Training: CompTIA
# CompTIA CySA+ Prep Course

## TRAINING GOALS:

CompTIA's CySA+ certification is an intermediate-level certification designed for professionals with four years of hands-on experience as an incident response analyst or security operations center (SOC) analyst.

This course can benefit you in two ways. If you intend to pass the CompTIA CySA+ (Exam CS0-003) certification examination, this course can be a significant part of your preparation. But certification is not the only key to professional success in the field of security analyst. Today's job market demands individuals with demonstrable skills, and the information and activities in this course can help you build your security analyst skill set so that you can confidently perform your duties in any security analyst role.

On course completion, you will be able to achieve the following:

- Understand vulnerability response, handling, and management
- Explore threat intelligence and threat hunting concepts
- Explain important system and network architecture concepts
- Understand process improvement in security operations
- Implement vulnerability scanning methods
- Perform vulnerability analysis
- Classify vulnerability information
- Explain incident response activities.
- Demonstrate incident response communication
- Apply tools to identify malicious activity
- Analyze potentially malicious activity
- Understand application vulnerability assessment
- Explore scripting tools and analysis concepts
- Understand application security and attack mitigation best practices



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

Skills you'll learn

- Enhance security operations processes, differentiate threat intelligence and threat hunting, and identify malicious activity using appropriate tools.
- Conduct vulnerability assessments, prioritize vulnerabilities, and recommend effective mitigation strategies for vulnerability management.
- Apply attack methodology frameworks, perform incident response, and understand the incident management lifecycle to handle security incidents effectively.
- Utilize communication best practices to report on vulnerability management and incident response, providing stakeholders with actionable plans and meaningful metrics.

Job roles that benefit from CySA+ skills

- Application Security Analyst
- Threat Hunter
- Threat Intelligence Analyst
- Vulnerability Analyst
- Security Operations Center (SOC) Analyst
- Security Architect
- Cybersecurity Engineer

*Each participant in an authorized training CompTIA CySA+ Prep Course held in Compendium CE will receive a free CS0-003 CompTIA CySA+ Certification Exam vouchers.*

## CONSPECT:

- Understanding Vulnerability Response, Handling, and Management
  - Understanding Cybersecurity Leadership Concepts
    - Explore Policy and Governance Topics
    - Explain Risk Management Principles
    - Explore Threat Modeling
    - Assisted Live Lab: Exploring the Lab Environment
  - Exploring Control Types and Methods
    - Security Control Categories
    - Security Control Functional Types
    - Managing Attack Surfaces
    - Assisted Live Lab: Configuring Controls



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Explaining Patch Management Concepts
  - Explain Software Patching and Host Protections
  - Explore Configuration Management
  - Understand Maintenance Windows
- Threat Intelligence and Threat Hunting
  - Exploring Threat Actor Concepts
    - Threat Actor Types
    - Advanced Persistent Threat (APT)
    - Tactics, Techniques, and Procedures
  - Identifying Active Threats
    - Open-Source Intelligence (OSINT)
    - Proprietary/Closed-Source Intelligence Sources
    - Information Sharing and Analysis Centers (ISACs)
    - Threat Intelligence Sharing
    - Assisted Live Lab: Reviewing IoC and Threat Intelligence Sources
  - Exploring Threat-Hunting Concepts
    - Understand Threat Hunting Concepts
    - Explain Indicators of Compromise (IoC)
    - Decoy Methods and Concepts
    - PBQ: Performing Threat Intelligence
    - Assisted Live Lab: Performing Threat Hunting
- System and Network Architecture Concepts
  - Reviewing System and Network Architecture Concepts
    - Explore Operating System Concepts
    - Understanding Virtualization, Containers, and Emulation
    - Understanding Cloud Deployment Models
    - Explore Impacts of Serverless Computing and SDN
    - Explore Software-Defined Networks
    - Understanding Deperimeterization and Zero Trust
    - PBQ: Analyzing Network Infrastructure
    - Applied Live Lab: Performing System Hardening
  - Exploring Identity and Access Management (IAM)
    - Explain Authentication Mechanisms
    - Understand Federated Trust Methods
    - Explain Cloud Access Security Broker
    - Assisted Live Lab: Configuring Centralized Logging



