Szkolenie: CompTIA
CompTIA CySA+ Prep Course

DOSTĘPNE TERMINY

2026-11-23 | 5 dni | Kraków / Wirtualna sala *(Termin gwarantowany)*
2026-12-14 | 5 dni | Kraków / Wirtualna sala *(Termin gwarantowany)*

Cel szkolenia:

CompTIA Cybersecurity Analyst (CySA+) to certyfikacja z obszaru cyberbezpieczeństwa, która potwierdza umiejętność wykrywania, analizowania i reagowania na zagrożenia w rolach związanych z operacjami bezpieczeństwa oraz zarządzaniem podatnościami. Koncentruje się na wykrywaniu incydentów, reagowaniu na nie i ciągłym monitorowaniu nowoczesnych środowisk, a także na zarządzaniu podatnościami oraz skutecznej komunikacji kluczowych ryzyk.

Szkolenie wspiera uczestników na dwa sposoby. Jeśli planujesz przystąpić do egzaminu certyfikacyjnego CompTIA CySA+ (CS0-004), kurs może stanowić istotny element przygotowania. Certyfikacja nie jest jednak jedynym kluczem do sukcesu zawodowego w roli analityka bezpieczeństwa. Dzisiejszy rynek pracy wymaga praktycznych, możliwych do potwierdzenia kompetencji, a wiedza i ćwiczenia zawarte w tym kursie pomagają rozwijać umiejętności niezbędne do pewnego wykonywania zadań w każdej roli analityka cyberbezpieczeństwa.

Umiejętności, które zdobędziesz

- Identyfikowanie i badanie podejrzanej aktywności w sieciach, na punktach końcowych oraz w środowiskach chmurowych w celu wykrywania potencjalnych zagrożeń bezpieczeństwa.
- Monitorowanie i analizowanie danych z wykorzystaniem standardowych narzędzi branżowych, takich jak platformy SIEM i EDR.
- Identyfikowanie, priorytetyzowanie i ograniczanie podatności z wykorzystaniem podejścia opartego na ryzyku.
- Badanie incydentów bezpieczeństwa i reagowanie na nie z użyciem uporządkowanych procesów oraz technik stosowanych w praktyce.
- Jasne komunikowanie ustaleń dotyczących bezpieczeństwa i ryzyk interesariuszom za pomocą raportów oraz pulpitów informacyjnych.
- Stosowanie praktyk bezpieczeństwa w środowiskach chmurowych i hybrydowych przy jednoczesnym wspieraniu efektywnych operacji bezpieczeństwa.

Compendium Centrum Edukacyjne Spółka z o.o.
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.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

Role zawodowe, które korzystają z umiejętności CySA+

- Analityk bezpieczeństwa aplikacji
- Threat Hunter
- Analityk cyber threat intelligence
- Analityk podatności
- Analityk Security Operations Center (SOC)
- Architekt bezpieczeństwa
- Inżynier cyberbezpieczeństwa

Każdy uczestnik autoryzowanego szkolenia CompTIA CySA+ Prep Course realizowanego w Compendium CE otrzyma bezpłatny voucher na egzamin certyfikacyjny CS0-004 CompTIA CySA+.

Plan szkolenia:

- Podstawy Security Operations
  - Podstawy cyberbezpieczeństwa
    - Czym jest cyberbezpieczeństwo
    - Rola Security Operations Center
    - Role zawodowe w SOC
    - Role zawodowe wykorzystujące CySA+
    - Incident Lifecycle
  - Governance, Policies, and Controls
    - Rola governance
    - Koncepcje dotyczące polityk
    - Policies
    - Service Level Objectives
    - Typy kontroli
    - Funkcje kontroli
  - Wprowadzenie do Incident Response w SOC
    - Incident Response i role
    - Ścieżki eskalacji
    - Incident Response Lifecycle
- Stosowanie strategii Risk Management

