kod szkolenia: BS.IT SOC AI / PL DL 3d NIS2

# Od Alertu do Incydentu (z użyciem AI): wprowadzenie do pracy Analityka SOC

Szkolenie pokazuje, jak wygląda praca Analityka SOC – od analizy alertów bezpieczeństwa, przez triage i klasyfikację zdarzeń, aż po eskalację oraz dokumentowanie incydentów.

Jest przeznaczone dla osób rozpoczynających pracę w cyberbezpieczeństwie, specjalistów IT oraz wszystkich, którzy chcą lepiej zrozumieć proces monitorowania i obsługi zagrożeń.

Uczestnicy poznają podstawy analizy logów, Incident Response oraz współpracy pomiędzy zespołami bezpieczeństwa i IT. Dodatkowo nauczą się wykorzystywać narzędzia AI i modele językowe (LLM) do wspierania analizy zdarzeń, weryfikacji wniosków oraz przyspieszania codziennej pracy analitycznej.

## Odbiorcy szkolenia

- Administratorzy IT współpracujący z zespołami SOC lub budujący funkcje monitorowania bezpieczeństwa
- Początkujący Analitycy SOC
- Osoby przygotowujące się do roli Junior SOC Analyst
- Pracownicy Help Desk i IT Support obsługujący zgłoszenia związane z bezpieczeństwem
- Administratorzy sieci i systemów
- Specjaliści ds. cyberbezpieczeństwa na początku ścieżki zawodowej
- Osoby odpowiedzialne za monitorowanie infrastruktury IT i analizę zdarzeń bezpieczeństwa
- Osoby przygotowujące się do certyfikacji CompTIA Security+, CompTIA CySA+, ECIH lub podobnych

## Korzyści

- Praca Analityka SOC – zrozumiesz proces obsługi alertów bezpieczeństwa od wykrycia zdarzenia do jego eskalacji i dokumentacji
- Analiza alertów – nauczysz się oceniać alerty oraz odróżniać fałszywe alarmy od rzeczywistych incydentów
- Klasyfikacja zdarzeń – rozróżnisz zdarzenia, alerty i incydenty oraz określisz ich priorytet biznesowy
- Analiza logów – wykorzystasz dane z różnych źródeł do weryfikacji zdarzeń i budowania kontekstu bezpieczeństwa
- Detekcja zagrożeń – poznasz podstawowe mechanizmy wykrywania ataków oraz interpretacji alertów bezpieczeństwa
- Współpraca SOC i IT – zrozumiesz role, odpowiedzialności i zasady skutecznej komunikacji podczas obsługi incydentów
- Wykorzystanie AI – nauczysz się korzystać z modeli językowych (LLM) do wspierania analizy i dokumentowania zdarzeń bezpieczeństwa

## Program szkolenia

1. Podstawy Incident Response i triage w SOC
   - Rola SOC i warsztat analityka: alert / zdarzenie / incydent, false positive, severity vs priority, schemat myślenia
   - Proces Incident Response (PICERL): identyfikacja, klasyfikacja, eskalacja i współpraca z zespołami
   - Artefakty i wskaźniki kompromitacji: IoC vs TTP, MITRE ATT&CK, Pyramid of Pain, korelacja zdarzeń
   - Kodowanie, szyfrowanie i hashowanie w analizie incydentów
   - Dokumentacja: timeline, ticket, raport — warsztat „od alertu do eskalacji”
2. Monitorowanie bezpieczeństwa i analiza logów
   - Monitorowanie sieci: normalne i anomalne zachowania, granice widoczności
   - Protokoły w analizie SOC: DNS, HTTP, SMTP, TLS; synchronizacja czasu
   - Logi systemowe, webowe i endpointowe: Windows Event ID, Sysmon, tożsamość i chmura jako obszar analizy
   - Warsztat CLI: filtrowanie logów (grep/awk/sort), budowa osi czasu zdarzeń
   - Systemy SIEM: korelacja, reguły, Sigma / Detection-as-Code, czytanie zapytań SPL
3. Detekcja zagrożeń, analiza techniczna i AI w SOC
   - Systemy IDS/IPS: Snort i Suricata, budowa reguł, interpretacja i weryfikacja alertów
   - Wstępna analiza malware: bezpieczny statyczny triage, hash, reputacja, strings, YARA
   - Analiza phishingu: nagłówki, SPF/DKIM/DMARC, BEC, analiza linków i załączników — warsztat na próbce .eml
   - AI w pracy analityka SOC: możliwości i ograniczenia LLM, prompting, audyt werdyktów AI,

bezpieczeństwo danych
- Gotowość organizacji do współpracy z SOC: logi i retencja, właścicielstwo systemów, protokół komunikacji administrator ↔ SOC
- Kierunki rozwoju analityka: NSM/Zeek, threat hunting, chmura

## Oczekiwane przygotowanie uczestnika

- Podstawowa znajomość systemów operacyjnych i sieci komputerowych
- Znajomość podstawowych zagadnień z zakresu bezpieczeństwa IT
- Doświadczenie w administracji systemami, wsparciu technicznym lub pracy z infrastrukturą IT będzie dodatkowym atutem

Nie jest wymagane wcześniejsze doświadczenie w pracy SOC.

## Szkolenie obejmuje

- 3 dni pracy z trenerem
- Nadzór trenera
- Kontakt ze społecznością
- Podręcznik w wersji elektronicznej
- Środowisko laboratoryjne na czas szkolenia

Metoda szkolenia:

- wykład
- warsztaty (praca indywidualna i w małych grupach)

## Czas trwania

3 dni / 21 godzin

## Język

- Szkolenie: polski
- Materiały: polski