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Maintaining Operational Visibility
  - Understand Data Loss Prevention Concepts
  - Explain Different Data Types
  - Understand the Role of Public Key Infrastructure (PKI)
  - Explain Logging Concepts
  - Assisted Live Lab: Assess Time Sync Errors
- Process Improvement in Security Operations
  - Exploring Leadership in Security Operations
    - Maximizing Security Operations Through Automation
    - Orchestrating Threat Intelligence Data
    - Assisted Live Lab: Configuring Automation
  - Understanding Technology for Security Operations
    - Understand Single Pane of Glass
    - Explore Customization Features
    - PBQ: Responding to a Security Incident
- Vulnerability Scanning Methods
  - Explaining Compliance Requirements
    - Explore Industry Standard Publishers
    - Explain Regulations and Standards
    - Open Worldwide Application Security Project (OWASP)
    - Understand Center for Internet Security (CIS) Benchmarks
    - Understand Payment Card Industry Data Security Standard (PCI DSS)
  - Understanding Vulnerability Scanning Methods
    - Explain Assessment Scope Considerations
    - Understand Vulnerability Analysis Methods
    - Explain Device Hardening Options
    - Understand Configuration Baselines
    - PBQ: Implementing Vulnerability Scanning Methods
    - PBQ: Analyzing Vulnerability Scans
    - Assisted Live Lab: Performing Asset Discovery
    - Assisted Live Lab: Performing Passive Scanning
  - Exploring Special Considerations in Vulnerability Scanning
    - Explore Special Considerations for Scanning
    - Explain Different Types of Industrial Computer Systems
    - Assisted Live Lab: Performing Vulnerability Scanning
- Vulnerability Analysis



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Understanding Vulnerability Scoring Concepts
  - Explain Security Content Automation Protocol (SCAP)
  - Explore Common Vulnerability Scoring System (CVSS)
  - Common Vulnerability Scoring System (CVSS) Metrics
  - PBQ: Analyzing Data to Prioritize Vulnerabilities
- Exploring Vulnerability Context Considerations
  - Explore Vulnerability Validation Concepts
  - Explore CVSS Scoring Considerations
  - Assisted Live Lab: Establishing Context Awareness

- Communicating Vulnerability Information
  - Explaining Effective Communication Concepts
    - Explore Vulnerability Management Reporting
    - Explain Vulnerability Report Best Practices
    - Understand Key Performance Indicators (KPI)
    - Assisted Live Lab: Analyzing Vulnerability Reports
  - Understanding Vulnerability Reporting Outcomes and Action Plans
    - Understand Action Plans
    - Explore Common Action Plan Outcomes
    - Understand Inhibitors to Vulnerability Remediation
    - PBQ: Performing Vulnerability Assessment
    - Assisted Live Lab: Detecting Legacy Systems

- Incident Response Activities
  - Exploring Incident Response Planning
    - Understand Incident Response Planning Processes
    - Common Incident Response Plan Components
    - Explore Incident Detection and Analysis
    - Triage and Incident Response Concepts
    - Explore Incident Response Training and Testing
    - Understand Post-Incident Activities
    - Understand BCDR Concepts
    - Adaptive Live Lab: Performing Playbook Incident Response
    - Applied Live Lab: Performing IoC Detection and Analysis
  - Performing Incident Response Activities
    - Understand Incident Response Procedures
    - Explain Digital Forensic Concepts
    - Understand Legal Process Requirements



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Explore Impact Analysis
- Understand Containment and Recovery Concepts
- Applied Live Lab: Performing Post-Incident Forensic Analysis
- Applied Live Lab: Collecting Forensic Evidence

- Incident Response Communication
  - Understanding Incident Response Communication
    - Explore Stakeholder Communication
    - Understand Reporting Requirements
    - PBQ: Performing Incident Response Reporting
  - Analyzing Incident Response Activities
    - Understand the Importance of Incident Response (IR) Reporting
    - Understand Continuous Improvement Activities
    - Assisted Live Lab: Performing Root Cause Analysis

- Tools to Identify Malicious Activity
  - Identifying Malicious Activity
    - Explore Packet Capture Tools
    - Explore Endpoint Detection and Response (EDR)
    - Use Common Analysis Tools
    - Sandboxing for Malware Analysis
    - Explore Security Information and Event Management (SIEM)
    - Understand Security Orchestration, Automation, and Response (SOAR)
    - PBQ: Utilizing Digital Forensics and Indicator Analysis Techniques
    - PBQ: Analyzing Malicious Activity
    - Assisted Live Lab: Using File Analysis Techniques
    - Assisted Live Lab: Analyzing Potentially Malicious Files
    - Applied Live Lab: Using Network Sniffers
  - Explaining Attack Methodology Frameworks
    - Explore Kill Chain Concepts
    - Explore MITRE ATT&CK Framework
    - Understand the Diamond Model of Intrusion Analysis
    - Explore the Open-Source Security Testing Methodology Manual
  - Explaining Techniques for Identifying Malicious Activity
    - Email Message Internet Header Analysis
    - Email Malicious Content Analysis
    - Explore Email Server Security
    - Interpreting Suspicious Commands



