kod szkolenia: CySA+ (+ exam) / ENG AA 5d

Workshops on CompTIA Cybersecurity Analyst (CySA+) with CS0-003 exam voucher - authorized training

Zobacz film: https://youtu.be/AMMd7j0ZMSg

If you want to become a professional cybersecurity analyst, gain skills in detecting, preventing, and responding to cyber threat incidents, and learn to continuously monitor system security, then the CompTIA Cybersecurity Analyst (CySA+) certification is perfect for you.

The CompTIA Cybersecurity Analyst (CySA+) certification verifies that candidates have the knowledge and skills necessary to detect and analyze signs of malicious activity, understand intelligence and threat management, respond to attacks and vulnerabilities, perform incident response actions, and report and communicate on cybersecurity-related topics.

Purpose of the training

The training is aimed at individuals working in the following positions:

- IT Security Analyst
- Cybersecurity Analyst
- Security Operations Center (SOC) Analyst
- IT Security Engineer
- Cybersecurity Specialist

Benefits of completing the training

In this training, you will learn tools and methods for managing cyber risk, recognizing different types of common threats, assessing the security level of an organization, gathering and analyzing information on cybercrime, and handling crisis situations.
Participants of the training will gain knowledge and skills in:

- Searching and automation
- Monitoring network traffic security
- Software and application security

Examination method

To take the exam, you can do so at authorized PearsonVue exam centers.
Exam Information: CS0-003
Title: The CompTIA Cybersecurity Analyst (CySA+)
Exam Format: Multiple choice and performance-based
Number of Questions: Up to 85
Duration: 165 minutes
Passing Score: 750 (on a scale of 100-900)
For detailed information about the exam, visit the CompTIA webpage for The CompTIA Cybersecurity Analyst (CySA+).

Expected Listener Preparation

Required knowledge from the training:

- SPLUS+ – Workshops on CompTIA Security+ (preparation for the SY0-701 exam)
- Minimum 3-4 years of experience working as a security administrator.

Training Language

Training: English
Materials: English

Training Includes

- 5 days of training with an instructor
- Instructor supervision
- Authorized textbook: The Official CompTIA CySA+
- Lab environment
- Voucher for the CS0-003 exam

Training method:

- Lecture
- Workshops

4o

Czas trwania

5 dni / 35 godzin

Training agenda

1. Understanding ACCybersecurity Leadership Concepts
   - Exploring Control Types and Methods
   - Explaining Patch Management Concepts
2. Exploring Threat Intelligence and Threat Hunting Concepts
   - Exploring Threat Actor Concepts
   - Identifying Active Threats
   - Exploring Threat-Hunting Concepts
3. Explaining Important System and Network Architecture Concepts
   - Reviewing System and Network Architecture Concepts
   - Exploring Identity and Access Management (IAM)
   - Maintaining Operational Visibility
4. Understanding Process Improvement in Security Operations
   - Exploring Leadership in Security Operations

- Understanding Technology for Security Operations

5. Implementing Vulnerability Scanning Methods
   - Explaining Compliance Requirements
   - Understanding Vulnerability Scanning Methods
   - Exploring Special Considerations in Vulnerability Scanning
6. Performing Vulnerability Analysis
   - Understanding Vulnerability Scoring Concepts
   - Exploring Vulnerability Context Considerations
7. Communicating Vulnerability Information
   - Explaining Effective Communication Concepts
   - Understanding Vulnerability Reporting Outcomes and Action Plans
8. Explaining Incident Response Activities
   - Exploring Incident Response Planning
   - Performing Incident Response Activities
9. Demonstrating Incident Response Communication
   - Understanding Incident Response Communication
   - Analyzing Incident Response Activities
10. Applying Tools to Identify Malicious Activity
    - Identifying Malicious Activity
    - Explaining Attack Methodology Frameworks
    - Explaining Techniques for Identifying Malicious Activity
11. Analyzing Potentially Malicious Activity
    - Exploring Network Attack Indicators
    - Exploring Host Attack Indicators
    - Exploring Vulnerability Assessment Tools

12. Understanding Application Vulnerability Assessment
    - Analyzing Web Vulnerabilities
    - Analyzing Cloud Vulnerabilities
13. Exploring Scripting Tools and Analysis Concepts
    - Understanding Scripting Languages
    - Identifying Malicious Activity Through Analysis
14. Understanding Application Security and Attack Mitigation Best Practices
    - Exploring Secure Software Development Practices
    - Recommending Controls to Mitigate Successful Application Attacks
    - Implementing Controls to Prevent Attacks