Compendium Centrum Edukacyjne Spółka z o.o.
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.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Koncepcje ryzyka
  - Risk mindset
  - Stany ryzyka
  - Dobór odpowiednich strategii ryzyka
  - Risk Management Response
- Threat Modeling Frameworks
  - Threat Modeling
  - Analiza Threat Modeling
  - STRIDE Framework

- Zarządzanie bezpieczeństwem systemów i konfiguracjami
  - Attack Surface Management
    - Attack Surfaces
    - Wskaźniki złośliwej aktywności
    - Skanowanie otwartych portów z użyciem Netstat
    - Discovery Scanning
    - Narzędzia do skanowania sieci
    - Śledzenie użycia portów z użyciem TCPView
    - Aktywne zagrożenia
    - Wykrywanie złośliwego ruchu sieciowego z użyciem honeypota
    - Priorytetyzacja zagrożeń
    - Strategie mitygacji
    - Wyłączenie IIS Banner Broadcasting
    - Wyłączenie DNS Zone Transfers
  - System Hardening
    - Etapy hardeningu
    - Systemy plików
    - System plików Windows
    - Przegląd usług Windows
    - System plików Linux
    - Przegląd usług Linux
    - Procesy systemowe
    - Patch Management
    - Configuration Management
- Porównanie architektur systemowych
  - Infrastruktura i architektura systemowa
    - Podstawy infrastruktury i architektury systemowej

Compendium Centrum Edukacyjne Spółka z o.o.
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.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Cloud-Native Technologies
- Virtualization
- Containerization
- Application Programming Interfaces (APIs)

- Nowoczesne architektury sieciowe
  - Zero Trust Network Architecture
  - Network Segmentation
  - Wdrożenie Zero Trust
  - Stosowanie koncepcji architektury systemowej i sieciowej w Security Operations
  - Secure Access Service Edge
  - Hybrid Cloud
  - Konfiguracja Hybrid Cloud
  - Bezpieczeństwo Hybrid Cloud
  - Cloud Access Security Broker
- Critical Infrastructure and Industrial Controls
  - Operational Technology (OT)
  - Skanowanie IoT z użyciem Nmap
  - Industrial Control Systems (ICS)
  - Supervisory Control and Data Acquisition (SCADA) Systems
  - Bezpieczeństwo Industrial Control Systems

- Stosowanie Access Management
  - Identity and Access Management
    - Koncepcje tożsamości
    - Analiza Privilege Creep
    - Metody uwierzytelniania
    - Konfiguracja Password Policies
    - Konfiguracja User Account Control
    - Federated Identity Management
    - Authorization
    - Eskalacja uprawnień z użyciem Curl
    - Privileged Access Management
    - Zmiana uprawnień plików z użyciem icacls
    - Secrets Management
  - Device and Endpoint Management
    - Mobile Device Management
    - Kontrole urządzeń mobilnych

Compendium Centrum Edukacyjne Spółka z o.o.
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.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Zabezpieczanie urządzeń mobilnych
- Mobile Device Security
- Odzyskiwanie usuniętych plików z użyciem Recuva
- Endpoint Management
- Szyfrowanie dysku twardego
- Czyszczenie wolnej przestrzeni dyskowej

- Data Protection and Cryptography
  - Podstawy Data Protection
  - Data Loss Prevention
  - Cryptography
  - Symmetric Encryption
  - Asymmetric Encryption
  - Hashing
  - Weryfikacja integralności MD5 Hash

- Threat Intelligence and Threat Hunting
  - Koncepcje Threat Actor
    - Threat Actors
    - Advanced Persistent Threat
    - Tactics, Techniques, and Procedures
    - Pyramid of Pain
    - Heat Maps
  - Źródła Threat Intelligence
    - Źródła Intelligence Collection
    - Reconnaissance z użyciem theHarvester
    - Reconnaissance z użyciem Nmap
    - Metody Intelligence Collection
    - Confidence Levels
    - Czynniki Confidence Level
    - Typy Indicators of Compromise
    - Analiza i zastosowanie Indicators of Compromise
  - Threat Hunting
    - Threat Mapping
    - Cyber Deception
    - Breadcrumbs and Deceptive Endpoints

