Szkolenie: EC-Council

CSA - Certified SOC Analyst v2

DOSTĘPNE TERMINY

2026-04-27 | 3 dni | Warszawa / Wirtualna sala
2026-05-11 | 3 dni | Warszawa / Wirtualna sala *(Termin gwarantowany)*
2026-05-20 | 3 dni | Kraków / Virtual Classroom
2026-05-26 | 3 dni | Kraków / Wirtualna sala
2026-06-24 | 3 dni | Warszawa / Virtual Classroom
2026-06-30 | 3 dni | Warszawa / Wirtualna sala

Cel szkolenia:

Program szkolenia Certified SOC Analyst obejmuje szeroki zakres tematów, takich jak: popularne wektory ataków, wykorzystanie narzedzi i technologii bezpieczenstwa, zarzadzanie informacjami oraz zdarzeniami zwiazanymi z bezpieczenstwem (SIEM), procesy reagowania na incydenty, koordynacja dzialan oraz budowa i zarzadzanie zespolem SOC. Uczestnicy zdobywaja umiejetnosci w zakresie scentralizowanego zarzadzania logami (CLM), priorytetyzacja incydentów, rozpoznawania wskazników naruszenia bezpieczenstwa (IoC) oraz tzw. cyber kill chain, co pozwala na proaktywne reagowanie na potencjalne zagrozenia. Ponadto ucza sie rozpoznawania pojawiajacych sie wzorców zagrozen, tworzenia regul korelacji oraz przygotowywania skutecznych raportów, które wspieraja organizacje w utrzymaniu wysokiego poziomu bezpieczenstwa. Szkolenie obejmuje równiez wykorzystanie narzedzi i platform zintegrowanych ze sztuczna inteligencja, które wspomagaja funkcje SIEM, analize zachowan, priorytetyzacje alertów oraz automatyzacje wykrywania i polowania na zagrozenia (np. Splunk AI, Elastic AI, Copilot, ChatGPT, PowerShell AI).

Ukonczenie kursu EC-Council C|SA dostarcza uczestnikom kompetencje niezbedne do efektywnej pracy w ramach SOC, zwiekszajac ich umiejetnosci wykrywania zagrozen oraz szybkiego reagowania 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

Czego nauczysz sie podczas szkolenia:

- Zdobedziesz wszechstronna wiedze na temat procesów, procedur, technologii oraz przeplywów pracy w obrebie SOC.
- Rozwiniesz wiedze na temat zagrozen bezpieczenstwa, technik ataków, podatnosci, zachowan atakujacych oraz modelu cyber kill chain.
- Nauczysz sie identyfikowac narzedzia, taktyki i procedury stosowane przez atakujacych oraz rozpoznawac wskazniki naruszenia bezpieczenstwa (IoC) podczas biezacych i przyszlych analiz.
- Bedziesz monitorowac i analizowac logi oraz alerty pochodzace z róznych technologii i platform, w tym systemów IDS/IPS, ochrony punktów koncowych, serwerów i stacji roboczych.
- Zrozumiesz proces scentralizowanego zarzadzania logami (CLM) oraz jego znaczenie w dzialaniach zwiazanych z bezpieczenstwem.
- Nauczysz sie zbierac, monitorowac i analizowac zdarzenia oraz logi bezpieczenstwa.
- Zdobedziesz praktyczna wiedze i doswiadczenie w obszarze systemów SIEM.
- Nauczysz sie podstaw zarzadzania i konfiguracji systemów SIEM taich jak Splunk, AlienVault, OSSIM oraz ELK Stack.
- Zdobedziesz doswiadczenie w tworzeniu przypadków uzycia (use cases) w SIEM na potrzeby wykrywania zagrozen.
- Nauczysz sie opracowywac reguly korelacji oraz przygotowywac szczególowe raporty dotyczace wykrytych zagrozen.
- Poznasz najczesciej stosowane scenariusze uzycia SIEM w róznych srodowiskach.
- Nauczysz sie planowac, organizowac i realizowac procesy monitorowania oraz analizy zagrozen w srodowisku korporacyjnym.
- Bedziesz monitorowac pojawiajace sie wzorce zagrozen i przeprowadzac kompleksowe analizy bezpieczenstwa.
- Zdobedziesz praktyczne doswiadczenie w priorytetyzacja alertów dla efektywnego zarzadzania zagrozeniami.
- Nauczysz sie eskalowac incydenty do odpowiednich zespolów w celu ich dalszego badania i eliminacji.
- Skorzystasz z systemów zgloszen (ticketing) do skutecznego sledzenia i rozwiazywania incydentów.
- Bedziesz przygotowywac szczególowe briefingi i raporty obrazujace zastosowane metody analityczne oraz uzyskane wyniki.
- Nauczysz sie integrowac informacje wywiadowcze o zagrozeniach (threat intelligence) z systemami SIEM, aby poprawic wykrywanie i reagowanie na incydenty.
- Nauczysz sie jak wykorzystywac zródla informacji o zagrozeniach (threat intelligence).
- Zdobedziesz wiedze na temat procesu reagowania na incydenty oraz najlepszych praktyk zarzadzania incydentami bezpieczenstwa.
- Poznasz zasady wspólpracy SOC z zespolem ds. reagowania na incydenty (IRT), aby usprawnic zarzadzanie incydentami.

