Szkolenie: CompTIA
CompTIA CySA+ Prep Course

DOSTĘPNE TERMINY

2026-06-22 | 5 dni | Warszawa / Wirtualna sala
2026-08-24 | 5 dni | Warszawa / Wirtualna sala
2026-09-28 | 5 dni | Kraków / Wirtualna sala
2026-10-26 | 5 dni | Warszawa / Wirtualna sala
2026-11-30 | 5 dni | Kraków / Wirtualna sala
2026-12-07 | 5 dni | Warszawa / Wirtualna sala
2026-12-14 | 5 dni | Kraków / Wirtualna sala

Cel szkolenia:

CompTIA CySA+ to certyfikacja na poziomie średniozaawansowanym, przeznaczona dla specjalistów z około czteroletnim doświadczeniem praktycznym w obszarze cyberbezpieczeństwa – w szczególności dla analityków reagowania na incydenty oraz pracowników Security Operations Center (SOC).

Szkolenie wspiera rozwój zawodowy na dwóch płaszczyznach:

- **Certyfikacja:** Jeśli planujesz przystąpić do egzaminu CompTIA CySA+ (CS0-003), otrzymasz solidne i uporządkowane przygotowanie merytoryczne, zgodne z najnowszymi wytycznymi.
- **Kompetencje praktyczne:** Niezależnie od certyfikacji, rozwiniesz kluczowe umiejętności wymagane w nowoczesnym SOC. Dowiesz się, jak wykorzystać **AI do automatyzacji zadań** i syntezy danych, jak projektować **mechanizmy aktywnej obrony** (Deception Technology) oraz jak skutecznie zarządzać **bezpieczeństwem w chmurze** i wymogami zgodności.

Dzięki takiemu podejściu łatwiej przełożysz zdobytą wiedzę na codzienne operacje, optymalizując czas obsługi incydentów oraz wzmacniając odporność infrastruktury organizacji.

Po ukończeniu szkolenia będziesz potrafić:

- Zarządzać cyklem życia podatności, od ich wykrywania po proces mitygacji i weryfikacji.
- Wykorzystywać mechanizmy Threat Intelligence i Threat Hunting do proaktywnego wykrywania zagrożeń.
- Analizować architekturę systemów i sieci pod kątem zaawansowanych wektorów ataków (np. VLAN Hopping, Rogue DHCP).

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

- Optymalizować i automatyzować procesy w Security Operations Center (SOC).
- Dobierać i konfigurować narzędzia do skanowania podatności w zróżnicowanych środowiskach.
- Klasyfikować i priorytetyzować ryzyka w oparciu o ich analizę i wpływ na działanie biznesu.
- Realizować pełną procedurę Incident Response, w tym profesjonalną analizę poincydentową.
- Stosować standardy komunikacji i raportowania podczas obsługi incydentów krytycznych.
- Identyfikować i analizować symptomy złośliwej aktywności przy użyciu narzędzi detekcyjnych.
- Oceniać bezpieczeństwo aplikacji webowych oraz infrastruktury chmurowej.
- Wykorzystywać AI do tworzenia automatyzacji oraz szybkiej syntezy danych technicznych.
- Wdrażać najlepsze praktyki bezpieczeństwa aplikacji i skutecznie mitygować ataki w warstwie siódmej (L7) modelu OSI.

Jakie umiejętności rozwiniesz:

- **Analityka i detekcja zagrożeń:** Nauczysz się optymalizować operacje bezpieczeństwa, skutecznie wdrażać procesy **Threat Intelligence i Threat Hunting** oraz precyzyjnie identyfikować incydenty przy użyciu zaawansowanego stosu narzędziowego.
- **Zaawansowane zarządzanie podatnościami:** Opanujesz przeprowadzanie kompleksowych ocen bezpieczeństwa, priorytetyzację ryzyk oraz projektowanie strategii mitygacji, które realnie ograniczają powierzchnię ataku.
- **Operacyjne reagowanie na incydenty:** Poznasz praktyczne zastosowanie ram metodyk ataków (np. **MITRE ATT&CK**) oraz przejmiesz pełną kontrolę nad cyklem życia incydentu – od detekcji, przez izolację, aż po skuteczne usunięcie skutków ataku.
- **Raportowanie i komunikacja techniczna:** Rozwiniesz umiejętność tworzenia profesjonalnej dokumentacji i raportów, przekładając techniczne parametry i metryki na zrozumiałe plany działań dla interesariuszy biznesowych.