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Explore Abnormal Activity
- PBQ: Identifying Malicious Activity
- Applied Live Lab: Researching DNS and IP Reputation

- Analyzing Potentially Malicious Activity
  - Exploring Network Attack Indicators
    - Understand Traffic Spikes and DDoS
    - Explore Beaconing Intrusion IoCs
    - Explore Irregular Communication Patterns
    - Review Rogue Devices and Discovery Scans
    - Explore Protocol and Port Use Scenarios
  - Exploring Host Attack Indicators
    - Explore Memory and Processor Consumption
    - Understanding Disk and File System Use
    - Review Unauthorized Software Concepts
    - Explore Malicious Process Concepts
    - Understand Unauthorized Change Concepts
    - Review Data Exfiltration Methods
  - Exploring Vulnerability Assessment Tools
    - Explore Nessus Vulnerability Scanner
    - Explore OpenVAS and Qualys Scanners
    - Review Nmap Discovery Scan Options
    - Explore Nmap Fingerprinting Concepts
    - Measuring Social Engineering Vulnerabilities
    - Understand URL Obfuscation Techniques
    - Explore Additional Assessment Tools
    - PBQ: Exploring Vulnerability Assessment Tools
    - Assisted Live Lab: Using Nontraditional Vulnerability Scanning Tools

- Application Vulnerability Assessment
  - Analyzing Web Vulnerabilities
    - Explore Burp Suite
    - Review the OWASP Zed Attack Proxy (ZAP)
    - Explore Additional Web Application Scanners
    - Review Application Debuggers
    - Applied Live Lab: Performing Web Vulnerability Scanning
  - Analyzing Cloud Vulnerabilities
    - Cloud Infrastructure Assessment Tools



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- ScoutSuite Output Analysis
- PBQ: Analyzing Cloud Vulnerability Assessment Output
- Assisted Live Lab: Analyzing Cloud Vulnerabilities

- Scripting Tools and Analysis Concepts
  - Understanding Scripting Languages
    - Review Essential Shell Scripting Commands
    - Explore Bash Shell Variables and Loops
    - Review Metacharacters, Quotes, and Redirection
    - Review Windows PowerShell
    - Explore Additional Scripting Tools
    - JavaScript Object Notation (JSON)
    - Extensible Markup Language (XML)
    - PBQ: Identifying Programming Languages
  - Identifying Malicious Activity Through Analysis
    - Using Analysis to Identify Malicious Activity
    - Identifying Anomalous Activity Example
    - PBQ: Identifying Malicious Activity through Analysis
- Application Security and Attack Mitigation Best Practices
  - Exploring Secure Software Development Practices
    - Explore Secure Software Development Practices
    - Authentication Attack Types and Best Practices
    - Understand Secure Coding Best Practices
    - Assisted Live Lab: Exploiting Weak Cryptography
  - Recommending Controls to Mitigate Successful Application Attacks
    - Overflow Attack Types and Vulnerabilities
    - SQL Injection and XML Attacks and Vulnerabilities
    - Understand Web Application Attacks
    - Review Session Hijacking Attack Types
    - Explore Application Vulnerabilities and Mitigations
    - PBQ: Applying Security Solutions for Software Assurance
    - Assisted Live Lab: Performing and Detecting Directory Traversal and Command Injection
    - Assisted Live Lab: Performing and Detecting XSS
    - Assisted Live Lab: Performing and Detecting LFI/RFI
    - Assisted Live Lab: Performing and Detecting SQLi
    - Assisted Live Lab: Performing and Detecting CSRF



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Implementing Controls to Prevent Attacks
  - Application Attack Mitigation Checklists
  - Assisted Live Lab: Performing and Detecting Privilege Escalation
  - Applied Live Lab: Detecting and Exploiting Security Misconfiguration

## REQUIREMENTS:

Recommended experience: Network+, Security+, or equivalent knowledge, with a minimum of 4 years of hands-on experience as an incident response analyst, security operations center (SOC) analyst, or equivalent experience

## Difficulty level

## CERTIFICATE:

The participants will obtain certificates signed by CompTIA (course completion). This course will help prepare you for the CompTIA CySA+ certification exam, which is available through the Pearson VUE test centers.

*Each participant in an authorized training CompTIA CySA+ Prep Course held in Compendium CE will receive a free CS0-003 CompTIA CySA+ Certification Exam vouchers.*

## TRAINER:

Authorized CompTIA Trainer.



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007