CyberGate ACADEMY

CySA+

COMPTIA CYSA+ CYBERSECURITY ANALYST COURSE

Course Overview

CompTIA Cybersecurity Analyst (CySA+) is a certification for cyber professionals tasked with incident detection, prevention and response through continuous security monitoring. CySA+ is a global, vendor-neutral certification covering intermediate-level knowledge and skills required by information security analyst job roles. It helps identify a cybersecurity professional's ability to proactively defend an organization using secure monitoring, threat identification, incident response and teamwork. The CompTIA CySA+ CS0-003 course and certification exam ensures the candidate has the knowledge and skills required to:

- Detect and analyze indicators of malicious activity.
- Understand threat hunting and threat intelligence concepts.
- Use appropriate tools and methods to manage, prioritize and respond to attacks and vulnerabilities.
- Perform incident response processes.
- Understand reporting and communication concepts related to vulnerability management and incident response activities

Course Duration

5 Days (40 Hours).

Target Audience

The course is aimed at Security Analysts, Security Operations Center (SOC) Analysts, Incident Response Analysts, Vulnerability Management Analysts and Security Engineers.

During this course you should learn

1. Proactively Monitor and Detect. Demonstrate your skills in detecting and analyzing indicators of malicious activity using the most up-to-date methods and tools, such as threat intelligence, security information and event management (SIEM), endpoint detection and response (EDR) and extended detection and response (XDR).

2. Respond to Threats, Attacks and Vulnerabilities. Prove your knowledge of incident response and vulnerability management processes and highlight the communication skills critical to security analysis and compliance.

3. Demonstrate Competency of Current Trends. Valuable team members can show knowledge of current trends that affect the daily work of security analysts, such as cloud and hybrid environments.

Course Content

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.

Prerequisites

Attendees should meet the following prerequisites:

- At least two years (recommended) of experience or education in computer network security technology or a related field.
- The ability or curiosity to recognize information security vulnerabilities and threats in the context of risk management.
- 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 VPNs.
- General 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.
- Foundation-level skills with some of the common operating systems for computing environments.
- Entry-level understanding of some of the common concepts for network environments, such as routing and switching.
- General or practical knowledge of major TCP/IP networking protocols, including, but not limited to, TCP, IP, UDP, DNS, HTTP, ARP, ICMP, and DHCP.

Course Agenda

Day 1	Lesson 1: Assessing Cybersecurity Risk Lesson 2: Analyzing the Threat Landscape Lesson 3: Analyzing Reconnaissance Threats to Computing and Network
Day 2	Lesson 4: Analyzing Attacks on Computing and Network Environments Lesson 5: Analyzing Post-Attack Techniques
Day 3	Lesson 6: Assessing the Organization's Security Posture Lesson 7: Collecting Cybersecurity Intelligence
Day 4	Lesson 8: Analyzing Log Data Lesson 9: Performing Active Asset and Network Analysis
Day 5	Lesson 10: Responding to Cybersecurity Incidents Lesson 11: Investigating Cybersecurity Incidents

Technical Requirement

1. Laptop with minimum 8GB Ram
2. Connected Monitor for iLabs.
3. Hi speed Internet Connection as All the labs it will be accessed through EC-Council Cloud

Exam Voucher Validity

It will be valid for 12month starting from the last day of the course.

Certification Expiry

It will be valid for 3 years.

CyberGate ACADEMY

YOUR TRUSTED DEFENDERS

ADDRESS

CyberGate Academy
ADPOLY, MBZ City

WEB

academy@cybergate.tech
training@cybergate.tech