Role zawodowe, którym przydadzą się umiejętności CySA+

- Analityk bezpieczeństwa aplikacji
- Threat Hunter
- Threat Intelligence Analyst
- Analityk podatności
- Analityk SOC (Security Operations Center)
- Architekt bezpieczeństwa
- Inżynier cyberbezpieczeństwa

Każdy uczestnik autoryzowanego szkolenia CompTIA CySA+ Prep Course realizowanego w

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

Compendium CE otrzyma bezpłatny voucher na egzamin certyfikacyjny CompTIA CySA+ CS0-003.

Plan szkolenia:

- Zarządzanie cyklem życia podatności, ich mitygacja oraz operacyjna obsługa zagrożeń
  - Kształtowanie postaw przywódczych i strategii zarządzania w cyberbezpieczeństwie
    - Omówienie zagadnień polityk i ładu korporacyjnego
    - Wyjaśnienie zasad zarządzania ryzykiem
    - Wprowadzenie do koncepcji modelowania zagrożeń
    - Laboratorium: zapoznanie ze środowiskiem laboratoryjnym
  - Rodzaje i metody kontroli bezpieczeństwa
    - Kategorie i typy kontroli bezpieczeństwa
    - Funkcjonalne typy kontroli bezpieczeństwa
    - Zarządzanie i redukcja powierzchni ataków cybernetycznych
    - Laboratorium: konfiguracja kontroli bezpieczeństwa
  - Koncepcje zarządzania poprawkami
    - Poprawki oprogramowania i zabezpieczenia hostów
    - Zarządzanie konfiguracją systemów
    - Planowanie okien konserwacyjnych oraz mitygacja ryzyka podczas prac serwisowych
- Operacyjne wykorzystanie Threat Intelligence i metodyk Threat Hunting
  - Modelowanie charakterystyki adwersarzy w procesie analizy ryzyka
    - Taksonomia aktorów zagrożeń: od grup APT po zagrożenia wewnętrzne
    - Analiza zaawansowanych trwałych zagrożeń (APT): charakterystyka i cykl życia
    - Identyfikacja wzorców zachowań intruzów poprzez mapowanie TTP (Tactics, Techniques, and Procedures)
  - Identyfikacja aktywnych zagrożeń
    - Wywiad ze źródeł otwartych (OSINT)
    - Źródła wywiadu zamkniętego i komercyjnego
    - Rola organizacji ISAC w ekosystemie wymiany informacji o zagrożeniach
    - Mechanizmy i standardy współdzielenia danych wywiadowczych
    - Laboratorium: przegląd IoC i źródeł Threat Intelligence
  - Koncepcje polowania na zagrożenia (Threat Hunting)
    - Podstawowe założenia Threat Hunting
    - Wskaźniki kompromitacji (IoC)
    - Architektura aktywnych mechanizmów obronnych oparta na koncepcji wabików

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

- PBQ: realizacja zadania z Threat Intelligence
- Laboratorium: aktywne wykrywanie intruzów przy użyciu metod Threat Hunting

- Koncepcje architektury systemów i sieci
  - Przegląd koncepcji architektury systemów i sieci
    - Koncepcje systemów operacyjnych
    - Wirtualizacja, kontenery i emulacja systemów i aplikacji
    - Modele wdrożeń chmurowych
    - Analiza wpływu architektur Serverless oraz SDN na model bezpieczeństwa
    - Sieci definiowane programowo (SDN)
    - Deperymetryzacja i Zero Trust
    - PBQ: analiza infrastruktury sieciowej
    - Laboratorium: Praktyczne utwardzanie systemów i konfiguracja mechanizmów obronnych
  - Zarządzanie tożsamością i dostępem
    - Mechanizmy uwierzytelniania
    - Metody zaufania federacyjnego
    - Implementacja i rola brokera CASB w ochronie zasobów chmurowych
    - Laboratorium: konfiguracja scentralizowanego logowania
  - Utrzymanie widoczności operacyjnej
    - Koncepcje systemów Data Loss Prevention (DLP)
    - Różne typy danych i metody ich ochrony
    - Rola infrastruktury klucza publicznego (PKI)
    - Koncepcje logowania
    - Laboratorium: ocena błędów synchronizacji czasu
- Doskonalenie procesów w operacjach bezpieczeństwa
  - Rola lidera w koordynacji procesów detekcji i reagowania na incydenty
    - Maksymalizacja efektywności SecOps dzięki automatyzacji
    - Orkiestracja danych Threat Intelligence
    - Laboratorium: konfiguracja automatyzacji
  - Technologie wspierające operacje bezpieczeństwa
    - Koncepcja „single pane of glass”
    - Konfigurowalność platform bezpieczeństwa i dostosowanie do procesów operacyjnych
    - PBQ: reakcja na incydent bezpieczeństwa
- Metody skanowania podatności
  - Standardy regulacyjne dotyczące częstotliwości i zakresu skanowania podatności
    - Organizacje publikujące standardy branżowe

