Sekoia

PLATFORMA AI SOC I SEKOIA DEFEND

Podnieś poziom operacji bezpieczeństwa

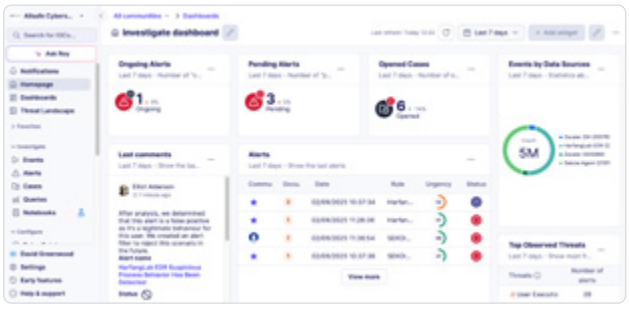
Sekoia Defend zapewnia zespołom bezpieczeństwa pełną widoczność, inteligentną detekcję oraz szybką reakcję wspieraną przez AI - zarówno w środowiskach chmurowych, jak i on-premise.

Dlaczego Sekoia Defend?

Organizacje korzystają z wielu narzędzi bezpieczeństwa. Jednak takie silosowe podejście nie jest skuteczne. Gdy zespoły pracują na odseparowanych rozwiązaniach, atakujący mogą łatwo wykorzystać luki pomiędzy nimi, a reakcja na incydenty zajmuje więcej czasu. W efekcie analitycy tracą czas na analizowanie kolejnych alertów bez kontekstu potrzebnego do podjęcia właściwych działań.

SEKOIA DEFEND TO ZMIENIA.

Łączy threat intelligence, detekcję, analizę i reakcję na incydenty w jednej, łatwej w obsłudze platformie SaaS, stworzonej z myślą o jak najszerszej detekcji zagrożeń.



Najważniejsze cechy

- Ujednolicona platforma SaaS: Jeden interfejs dla funkcji SIEM, SOAR i XDR.
- CTI jako fundament: Platforma zbudowana w oparciu o threat intelligence jako sercu rozwiązania.
- Otwarta i rozszerzalna architektura: Ponad 300 gotowych integracji z najpopularniejszymi rozwiązanimi oraz możliwość tworzenia własnych konektorów.
- Szybkie Time-to-Value: Wdrożenie w ciągu kilku godzin, a nie miesięcy, dzięki natychmiastowemu pokryciu zapewnianemu przez agenta, threat intelligence i zweryfikowanym regułom detekcji.

Jak to działa

MONITORUJ

Pełna widoczność infrastruktury - zarówno chmurowej, jak i lokalnej.

WYKRYWAJ

Reguły wzbogacone o CTI, detekcja anomalii i analiza behawioralna pozwalają wykrywać zagrożenia, które umykają innym rozwiązaniom.

ANALIZUJ

Wspierane przez AI zarządzanie incydentami automatycznie grupuje alerty i dostarcza niezbędny kontekst.

REAGUJ

Uruchamiaj ręczne lub automatyczne działania reakcyjne na dużą skalę, korzystając z AI oraz gotowych playbooków.

Korzyści w skrócie

DOWOLNE DANE, DOWOLNE ŹRÓDŁO

Zbieraj dane z usług chmurowych, systemów lokalnych i punktów końcowych przy użyciu agenta Sekoia. Twórz własne integracje dzięki intuicyjnemu interfejsowi - bez uzależnienia od jednego producenta.

ZGODNOŚĆ Z REGULACJAMI JUŻ NA ETAPIE PROJEKTOWANIA

Regionalna lokalizacja danych pozwala wybrać miejsce ich przechowywania zgodnie z lokalnymi regulacjami. Platforma zapewnia pełną własność i widoczność danych oraz mechanizmy audytowe wspierające spełnienie nawet najbardziej wymagających wymagań regulacyjnych.

CTI W CENTRUM OPERACJI

Platforma wykorzystuje wiedzę zespołu threat intelligence Sekoia, wzbogacając każdy alert o praktyczny kontekst umożliwiający szybszą i skuteczniejszą reakcję analityków.

DETEKCJA W CZASIE RZECZYWISTYM, W DOWOLNEJ SKALI

Uzyskaj dostęp do tysięcy wyselekcjonowanych reguł Sigma obejmujących najnowsze techniki i taktyki atakujących (TTP). Łatwa personalizacja i rozbudowa - bez konieczności stosowania zamkniętej składni.

TWÓJ WSPÓŁPILOT BEZPIECZEŃSTWA: ROY

Nasz asystent AI, wytrenowany na najlepszych praktykach bezpieczeństwa, pomaga analitykom tworzyć reguły detekcji, analizować alerty i reagować na zagrożenia. ROY zwiększa produktywność Zespołów IT a także doświadczone zespoły SOC.

ZARZĄDZANIE INCYDENTAMI WSPIERANE PRZEZ AI

Sekoia automatycznie koreluje alerty w incydenty, zapewniając pełną świadomość sytuacyjną. Uruchamiaj playbooki reakcji i skracaj czas potrzebny do rozwiązania incydentu.

Porównanie planów

	Core	Prime
Zbieranie danych (w tym agent endpoint)	✓	✓
Odkrywanie zasobów	✓	✓
30-dniowy hot storage	✓	✓
Zweryfikowane reguły detekcji	✓	✓
Asystent AI (ROY)	✓	✓
Cloud SOAR	✓	✓
Alerty wzbogacone o CTI		✓
Kontrola dostępu oparta na rolach		✓
Własne kolekcje IoC		5 mln
On-prem SOAR		✓
Zarządzanie incydentami wspierane przez AI		✓
Dostęp do Intelligence Prime*	Opcjonalnie	✓ od 3 000 chronionych zasobów (assetów)

*Szczegółowe informacje znajdują się na blogu Sekoia.

FORRESTER®

“Sekoia została wskazana jako znaczący dostawca w raporcie The Security Analytics Platform Landscape.”

Security Analytics Platform Landscape 2024

Gartner

„Sekoia rozwija zaawansowane możliwości detekcji i reakcji, wykorzystując generatywną AI, ITDR oraz proaktywne mechanizmy bezpieczeństwa.”

Techscape for Detection and Response Startups 2025

Dowiedz się więcej na www.sekoia.dagma.pl

Gotowy na modernizację swojego SOC?

Sekoia Defend oferuje szybszy, inteligentniejszy sposób zabezpieczania organizacji.

CYBERSECURITY FROM EUROPE

Autoryzowany dystrybutor Sekoia w Polsce:
DAGMA Bezpieczeństwo IT

Dawid Dziobek
Product Manager Sekoia
tel. +48 538 857 641
dziobek.d@dagma.pl