COMPTIA CYBERSECURITY ANALYST (CYSA+)

Duration: 5 Day(s)

Course Overview

The CompTIA Cybersecurity Analyst (CySA+) course is an international, vendor-neutral cybersecurity certification that applies behavioural analytics to improve the overall state of IT security. The CySA+ course validates knowledge and skills that are required to prevent, detect and combat cybersecurity threats. In addition, this course covers the duties of those 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 students to tools and tactics to manage cybersecurity risks, identify various types of common threats, evaluate the organization's security, collect and analyse cybersecurity intelligence and handle incidents as they occur. Ultimately, the course promotes a comprehensive approach to security aimed towards those on the front lines of defence.

Who Should Attend

This course is designed primarily for cybersecurity practitioners who perform job functions related to protecting information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation. This course focuses on the knowledge, ability and skills necessary to provide for the defence of those information systems in a cybersecurity context, including protection, detection, analysis, investigation and response processes. In addition, the course ensures that all members of an IT team, everyone from helpdesk staff to the Chief Information Officer to understand their roles in these security processes.

Course Objectives

After completing the CompTIA CySA+ course, students will have the skills and knowledge to:

- assess information security risk in computing and network environments
- analyse the cybersecurity threat landscape
- analyse reconnaissance threats to computing and network environments
- analyse attacks on computing and network environments
- analyse post-attack techniques on computing and network environments
- implement a vulnerability management program
- evaluate the organization's security through penetration testing
- collect cybersecurity intelligence
- analyse data collected from security and event logs
- perform active analysis on assets and networks
- respond to cybersecurity incidents
- investigate cybersecurity incidents
- address security issues with the organization's technology architecture

Prerequisites

To ensure success in this course, students should meet the following requirements:

- At least two years (recommended) of experience in computer network security technology or a related field
- The ability to recognize information security vulnerabilities and threats in the context of risk management

- Foundation-level operational skills with some of the common operating systems for computing environments
- Foundational 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 understanding of some of the common concepts for network environments such as routing and switching
- Foundational knowledge of major TCP/IP networking protocols including but not limited to TCP, IP, UDP, DNS, HTTP, ARP, ICMP and DHCP
- 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

Training Information

Training Provider	:	Allied View Centre Sdn Bhd
Course Title	:	CompTIA Cybersecurity Analyst (CySA+)
Training Venue (full address of training venue)	:	16-1, 1st Floor, Commerce One, Lorong 2/137C, Off Jalan Klang Lama, 58200 Kuala Lumpur
Start Date	:	5th July 2020
Completion Date	:	19th July 2020
Duration	:	5 Days (weekends)
Time	:	9:00 am – 5:00 pm

Course Outline:

Lesson 1: Assessing Information Security Risk
- Identify the Importance of Risk Management
- Assess Risk
- Mitigate Risk
- Integrate Documentation into Risk Management

Lesson 2: Analysing the Threat Landscape
- Classify Threats and Threat Profiles
- Perform Ongoing Threat Research

Lesson 3: Analysing Reconnaissance Threats to Computing and Network Environments
- Implement Threat Modelling
- Assess the Impact of Reconnaissance Incidents
- Assess the Impact of Social Engineering

Lesson 4: Analysing Attacks on Computing and Network Environments
- Assess the Impact of System Hacking Attacks
- Assess the Impact of Web-Based Attacks

- Assess the Impact of Malware
- Assess the Impact of Hijacking and Impersonation Attacks
- Assess the Impact of DoS Incidents
- Assess the Impact of Threats to Mobile Security
- Assess the Impact of Threats to Cloud Security

Lesson 5: Analysing Post-Attack Techniques
- Assess Command and Control Techniques
- Assess Persistence Techniques
- Assess Lateral Movement and Pivoting Techniques
- Assess Data Exfiltration Techniques
- Assess Anti-Forensics Techniques

Lesson 6: Managing Vulnerabilities in the Organization
- Implement a Vulnerability Management Plan
- Assess Common Vulnerabilities
- Conduct Vulnerability Scans

Lesson 7: Implementing Penetration Testing to Evaluate Security
- Conduct Penetration Tests on Network Assets
- Follow Up on Penetration Testing

Lesson 8: Collecting Cybersecurity Intelligence
- Deploy a Security Intelligence Collection and Analysis Platform
- Collect Data from Network-Based Intelligence Sources
- Collect Data from Host-Based Intelligence Sources

Lesson 9: Analysing Log Data
- Use Common Tools to Analyse Logs
- Use SIEM Tools for Analysis
- Parse Log Files with Regular Expressions

Lesson 10: Performing Active Asset and Network Analysis
- Analyse Incidents with Windows-Based Tools
- Analyse Incidents with Linux-Based Tools
- Analyse Malware
- Analyse Indicators of Compromise

Lesson 11: Responding to Cybersecurity Incidents
- Deploy an Incident Handling and Response Architecture
- Mitigate Incidents
- Prepare for Forensic Investigation as a CSIRT

Lesson 12: Investigating Cybersecurity Incidents
- Apply a Forensic Investigation Plan
- Securely Collect and Analyse Electronic Evidence
- Follow Up on the Results of an Investigation

Lesson 13: Addressing Security Architecture Issues
- Remediate Identity and Access Management Issues
- Implement Security during the SDLC