TEHTRIS
FACE THE UNPREDICTABLE

NEUTRALIZACJA ZNANYCH I NIEZNANYCH ZAGROŻEŃ W CZASIE RZECZYWISTYM BEZ INTERAKCJI CZŁOWIEKA

# EDR

## Endpoint Detection & Response

Klasyczne rozwiązania antywirusowe są bezsilne wobec współczesnych, wyrafinowanych cyberataków. Aby zabezpieczyć wszystkie punkty końcowe, potrzebujesz czegoś więcej. Postaw na firmę **TEHTRIS** i jej autorskie technologie.

Gartner

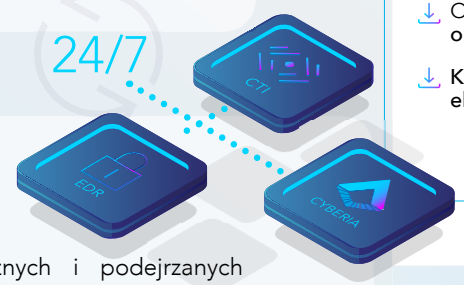
*TEHTRIS został uznany za reprezentatywnego producenta w ramach zestawienia 2021 Market Guide for Extended Detection and Response*.*

**TEHTRIS EDR zapewnia optymalną ochronę wszystkich punktów końcowych oraz pełny wgląd we wszystkie zasoby IT przy wykorzystaniu pełnej automatyzacji.**

- **Wykrywanie i neutralizacja w trybie 24/7** bez interakcji człowieka
- **Analiza statyczna** plików
- **Wstrzymywanie i wyłączanie procesów** oraz **kwarantanna**
- **Sieci neuronowe** (głębokie uczenie)
- Dostosowywanie **poziomu automatyzacji**
- Dostęp do rozwiązania **TEHTRIS XDR Platform** i jego technologii (SOAR, CTI, CYBERIA)
- Rozbudowane **panele informacyjne i raportowanie**
- Dostępność w modelu **SaaS i lokalnie**
- Ochrona **wszystkich systemów operacyjnych**
- **Kompatybilność z istniejącymi ekosystemami** poprzez API

## Monitoring punktów końcowych w trybie 24/7

**TEHTRIS EDR** chroni wszystkie punkty końcowe i serwery, łącząc w jednym agencie możliwości wykrywania i reagowania (**Endpoint Detection and Response – EDR**) oraz technologie antywirusowe następnej generacji (**Next Generation AntiVirus – NGAV**), by automatycznie identyfikować i neutralizować nawet najbardziej zaawansowane, nieznane cyber-zagrożenia w czasie rzeczywistym, bez interakcji człowieka.




## Niezrównane możliwości wykrywania i reagowania

**TEHTRIS EDR** przewiduje i blokuje cyberataki na wszystkie zasoby IT. Dzięki wykorzystaniu autorskiej sztucznej inteligencji **TEHTRIS CYBERIA** i jej zaawansowanych sieci neuronowych rozwiązanie osiąga niezrównaną skuteczność wykrywania znanych oraz nieznanych zagrożeń. Dzięki wsparciu technologii **TEHTRIS CTI (Cyber Threat Intelligence)** EDR oferuje wszystkie narzędzia niezbędne do zapewnienia bezpieczeństwa całej infrastruktury IT: natychmiastowa analiza niebezpiecznych i podejrzanych obiektów, sandboxing oraz aktywne polowanie na nowe zagrożenia. W połączeniu z rozbudowanymi funkcjami neutralizacji (wstrzymywanie i wyłączanie niebezpiecznych procesów, kwarantanna oraz regularne skanowanie dysków), **TEHTRIS EDR** eliminuje zagrożenia zanim zdążą wykonać jakiekolwiek szkodliwe działania.

## Orkiestracja ochrony

Dzięki zintegrowanej technologii orkiestracji **TEHTRIS SOAR**, rozwiązanie **TEHTRIS EDR** reaguje autonomicznie na nieznane cyberataki w trybie 24/7 i natychmiast je neutralizuje - bez interakcji człowieka.

Twoi eksperci mogą wybierać scenariusze reagowania na zagrożenia lub tworzyć własne reguły, dzięki czemu skupiają się na tym, co najważniejsze.

