Szkolenie: CompTIA
CompTIA Security+ Prep Course

CompTIA Authorized Partner DELIVERY PARTNER

DOSTĘPNE TERMINY

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

Cel szkolenia:

Certyfikacja CompTIA Security+ to globalny standard potwierdzający fundamentalne kompetencje z zakresu cyberbezpieczeństwa. Szkolenie zostało zaprojektowane, aby kompleksowo przygotować uczestników do egzaminu SY0-701 oraz wyposażyć ich w praktyczne umiejętności niezbędne do pracy na stanowiskach pierwszej linii w obszarze bezpieczeństwa IT.

Program łączy przygotowanie teoretyczne z intensywnymi ćwiczeniami, pozwalając na zdobycie kompetencji realnie oczekiwanych przez współczesny rynek pracy. Uczestnicy zdobędą wiedzę niezbędną do realizacji kluczowych zadań związanych z zabezpieczaniem zasobów, identyfikacją zagrożeń oraz skutecznym reagowaniem na incydenty, co stanowi solidny fundament do budowy kariery w sektorze Cybersecurity.

Po ukończeniu szkolenia będziesz potrafił:

- Charakteryzować kluczowe koncepcje bezpieczeństwa oraz ich wpływ na infrastrukturę IT.
- Klasyfikować i porównywać współczesne typy zagrożeń, podatności oraz wektory ataków.
- Dobierać optymalne rozwiązania kryptograficzne w celu zapewnienia poufności i integralności danych.
- Implementować systemy zarządzania tożsamością i dostępem zgodnie z najlepszymi praktykami.
- Projektować bezpieczną architekturę sieciową zarówno w środowiskach lokalnych, jak i chmurowych.
- Stosować zasady odporności systemów oraz mechanizmy bezpieczeństwa fizycznego i obiektowego.
- Zarządzać procesem wykrywania i mitygowania podatności w strukturach organizacji.
- Audytować i oceniać poziom bezpieczeństwa sieci oraz urządzeń klienckich.
- Wzmacniać bezpieczeństwo aplikacji na różnych etapach ich cyklu życia.
- Monitorować środowisko IT i skutecznie reagować na incydenty naruszenia 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

- Analizować wskaźniki ataku i kompromitacji systemu.
- Operować w ramach ładu organizacyjnego, uwzględniając analizę ryzyka i zarządzanie procesami bezpieczeństwa.
- Implementować ochronę danych oraz stosować zasady zgodność z obowiązującymi regulacjami i standardami w podstawowym zakresie.

Role zawodowe, które skorzystają na kompetencjach Security+

- Analityk cyberbezpieczeństwa (Cybersecurity Analyst) / analityk SOC (SOC Analyst)
- Administrator bezpieczeństwa (Security Administrator)
- Administrator systemów (Systems Administrator)
- Administrator sieci (Network Administrator)
- Młodszy audytor IT (Junior IT Auditor)
- Konsultant ds. bezpieczeństwa (Security Consultant)
- Inżynier wsparcia technicznego (Technical Support Engineer)
- Specjalista ds. bezpieczeństwa (Security Specialist)

Każdy uczestnik autoryzowanego szkolenia CompTIA Security+ Prep Course realizowanego w Compendium CE otrzyma bezpłatny voucher na egzamin certyfikacyjny CompTIA Security+ (SY0-701).

Plan szkolenia:

- Podsumowanie podstawowych koncepcji bezpieczeństwa
  - Koncepcje bezpieczeństwa
    - Bezpieczeństwo informacji
    - Ramy cyberbezpieczeństwa
    - Badanie poziomu bezpieczeństwa obecnego względem docelowego (Gap Analysis)
    - Kontrola dostępu
    - Laboratorium: poznanie środowiska laboratoryjnego
    - Laboratorium: analiza luk w konfiguracji systemu
  - Mechanizmy kontroli bezpieczeństwa
    - Kategorie mechanizmów kontrolnych
    - Typy funkcjonalne mechanizmów kontrolnych
    - Role i odpowiedzialności w bezpieczeństwie informacji

