Course overview

CompTIA Cybersecurity Analyst+ Certification (Exam CS0-001) Study Guide

(G720eng v057)

Target Audience

This course is intended for those wishing to qualify with CompTIA Cybersecurity Analyst+ Certification (CySA+). CompTIA's CySA+ Certification is an intermediate-level certificate for IT professionals with previous experience of working in the field of IT security.

> *The CompTIA Cybersecurity Analyst+ examination is designed for IT security analysts, vulnerability analysts, or threat intelligence analysts. The exam will certify that the successful candidate has the knowledge and skills required to configure and use threat detection tools, perform data analysis, and interpret the results to identify vulnerabilities, threats, and risks to an organization with the end goal of securing and protecting applications and systems within an organization.*
>
> *CompTIA Cybersecurity Analyst+ Syllabus*

Certification track

This courseware bears the seal of CompTIA Approved Quality Content. This seal signifies this content covers 100% of the exam objectives and implements important instructional design principles. CompTIA recommends multiple learning tools to help increase coverage of the learning objectives. The contents of this training material were created for the CompTIA Cybersecurity Analyst+ Certification CS0-001 exam covering the 2017 Edition certification exam objectives.

Target audience and course prerequisites

CompTIA CySA+ certification is aimed at IT professionals with (or seeking) job roles such as IT Security Analyst, Security Operations Center (SOC) Analyst, Vulnerability Analyst, Cybersecurity Specialist, Threat Intelligence Analyst, and Security Engineer.

Ideally, you should have successfully completed gtslearning's "CompTIA Network+ Certification" and "CompTIA Security+ Certification" courses or have equivalent knowledge. Specifically, it is recommended that you have the following skills and knowledge before starting this course:

- Know basic network terminology and functions (such as OSI Model, Topology, Ethernet, Wi-Fi, switches, routers).
- Understand TCP/IP addressing, core protocols, and troubleshooting tools.
- Identify network attack strategies and defenses.
- Know the technologies and uses of cryptographic standards and products.
- Identify network- and host-based security technologies and practices.
- Describe the standards and products used to enforce security on web and communications technologies.

Course outcomes

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+ CS0-001 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, including CompTIA Advanced Security Practitioner (CASP) and ISC's CISSP (Certified Information Systems Security Professional).

On course completion, you will be able to:

- Identify tools and techniques to use to perform an environmental reconnaissance of a target network or security system.
- Collect, analyze, and interpret security data from multiple log and monitoring sources.
- Use network host and web application vulnerability assessment tools and interpret the results to provide effective mitigation.
- Understand and remediate identity management, authentication, and access control issues.
- Participate in a senior role within an incident response team and use forensic tools to identify the source of an attack.
- Understand the use of frameworks, policies, and procedures and report on security architecture with recommendations for effective compensating controls.

Course contents

The course consists of a study volume, containing indexed notes and review questions, plus exam objectives mapping, exam information, and a comprehensive glossary. The course also comes with an online practice exam, pre-requisites test, and pre-/post-unit assessment tests.

An instructor edition of the course is available with margin notes and tips for the trainer. Access to course resources (setup guides and data, PowerPoint slides, timetables, and extra exam information) on gtslearning's trainer portal is also available, subject to meeting minimum order requirements.

Module 1 / Threat Management (1)

- **Cybersecurity Analysts** • Cybersecurity Roles and Responsibilities • Frameworks and Security Controls • Risk Evaluation • Penetration Testing Processes
- **Reconnaissance Techniques** • The Kill Chain • Open Source Intelligence • Social Engineering • Topology Discovery • Service Discovery • OS Fingerprinting • **Labs** • OSINT • VM Orientation • Host, Topology, and Service Discovery with Nmap

Module 2 / Vulnerability Management

- **Managing Vulnerabilities** • Vulnerability Management Requirements • Asset Inventory • Data Classification • Vulnerability Management Processes • Vulnerability Scanners • Microsoft Baseline Security Analyzer • Vulnerability Feeds and SCAP • Configuring Vulnerability Scans • Vulnerability Scanning Criteria • Exploit Frameworks • **Labs** • Vulnerability Scanning with OpenVAS and MBSA
- **Remediating Vulnerabilities** • Analyzing Vulnerability Scans • Remediation and Change Control • Remediating Host Vulnerabilities • Remediating Network Vulnerabilities • Remediating Virtual Infrastructure Vulnerabilities
- **Secure Software Development** • Software Development Lifecycle • Software Vulnerabilities • Software Security Testing • Interception Proxies • Web Application Firewalls • Source Authenticity • Reverse Engineering • **Labs** • Web Application Testing with Nikto and Burpsuite

Module 3 / Threat Management (2)

- **Security Appliances** • Configuring Firewalls • Intrusion Detection and Prevention • Configuring IDS • Malware Threats • Configuring Anti-virus Software • Sysinternals • Enhanced Mitigation Experience Toolkit • **Labs** • Network Security Monitoring with Snort and Security Onion • Malware Analysis with Sysinternals

- **Logging and Analysis** • Packet Capture • Packet Capture Tools • Monitoring Tools • Log Review and SIEM • SIEM Data Outputs • SIEM Data Analysis • Point-in-Time Data Analysis • **Labs** • Packet Analysis with Wireshark and Network Miner • SIEM with OSSIM

Module 4 / Cyber Incident Response

- **Incident Response** • Incident Response Processes • Threat Classification • Incident Severity and Prioritization • Types of Data
- **Forensics Tools** • Digital Forensics Investigations • Documentation and Forms • Digital Forensics Crime Scenes • Digital Forensics Kits • Image Acquisition • Password Cracking • Analysis Utilities • **Labs** • Forensic Image Analysis with Autopsy
- **Incident Analysis and Recovery** • Analysis and Recovery Frameworks • Analyzing Network Symptoms • Analyzing Host Symptoms • Analyzing Data Exfiltration • Analyzing Application Symptoms • Using Sysinternals • Containment Techniques • Eradication Techniques • Validation Techniques • Corrective Actions • **Labs** • Red Team Versus Blue Team

Module 5 / Security Architecture

- **Secure Network Design** • Network Segmentation • Blackholes, Sinkholes, and Honeypots • System Hardening • Group Policies and MAC • Endpoint Security • **Labs** • Network Segmentation with pfSense
- **Managing Identities and Access** • Network Access Control • Identity Management • Identity Security Issues • Identity Repositories • Context-based Authentication • Single Sign On and Federation • Exploiting Identities • Exploiting Web Browsers and Applications • **Labs** • Secure Appliance Administration • Email Spoofing and XSS
- **Security Frameworks and Policies** • Frameworks and Compliance • Reviewing Security Architecture • Procedures and Compensating Controls • Verifications and Quality Control • Security Policies and Procedures • Personnel Policies and Training