Course: **Cybersecurity Analyst (CySA+)**

Contact Hours: **36**

Pre-requisite: **Network+, Security+ or equivalent knowledge**

Abstract

This is a vendor neutral certification that includes intermediate-level security skills and knowledge. CySA+ covers security analytics, intrusion detection and response. It is the most up-to-date security analyst credential that covers persistent threats in today's cybersecurity environment.

Target Audience

- IT Security Analysts
- Persons who would like to start a career in cybersecurity

Exam

- Required exam: CS0-001
- Number of questions: Maximum of 85
- Types of questions: Multiple choice and performance-based
- Length of test: 165 Minutes
- Recommended experience: Network+, Security+, or equivalent knowledge; Minimum of 3-4 years of hands-on information security or related experience. While there is no required prerequisite, CySA+ is intended to follow CompTIA Security+ or equivalent experience and has a technical, "hands-on" focus.
- Passing score: 750 (on a scale of 100–900)

Learning outcomes

On completion of this course, learners will be able to do the following.

1.0 Threat Management

1.1 Apply environmental reconnaissance techniques using appropriate tools and processes.
1.2 Analyze the results of a network reconnaissance.
1.3 Given a network-based threat, implement or recommend the appropriate response and countermeasure.
1.4 Explain the purpose of practices used to secure a corporate environment

2.0 Vulnerability Management

2.1 Implement an information security vulnerability management process.
2.2 Analyze the output resulting from a vulnerability scan.
2.3 Compare and contrast common vulnerabilities found in the following targets within an organization.

3.0 Cyber Incident Response

3.1 Distinguish threat data or behavior to determine the impact of an incident.
3.2 Prepare a toolkit and use appropriate forensics tools during an investigation
3.3 Explain the importance of communication during the incident response process
3.4 Analyze common symptoms to select the best course of action to support incident response
3.5 Summarize the incident recovery and post-incident response process

4.0 Security Architecture and Tool Sets

4.1 Explain the relationship between frameworks, common policies, controls, and procedures.
4.2 Use data to recommend remediation of security issues related to identity and access management.
4.3 Review security architecture and make recommendations to implement compensating controls.
4.4 Use application security best practices while participating in the Software Development Life Cycle (SDLC).

Course Content

1.0 Threat Management

1.1 Apply environmental reconnaissance techniques using appropriate tools and processes.
Procedures/common tasks; Variables; Tools

1.2 Analyze the results of a network reconnaissance
Point-in-time data analysis; Data correlation and analytics; Data output; Tools

1.3 Given a network-based threat, implement or recommend the appropriate response and countermeasure.
Network Segmentation; Honeypot; Endpoint security; Group policies; ACLs; hardening; Network Access Control (NAC)

1.4 Explain the purpose of practices used to secure a corporate environment.
Penetration testing; Reverse Engineering; Training and exercises; Risk evaluation

2.0 Vulnerability Management

2.1 Implement an information security vulnerability management process.
Identification of requirements; Establish scanning frequency; Configure tools to perform scans according to specification; Execute scanning; Generate reports; Remediation; Ongoing scanning and continuous monitoring

2.2 Analyze the output resulting from a vulnerability scan.
Analyze reports from a vulnerability scan; Validate results and correlate other data points

2.3 Compare and contrast common vulnerabilities found in the following targets within an organization.
Servers; Endpoints; Network infrastructure; Network appliances; Virtual Infrastructure; Mobile devices; Interconnected networks; Virtual Private Networks (VPNs); Industrial Control Systems (ICSs); SCADA devices

3.0 Cyber Incident Response

3.1 Distinguish threat data or behavior to determine the impact of an incident.
Threat classification; Factors contributing to incident severity and prioritization

3.2 Prepare a toolkit and use appropriate forensics tools during an investigation.
Forensics kit; Forensic Investigation suite

3.3 Explain the importance of communication during the incident response process.
Stakeholders; Purpose of communication processes; Role-based responsibilities

3.4 Analyze common symptoms to select the best course of action to support incident response.
Common network-related symptoms; Common host-related symptoms; Common application-related symptoms

3.5 Summarize the incident recovery and post-incident response process.
Containment techniques; Eradication techniques; Validation; Corrective actions; Incident summary report

4.0 Security Architecture and Tool Sets

4.1 Explain the relationship between frameworks, common policies, controls, and procedures.
Regulatory compliance; Frameworks; Policies; Controls; Procedures; Verifications and quality control

4.2 Use data to recommend remediation of security issues related to identity and access management.
Security issues associated with context-based authentication; Security issues associated with identities; Security issues associated with identity repositories; Security issues associated with federation and single sign-on; Exploits

4.3 Review security architecture and make recommendations to implement compensating controls.
Security data analytics; Manual review; Defense in depth;

4.4 Use application security best practices while participating in the Software Development Life Cycle (SDLC).
Best practices during software development; Secure coding best practices

Essential Learning Resources

Websites:

- https://certification.comptia.org/certifications/cybersecurity-analyst#overview
- Detailed outline: https://www.comptia.jp/pdf/comptia-cybersecurity-analyst-(cs0-001).pdf