- Ocena podatności sieciowych
  - Podstawy Vulnerability Scanning

Compendium Centrum Edukacyjne Spółka z o.o.
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.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Asset Inventory
- Wpływ Vulnerability Scan
- Planowanie Vulnerability Scan
- Przypadki specjalne dla Vulnerability Scans
- Wdrażanie metod i koncepcji Vulnerability Scanning

- Typy Vulnerability Scan
  - Ustanowienie baseline
  - Skanowania wewnętrzne i zewnętrzne
  - Skanowania agentowe i bezagentowe
  - Skanowania z poświadczeniami i bez poświadczeń
  - Skanowanie pasywne i aktywne
  - Mapping i Fingerprinting Scans
- Wybrane narzędzia do analizy podatności
  - Podstawy enumeracji
  - Angry IP Scanner
  - Masscan
  - Nmap i Zenmap
  - Metasploit
  - Enumeracja z użyciem Metasploit
  - Bypass Windows Firewall z użyciem Metasploit
  - Maltego
  - Recon-ng
  - Nessus
  - Konfiguracja skanowania Nessus
  - Analiza wyników skanowania z raportu Nessus
  - Nuclei
  - Open Vulnerability Assessment Scanner (OpenVAS)
  - Atomic Red Team
  - Caldera
- Analiza i priorytetyzacja podatności
  - Kryteria oceny podatności
  - Analiza danych w celu priorytetyzacji podatności
  - Common Vulnerability Scoring System (CVSS)
  - Przegląd grup metryk CVSS
  - CVSS Base Metrics
  - CVSS Environmental Metrics

Compendium Centrum Edukacyjne Spółka z o.o.
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.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

        - CVSS Supplemental Metrics
        - CVSS Threat Metric
        - Exploitability Prediction Scoring System (EPSS)
        - Wdrożenie EPSS
        - Podatności w kontekście
        - Strategie mitygacji
    - Raportowanie podatności i incydentów
        - Cel raportowania i komunikacji
        - Koncepcje raportowania
        - Planowanie i śledzenie remediation
        - Czynniki utrudniające remediation
        - Metrics and Key Performance Indicators
- Zarządzanie Incident Response i komunikacją
    - Zarządzanie logami
        - Podstawy logowania zdarzeń
        - Konfiguracja logów
        - Konfiguracja Collector-Initiated Subscriptions
        - Konfiguracja Source-Initiated Subscriptions
        - Log Ingestion
        - Użycie pfSense do logowania zdarzeń
        - Bezpieczeństwo logów
        - Time Synchronization
        - Log Retention
        - Ocena Event Logs w pfSense
    - Incident Escalation
        - Deklaracja i eskalacja incydentu
        - Plan komunikacji
        - Realizacja raportowania i komunikacji Incident Response
        - Executive Summary
    - Działania post-incident
        - Przygotowanie do faz działań post-incident
        - Raportowanie post-incident
        - After-action Reports
        - Lessons Learned Meetings
        - Root Cause Analysis
        - Shift and Turnover Reports

