POUR PROTÉGER VOS SMARTPHONES ET TABLETTES DES CYBER ATTAQUES

MTD

Mobile Threat Defense

Installée en quelques secondes sur un mobile, l'application offre une protection complète en récoltant les évènements de sécurité sur un serveur dédié et sécurisé pour produire des alertes en temps réel sur la console unifiée TEHTRIS XDR AI PLATFORM.

afaq ISO 27001 Information Security AFNOR CERTIFICATION 2009/102155

Le mobile, la faille négligée de votre parc informatique...

Accès aux emails et autres applications de communication, répertoires de contacts, localisations GPS, téléchargement de fichiers, mélange des usages privés/professionnels (BYOD – Bring Your Own Device)... les informations de vos smartphones sont de plus en plus sensibles.
Point d'accès sous-estimé à votre parc informatique, votre flotte mobile nécessite plus que jamais d'être protégée face aux cyber attaques de plus en plus nombreuses et sophistiquées.

MTD protège en **TEMPS RÉEL** sur Android, iOS & iPadOS

iOS

Divers types de menaces sont détectées et identifiées !

- La protection est assurée par une approche multi-niveaux : système, réseau et application. Concernant les détections bas niveau, MTD est capable de détecter les fonctionnements anormaux des mobiles tels que l'utilisation d'émulateur et de débuggeur ou un mobile qui a subi un jailbreak ou qui a été rooted.
- Les outils de hacking sur iOS sont détectés et identifiés, ainsi que les stores d'application alternatifs.
- La solution assure une protection robuste contre l'ouverture de ports en identifiant les services associés.
- Les interceptions TLS des attaques MiTM (Man-in-The-Middle) sont repérées.
- L'accès à des sites web malveillants est bloqué par le DNS Firewall.
- L'installation d'applications Android malveillantes passe par une pluri-analyse antivirus des fichiers APK via la TEHTRIS Threat Intelligence dont un NGAV enrichi par l'Intelligence Artificielle développé par TEHTRIS. Cette base de connaissance des menaces est mise à jour 24/7 pour détecter, identifier et neutraliser toutes les nouveaux risques.

Une protection en temps réel associée à des options de remédiation automatique préserve votre flotte mobile en réduisant la surface d'attaque, notamment par l'isolation DNS des mobiles compromis.

BÉNÉFICES

SIMPLICITE

- Installation rapide
- Déploiement zero-touch (disponible sur Android)

EFFICACITE

- Compatible et complémentaire avec tout MDM
- Détection de menaces multi-niveaux
- Remédiation Automatique

PERSONNALISATION

- 2 configurations par défaut, entièrement paramétrables à vos politiques de sécurité
- Playbooks de remédiation (via TEHTRIS SOAR)

AUTONOMIE

- Scans de sécurité effectués en tâche de fond
- Surveillance centralisée depuis la console TEHTRIS XDR AI PLATFORM

Un bouclier complémentaire à votre arsenal de défense

Bénéficier de la complémentarité MDM/MTD

L'application est déployée via MDM en zero-touch sans modification des paramètres des mobiles ni action requise de l'utilisateur. La protection de votre flotte est opérée à distance depuis une console dédiée, incluant le paramétrage, l'intégration, le déploiement et le maintien en conditions opérationnelles.

Intégration totale aux modules de la TEHTRIS XDR AI PLATFORM

Profitez de l'interface unifiée TEHTRIS XDR AI PLATFORM et de ses capacités étendues de détection via les fonctionnalités de la TEHTRIS Threat Intelligence (base de connaissance mise à jour en continu enrichie par l'IA), et des capacités de réponse automatique grâce à l'orchestration du SOAR.

Un outil de notification transverse multiproduit TEHTRIS

Clients multiproduits TEHTRIS, vous êtes informés en temps réel via MTD des attaques sur votre parc informatique complet en recevant les notifications d'alertes de sécurité de la TEHTRIS XDR AI PLATFORM.

Sur la TEHTRIS XDR AI PLATFORM,

Des dashboards conçus pour optimiser les missions des analystes SOC !

Une vision centralisée de la flotte mobile

- Un visuel qui permet une évaluation rapide de la situation de la flotte
- Chaque mobile est répertorié avec son niveau de risque
- Une vision de toutes les applications Android installées sur le parc

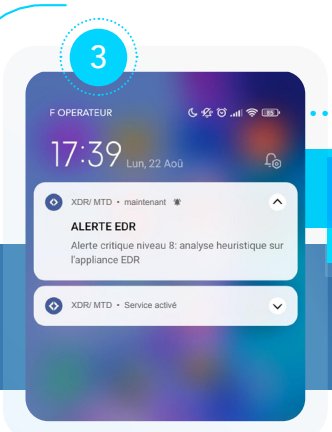
Un outil de visualisation des alertes dédié à l'analyse

- Le suivi en temps réel des alertes et évènements de sécurité
- Des données statistiques à filtrer pour affiner les investigations
- Un gain de temps pour rédiger des comptes-rendus

Détection et neutralisation automatique en temps réel

Surveillance 24/7 de vos mobiles

- **Analyse** des applications dès leur installation
- **Scan en profondeur** des menaces bas-niveau système
- **Identification** des applications malveillantes depuis la console
- **Protection DNS Firewall** et blocage d'accès aux sites web malveillants
- **Remédiation : isolation DNS** ciblée en cas de compromission d'un mobile



MTD permet l'envoi de Push Notification pour rester informé en temps réel afin d'optimiser votre réaction aux incidents de sécurité.

