TEHTRIS
FACE THE UNPREDICTABLE

Wykrywanie i reagowanie na urządzeniach mobilnych

OCHRONA SMARTFONÓW PRZED CYBERATAKAMI

MTD
Mobile Threat Defense

Aplikacja **TEHTRIS MTD** wykrywa i neutralizuje w czasie rzeczywistym wszelkie rodzaje ataków i podejrzane zachowanie na wszystkich Twoich smartfonach. Instalacja rozwiązania trwa zaledwie kilka chwil.

Gartner

TEHTRIS został uznany za reprezentatywnego producenta w ramach zestawienia 2021 Market Guide for Mobile Threat Defense*.

- **Szybka instalacja** (z chmury)
- **Scentralizowana kontrola i zunifikowana konsola**
- **Kontrola aplikacji** - od instalacji po uaktualnienia
- Wersje dla systemów **Android, iOS, iPadOS** oraz **Chrome OS**
- Dostęp do rozwiązania **TEHTRIS XDR Platform**

Twój smartfon… często zaniedbywana podatność infrastruktury IT na ataki

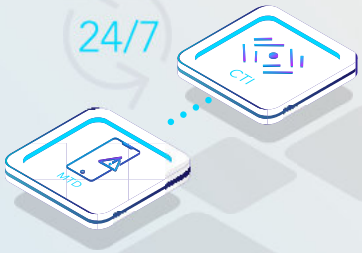
Informacje zapisywane na smartfonach są coraz bardziej poufne: e-maile, pliki, dokumenty, zdjęcia itd. Co gorsza, często urządzenia te przechowują zarówno dane prywatne jak i firmowe. Twoja flota mobilna może stać się słabym ogniwem w łańcuchu bezpieczeństwa i dlatego należy zadbać o jej należytą ochronę.

Wykrywanie i reagowanie na urządzeniach mobilnych w **CZASIE RZECZYWISTYM**

Android, iOS, iPadOS, Chrome OS

TEHTRIS MTD

w czasie rzeczywistym wykrywa i reaguje na ataki na Twoją flotę mobilną.



Baza wiedzy z informacjami o złośliwych programach i atakach, połączona z rozwiązaniem TEHTRIS CTI (ekspercka wiedza o cyberzagrożeniach), jest uaktualniana w trybie 24/7, by identyfikować, wykrywać i reagować na wszelkie rodzaje niebezpieczeństw: instalacja złośliwych aplikacji, aktualizacje wprowadzające niepożądane funkcje (łącznie z uaktualnieniami systemu), próby ataków siłowych mających na celu łamanie haseł, ataki typu man-in-the-middle, podatności w lokalnej konfiguracji itd.

Ochrona w czasie rzeczywistym połączona z wykrywaniem nowych luk w zabezpieczeniach: podatności są identyfikowane w systemach iOS, iPadOS, Android oraz na urządzeniach Chromebook. Rozwiązanie reaguje na ataki w trybie automatycznym, co pozwala na zmniejszenie powierzchni ataku, np. poprzez odizolowanie zainfekowanych urządzeń.

KORZYŚCI

WYDAJNOŚĆ
- **Szybkie wdrożenie**
- **Kompatybilność z EMM/MDM**
- **Automatyczne reagowanie na zagrożenia**

PERSONALIZACJA
- **Dostosowywanie ustawień zasad ochrony**
- **Czarna lista aplikacji**
- **Scenariusze reagowania**

AUTONOMICZNE DZIAŁANIE
- **Skanowanie bezpieczeństwa w tle**
- **Scentralizowany monitoring z konsoli**

Pełny wgląd w ochronę Twojej floty mobilnej

Instalacja i wdrożenie rozwiązania TEHTRIS MTD zajmuje zaledwie kilka chwil.