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

- Regulacje i standardy
- OWASP (Open Worldwide Application Security Project)
- CIS Benchmarks (Center for Internet Security)
- PCI DSS (Payment Card Industry Data Security Standard)

- Metody skanowania podatności
  - Ustalanie granic skanowania i parametrów operacyjnych oceny podatności
  - Metody analizy podatności
  - Implementacja mechanizmów obronnych i optymalizacja ustawień bezpieczeństwa sprzętu
  - Bazowe konfiguracje bezpieczeństwa
  - PBQ: wdrażanie metod skanowania podatności
  - PBQ: analiza wyników skanów podatności
  - Laboratorium: identyfikacja zasobów
  - Laboratorium: skanowanie pasywne
- Szczególne aspekty skanowania podatności
  - Szczególne przypadki i ograniczenia skanowania podatności
  - Typy przemysłowych systemów komputerowych
  - Laboratorium: wykonywanie skanowania podatności

- Analiza podatności
  - Metodyki punktacji i priorytetyzacji podatności
    - SCAP (Security Content Automation Protocol)
    - CVSS (Common Vulnerability Scoring System)
    - Metryki CVSS
    - PBQ: analiza danych do priorytetyzacji podatności
  - Kontekst podatności
    - Walidacja podatności
    - Uwarunkowania przy ocenie CVSS
    - Laboratorium: budowanie świadomości kontekstu

- Komunikowanie informacji o podatnościach
  - Koncepcje skutecznej komunikacji
    - Raportowanie w zarządzaniu podatnościami
    - Dobre praktyki tworzenia raportów o podatnościach
    - Kluczowe wskaźniki efektywności (KPI)
    - Laboratorium (prowadzone): analiza raportów podatności
  - Rezultaty raportowania podatności i plany działań
    - Plany działań

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

- Typowe rezultaty planów działań
- Czynniki utrudniające usuwanie podatności
- PBQ: wykonanie oceny podatności
- Laboratorium: Wykrywanie przestarzałych technologii i ocena ryzyka systemów typu Legacy

- Działania w ramach reagowania na incydenty
  - Planowanie reagowania na incydenty
    - Procesy planowania IR
    - Typowe elementy planu IR
    - Wykrywanie i analiza incydentów
    - Metodyka triażu i strategiczne koncepcje reagowania na incydenty
    - Szkolenia i testowanie planów IR
    - Działania po incydencie
    - Podstawy i koncepcje BCDR
    - Laboratorium: operacyjne wykorzystanie playbooków w procesie Incident Response
    - Laboratorium: wykrywanie i analiza IoC
  - Realizacja działań IR
    - Procedury reagowania na incydenty
    - Podstawy informatyki śledczej
    - Wymagania procesów prawnych
    - Szacowanie skutków incydentu i ocena skali szkód w organizacji
    - Koncepcje izolacji i odtwarzania po awarii lub incydencie
    - Laboratorium: analiza powłamaniowa po incydencie
    - Laboratorium: zbieranie dowodów cyfrowych
- Komunikacja w reagowaniu na incydenty
  - Komunikacja podczas reagowania na incydent
    - Komunikacja z interesariuszami
    - Wymagania raportowe
    - PBQ: raportowanie działań IR
  - Analiza działań IR
    - Znaczenie raportowania IR
    - Strategie ciągłego doskonalenia procesów bezpieczeństwa w organizacji
    - Laboratorium: analiza przyczyn źródłowych incydentu
- Narzędzia do identyfikacji złośliwej aktywności
  - Identyfikacja złośliwej aktywności
    - Narzędzia do przechwytywania pakietów

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

- EDR, XDR, MDR
- Typowe narzędzia analityczne
- Dynamiczna analiza złośliwego oprogramowania z użyciem technologii Sandbox
- SIEM (Security Information and Event Management)
- SOAR (Security Orchestration, Automation, and Response)
- PBQ: techniki analizy wskaźników i informatyki śledczej
- PBQ: analiza złośliwej aktywności
- Laboratorium: techniki analizy plików
- Laboratorium: analiza potencjalnie złośliwych plików
- Laboratorium: przechwytywanie i inspekcja pakietów w diagnostyce bezpieczeństwa

- Ramy metodyk ataków
  - Metodyka Cyber Kill Chain: analiza faz ataku i punktów mitygacji
  - MITRE ATT&CK
  - Analiza włamań z wykorzystaniem modelu diamentowego
  - OSSTMM
- Techniki identyfikacji złośliwej aktywności
  - Analiza nagłówków wiadomości e-mail
  - Analiza złośliwej zawartości wiadomości e-mail
  - Bezpieczeństwo serwerów pocztowych
  - Interpretacja podejrzanych poleceń
  - Identyfikacja nietypowej aktywności
  - PBQ: identyfikacja złośliwej aktywności
  - Laboratorium: badanie reputacji DNS i IP

