysis
- Examine indicators of compromise (IOCs)

Module 9: Responding to Cybersecurity Incidents

- Deploy an effective incident response architecture
- Mitigate active threats
- Prepare your CSIRT team for forensic investigation

Module 10: Investigating Cybersecurity Incidents

- Apply a structured forensic investigation plan
- Securely collect and analyze electronic evidence
- Conduct post-investigation follow-up and reporting

Module 11: Addressing Security Architecture Issues

- Resolve identity and access management (IAM) problems
- Integrate security considerations throughout the Software Development Life Cycle (SDLC)