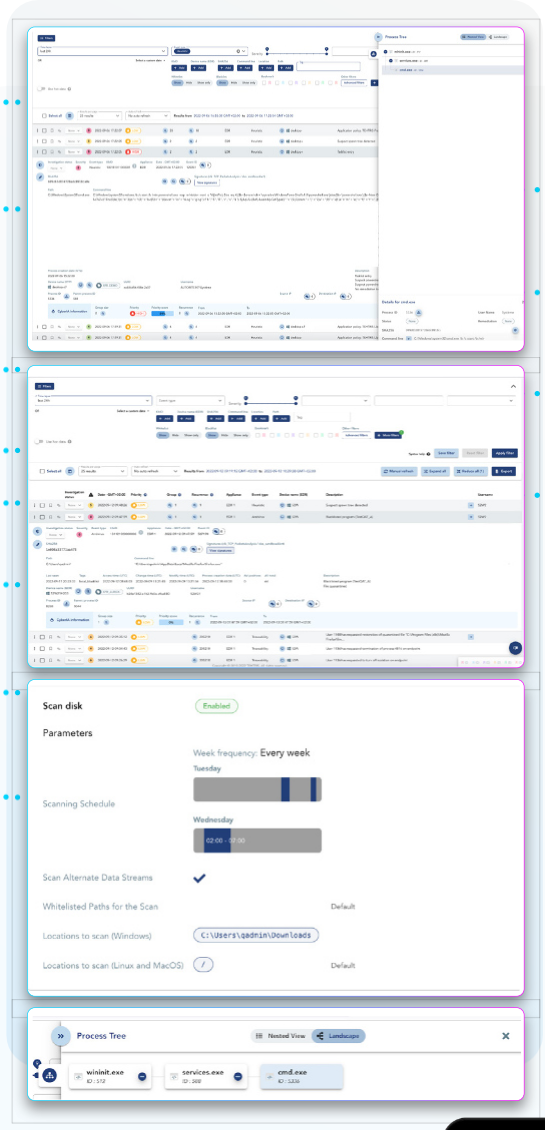
## KORZYŚCI

- Integracja z Centrum Bezpieczeństwa systemu Windows
- Pełny monitoring punktów końcowych i serwerów
- Wgląd w bezpieczeństwo całej infrastruktury IT
- Scentralizowane i zdalne zarządzanie
- Łatwe i szybkie wdrożenie

# KLUCZOWE FUNKCJE

## WYKRYWANIE

- **Kontrola i monitoring w czasie rzeczywistym** wszystkich punktów końcowych i serwerów
- **Skanowanie dysku** i przetwarzanie zgromadzonych informacji z użyciem sztucznej inteligencji CYBERIA oraz eksperckiej wiedzy o cyberzagrożeniach
- **Prace dochodzeniowe** i wyszukiwanie wskaźników włamań
- **Czarne i białe listy**
- **Szukanie luk na punktach końcowych** oraz audyty zgodności
- **Shadow IT:** wykrywanie niechronionych elementów w środowisku IT
- **SoC in the Box:** inteligentne i automatyczne przetwarzanie alertów
- **Wykrywanie ataków wykorzystujących PowerShell** i monitorowanie rejestru systemu Windows




## REAGOWANIE

- **Automatyczna, szczegółowa analiza** znanych i nieznanych zagrożeń
- **Natychmiastowe blokowanie zagrożeń** oraz ich neutralizacja
- **Kwarantanna** dla złośliwego i podejrzanego oprogramowania
- Rozbudowane **panele informacyjne** oraz raportowanie

### Obsługa wszystkich systemów operacyjnych

**Windows XP - Windows 11**
**Windows Server 2003 - 2022**

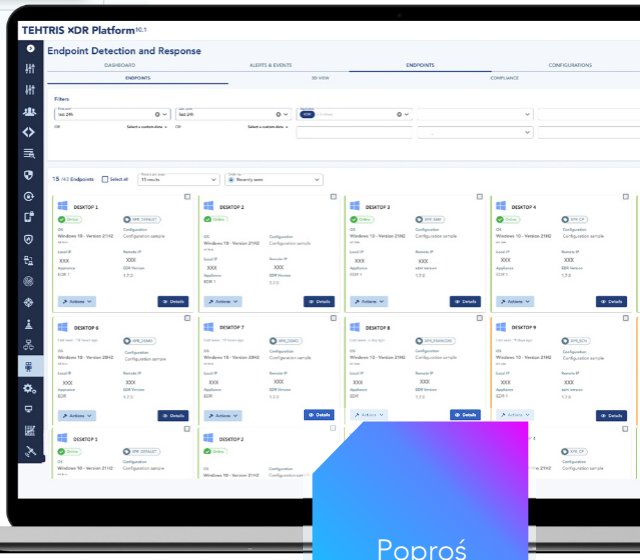
**macOS Sierra, High Sierra, Mojave, Catalina, Big Sur, Monterey, Ventura**

**Linux**

*TEHTRIS jest naszym kluczowym partnerem w zabezpieczaniu inteligentnego miasta. Rozwiązania firmy są innowacyjne, wyjątkowo wydajne i skuteczne, a zespół techniczny posiada olbrzymią wiedzę ekspercką.*

*przesłano 19 marca 2021 r.*

Gartner peerinsights




Rozwiązanie **TEHTRIS XDR Platform** jest w 100% kompatybilne ze standardem

**MITRE ATT&CK®**

Poproś o demo

*Logo GARTNER PEER INSIGHTS jest znakiem handlowym i usługowym należącym do organizacji Gartner Inc. i/lub podmiotów stowarzyszonych. «Recenzje publikowane w ramach programu 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, PaulWebber, 8 listopada 2021 r.*

TEHTRIS XDR Platform

EDR · EPP · MTD · SOAR · SIEM · NTA · Deceptive Response · DNS Firewall · Zero Trust · CWPP · Email Protection · Identity Access Management

## KONTAKT

tehtris@dlp-expert.pl
dlp-expert.pl/tehtris