Soyez notifié directement sur votre mobile par la TEHTRIS XDR AI PLATFORM en cas d'alerte critique émise par les solutions TEHTRIS sur votre parc informatique.

Quand et à quel niveau d'alerte être notifié ? C'est vous qui décidez !

Vos analystes SOC en capacité de vous contacter en direct par push notification personnalisée !

FONCTIONNALITÉS CLÉS

DÉTECTION EN TEMPS RÉEL

Surveillance 24/7

- DNS Firewall : alerte lors des tentatives de connexion à un nom de domaine frauduleux
- APK (Android) : détection d'applications malveillantes
- Détection d'interception TLS : attaques Man-in-The-Middle
- Évènements liés à l'enrôlement d'un appareil
- Liste des ports TCP/UDP ouverts sur le mobile

Scan de sécurité

- Fréquence paramétrable
- Analyse bas niveau : des tests de sécurité en continu dont
  - Détection d'un processus de débogage et d'émulateur illégitime
  - Détection Root/Jailbreak
  - Détection d'un store d'application tiers indésirable

CONFORMITÉ

- Déploiement simplifié (zero-touch disponible sur Android)
- Sécurité de l'appareil : chiffrement, mot de passe, biométrie
- Mise à jour OS : notification en cas d'obsolescence (iOS)
- Fonctionnalité d'exception pour réduire les faux positifs (Android)

REMÉDIATION AUTOMATIQUE

- Accès vers des sites malveillants bloqués
- Isolation DNS ciblée

DASHBOARDS & REPORTING

Console unifiée pour une visibilité totale 24/7

- Dashboard sur l'état de la flotte en temps réel :
  - Situation des mobiles : compromis, à risque ou sécurisé
  - Indicateur déploiement MTD
  - Cartographie des OS
- Dashboard de répartition des alertes :
  - par sévérité, statut, type et sous-type, chronologie
  - Statistiques prêtes à être exploitées
  - Investigations affinées

Raw Data : Traçabilité des données de sécurité pour enquêter efficacement

- Logs système, réseau, application, DNS
- Historique des scans de sécurité
- Export des données

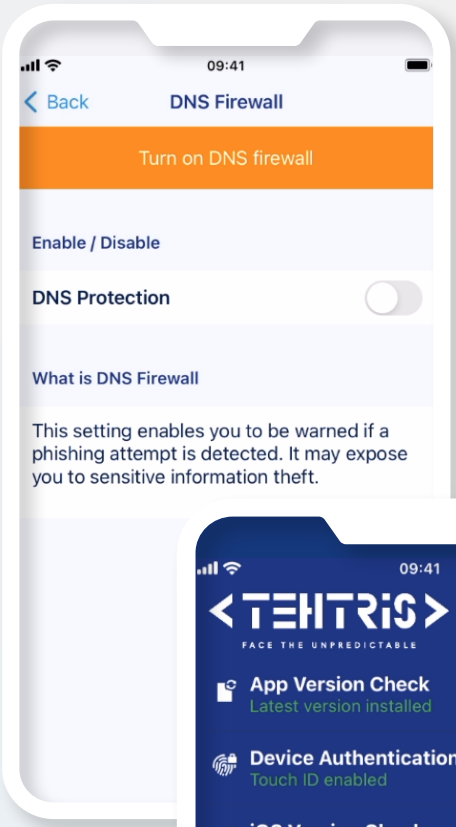
ALERTES

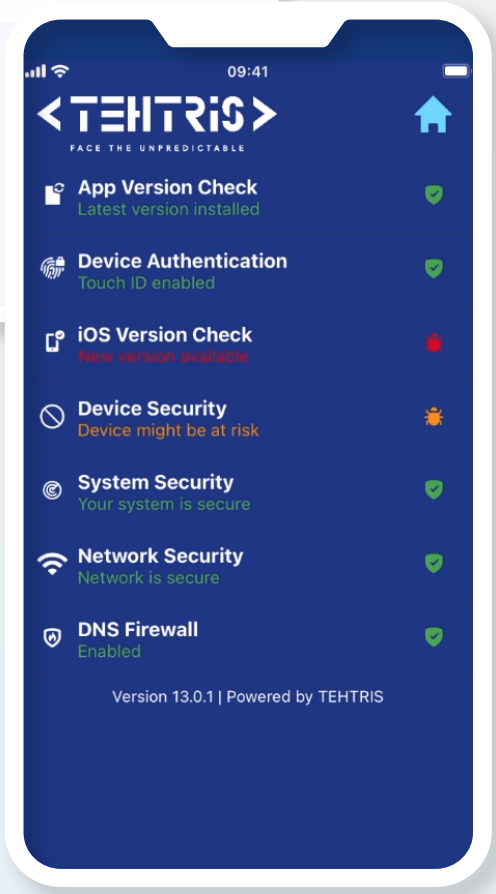
- Alertes & évènements
- Qualifications des évènements
- Alerte de sécurité critique via SOAR intégré
- Envoi de push notifications personnalisées

Maintenance continue opérée par TEHTRIS en mode SaaS

Dès
Android 10.0

Dès
iOS / iPadOS 15.0





La TEHTRIS XDR AI PLATFORM
est compatible à 100%
avec la matrice
MITRE ATT&CK®

Demandez une démonstration gratuite !

Oct.2024 - V_13

TEHTRIS XDR AI PLATFORM

EDR · MTD · SIEM · NTA · Honeypots · eGuardian · Threat Intel · SOAR · Zero Trust · Email Protection · Identity Access Management

CONTACTEZ-NOUS

tehtris.com/contact
business@tehtris.com