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

- Bedziesz wspierac dzialania zwiazane z reagowaniem na incydenty oraz ich badanie za pomoca technik informatyki sledczej (forensic).
- Dowiesz sie, jak wykrywac zagrozenia w srodowiskach chmurowych oraz jak adaptowac techniki do platform AWS, Azure i GCP.
- Bedziesz proaktywnie wykrywac zagrozenia, uczestniczac w cwiczeniach typu threat hunting.
- Rozwiniesz umiejetnosci tworzenia dashboardów SIEM, generowania raportów SOC oraz budowania zaawansowanych regul korelacji dla skuteczniejszego wykrywania zagrozen.
- Zdobedziesz praktyczne doswiadczenie w analizie zlosliwego oprogramowania (malware).
- Poznasz mozliwosci wykorzystania sztucznej inteligencji (AI) oraz uczenia maszynowego (ML) w celu usprawnienia wykrywania i reagowania na zagrozenia w operacjach SOC.

Szkolenie CSA v2 jest dedykowane dla:

- Kazdego specjalisty ds. cyberbezpieczenstwa, który chce rozszerzyc swoja wiedze z zakresu bezpieczenstwa defensywnego.
- Analityków SOC (Tier I i Tier II)
- Administratorów i inzynierów sieci i bezpieczenstwa
- Specjalistów ds. obrony sieci i analizy zagrozen
- Mlodszych specjalistów ds. cyberbezpieczenstwa
- Osób planujacych rozpoczecie kariery w SOC

Kazdy uczestnik autoryzowanego szkolenia CSA - Certified SOC Analyst v2 realizowanego w Compendium CE, otrzymuje darmowy voucher egzaminacyjny CSA v2.

Plan szkolenia:

- Module 1 - Security Operations and Management
  - Poznasz, jak SOC wzmacnia zarzadzanie bezpieczenstwem w organizacji oraz zrozumiesz znaczenie kluczowych ról, technologii i procesów.
- Module 2 - Understanding Cyber Threats, IoCs, and Attack Methodology
  - Nauczysz sie rozpoznawac rózne rodzaje cyberataków, wskazniki naruszenia bezpieczenstwa oraz taktyki, techniki i procedury (TTP) stosowane przez cyberprzestepców.
- Module 3 - Log Management
  - Poznasz zasady zarzadzania logami w systemach SIEM, w tym ich generowanie, przechowywanie, centralne zbieranie, normalizacje oraz korelacje danych.

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

- Module 4 - Incident Detection and Triage
  - Zapoznasz sie z podstawami systemów SIEM, strategiami ich wdrozenia, tworzeniem przypadków uzycia oraz sposobami wspierania analityków SOC w wykrywaniu anomalii, priorytetyzacja alertów i raportowaniu incydentów.
- Module 5 - Proactive Threat Detection
  - Poznasz role proaktywnego wywiadu zagrozen oraz polowania na zagrozenia (threat hunting) oraz ich integracje z systemem SIEM w celu ograniczenia liczby falszywych alarmów i przyspieszenia procesu triage.
- Module 6 - Incident Response
  - Poznasz etapy procesu reagowania na incydenty oraz współprace zespolu IRT z SOC przy obsludze eskalowanych przypadków.
- Module 7 - Forensic Investigation and Malware Analysis
  - Poznasz role informatyki sledczej oraz analizy zlosliwego oprogramowania w operacjach SOC, co pozwoli Ci lepiej zrozumiec metody ataków oraz identyfikowac wskazniki naruszenia bezpieczenstwa.
- Module 8 - SOC for Cloud Environments
  - Zapoznasz sie z procesami SOC w chmurze, w tym z monitoringiem, wykrywaniem incydentów, automatyzacja reakcji oraz zabezpieczeniami w srodowiskach AWS, Azure i GCP z wykorzystaniem natywnych narzedzi chmurowych.

Wymagania:

Minimum rok doswiadczenia zawodowego w obszarze administracji siecia lub bezpieczenstwem (np. sieci, bezpieczenstwo IT).

Poziom trudności

Certyfikaty:

Uczestnicy szkolenia otrzymuja certyfikat ukonczenia szkolenia sygnowany przez EC-Council (ukonczenie szkolenia). Kurs ten przygotowuje takze do egzaminu certyfikacyjnego CSA v2.

Szczegóły egzaminu CSA v2

- Kod egzaminu: 312-39
- Liczba pytan: 100
- Czas trwania: 3 godziny
- Forma: egzamin wielokrotny wybór (Multiple Choice)

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

Kazdy uczestnik autoryzowanego szkolenia CSA - Certified SOC Analyst v2 realizowanego w Compendium CE, otrzymuje darmowy voucher egzaminacyjny CSA v2.

Prowadzący:

Certified EC-Council Instructor (CEI)

Informacje dodatkowe:

Materialy szkoleniowe skladaja sie z oficjalne podreczniki EC-Council w wersji elektronicznej, dostep do laboratoriów iLabs na okres 180 dni i vouchera egzaminacyjnego.

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