# Analityk SOC - monitoring, detekcja, reagowanie (kod: SOC)

**Zapytaj o szczegóły**
tel. 22 63 64 164
akademia@alx.pl

## Opis i cel szkolenia

Alert z antywirusa, dziwny wpis w logach, telefon od użytkownika, że „system zachowuje się inaczej", podejrzenia włamania... W wielu firmach i instytucjach nie ma od tych rzeczy osobnego zespołu. Zajmuje się tym administrator systemów, inżynier sieci, ktoś ze wsparcia IT albo osoba od bezpieczeństwa, która akurat ma czas. Nasze szkolenie jest dla nich wszystkich; jak również dla specjalistów IT "wchodzących" na pierwszą linię zespołów SOC; dla technicznych kierowników - oraz dla tych, którzy odbierają i oceniają usługi monitoringu systemów i sieci od zewnętrznego dostawcy.

**Po tych trzech dniach:**

- zobaczysz, co w Twojej infrastrukturze jest widoczne dla monitoringu, a co dzieje się całkowicie poza jego zasięgiem;
- postawisz działający system zbierania i analizy logów - i podepniesz do niego stacje Windows oraz serwery Linux;
- napiszesz własne reguły detekcji i dostroisz je tak, żeby nie zasypały zespołu fałszywymi alarmami;
- przejdziesz przez kilkanaście realnych alertów i nauczysz się oddzielać szum od rzeczywistego ataku;
- poprowadzisz incydent - od pierwszego sygnału, po raport i zgłoszenie. Nie niszcząc przy tym materiału dowodowego.

Przez trzy dni pracujemy na jednym środowisku, które uczestnicy stopniowo rozbudowują: kilka maszyn, kolektor logów, agenci na stacjach. Odtwarzamy na tym środowisku kolejne rodzaje/etapy symulowanego ataku i za każdym razem sprawdzamy: czy monitoring go zobaczył? A jeśli nie, to czego zabrakło i jak to naprawić, itd. Wykłady są krótkie i służą głównie temu, żeby wiedzieć, co za chwilę będzie się robiło przy konsoli.

Całość opieramy na narzędziach otwartych - przede wszystkim na platformie **Wazuh**, uzupełnionej o rozszerzoną telemetrię stacji, detekcję w ruchu sieciowym i reguły w formacie **Sigma**. To świadoma decyzja: uczestnik wychodzi z konfiguracją, którą może uruchomić u siebie następnego dnia - bez kupowania licencji, bez czekania na zgodę na wydatek. Natomiast mechanizmy, których uczymy - korelacja zdarzeń, strojenie reguł, triage, mapowanie na **MITRE ATT&CK** - są uniwersalne i działają podobnie, zarówno w rozwiązaniach otwartych, jak i komercyjnych od różnych dostawców.

Osobny moduł szkolenia poświęcamy temu, do czego w tej pracy realnie nadaje się AI (modele językowe). Pokazujemy, gdzie ułatwiają i przyspieszają analizę, a gdzie potrafią pewnym siebie tonem podawać zmyślony wniosek. Ale też: jak wygląda atak na samego asystenta - przez dane, które dostaje. Uwaga: szerzej, zastosowanie AI w cyberbezpieczeństwie i bezpieczeństwo samych systemów opartych na AI - omawiamy na osobnym szkoleniu AI w cyberbezpieczeństwie.

Uwaga: to szkolenie nie przygotowuje do konkretnego egzaminu i nie zastępuje informatyki śledczej (również z niej oferujemy osobne zajęcia). Analizę nośników i pamięci poruszamy tutaj tylko w zakresie potrzebnym, żeby nie zniszczyć śladów przed przekazaniem sprawy dalej. Nie skupiamy się też na nauce testów penetracyjnych - techniki atakujących na tym szkoleniu pokazujemy głównie po to, żeby wiedzieć, jaki zostawiają ślad w systemach i w danych (zaś stricte z technik ofensywnych także posiadamy osobne szkolenia, na które serdecznie zapraszamy).