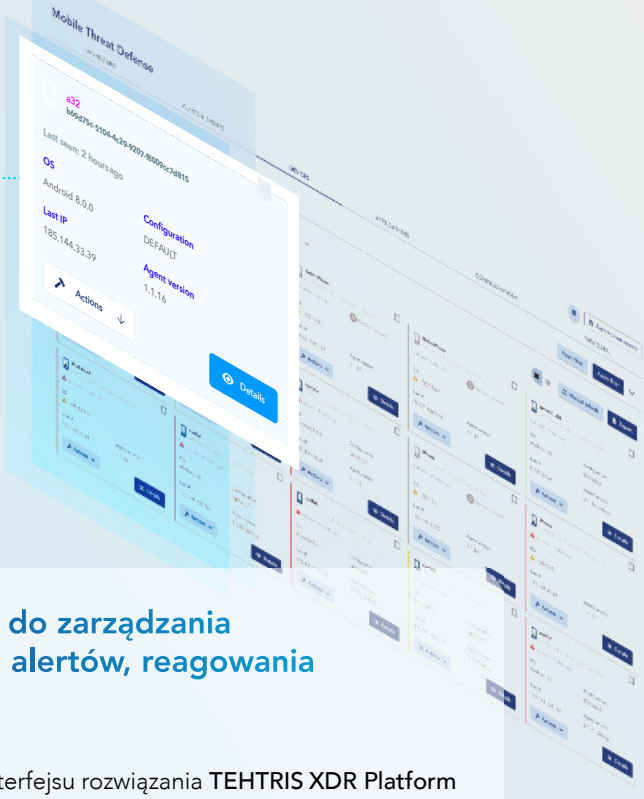
Jeżeli korzystasz z rozwiązań BYOD lub MDM, wdrożenie aplikacji nie wymaga żadnych zmian w ustawieniach, ani jakichkolwiek działań ze strony użytkowników. Zarządzanie ochroną urządzeń mobilnych odbywa się zdalnie, w modelu SaaS, i obejmuje konfigurację, integrację, wdrożenie oraz prace konserwacyjne. Do zarządzania Twoją flotą mobilną korzystasz ze specjalnie przygotowanej maszyny wirtualnej, która działa we w pełni zabezpieczonej chmurze TEHTRIS.

Jako klient firmy TEHTRIS jesteś informowany w czasie rzeczywistym o atakach na urządzenia mobilne - powiadomienia o alertach bezpieczeństwa są dostarczane z poziomu rozwiązania TEHTRIS XDR Platform.

Scentralizowany wgląd w Twoją flotę mobilną

Kontrola urządzeń wchodzących w skład Twojej **floty mobilnej**

- Dostęp do alertów i informacji o zdarzeniach
- Dostosowywanie interakcji z każdym urządzeniem mobilnym



Zunifikowana konsola do zarządzania urządzeniami, obsługi alertów, reagowania i raportowania

Korzystaj ze zunifikowanego interfejsu rozwiązania **TEHTRIS XDR Platform** oraz z rozszerzonych możliwości wykrywania i reagowania dzięki nieustannie uaktualnianej bazie wiedzy o cyberatakach (CTI), polowaniu na nowe zagrożenia, kontroli zgodności z zasadami ochrony oraz zarządzaniu incydentami. Wszystkie funkcje zostały zintegrowane przy użyciu technologii orkiestracji SOAR.

Automatyczne wykrywanie i neutralizowanie zagrożeń w czasie rzeczywistym

Monitorowanie urządzeń mobilnych w trybie 24/7

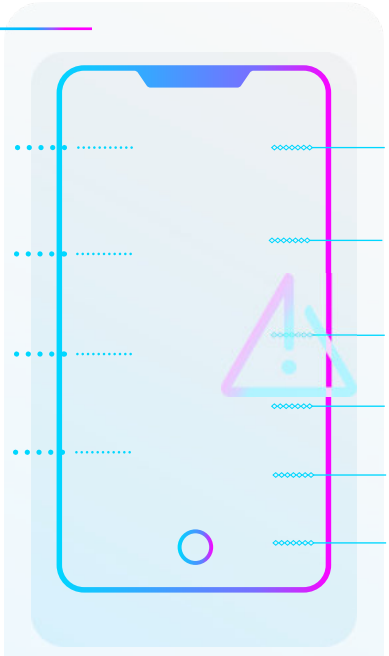
Anti-Jailbreak
Anti-Smishing
Zgodność z zasadami

Monitoring
aplikacji - od instalacji po uaktualnienia

Analiza
uprawnień aplikacji

Skanowanie niskopoziomowe:
wykrywanie jailbreaka, alternatywnych sklepów czy niedozwolonych portów

Analiza MAST*
statyczna i dynamiczna analiza kodu aplikacji zainstalowanych w Twojej flocie mobilnej lub podczas ich wewnętrznego rozwijania



Usuwanie
złośliwych aplikacji z poziomu konsoli

Łatwe wymazywanie/resetowanie
urządzenia mobilnego z poziomu konsoli - w przypadku kradzieży lub zgubienia

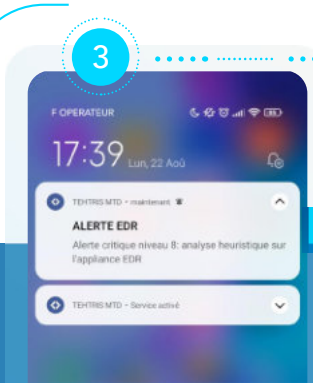
Czarna lista i zdalna dezinstalacja
aplikacji

TEHTRIS DNS Firewall
jako opcja z możliwością dostosowania

Izolowanie wg DNS
w przypadku ataku na urządzenie mobilne

Czarna lista DNS
z możliwością konfiguracji

TEHTRIS MTD
wykrywa i neutralizuje wszelkie rodzaje zagrożeń, łącznie z atakami siłowymi oraz man-in-the-middle.