- Analiza potencjalnie złośliwej aktywności
  - Wskaźniki ataków sieciowych
    - Mitygacja skutków nagłych skoków ruchu i odpieranie ataków DDoS
    - Analiza wzorców beaconingu jako kluczowych wskaźników kompromitacji (IoC)
    - Nieregularne wzorce komunikacji
    - Identyfikacja nieautoryzowanych urządzeń w architekturze sieciowej
    - Praktyczne scenariusze wykorzystania protokołów i portów w komunikacji sieciowej
  - Wskaźniki ataków na hosty
    - Zużycie pamięci i procesora
    - Użycie dysku i systemu plików
    - Nieautoryzowane oprogramowanie
    - Złośliwe procesy

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

- Nieautoryzowane zmiany
- Techniki i kanały eksfiltracji danych w nowoczesnych cyberatakach
- Narzędzia do oceny podatności
  - Nessus
  - OpenVAS i Qualys
  - Opcje skanów wykrywania w Nmap
  - Fingerprinting w Nmap
  - Metodyka pomiaru podatności pracowników na ataki socjotechniczne
  - Mechanizmy maskowania linków i identyfikacja złośliwych przekierowań
  - PBQ: przegląd narzędzi do oceny podatności
  - Laboratorium: użycie nietypowych narzędzi skanowania podatności
- Ocena podatności aplikacji
  - Analiza podatności aplikacji webowych
    - Burp Suite
    - OWASP Zed Attack Proxy (ZAP)
    - Dodatkowe skanery aplikacji webowych
    - Debuggery aplikacji
    - Laboratorium: skanowanie podatności aplikacji webowej
  - Analiza podatności w chmurze
    - Narzędzia do oceny infrastruktury chmurowej
    - Analiza wyników ScoutSuite
    - PBQ: analiza wyników oceny podatności w chmurze
    - Laboratorium: analiza podatności w chmurze
- Narzędzia skryptowe i koncepcje analizy
  - Języki skryptowe
    - Fundamenty automatyzacji: wykorzystanie wiersza poleceń i interpretera Bash
    - Zmienne i pętle w Bash
    - Zastosowanie metaznaków, mechanizmów cytowania i przekierowań strumieni
    - Windows PowerShell
    - Dodatkowe narzędzia skryptowe
    - JSON
    - XML
    - PBQ: identyfikacja języków programowania
  - Identyfikacja złośliwej aktywności poprzez analizę
    - Wykorzystanie analizy do wykrywania złośliwej aktywności
    - Przykład identyfikacji anomalii

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

- PBQ: identyfikacja złośliwej aktywności na podstawie analizy

- Dobre praktyki bezpieczeństwa aplikacji i mitygacji ataków
  - Praktyki bezpiecznego kodowania
    - Implementacja mechanizmów bezpieczeństwa w cyklu życia aplikacji
    - Ataki na mechanizmy uwierzytelniania: przegląd wektorów i dobre praktyki obronne
    - Laboratorium: wykorzystanie słabej kryptografii
  - Dobór kontroli ograniczających skuteczne ataki na aplikacje
    - Mechanizmy naruszania pamięci: od Buffer Overflow po błędy typu Integer Overrun
    - Wstrzykiwanie kodu: analiza podatności SQL Injection oraz ataków na parsery XML
    - Typy ataków na aplikacje webowe
    - Analiza kradzieży identyfikatorów sesji i metod nieautoryzowanego dostępu
    - Podatności aplikacji webowych i sposoby mitygacji
    - PBQ: zastosowanie rozwiązań bezpieczeństwa dla zapewnienia jakości
    - Laboratorium: Eksploatacja i detekcja podatności Directory Traversal oraz Command Injection
    - Laboratorium: XSS - wykonanie i detekcja
    - Laboratorium: LFI/RFI - wykonanie i detekcja
    - Laboratorium: SQLi - wykonanie i detekcja
    - Laboratorium: CSRF - wykonanie i detekcja
  - Wdrażanie kontroli zapobiegających atakom
    - Listy kontrolne zabezpieczeń: praktyczne kroki w ograniczaniu ryzyka dla aplikacji
    - Laboratorium: eskalacja uprawnień - wykonanie i detekcja
    - Laboratorium: detekcja i wykorzystanie błędnej konfiguracji bezpieczeństwa

Wymagania:

Rekomendowane doświadczenie: Network+, Security+ lub równoważna wiedza; co najmniej 4 lata praktycznego doświadczenia jako analityk reagowania na incydenty, analityk SOC lub na stanowisku o podobnym profilu.

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

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

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 CompTIA CySA+ CS0-003.

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