

SIEM

Security Information & Event Management

Różne źródła w Twojej infrastrukturze IT nieustannie generują mnóstwo zdarzeń. **TEHTRIS SIEM** analizuje te zdarzenia i koreluje je, by skutecznie identyfikować potencjalne cyberataki.

Gartner

TEHTRIS został uznany za reprezentatywnego producenta w ramach zestawienia 2021 Market Guide for Extended Detection and Response*

Gromadzenie,
archiwizowanie, korelowanie
i ostrzeganie - w trybie 24/7

24/7

Walcz z coraz bardziej zaawansowanymi zagrożeniami

TEHTRIS SIEM gromadzi i przetwarza zdarzenia oraz generuje alerty, które usprawniają procesy decyzyjne w zakresie cyberbezpieczeństwa. Produkt jest zintegrowany z rozwiązaniem TEHTRIS XDR Platform oraz technologią SOAR.

Niezależnie od tego, jakie są Twoje źródła oraz ich formaty (Syslog, Leef, CEF, JSON, CSV, KVP, XML itd.), **TEHTRIS SIEM** może gromadzić informacje z dzienników zdarzeń dzięki nieustannie uaktualnianej bibliotece obsługiwanych platform.

Rozwiązanie daje możliwość automatycznej analizy wszystkich zdarzeń i oferuje zestaw ponad 1 600 reguł korelacyjnych. Ponadto, TEHTRIS SIEM korzysta z silnika analizy behawioralnej (UEBA), by identyfikować nietypową aktywność w ramach Twoich zasobów IT.

W zależności od Twojej polityki bezpieczeństwa możesz dostosować poziom generowania alertów (okno i próg wykrywania, poziom ochrony itd.) oraz tryb powiadamiania (e-mail, SMS itd.).

↓ Obsługiwane źródła: AWS, 0365, Proofpoint, Zscaler...

↓ Nadzór wszystkich systemów operacyjnych

↓ Monitoring, wykrywanie i ostrzeganie o incydentach bezpieczeństwa w czasie rzeczywistym

↓ Integracja z rozwiązaniem TEHTRIS XDR Platform

↓ Dostępność w modelu SaaS

Automatyczne prace dochodzeniowe i reagowanie

TEHTRIS SIEM jest zintegrowany z platformą XDR i w pełni korzysta z całkowitej automatyzacji ochrony oferowanej przez technologię SOAR.

Wyszukiwanie i monitorowanie wskaźników włamań

Dodawaj wskaźniki włamań do białej lub czarnej listy, by szybko identyfikować podejrzane zachowanie, dostosowywać bazy danych IoC oraz ułatwiać Twoim analitykom prowadzenie prac dochodzeniowych.

KORZYŚCI

- ▶ Łatwa instalacja i użytkowanie
- ▶ Nieustannie ewoluująca biblioteka źródeł i reguł
- ▶ Autonomiczne tworzenie i zarządzanie regułami
- ▶ Kompletny wgląd w Twoją infrastrukturę
- ▶ Pełne monitorowanie sieci w trybie 24/7
- ▶ Automatyzacja działań zespołu SOC

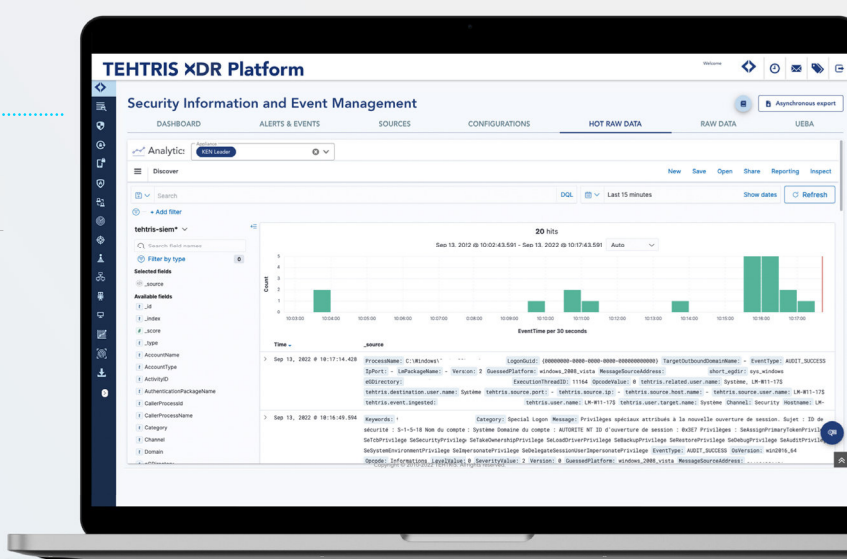
Parametry przechowywania danych

Optymalizuj badania związane z kryminalistyką cyfrową dzięki możliwości **konfigurowania czasu przechowywania danych** z dzienników zdarzeń. Zapewnij zgodność z zasadami RODO i protokołami bezpieczeństwa.



Nadzoruj cyberbezpieczeństwo swojej infrastruktury

Twórz własne panele informacyjne i monitoruj w czasie rzeczywistym kluczowe funkcje infrastruktury IT.



XDR

TEHTRIS XDR Platform

GROMADZENIE

ARCHIWIZACJA

KORELOWANIE

OSTRZEGANIE

KLUCZOWE
FUNKCJE

Monitoring w czasie rzeczywistym wszystkich Twoich zasobów IT

Kompatybilność ze wszystkimi elementami Twojej infrastruktury: serwery, urządzenia, sieci, sprzęt związany z bezpieczeństwem

Obsługa wszystkich formatów i protokołów

Architektura chmurowa

Ponad 1 600 reguł korelacyjnych w pakiecie

Pełna automatyzacja ochrony dzięki technologii TEHTRIS SOAR

Silnik analizy behawioralnej (UEBA)

Panele informacyjne z możliwością personalizacji

Prace dochodzeniowe przy użyciu danych z dzienników zdarzeń

Wyszukiwanie i monitorowanie wskaźników włamania

Rozwiązanie **TEHTRIS XDR Platform** jest w 100% kompatybilne ze standardem MITRE ATT&CK

**MITRE
ATT&CK®**

Logo GARTNER PEER INSIGHTS jest zarejestrowanym znakiem handlowym i usługowym należącym do organizacji Gartner Inc. i/lub podmiotów stowarzyszonych. «Recenzje publikowane w ramach Gartner Peer Insights obejmują subiektywne opinie użytkowników końcowych, publikowane w oparciu o ich doświadczenia i nie stanowią opinii organizacji Gartner ani podmiotów z nią stowarzyszonych.»

*Gartner oraz Market Guide są zarejestrowanymi znakami handlowymi organizacji Gartner Inc. i/lub podmiotów stowarzyszonych na terenie Stanów Zjednoczonych oraz globalnie. Znaki te zostały użyte w niniejszych materiałach za zgodą. Wszelkie prawa zastrzeżone.

TEHTRIS został uznany reprezentatywnym producentem w branży w raporcie 2021 Market Guide for Extended Detection and Response, Craig Lawson, Peter Firstbrook, Paul Webber, 8 listopada 2021 r.

Poproś
o demo

TEHTRIS XDR Platform

KONTAKT

tehttris@dlp-expert.pl
dlp-expert.pl/tehttris

