

MULTIKOM SOC

Profesjonalne usługi Security Operations Center (SOC) - ochrona Twojej infrastruktury IT w modelu 24/7

W pełni zarządzany Security Operations Center (SOC) oparty o najlepsze narzędzia open-source klasy enterprise bez vendor lock-in i ukrytych kosztów licencyjnych.

Multikom SOC zapewnia organizacji **ciągły nadzór nad infrastrukturą IT, szybkie wykrywanie zagrożeń oraz ustrukturyzowane reagowanie na incydenty** zgodnie z najlepszymi praktykami branżowymi.

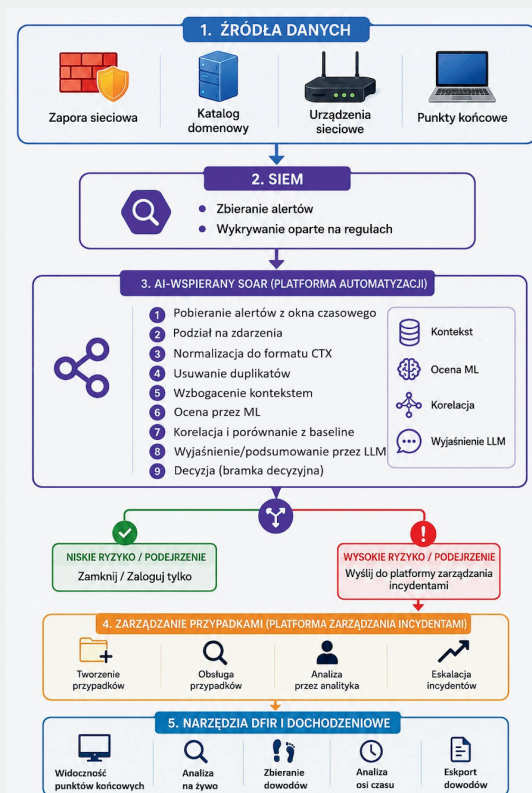
Platforma integruje **zaawansowane mechanizmy wykrywania oparte o reguły korelacyjne, uczenie maszynowe oraz analizę behawioralną**, co pozwala identyfikować zarówno znane zagrożenia, jak i wcześniej nieobserwowane wzorce ataków. Każdy **incydent jest rejestrowany, badany i dokumentowany** w sposób zapewniający pełną audytowalność i zgodność z wymaganiami regulacyjnymi.

Automatyzacja procesów reagowania **skraca czas od wykrycia zagrożenia do jego neutralizacji** - bez uzależnienia od decyzji człowieka w krytycznych momentach. Uzupełnieniem jest **stały monitoring bazy podatności CVE** oraz **proaktywne zarządzanie ryzykiem**, zanim luki zostaną wykorzystane przez atakujących.

Działanie procesu Multikom SOC

Poszczególne etapy odpowiadają temu, jak mechanizm przepływu informacji faktycznie obrabia zdarzenie od telemetrii do decyzji:

- ① **Zbieranie logów**
SIEM gromadzi dane z firewalli, serwerów, stacji roboczych, sieci i chmury.
- ② **Porządkowanie alertów**
Automatyzacja normalizuje dane, usuwa duplikaty i dzieli alerty na zdarzenia.
- ③ **Ocena anomalii**
ML nadaje priorytet i wykrywa odstępstwa od normalnego zachowania.
- ④ **Kontekst historyczny**
Analiza wcześniejszych zdarzeń dla IP, użytkownika i hosta.
- ⑤ **Weryfikacja zagrożenia**
Sprawdzenie, czy to sekwencja ataku czy pojedynczy sygnał.
- ⑥ **Klasyfikacja decyzji**
Odrzucenie / sprawdzenie / alert (ML nie decyduje samodzielnie).
- ⑦ **Wsparcie AI (LLM)**
Streszczenie zdarzenia i rekomendacje dla analityka SOC.
- ⑧ **Incident i reakcja**
Obsługa incydentu, izolacja, blokada, remediacja + dashboard KPI.



MULTIKOM SOC

**Profesjonalne usługi Security Operations Center (SOC)
- ochrona Twojej infrastruktury IT w modelu 24/7**

WARIANT PODSTAWOWY MONITOROWANIE

- SIEM zbiera i koreluje zdarzenia z całej infrastruktury
- Automatyzacja porządkuje alerty i eliminuje duplikaty
- ML nadaje priorytet i dostarcza kontekst
- LLM (AI) wspiera analityka w analizie zdarzeń
- Analityk SOC prowadzi triaż i eskaluje alerty

CO OTRZYMUJESZ?

- Monitoring 24/7
- Redukcję szumu i fałszywych alarmów
- Lepszą jakość i kontekst alertów
- Raportowanie i identyfikację potencjalnych incydentów
- Jasną informację: sygnał vs zagrożenie



**DZIAŁANIA REAKCYJNE PODEJMujesz
WE WŁASNYM ZAKRESIE**

WARIANT ROZSZERZONY REAGOWANIE

- Automatyczna eskalacja do SOAR
- Wzbogacanie incydentów o IoC
- Analiza DFIR i dochodzenie
- Automatyczna reakcja i remediacja (izolacja, blokady, łatanie, utwardzanie systemów)

CO OTRZYMUJESZ?

- Pełną obsługę incydentów 24/7
- Szybką reakcję i neutralizację zagrożeń
- Automatyzację działań bezpieczeństwa
- Zamkniętą pętlę bezpieczeństwa (detekcja → analiza → reakcja → remediacja)
- Minimalizację wpływu incydentów na biznes



**MULTIKOM IT REALIZUJE PEŁNY PROCES
REAKCJI I ZABEZPIECZENIA ŚRODOWISKA.**

Główne korzyści Multikom SOC



**Wczesne wykrywanie zagrożeń
w czasie rzeczywistym** dzięki
zaawansowanym metodom
detekcji i korelacji zdarzeń



**Automatyczna kwalifikacja
zdarzeń i identyfikacja incydentów**
– mniej szumu, więcej realnych
sygnałów bezpieczeństwa



**Skrócenie czasu analizy incydentów
do minut** dzięki wykorzystaniu
mechanizmów AI i kontekstowej analizy
danych



Odciążenie zespołu SOC poprzez
ograniczenie liczby fałszywych
alarmów i automatyzację triażu



**Automatyczna reakcja na incydenty
(wersja rozszerzona)** zanim zagrożenia
wpłyną na działanie organizacji



Proaktywne zarządzanie ryzykiem
poprzez identyfikację i eliminację podatności
jeszcze przed ich wykorzystaniem



Wsparcie zgodności regulacyjnej
(KSC, NIS2, DORA, RODO, CER, CRA, KRI)
w zakresie monitorowania i reagowania



Zapewnienie ciągłości działania biznesu
dzięki szybkiemu wykrywaniu i skutecznemu
ograniczaniu skutków incydentów



43-600 Jaworzno,
Szczakowska 35



biznes@multikom.net.pl



32 413 99 08



www.multikom.net.pl