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

- Kompetencje w bezpieczeństwie informacji
- Jednostki biznesowe a bezpieczeństwo informacji
- Zadanie egzaminacyjne PBQ: porównanie typów mechanizmów kontrolnych i metodyk bezpieczeństwa informacji.
- Laboratorium: konfiguracja przykładów typów mechanizmów kontrolnych

- Porównanie typów zagrożeń
  - Podmioty zagrożeń
    - Podatność, zagrożenie i ryzyko
    - Atrybuty podmiotów zagrożeń
    - Motywacje podmiotów zagrożeń
    - Hakerzy vs haktywiści
    - Grupy APT
    - Zorganizowana przestępczość w obszarze cyberprzestrzeni
    - Zagrożenia wewnętrzne
  - Powierzchnie ataku
    - Powierzchnia ataku vs wektory ataku
    - Wektory związane z podatnym oprogramowaniem
    - Wektory sieciowe
    - Techniki wykorzystujące manipulację i wabiki
    - Wektory oparte na wiadomościach
    - Zagrożenia w łańcuchu dostaw
    - Laboratorium: wyszukiwanie otwartych portów usług sieciowych
  - Socjotechnika
    - Wektory ludzkie
    - Podszywanie się
    - Phishing i pharming
    - Typosquatting
    - Oszustwa klasy BEC
    - Zadanie egzaminacyjne PBQ: porównanie technik socjotechnicznych
    - Laboratorium: wykorzystanie narzędzia SET do działań socjotechnicznych

- Rozwiązania kryptograficzne
  - Algorytmy kryptograficzne
    - Podstawowe pojęcia kryptograficzne
    - Szyfrowanie symetryczne
    - Długość klucza
    - Szyfrowanie asymetryczne

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

- Funkcje skrótu
- Podpisy cyfrowe
- Zadanie egzaminacyjne PBQ: identyfikacja trybów pracy kryptografii
- Laboratorium praktyczne: szyfrowanie danych na nośnikach

- Infrastruktura klucza publicznego (PKI)
  - Urzędy certyfikacyjne w PKI
  - Certyfikaty cyfrowe
  - Źródło zaufania w systemie
  - Proces generowania CSR
  - Atrybuty certyfikatu
  - Proces unieważniania certyfikatów
  - Zarządzanie kluczami kryptograficznymi
  - Kryptoprocesory i bezpieczne enklawy
  - Depozyt kluczy kryptograficznych
  - Zadanie egzaminacyjne PBQ: wdrożenie certyfikatów i urzędów certyfikacji
- Rozwiązania kryptograficzne
  - Szyfrowanie a poufność
  - Szyfrowanie dysków i plików
  - Szyfrowanie baz danych
  - Szyfrowanie transmisji i wymiana klucza
  - Mechanizmy zabezpieczenia kluczy (PFS, Salting, Key Streching)
  - Podstawy Blockchain
  - Zaciemnianie logiki kodów
  - Laboratorium praktyczne: haszowanie i solenie

- Zarządzanie tożsamością i dostępem (IAM)
  - Uwierzytelnianie
    - Projektowanie procesów uwierzytelniania
    - Koncepcje haseł
    - Menedżer haseł
    - Uwierzytelnianie wieloskładnikowe (MFA)
    - Uwierzytelnianie biometryczne
    - Sprzętowe tokeny uwierzytelniania
    - Programowe tokeny uwierzytelniania
    - Uwierzytelnianie bezhasłowe
    - Laboratorium: zarządzanie bezpieczeństwem haseł
  - Autoryzacja

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

- Kontrola dostępu uznaniowa i obowiązkowa (DAC/MAC)
- Kontrola dostępu oparta na rolach i atrybutach (RBAC/ABAC
- Kontrola dostępu oparta na regułach
- Zasada najmniejszych uprawnień
- Nadawanie kont użytkowników
- Atrybuty kont i polityki dostępu
- Ograniczenia kont
- Zarządzanie dostępem uprzywilejowanym (PAM)
- Zadanie egzaminacyjne PBQ: wdrożenie modelu kontroli dostępu
- Laboratorium: zarządzanie uprawnieniami