Powiadomienia push pozwalają na otrzymywanie informacji w czasie rzeczywistym i szybkie reagowanie

W przypadku krytycznego alertu dotyczącego Twojej floty otrzymasz powiadomienie bezpośrednio na swój telefon za pośrednictwem rozwiązania TEHTRIS XDR Platform.

Kiedy i o czym będziesz informowany? **Ty decydujesz!**

Twoi analitycy z zespołu SOC mogą kontaktować się z Tobą poprzez powiadomienia push

* Mobile Automated Security Testing (MAST) - zautomatyzowana kontrola bezpieczeństwa mobilnego

KLUCZOWE FUNKCJE

WYKRYWANIE W CZASIE RZECZYWISTYM

Monitoring 24/7

- APK: **wykrywanie złośliwych lub nieznanych aplikacji**
- Dostęp: **zdarzenia związane z wdrożeniem nowego urządzenia oraz alerty dotyczące łączenia się z nowym hotspotem Wi-Fi**
- DNS: **rozwiązanie DNS Firewall powiadamia o próbach nawiązania połączenia z niebezpiecznymi domenami**
- Dziennik zdarzeń: **śledzenie działań wykonywanych zdanie na telefonach**
- Ataki siłowe: **wykrywanie i neutralizacja**
- Przechwytywanie TLS: **wykrywanie ataków typu man-in-the-middle**

Śledztwa i polowanie

- **Aplikacje ujęte w bazie danych CVE i polowanie na nowe zagrożenia**

Skanowanie bezpieczeństwa

- **Analiza dopuszczalnych uprawnień i uwierzytelniania w aplikacjach**
- Statyczna i dynamiczna analiza kodu: **(MAST - zautomatyzowana kontrola bezpieczeństwa mobilnego)**
- Analiza niskopoziomowa: **ponad 50 testów bezpieczeństwa**
- **Wykrywanie nieautoryzowanych procesów analizy kodu**
- **Wykrywanie** jailbreaka/rootowania
  Wykrywanie niechcianych aplikacji
  Wykrywanie wstrzykiwania złośliwych bibliotek

ZGODNOŚĆ Z ZASADAMI

- **Kontrola podatności na ataki siłowe**
- **Dostosowywanie minimalnego poziomu ochrony podczas odblokowywania urządzenia**
- **Czarna/biała lista aplikacji i adresów DNS**
- **Lokalizacja GPS**
- **Lista wykorzystywanych sieci Wi-Fi**

AUTOMATYCZNE REAGOWANIE

- **Zdalne wymazywania urządzenia**
- **Dezinstalacja aplikacji poprzez MDM**
- **Wymazywanie aplikacji poprzez MDM**
- **Czarna lista aplikacji i nazw domen**
- **Izolowanie atakowanych urządzeń**

PANELE I RAPORTY

Zunifikowana konsola dająca kompletną widoczność w trybie 24/7

- **Jailbreak/rootowanie**
- **Zainfekowane urządzenia mobilne**
- **Niezgodne urządzenia mobilne**
- **Informacje dot. wdrożeń TEHTRIS MTD**
- **Mapowanie systemów operacyjnych**

Historyzacja danych dot. bezpieczeństwa dająca większe możliwości śledzenia

- **DNS**
- **Geolokalizacja**
- **Historia skanowania**

Kontrola bezpieczeństwa

- **Raporty z analizy niskopoziomowej**
- **Raporty dot. systemów operacyjnych**

ALERTY

- **Alerty i zdarzenia**
- **Kategoryzacja zdarzeń**
- **Wysyłanie personalizowanych powiadomień push**
- **Krytyczne alerty dot. bezpieczeństwa poprzez zintegrowaną technologię SOAR**

Ciągły monitoring prowadzony przez firmę TEHTRIS w modelu SaaS

Usługi dostępne dla połączeń 3G/4G/5G Wi-Fi

«

Rozwiązanie TEHTRIS MTD uratowało nas przed atakiem wycelowanym w urządzenie, na którym wykonano jalibreak. / tak został natychmiast powstrzymany, a sam telefon funkcjonował dalej bez żadnych przerw. Dzięki temu rozwiązaniu nasza codzienna praca stała się znacznie łatwiejsza. Nie wyobrażamy sobie dalszego działania bez centralnego zarządzania naszą flotą mobilną.

»

Klient firmy TEHTRIS z sektora przemysłowego

Android 8.0
lub nowszy

iOS/iPadOS 14
lub nowszy

MITRE | ATT&CK®

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

Gartner Market Guide for Mobile Threat Defense, Dionisio Zumerle, Rob Smith, 29 marca 2021 r.

TEHTRIS XDR Platform

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

Autoryzowany partner

itxon systemy informatyczne

Systemy Informatyczne ITXON Sp. z o.o.
ul. Garncarska 34, 42-200 Częstochowa
(34) 399 25 00 / info@itxon.pl / www.itxon.pl