

Szkolenie: EC-Council
CSA - Certified SOC Analyst v2

EC-Council
Building A Culture Of Security

DOSTĘPNE TERMINY

2026-05-11 | 3 dni | Warszawa / Wirtualna sala (*Termin gwarantowany, Last minute*)
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 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 ucza 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 wszechstronna wiedze na temat procesów, procedur, technologii oraz przepływów pracy w obrębie SOC.
- Rozwiniesz wiedze 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 takich 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 priorytetyzacji 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 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 umiejetnosc tworzenia dashboardów SIEM, generowania raportów SOC oraz budowania zaawansowanych regul korelacji dla skutecznego 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 różne 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.
- Module 4 - Incident Detection and Triage

- Zapoznasz sie z podstawami systemów SIEM, strategiami ich wdrozenia, tworzeniem przypadków użycia 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 zespołu IRT z SOC przy obsłudze 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 sieci 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)

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:

Materiały szkoleniowe składają się z oficjalne podręczniki EC-Council w wersji elektronicznej, dostęp do laboratoriów iLabs na okres 180 dni i vouchera egzaminacyjnego.