Szkolenie: EC-Council
CSA - Certified SOC Analyst v2

DOSTĘPNE TERMINY

2026-12-01 | 3 dni | Kraków / Wirtualna sala

Cel szkolenia:

Program szkolenia Certified SOC Analyst obejmuje szeroki zakres tematów, takich jak: popularne wektory ataków, wykorzystanie narzędzi i technologii bezpieczeństwa, zarządzanie informacjami oraz zdarzeniami związanymi z bezpieczeństwem (SIEM), procesy reagowania na incydenty, koordynacja działań oraz budowa i zarządzanie zespołem SOC. Uczestnicy zdobywają umiejętności w zakresie scentralizowanego zarządzania logami (CLM), priorytetyzacja incydentów, rozpoznawania wskaźników naruszenia bezpieczeństwa (IoC) oraz tzw. cyber kill chain, co pozwala na proaktywne reagowanie na potencjalne zagrożenia. Ponadto uczą się rozpoznawania pojawiających się wzorców zagrożeń, tworzenia reguł korelacji oraz przygotowywania skutecznych raportów, które wspierają organizacje w utrzymaniu wysokiego poziomu bezpieczeństwa. Szkolenie obejmuje również wykorzystanie narzędzi i platform zintegrowanych ze sztuczną inteligencją, które wspomagają funkcje SIEM, analizę zachowań, priorytetyzację alertów oraz automatyzację wykrywania i polowania na zagrożenia (np. Splunk AI, Elastic AI, Copilot, ChatGPT, PowerShell AI).

Ukończenie kursu EC-Council C|SA dostarcza uczestnikom kompetencje niezbędne do efektywnej pracy w ramach SOC, zwiększając ich umiejętności wykrywania zagrożeń oraz szybkiego reagowania na incydenty.

Czego nauczysz się podczas szkolenia:

- Zdobędziesz wszechstronną wiedzę na temat procesów, procedur, technologii oraz przepływów

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

pracy w obrębie SOC.

- Rozwiniesz wiedzę na temat zagrożeń bezpieczeństwa, technik ataków, podatności, zachowań atakujących oraz modelu cyber kill chain.
- Nauczysz się identyfikować narzędzia, taktyki i procedury stosowane przez atakujących oraz rozpoznawać wskaźniki naruszenia bezpieczeństwa (IoC) podczas bieżących i przyszłych analiz.
- Będziesz monitorować i analizować logi oraz alerty pochodzące z różnych technologii i platform, w tym systemów IDS/IPS, ochrony punktów końcowych, serwerów i stacji roboczych.
- Zrozumiesz proces scentralizowanego zarządzania logami (CLM) oraz jego znaczenie w działaniach związanych z bezpieczeństwem.
- Nauczysz się zbierać, monitorować i analizować zdarzenia oraz logi bezpieczeństwa.
- Zdobędziesz praktyczną wiedzę i doświadczenie w obszarze systemów SIEM.
- Nauczysz się podstaw zarządzania i konfiguracji systemów SIEM taich jak Splunk, AlienVault, OSSIM oraz ELK Stack.
- Zdobędziesz doświadczenie w tworzeniu przypadków użycia (use cases) w SIEM na potrzeby wykrywania zagrożeń.
- Nauczysz się opracowywać reguły korelacji oraz przygotowywać szczegółowe raporty dotyczące wykrytych zagrożeń.
- Poznasz najczęściej stosowane scenariusze użycia SIEM w różnych środowiskach.
- Nauczysz się planować, organizować i realizować procesy monitorowania oraz analizy zagrożeń w środowisku korporacyjnym.
- Będziesz monitorować pojawiające się wzorce zagrożeń i przeprowadzać kompleksowe analizy bezpieczeństwa.
- Zdobędziesz praktyczne doświadczenie w priorytetyzacja alertów dla efektywnego zarządzania zagrożeniami.
- Nauczysz się eskalować incydenty do odpowiednich zespołów w celu ich dalszego badania i eliminacji.
- Skorzystasz z systemów zgłoszeń (ticketing) do skutecznego śledzenia i rozwiązywania incydentów.
- Będziesz przygotowywać szczegółowe briefingi i raporty obrazujące zastosowane metody analityczne oraz uzyskane wyniki.
- Nauczysz się integrować informacje wywiadowcze o zagrożeniach (threat intelligence) z systemami SIEM, aby poprawić wykrywanie i reagowanie na incydenty.
- Nauczysz się jak wykorzystywać źródła informacji o zagrożeniach (threat intelligence).
- Zdobędziesz wiedzę na temat procesu reagowania na incydenty oraz najlepszych praktyk zarządzania incydentami bezpieczeństwa.
- Poznasz zasady współpracy SOC z zespołem ds. reagowania na incydenty (IRT), aby usprawnić zarządzanie incydentami.
- Będziesz wspierać działania związane z reagowaniem na incydenty oraz ich badanie za pomocą technik informatyki śledczej (forensic).
- Dowiesz się, jak wykrywać zagrożenia w środowiskach chmurowych oraz jak adaptować techniki do platform AWS, Azure i GCP.

