CySA+ (CS0-002) 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: Threat and Vulnerability Management **(22%)**

Domain 2: Software and Systems Security **(18%)**

Domain 3: Security Operations and Monitoring **(25%)**

Domain 4: Incident Response **(22%)**

Domain 5: Compliance and Assessment **(13%)**

Topics Covered

1. Explaining the Importance of Security Controls and Security Intelligence
2. Utilizing Threat Data and Intelligence
3. Analyzing Security Monitoring Data
4. Collecting and Querying Security Monitoring Data
5. Utilizing Digital Forensics and Indicator Analysis Techniques
6. Applying Incident Response Procedures

Topics Covered (cont.)

7. Applying Risk Mitigation and Security Frameworks
8. Performing Vulnerability Management
9. Applying Security Solutions for Infrastructure Management
10. Understanding Data Privacy and Protection
11. Applying Security Solutions for Software Assurance
12. Applying Security Solutions for Cloud and Automation

Labs

1. Analyzing Output from Network Security Monitoring Tools
2. Discovering the Lab Environment
3. Analyzing Output from Security Appliance Logs
4. Analyzing Output from Endpoint Security Monitoring Tools
5. Analyzing Email Headers
6. Configuring SIEM Agents and Collectors
7. Analyzing, Filtering, and Searching Event Log and syslog Output
8. Collecting and Validating Digital Evidence

Labs (cont.)

9. Analyzing Network-related IoCs
10. Analyzing Host and Application IoCs
11. Observing IoCs during a Security Incident
12. Analyzing Output from Topology and Host Enumeration Tools
13. Testing Credential Security
14. Configuring Vulnerability Scanning and Analyzing Outputs
15. Assessing Vulnerability Scan Outputs
16. Assessing the Impact of Regulation on Vulnerability Management

Labs (cont.)

17. Performing Account and Permissions Audits
18. Configuring Network Segmentation and Security
19. Configuring and Analyzing Share Permissions
20. Assessing the Impact of Web Application Vulnerabilities
21. Analyzing Output from Web Application Assessment Tools
22. Analyzing Output from Cloud Infrastructure Assessment Tools

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 Labs ?
  - **Yes**, If you will implement course labs in your computer.
  - For me as an Instructor I will show you how to implement labs using **CompTIA Labs** hosted in their cloud.

    CompTIA Labs for CySA+ (CS0-002) - Individual License - (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 & offline watching.

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