Compendium Centrum Edukacyjne Spółka z o.o.
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.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Internal Threat Intelligence Reports
- Incident Response Metrics
  - Key Performance Indicators
  - Wyzwania KPI
  - Mean Time Metrics
  - Alert Volume
  - True and False Positive Rates
  - Phishing Click Rates
- Realizacja Incident Response Plans
  - Attack Methodology Frameworks
    - Cyber Kill Chain
    - Etapy Cyber Kill Chain
    - Zastosowanie Cyber Kill Chain
    - Diamond Model of Intrusion Analysis
    - Zastosowanie Diamond Model
    - MITRE ATT&CK Framework
    - Komponenty MITRE ATT&CK
  - Proces Incident Response
    - Przegląd procesu Incident Response
    - Preparation
    - Detection
    - Przeszukiwanie Memory Dump pod kątem malware
    - Analysis
    - Containment
    - Eradication
    - Recovery
    - Post-Incident Activities
  - Techniki Incident Response
    - Incident Analysis and Triage
    - Techniki containment
    - Techniki eskalacji
    - Tworzenie forensic drive image z użyciem Guymager
    - Evidence Acquisition
    - Analiza forensic drive image z użyciem Autopsy
    - Techniki eradication
    - Continuous Monitoring

Compendium Centrum Edukacyjne Spółka z o.o.
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.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Analiza złośliwej aktywności
  - Narzędzia Threat Detection and Analysis
    - Decoding and Parsing
    - Koncepcje analizy logów
    - Analiza logów z użyciem platform SIEM
    - Threat Intelligence Platforms
    - File Formats
    - Koncepcje sandboxingu
    - Narzędzia sandboxingowe
  - Host Indicators of Compromise
    - Indicators of Compromise
    - Nietypowe zachowanie systemu
    - Skanowanie i kończenie procesów
    - System-Related Indicators of Compromise
    - Endpoint Security Tools
    - File Analysis Tools
  - Network Indicators of Compromise
    - Nietypowe zachowanie sieci
    - Wykrywanie rogue device
    - Koncepcje Packet Analysis
    - Irregular Peer-to-Peer Communication Intrusions IoCs
    - Wykrywanie Promiscuous Mode
    - Wireshark
    - Przechwytywanie ruchu sieciowego z użyciem Wireshark
    - tcpdump
    - Przechwytywanie ruchu z użyciem TCPDump
    - Uruchomienie ataku DoS i DDoS
    - Koncepcje Snort
    - Reguły Snort
    - Przypadki użycia Snort
    - Wykrywanie i zapobieganie włamaniom z użyciem Snort
    - Suricata
    - Zeek
    - Domain and IP Reputation
  - Application and Web-based Indicators
    - Nietypowe zachowanie aplikacji

Compendium Centrum Edukacyjne Spółka z o.o.
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.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Analiza Indicators of Compromise
- Identity-based Indicators
- Service Disruptions
- Wykonanie SYN Flood
- Email Indicators
- Social Engineering
- Użycie Social Engineer Toolkit

- Automatyzacja analizy danych
  - Podstawy skryptowania
    - Cel skryptów
    - Zmienne i tablice w skryptach
    - Znaki specjalne w skryptach
    - Funkcje i komentarze w skryptach
    - Wykonywanie skryptów
    - Pętle
    - Pętle for
    - Pętle while i until
    - Instrukcje warunkowe
    - Operatory
  - Języki skryptowe
    - Shell Scripting
    - Zmienne, tablice i escape characters w Shell
    - Funkcje, pętle i operatory w Shell
    - PowerShell
    - Zmienne, tablice i escape characters w PowerShell
    - Funkcje, pętle i operatory w PowerShell
    - Python
    - Komponenty Python
    - Tworzenie skryptów w Pythonie
    - Wykonanie skanowania z użyciem skryptów Nmap
  - Security Analytics and Pattern Recognition
    - Pattern Recognition
    - Regular Expressions
    - Przykład regex
    - Interpretacja podejrzanych poleceń
    - User and Entity Behavior Analytics (UEBA)

Compendium Centrum Edukacyjne Spółka z o.o.
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.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