## Czas trwania

3 dni

## Program

1. Monitoring bezpieczeństwa: po co i jak to się układa
   - Dlaczego antywirus i firewall nie wystarczają - co widać, a czego nie widać
   - Alert, zdarzenie, incydent - rozróżnienie, które porządkuje całą pracę zespołu
   - Linie SOC: podział zadań, co się eskaluje, do kogo i na jakiej podstawie
   - Cykl życia detekcji: telemetria, reguła, alert, triage, reakcja, nowa reguła
   - Wymagania KSC i NIS2 od strony technicznej: co trzeba wykrywać i w jakim czasie zgłaszać
2. Telemetria: skąd biorą się dane, na których pracuje analityk
   - Logi systemu Windows - zdarzenia, które naprawdę mają znaczenie, i te, które tylko zapychają
   - Rozszerzona telemetria stacji: rejestrowanie procesów, linii poleceń, połączeń sieciowych i zmian w rejestrze
   - Logi systemów Linux: uwierzytelnianie, podsystem audytu, dzienniki usług
   - Logi urządzeń sieciowych, serwerów usług i aplikacji
   - Czego brakuje w konfiguracji domyślnej i jak to włączyć, nie zalewając kolektora
   - Synchronizacja czasu, strefy czasowe i retencja - bez tego oś zdarzeń się nie klei
   - Ćwiczenie: uruchomienie kolektora, podpięcie stacji Windows i serwera Linux
3. Platforma SIEM w praktyce
   - Architektura: agent, kolektor, indeks, interfejs analityka
   - Normalizacja i wzbogacanie zdarzeń - dlaczego surowy log to za mało
   - Wyszukiwanie i filtrowanie: budowanie zapytań, które odpowiadają na konkretne pytanie śledcze
   - Pulpity i widoki dla pierwszej linii - co analityk powinien zobaczyć od razu
   - Ocena stanu stacji: podatności, zgodność konfiguracji, monitorowanie integralności plików
   - Ćwiczenie: samodzielne zapytania na danych z własnego środowiska
4. Detekcja: od danych do alertu
   - MITRE ATT&CK; jako wspólny język opisu ataku - taktyki, techniki, mapowanie reguł
   - Piramida wskaźników: dlaczego blokowanie adresów daje najmniej, a wykrywanie zachowań najwięcej
   - Anatomia reguły detekcyjnej: warunek, kontekst, próg, poziom istotności
   - Reguły w formacie Sigma i przenoszenie detekcji między platformami
   - Wykrywanie typowych technik: ataki na hasła, podejrzane logowania, uruchamianie narzędzi ofensywnych, utrwalanie dostępu, eskalacja uprawnień, wyprowadzanie danych
   - Detekcja w ruchu sieciowym: sygnatury, komunikacja z serwerami sterującymi, nadużycia DNS
   - Ćwiczenie: napisanie i uruchomienie własnych reguł
5. Strojenie detekcji i fałszywe alarmy
   - Dlaczego zbyt czuły system detekcji bywa gorszy niż jego brak
   - Wyjątki, listy dozwolonych, progi i okna czasowe
   - Mierzenie jakości detekcji - co liczyć, żeby wiedzieć, czy jest lepiej
   - Ćwiczenie: strojenie reguły, która generuje zbyt wiele alertów
6. Triage: pierwsze kilkanaście minut po alercie

**Zapytaj o szczegóły**
tel. 22 63 64 164
akademia@alx.pl

- Schemat oceny alertu - pytania, które zadaje się zawsze i w tej samej kolejności
- Istotność a priorytet: dlaczego to nie to samo i kto o tym rozstrzyga
- Wzbogacanie alertu: reputacja adresów, domen i plików, źródła informacji o zagrożeniach, wskaźniki kompromitacji
- Budowa osi czasu zdarzenia z wielu źródeł
- Kiedy zamknąć jako fałszywy alarm, a kiedy eskalować - i jak przekazać sprawę wyżej
- Ćwiczenie: triage serii alertów z jednego środowiska

