CySA+ (CS0-003) Course Introduction

Ahmed Sultan
Senior Technical Instructor
ahmedsultan.me/about

About the certification

- **CompTIA CySA+** focuses on the candidates ability to not only proactively capture, monitor, and respond to network traffic findings, but also emphasizes software and application security, automation, threat hunting, and IT regulatory compliance, which affects the daily work of security analysts.
- **CySA+** covers the most up-to-date core security analyst skills and upcoming job skills used by threat intelligence analysts, application security analysts, compliance analysts, incident responders/handlers, and threat hunters, bringing new techniques for combating threats inside and outside of the Security Operations Center (SOC).

https://www.comptia.org/certifications/cybersecurity-analyst

About the certification (cont.)

- **CySA+** will verify the successful candidate has the knowledge and skills required to:
  - Leverage intelligence and threat detection techniques
  - Analyze and interpret data
  - Identify and address vulnerabilities
  - Suggest preventative measures
  - Effectively respond to and recover from incidents

Course Prerequisites

To fully benefit from this course, you should have the following knowledge and skills:

- **Network+, Security+** or equivalent knowledge.
- Minimum of 4 years of hands-on information security or related experience.

IT Jobs Related to CompTIA CySA+

- Security analyst (Tier II SOC analyst and Security monitoring)
- Threat intelligence analyst
- Security engineer
- Application security analyst
- Incident response or handler
- Compliance analyst
- Threat hunter

Course Domains

Domain 1: Security Operations **(33%)**

Domain 2: Vulnerability Management **(30%)**

Domain 3: Incident Response and Management **(20%)**

Domain 4: Reporting and Communication **(17%)**

Official Topics

1. Understanding Vulnerability Response, Handling, and Management
2. Exploring Threat Intelligence and Threat Hunting Concepts
3. Explaining Important System and Network Architecture Concepts
4. Understanding Process Improvement in Security Operations
5. Implementing Vulnerability Scanning Methods
6. Performing Vulnerability Analysis
7. Communicating Vulnerability Information

CompTIA CertMaster Learn for CySA+ (CS0-003) - Individual License

Official Topics (cont.)

8. Explaining Incident Response Activities
9. Demonstrating Incident Response Communication
10. Applying Tools to Identify Malicious Activity
11. Analyzing Potentially Malicious Activity
12. Understanding Application Vulnerability Assessment
13. Exploring Scripting Tools and Analysis Concepts
14. Understanding Application Security and Attack Mitigation Best Practices

CompTIA CertMaster Learn for CySA+ (CS0-003) - Individual License

Official Labs

1. Configuring Controls
2. Reviewing IoC and Threat Intelligence Sources
3. Performing Threat Hunting
4. Configuring Centralized Logging
5. Assess Time Synch Errors
6. Configuring Automation
7. Performing Asset Discovery

CompTIA CertMaster Labs for CySA+ (CS0-003) - Individual License

Official Labs (cont.)

8. Performing Vulnerability Scanning
9. Performing Passive Scanning
10. Establishing Context Awareness
11. Analyzing Vulnerability Reports
12. Detecting Legacy Systems
13. Performing Post-Incident Forensic Analysis
14. Performing IoC Detection and Analysis

CompTIA CertMaster Labs for CySA+ (CS0-003) - Individual License

Official Labs (cont.)

15. Performing Root Cause Analysis
16. Using File Analysis Techniques
17. Analyzing Potentially Malicious Files
18. Using Nontraditional Vulnerability Scanning Tools
19. Exploiting Weak Cryptography
20. Performing and Detecting Directory Traversal and Command Injection
21. Performing and Detecting Privilege Escalation

CompTIA CertMaster Labs for CySA+ (CS0-003) - Individual License

Official Labs (cont.)

22. Performing and Detecting XSS
23. Performing and Detecting LFI/RFI
24. Performing and Detecting SQLi
25. Performing and Detecting CSRF

[CompTIA CertMaster Labs for CySA+ (CS0-003) - Individual License]

FAQs

- Should I have **Networks and Security** knowledge before taking this course ?
  - Yes, as recommended experience you should have finished **Network+, Security+** or **equivalent knowledge**.

- Do I need a powerful computer to implement the course's Labs ?
  - **Yes**, only If you will build your own Virtual Lab.
  - For me as an Instructor I will show you how to implement labs using **CompTIA Labs** hosted in their cloud.

    CompTIA CertMaster Labs for CySA+ (CS0-003) - (paid subscription)

"LABS ARE OPTIONAL, THERE IS NO LABS IN THE EXAM"

Resources for the online & recorded course

- We will provide you with the following course materials
  - ✓PDF slides for each topic.
  - ✓HD recorded videos in .mp4 format ready for online watching.
  - ✓Lifetime access to the course contents.

- Register here for the pre-recorded course - https://netriders.academy/courses/cysa-new/