        - Automated Log Analysis
    - Integracja technologii i narzędzi
        - Integracja narzędzi
        - Security Orchestration, Automation and Response
        - SOAR Workflows
        - Infrastructure as Code (IaC)
- Usprawnianie procesów z wykorzystaniem automatyzacji
    - Standaryzacja i koordynacja zespołu
        - Rola efektywności w Security Operations
        - Process Improvement
        - Waste in Security Workflows
        - Process Frameworks
        - Standaryzacja w Security Operations
        - Projektowanie standardowych procesów bezpieczeństwa
        - Utrzymywanie procesów i standardów
        - Playbooks and Runbooks
        - Playbook Maintenance
    - Automation, Orchestration, and Enrichment
        - Usprawnienie Security Operations
        - Data Enrichment
        - Rule and Alert Tuning
        - Dashboards
    - AI Risks and Governance
        - Zasady odpowiedzialnego użycia AI
        - Zasady AI w praktyce
        - Omawianie ryzyk związanych z AI
        - Ryzyka bezpieczeństwa AI
        - Ryzyka organizacyjne AI
        - AI Governance
        - AI Regulation Best Practices
        - Ważne AI Compliance Frameworks
        - Organizational AI Policies
        - External Compliance Impacts
    - AI w Security Operations
        - Narzędzia AI w Security Operations
        - AI Security Use Cases

Compendium Centrum Edukacyjne Spółka z o.o.
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.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Detection and Analysis
- Testing and Management
- AI and Incident Management
- AI in Security Scripting
- AI in Security Workflows
- Automatyzacja zadań bezpieczeństwa

- Ocena podatności aplikacji
  - Analiza podatności aplikacji webowych
    - Ataki na aplikacje webowe
    - Browser Exploitation
    - Skanowanie strony WWW z użyciem Acunetix
    - Burp Suite
    - Testowanie aplikacji webowej z użyciem Burp Suite
    - Zed Attack Proxy
    - Nikto
    - Skanowanie webservera z użyciem Nikto
    - Third-Party Risks
    - Supply Chain Attacks
    - Pozyskiwanie informacji o Web Server
  - Cloud Vulnerability Assessment
    - Cloud-Based Attacks
    - ScoutSuite
    - Użycie ScoutSuite do analizy Cloud Infrastructure
    - Dodatkowe Cloud Assessment Tools
    - Cloud-Related Indicators

- Zabezpieczanie aplikacji
  - Secure Software Development and Testing
    - Analiza podatności i rekomendowanie mitygacji ryzyka
    - Application Security Testing
    - Software Assurance Maturity Model
    - Testowanie oprogramowania z użyciem Python
    - Secure Coding Best Practices
  - Identyfikacja i mitygacja ataków na aplikacje
    - Packet Analysis
    - Wireshark and Packet Analysis
    - Wykorzystanie SQL na stronie WWW

Compendium Centrum Edukacyjne Spółka z o.o.
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.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Web Application Scanners
- Wykrywanie SQL Injection Flaws z użyciem sqlmap
- Risk Reduction and Acceptance
- Hidden Field Manipulation Attacks
- Third-Party Risk Management

Wymagania:

Zalecane doświadczenie: Network+, Security+ lub równoważna wiedza, a także co najmniej 4 lata praktycznego doświadczenia jako analityk reagowania na incydenty, analityk Security Operations Center (SOC) lub doświadczenie na podobnym stanowisku.

Poziom trudności



Certyfikaty:

Uczestnicy szkolenia otrzymują certyfikat ukończenia szkolenia wystawiony imiennie oraz na firmę sygnowany przez firmę CompTIA. Kurs pomaga przygotować się do egzaminu certyfikacyjnego CompTIA CySA+, który jest dostępny w centrach egzaminacyjnych Pearson VUE.

Każdy uczestnik autoryzowanego szkolenia CompTIA CySA+ Prep Course realizowanego w Compendium CE otrzyma bezpłatny voucher na egzamin certyfikacyjny CS0-004 CompTIA CySA+.

Prowadzący:

Autoryzowany trener CompTIA.

Compendium Centrum Edukacyjne Spółka z o.o.
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.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001