- Zarządzanie tożsamością
  - Uwierzytelnianie lokalne, sieciowe i
  - Usługi katalogowe (Directory Services) i Kerberos
  - Logowanie jednokrotne – uwierzytelnianie (SSO)
  - Uwierzytelnianie federacyjne
  - SAML
  - OAuth vs OIDC
  - API

- Zabezpieczanie architektury sieciowej w środowisku organizacji
  - Architektura sieci przedsiębiorstwa
    - Koncepcje architektury i infrastruktury
    - Infrastruktura sieciowa
    - Aspekty infrastruktury przełączania ruchu sieciowego
    - Aspekty infrastruktury trasowania ruchu sieciowego
    - Strefy bezpieczeństwa i segmentacja sieci
    - Powierzchnie ataków sieciowych
    - Bezpieczeństwo portów
    - Separacja fizyczna
    - Aspekty architektoniczne sieci
  - Urządzenia bezpieczeństwa sieci
    - Rozmieszczenie urządzeń
    - Atrybuty urządzeń
    - Zapory sieciowe przegląd rozwiązań i metody użycia
    - Typy i zastosowania serwerów proxy
    - Systemy wykrywania włamań (IDS, IPS)
    - Zarządzanie dystrybucją ruchu (LB)

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

- Bezpieczeństwo aplikacji webowych i zastosowania rozwiązań klasy Web Application Firewall
- Bezpieczna komunikacja
  - Architektura dostępu zdalnego
  - Tunelowanie z wykorzystaniem TLS
  - Tunelowanie z wykorzystaniem IPsec
  - IPSec w detalach
  - Pulpit zdalny
  - SSH
  - Zdalne zarządzanie Out-of-Band oraz serwery pośredniczące (Jump Servers)
  - Zadanie egzaminacyjne PBQ: wdrożenie bezpiecznych protokołów zdalnego dostępu
  - Laboratorium: konfiguracja dostępu zdalnego
  - Laboratorium: wykorzystanie tunelowania IPSec
- Zabezpieczanie architektury sieciowej w chmurze
  - Infrastruktura chmurowa
    - Modele wdrożenia chmury
    - Modele usług chmurowych
    - Macierz odpowiedzialności rozwiązań chmurowych
    - Przetwarzanie scentralizowane i zdecentralizowane
    - Zasady budowy systemów o wysokiej odporności
    - Wirtualizacja aplikacji i kontenery
    - Architektura chmurowa
    - Technologie automatyzacji chmury
    - Sieci definiowane programowo (SDN)
    - Cechy architektury chmurowej
    - Aspekty bezpieczeństwa chmury
    - Zadanie egzaminacyjne PBQ: analiza typów i funkcji infrastruktury
    - Laboratorium: praca z kontenerami
    - Laboratorium: wykorzystanie wirtualizacji
  - Systemy wbudowane i architektura Zero Trust
    - Systemy wbudowane
    - Przemysłowe systemy sterowania (ICS)
    - Internet Rzeczy (IoT)
    - Deperymetryzacja
    - Koncepcje bezpieczeństwa Zero Trust
- Odporność i bezpieczeństwo obiektowe

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

- Zarządzanie zasobami
  - Ewidencja zasobów
  - Koncepcje ochrony aktywów w organizacji
  - Kopie zapasowe danych
  - Zaawansowana ochrona danych
  - Bezpieczne niszczenie danych
  - Laboratorium praktyczne: wdrożenie kopii zapasowych
  - Laboratorium: sanityzacja nośników
- Strategie redundancji
  - Zapewnienie ciągłości działania (BCP) oraz odtwarzanie po awarii (DR)
  - Ryzyka związane z planowaniem zasobów
  - Wysoka dostępność (HA)
  - Klasteryzacja
  - Redundancja zasilania
  - Strategia obrony głębokiej i dywersyfikacja zabezpieczeń
  - Mechanizmy dezinformacji i pułapki systemowe
  - Testowanie odporności na awarie
  - Zadanie egzaminacyjne PBQ: uwzględnienie strategii redundancji
- Bezpieczeństwo fizyczne
  - Mechanizmy kontroli bezpieczeństwa fizycznego
  - Zabezpieczenia obwodowe i infrastruktura obiektu
  - Kontrola wejść i systemy zamknięć
  - Telewizja dozorowa (CCTV) i monitoring fizyczny
  - Systemy alarmowe i czujniki antywłamaniowe