7. Reagowanie na incydent
   - Etapy obsługi incydentu i typowe błędy popełniane na każdym z nich
   - Powstrzymanie: izolacja stacji, blokada konta, odcięcie komunikacji
   - Reakcja automatyczna - co warto zautomatyzować, a czego automatyzować nie wolno
   - Zabezpieczenie materiału dowodowego bez niszczenia śladów, gdy sprawa idzie do informatyki śledczej
   - Odtworzenie działania, zamknięcie sprawy i raport
   - Zgłoszenie incydentu: co, komu i w jakim terminie
   - Ćwiczenie: pełny scenariusz, od pierwszego alertu do zamkniętego incydentu
8. AI w pracy analityka
   - Gdzie modele językowe realnie skracają pracę: streszczenie alertu, wyjaśnienie podejrzanej linii poleceń, szkic raportu, przełożenie reguły na inny format
   - Gdzie nie pomagają i szkodzą: ocena istotności, decyzja o eskalacji, wymyślone wskaźniki podane pewnym tonem
   - Dane wrażliwe: czego nie wolno wkleić do modelu zewnętrznego i kiedy sięgnąć po model uruchomiony lokalnie
   - Wstrzykiwanie poleceń przez analizowane dane - log jako wektor ataku na własnego asystenta
   - Weryfikacja: każdy wniosek modelu potwierdzamy w danych źródłowych
   - Ćwiczenie: analiza incydentu z asystentem AI i wskazanie miejsc, w których się pomylił
9. Utrzymanie i rozwój monitoringu
   - Skąd brać nowe reguły i jak nadążać za zmianami technik ataku
   - Pętla po incydencie: każdy incydent kończy się nową detekcją
   - Co zrobić samodzielnie, a co kupić jako usługę - i jak rozliczać zewnętrznego dostawcę SOC
   - Możliwe kierunki dalszej nauki

## Przeznaczenie i wymagania

Szkolenie jest przeznaczone przede wszystkim dla:

- administratorów systemów i sieci, którzy odpowiadają - formalnie lub nieformalnie - za wykrywanie incydentów;
- inżynierów i specjalistów bezpieczeństwa, którzy dotąd nie pracowali z systemem klasy SIEM;
- osób rozpoczynających pracę na pierwszej linii zespołu SOC;
- pracowników wsparcia IT, do których trafiają zgłoszenia i alerty związane z bezpieczeństwem;
- osób odpowiedzialnych za techniczną stronę wymagań KSC i NIS2;
- osób, które zamawiają i odbierają usługę monitoringu od zewnętrznego dostawcy i chcą umieć ocenić, co za nią dostają.

**Zapytaj o szczegóły**
tel. 22 63 64 164
akademia@alx.pl

Oraz wszystkich zainteresowanych tematyką monitoringu, wykrywania i obrony przed atakami - dziedzin defensywnych, zwanych często również "Blue Team".

Od uczestników oczekujemy:

- pracy w wierszu poleceń systemu Linux i w środowisku Windows, w tym podstaw PowerShella;
- rozumienia działania sieci: TCP/IP, DNS, HTTP, adresacja, podstawy routingu;
- doświadczenia w administrowaniu systemami lub sieciami (w praktyce co najmniej roku);
- ogólnej orientacji w podstawowych rodzajach ataków.

Wcześniejszy kontakt z systemem klasy SIEM nie jest potrzebny - zaczynamy od zera.

Szkolenie będzie za trudne dla osób, które nie administrowały wcześniej żadnym systemem.

Dla doświadczonych analityków SOC, piszących reguły detekcyjne na co dzień, będzie za proste.

Zapewniamy całe niezbędne środowisko oraz sprzęt (w wypadku trybu stacjonarnego) lub maszyny cloudowe/obrazy maszyn do pracy (w wypadku trybu zdalnego).

**Zapytaj o szczegóły**
tel. 22 63 64 164
akademia@alx.pl

## Certyfikaty

Uczestnicy szkolenia otrzymują imienne certyfikaty sygnowane przez ALX.

## Lokalizacje

- Warszawa – ul. Jasna 14/16A
- Zdalnie – zajęcia realizowane poprzez platformę Zoom
- Kraków – ul. św. Filipa 23
- Warsaw (English) – Jasna 14/16A
- Online (English) – your home, office or wherever you want
- na życzenie dowolne miejsce w Polsce, lub UE (zajęcia prowadzone w języku angielskim)

## Cena szkolenia

2490 PLN netto (VAT 23%)

W cenę szkoleń organizowanych w naszej siedzibie wliczone są:

- autorskie materiały szkoleniowe,
- indywidualne stanowisko komputerowe do pracy podczas zajęć,
- certyfikaty ukończenia szkolenia,
- drobny poczęstunek oraz ciepłe i zimne napoje,
- możliwość jednorazowego kontaktu z instruktorem (instruktorami) po szkoleniu i zadawania pytań dotyczących materiału szkolenia.

Cena szkolenia nie zawiera obiadów. Można je dokupić w cenie 35 zł netto za obiad.