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

- Będziesz proaktywnie wykrywać zagrożenia, uczestnicząc w ćwiczeniach typu threat hunting.
- Rozwiniesz umiejętności tworzenia dashboardów SIEM, generowania raportów SOC oraz budowania zaawansowanych reguł korelacji dla skuteczniejszego wykrywania zagrożeń.
- Zdobędziesz praktyczne doświadczenie w analizie złośliwego oprogramowania (malware).
- Poznasz możliwości wykorzystania sztucznej inteligencji (AI) oraz uczenia maszynowego (ML) w celu usprawnienia wykrywania i reagowania na zagrożenia w operacjach SOC.

Szkolenie CSA v2 jest dedykowane dla:

- Każdego specjalisty ds. cyberbezpieczeństwa, który chce rozszerzyć swoją wiedzę z zakresu bezpieczeństwa defensywnego.
- Analityków SOC (Tier I i Tier II)
- Administratorów i inżynierów sieci i bezpieczeństwa
- Specjalistów ds. obrony sieci i analizy zagrożeń
- Młodszych specjalistów ds. cyberbezpieczeństwa
- Osób planujących rozpoczęcie kariery w SOC

Każdy 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 zarządzanie bezpieczeństwem w organizacji oraz zrozumiesz znaczenie kluczowych ról, technologii i procesów.
- Module 2 - Understanding Cyber Threats, IoCs, and Attack Methodology
  - Nauczysz się rozpoznawać różne rodzaje cyberataków, wskaźniki naruszenia bezpieczeństwa oraz taktyki, techniki i procedury (TTP) stosowane przez cyberprzestępców.
- Module 3 - Log Management
  - Poznasz zasady zarządzania logami w systemach SIEM, w tym ich generowanie, przechowywanie, centralne zbieranie, normalizację oraz korelację danych.
- Module 4 - Incident Detection and Triage
  - Zapoznasz się z podstawami systemów SIEM, strategiami ich wdrożenia, tworzeniem przypadków użycia oraz sposobami wspierania analityków SOC w wykrywaniu anomalii, priorytetyzacja alertów i raportowaniu incydentów.

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 5 - Proactive Threat Detection
  - Poznasz rolę proaktywnego wywiadu zagrożeń oraz polowania na zagrożenia (threat hunting) oraz ich integrację z systemem SIEM w celu ograniczenia liczby fałszywych alarmów i przyspieszenia procesu triage.
- Module 6 - Incident Response
  - Poznasz etapy procesu reagowania na incydenty oraz współpracę zespołu IRT z SOC przy obsłudze eskalowanych przypadków.
- Module 7 - Forensic Investigation and Malware Analysis
  - Poznasz rolę informatyki śledczej oraz analizy złośliwego oprogramowania w operacjach SOC, co pozwoli Ci lepiej zrozumieć metody ataków oraz identyfikować wskaźniki naruszenia bezpieczeństwa.
- Module 8 - SOC for Cloud Environments
  - Zapoznasz się z procesami SOC w chmurze, w tym z monitoringiem, wykrywaniem incydentów, automatyzacją reakcji oraz zabezpieczeniami w środowiskach AWS, Azure i GCP z wykorzystaniem natywnych narzędzi chmurowych.

Wymagania:

Minimum rok doświadczenia zawodowego w obszarze administracji siecią lub bezpieczeństwem (np. sieci, bezpieczeństwo IT).

Poziom trudności



Certyfikaty:

Uczestnicy szkolenia otrzymują certyfikat ukończenia szkolenia sygnowany przez EC-Council (ukończenie szkolenia). Kurs ten przygotowuje także do egzaminu certyfikacyjnego CSA v2.

Szczegóły egzaminu CSA v2

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

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

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

Prowadzący:

Certified EC-Council Instructor (CEI)

Informacje dodatkowe:

Materiały szkoleniowe składają się z oficjalne podręczniki EC-Council w wersji elektronicznej, dostęp 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