- Zarządzanie podatnościami
  - Podatności urządzeń i systemów operacyjnych
    - Podatności systemów operacyjnych
    - Typy podatności
    - Podatności typu zero-day
    - Podatności wynikające z błędnej konfiguracji
    - Podatności kryptograficzne
    - Naruszenia integralności systemów mobilnych: sideloading, rooting i jailbreaking
    - Zadanie egzaminacyjne PBQ: identyfikacja typów podatności
  - Podatności aplikacji i usług chmurowych
    - Podatności aplikacji
    - Ewaluacja podatności i artefaktów

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

- Ataki na aplikacje webowe
- Ataki na aplikacje w chmurze
- Łańcuch dostaw (Supply Chain)
- Laboratorium: wykorzystanie i wykrywanie SQL injection (SQLi)

- Metody identyfikacji podatności
  - Skanowanie podatności
  - Źródła informacji o zagrożeniach
  - Deep web i dark web
  - Inne metody oceny podatności
  - Laboratorium: praca ze źródłami informacji o zagrożeniach
- Analiza podatności i działania naprawcze
  - CVE, NVD, CVSS
  - Błędy detekcji (False Positives/Negatives) oraz analityka logów
  - Analiza podatności
  - Obsługa podatności i procesy remediacyjne
  - Laboratorium: wykonywanie skanów podatności

- Ocena możliwości w zakresie bezpieczeństwa sieci
  - Bazowe konfiguracje bezpieczeństwa sieci
    - Benchmarki i przewodniki bezpiecznych konfiguracji
    - Aspekty instalacji sieci bezprzewodowych w organizacjach
    - Szyfrowanie WLAN
    - Metody uwierzytelniania w sieciach WLAN
    - Kontrola dostępu do sieci
    - Zadanie egzaminacyjne PBQ: wdrożenie bezpiecznej infrastruktury bezprzewodowej
    - Laboratorium: zrozumienie bazowych konfiguracji bezpieczeństwa
  - Wzmacnianie możliwości bezpieczeństwa sieci
    - Filtrowanie ruchu i kontrola dostępu na poziomie sieci (ACL)
    - Wdrażanie rozwiązań IDS/IPS w architekturze sieciowej
    - Metody detekcji używane w systemach IDS i IPS
    - Systemy filtrowania treści internetowych (Web Filtering) i kontrola aplikacji
    - Laboratorium praktyczne: wdrażanie zapory sieciowej (firewall)
- Ocena możliwości w zakresie bezpieczeństwa urządzeń końcowych
  - Wdrażanie bezpieczeństwa na urządzeniach końcowych
    - Utwardzanie urządzeń końcowych
    - Ochrona urządzeń końcowych

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

- Zaawansowana ochrona urządzeń końcowych
- Konfiguracja urządzeń końcowych
- Techniki utwardzania
- Utwardzanie urządzeń specjalizowanych
- Laboratorium z asystą: wykorzystanie zasad grupy (GPO)
- Laboratorium praktyczne: utwardzanie (hardening)

- Utwardzanie urządzeń mobilnych
  - Techniki utwardzania urządzeń mobilnych
  - Szyfrowanie całego urządzenia oraz zewnętrznych nośników pamięci
  - Usługi lokalizacyjne
  - Metody łączności komórkowej i GPS
  - Metody łączności Wi-Fi i tethering
  - Metody łączności Bluetooth
  - NFC i płatności mobilne (NFC)
  - Zadanie egzaminacyjne PBQ: wdrożenie MDM (Mobile Device Management)

- Wzmacnianie bezpieczeństwa aplikacji
  - Bazowe zabezpieczenia protokołów aplikacyjnych
    - Protokoły bezpieczne
    - TLS
    - Bezpieczne usługi katalogowe
    - Bezpieczeństwo SNMP
    - Usługi transferu plików
    - Usługi pocztowe
    - Bezpieczeństwo poczty elektronicznej
    - DLP systemów pocztowych
    - Filtrowanie DNS
    - Zadanie egzaminacyjne PBQ: zmiany w organizacji w kontekście wzmocnienia bezpieczeństwa
    - Laboratorium z asystą: filtrowanie DNS
  - Bezpieczeństwo aplikacji w chmurze i aplikacji webowych
    - Techniki bezpiecznego programowania
    - Zabezpieczenia aplikacji
    - Koncepcja piaskownicy
    - Laboratorium z asystą: konfiguracja monitorowania systemu

- Reagowanie na incydenty i monitorowanie zdarzeń
  - Reagowanie na incydenty

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

- Procesy reagowania na incydenty
- Przygotowanie
- Wykrywanie
- Analiza incydentów
- Ograniczanie skutków incydentu
- Usuwanie zagrożenia i odtwarzanie po incydencie bezpieczeństwa
- Wnioski (RCA i LL)
- Testy i szkolenia bezpieczeństwa w organizacji
- Koncepcja Threat hunting
- Zadanie egzaminacyjne PBQ: podsumowanie procedur reagowania na incydenty
- Laboratorium praktyczne: detekcja w procesie reagowania na incydent

- Informatyka śledcza
  - Należyta staranność i zabezpieczenie prawne
  - Pozyskanie materiału dowodowego
  - Zabezpieczenie materiału dowodowego
  - Raportowanie
  - Laboratorium praktyczne: wykonywanie czynności informatyki śledczej
- Źródła danych
  - Źródła danych, pulpity i raporty
  - Dane z logów
  - Logi systemu operacyjnego
  - Logi aplikacji
  - Sieciowe źródła danych
  - Przechwytywanie i analiza pakietów
  - Metadane
  - Laboratorium praktyczne: wykorzystanie snifferów sieciowych
- Systemy monitorowania i powiadamiania o zdarzeniach
  - SIEM (Security Information and Event Management)
  - Operacyjne monitorowanie i obsługa alertów
  - Dostrajanie alertów i powiadomień
  - Monitorowanie infrastruktury
  - Monitorowanie systemów i aplikacji
  - Benchmarki
  - Laboratorium: analiza przyczyn źródłowych incydentu

- Analiza wskaźników złośliwej aktywności
  - Wskaźniki ataków z użyciem złośliwego oprogramowania

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

- Klasyfikacja malware
- Wirusy komputerowe
- Robaki i malware bezplikowy
- Spyware i keyloggery
- Backdoor i trojany
- Rootkity
- Ransomware, krypto-malware i bomby logiczne
- Wskaźniki złośliwej aktywności
- Zadanie egzaminacyjne PBQ: analiza wskaźników ataków opartych na malware
- Laboratorium: wykrywanie i reagowanie na malware

- Wskaźniki ataków fizycznych i sieciowych
  - Ataki fizyczne
  - Ataki sieciowe
  - Ataki typu DOS I DDoS
  - Ataki on-path / MITM
  - Ataki na usługi DNS i NTP
  - Ataki na sieci bezprzewodowe
  - Ataki na hasła
  - Ataki polegające na przechwytywaniu i powtórnym użyciu poświadczeń
  - Ataki kryptograficzne
  - Wskaźniki złośliwego kodu
  - Laboratorium z asystą: zrozumienie ataków on-path
- Wskaźniki ataków na aplikacje
  - Ataki na aplikacje
  - Ataki odtworzeniowe
  - Ataki fałszowania poświadczeń
  - Wstrzykiwanie złośliwych instrukcji
  - Wymuszanie ścieżek dostępu i nieautoryzowany dostęp do plików
  - Analiza adresów URL
  - Logi serwera WWW

- Ład organizacyjny w obszarze bezpieczeństwa (security governance)
  - Polityki, standardy i procedury
    - Polityki
    - Procedury
    - Standardy
    - Dobre praktyki 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

- Uwarunkowania prawne i regulacyjne
- Nadzór i rozliczalność w organizacji
- Zadanie egzaminacyjne PBQ: zastosowanie właściwych polityk i regulacji
- Laboratorium: automatyzacja reakcji z wykorzystaniem playbooków

- Zarządzanie zmianą w organizacji
  - Programy zarządzania zmianami
  - Zmiany dozwolone i blokowane
  - Restarty, zależności i przestoje
  - Dokumentacja i kontrola wersji
  - Laboratorium: wdrażanie list dozwolonych i blokujących
- Automatyzacja i orkiestracja
  - Automatyzacja procesów i wykorzystanie skryptów w bezpieczeństwie
  - Wdrażanie automatyzacji i orkiestracji w aspekcie cyberbezpieczeństwa
  - Laboratorium: przypadki użycia automatyzacji oraz skryptów

- Procesy zarządzania ryzykiem
  - Procesy i koncepcje zarządzania ryzykiem
    - Identyfikacja i ocena ryzyka
    - Strategie zarządzania ryzykiem
    - Procesy zarządzania ryzykiem
    - Analiza krytyczności procesów biznesowych (BIA)
  - Koncepcje zarządzania dostawcami
    - Wybór dostawcy
    - Metody oceny dostawców
    - Umowy prawne
    - Audytowanie i ewaluacja mechanizmów kontrolnych
    - Poświadczanie (Attestation) i przeglądy stanu bezpieczeństwa
    - Testy penetracyjne
    - Rodzaje ćwiczeń i symulacji kryzysowych
    - Laboratorium: pentest - rozpoznanie
    - Laboratorium: wykonywanie testów penetracyjnych

- Ład informacyjny: ochrona danych oraz ramy regulacyjne
  - Kategoryzacja danych oraz ramy regulacyjne
    - Typy danych w organizacji
    - Poziomy klasyfikacje danych
    - Suwerenność danych i uwarunkowania geograficzne
    - Dane wrażliwe i ochrona danych osobowych

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

- Incydenty naruszenia prywatności i wycieki danych osobowych
- Monitorowanie i raportowanie w aspekcie ochrony rożnego typu danych.
- Zapobieganie utracie danych (DLP)
- Zadanie egzaminacyjne PBQ: wyjaśnienie koncepcji prywatności i wrażliwości danych
- Zadanie egzaminacyjne PBQ: zastosowanie właściwych technik zabezpieczenia danych

- Polityki personalne
  - Zasady postępowania w organizacji i etyki zawodowej
  - Tematy i techniki przeprowadzania szkoleń z zakresu bezpieczeństwa
  - Program budowania kultury bezpieczeństwa i świadomości zagrożeń
  - Laboratorium: szkolenia i budowanie świadomości przez symulację zagrożenia
  - Laboratorium: analiza powłamaniowa i remediacja incydentów sieciowych

Wymagania:

Rekomendowane doświadczenie: certyfikat CompTIA Network+ oraz 2 lata doświadczenia w pracy na stanowisku związanym z bezpieczeństwem lub administracją systemami.

Poziom trudności



Certyfikaty:

Uczestnicy szkolenia otrzymują certyfikat ukończenia szkolenia wystawiony imiennie oraz na firmę sygnowany przez firmę CompTIA. Kurs przygotowuje do egzaminu certyfikacyjnego CompTIA Security+, dostępnego w centrach egzaminacyjnych Pearson VUE.

Każdy uczestnik autoryzowanego szkolenia CompTIA Security+ Prep Course realizowanego w Compendium CE otrzyma bezpłatny voucher na egzamin certyfikacyjny CompTIA Security+ (SY0-701).

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