

XDR/ MTD

Mobile Threat Defense

Installée en quelques secondes, l'application **XDR/ MTD** offre une protection inédite en détectant et neutralisant en temps réel tous types d'attaques et comportements anormaux sur vos smartphones.



INDUSTRY RECOGNITION

TEHTRIS recognized as a Representative Vendor in the 2022 Gartner® Market Guide for Network Detection and Response*.

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

Accès aux emails, répertoires, téléchargement de fichiers, mélange des usages privés/professionnels... les informations de vos smartphones sont sensibles. Point d'accès sous-estimé à votre parc informatique, votre flotte mobile nécessite plus que jamais d'être protégée.

Mobile Détection & Réponse en TEMPS RÉEL

Android, iOS, iPadOS, Chrome OS



- ↓ Installation rapide (Cloud)
- ↓ Pilotage centralisé & console unifiée
- ↓ Contrôle de vos applications de l'installation à la mise à jour
- ↓ Disponible sur Android, Chrome OS, iOS et iPadOS
- ↓ Accès à la TEHTRIS XDR Platform

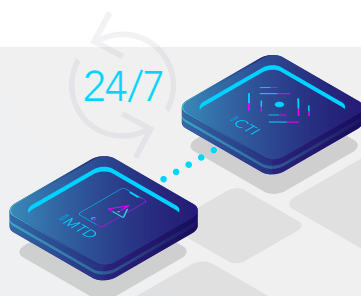
XDR/ MTD

détecte et remédie aux attaques sur votre flotte mobile en temps réel.

Sa base de connaissances des menaces - connectée à XDR/ CTI (Cyber Threat Intelligence) - est mise à jour 24/7 pour identifier, détecter et répondre à tous les types de menaces : de l'installation d'une application malveillante à sa mise à jour (y compris les applications système), les attaques

man-in-the-middle ou la découverte de vulnérabilités dans la configuration locale, grâce à sa bibliothèque d'analyse de bas niveau.

Une protection en temps réel associée à la chasse aux vulnérabilités : les failles de sécurité sont immédiatement détectées sur Android, Chrome OS, iOS et iPadOS. La remédiation s'effectue automatiquement et préserve votre flotte mobile en réduisant la surface d'attaque, notamment par l'isolation DNS des devices corrompus.



Visibilité totale sur votre parc mobile

XDR/ MTD s'installe et se déploie rapidement pour assurer la protection & vision 360° de votre flotte mobile.

L'application est déployée via MDM sans modification des paramètres des mobiles ni action requise pour l'utilisateur. La protection de votre flotte est opérée à distance en SaaS, incluant le paramétrage, l'intégration, le déploiement et le maintien en conditions opérationnelles. Vous disposez d'une machine virtuelle dédiée pour piloter votre flotte, déployée dans le cloud sécurisé de TEHTRIS.

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

BÉNÉFICES

EFFICACITÉ

- Déploiement rapide
- Compatible et complémentaire avec un EMM / MDM
- Remédiation Automatique

PERSONNALISABLE

- Paramétrage adaptable aux politiques de sécurité
- Blocklist d'applications
- Scénarii de remédiation (Playbooks)

AUTONOMIE

- Scans de sécurité effectués en tâche de fond
- Surveillance centralisée depuis la console

Supervision centralisée de votre flotte mobile pour une visibilité totale

Pilotage des appareils de la flotte mobile

- ▶ Accès aux Alertes & Events collectés
- ▶ Interactions personnalisables avec chaque mobile

Console unifiée de gestion des appareils, alertes, remédiation & reportings

Bénéficiez de l'interface unifiée **TEHTRIS XDR Platform** et de sa capacité étendue de détection et réponse via les fonctionnalités de XDR/ CTI (base de connaissance mise à jour en continu), Hunting, Compliance et de Gestion d'incidents, associés à l'orchestration du SOAR intégré.

Une XDR dédiée ou mutualisée déployée dans le Cloud de confiance TEHTRIS pour assurer la cybersécurité de votre flotte mobile. Une console unique pour garantir la conformité à votre politique de sécurité !

Détection & Neutralisation automatique en temps réel

Surveillance 24/7 de vos mobiles

Surveillance continue des applications, de l'installation aux mises à jour

Analyse des droits et autorisations des applications

Scan d'analyse de bas-niveau (jailbreak, stores alternatifs, ports)

✓ **Suppression** des applications malveillantes depuis la console

✓ **Blocklist**

✓ **Protection XDR/ DNS Firewall** (personnalisable en option)

✓ **Isolation DNS** ciblée en cas de compromission d'un mobile

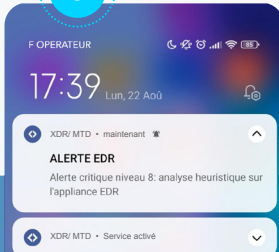
✓ **Blocklist DNS** (configurable)

XDR/ MTD

détecte tous les types d'attaques dont interceptions TLS dites man-in-the-middle attacks

Anti-smishing
Anti-Jailbreak
Conformité de sécurité

3



Push Notification restez informé en temps réel et optimisez votre réaction aux alertes

Soyez notifié directement sur votre mobile par la TEHTRIS XDR Platform en cas d'alerte critique sur votre parc.

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

NOUVEAU

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

FONCTIONNALITÉS CLÉS

DÉTECTION EN TEMPS RÉEL

Surveillance 24/7

- ▶ **APK** : Détection d'applications malveillantes ou inconnues
- ▶ **Access** :
Évènements liés à l'enrôlement d'un appareil
Alertes liées à la connexion à un nouveau Wi-Fi
- ▶ **DNS Firewall** : alerte lors des tentatives de connexion à un nom de domaine malveillant
- ▶ **Event Log** : Traçage des actions effectuées à distance sur les téléphones
- ▶ Détection **d'interception TLS**
(Man-in-the-middle Attacks)

Investigation & IOC Hunting

- ▶ CVE OS et applications. Chasse ciblée

Scan de sécurité

- ▶ Analyse des droits et autorisations des applications
- ▶ **Analyse bas niveau**: Plus de 50 tests de sécurité en continu
- ▶ Détection d'un processus de débogage illégitime
- ▶ Détection **Root Jailbreak**
Détection **d'un store tiers indésirable**
Détection **Injection malveillante de bibliothèque**

CONFORMITÉ

- ▶ Personnalisation de la sécurité minimale de déverrouillage de l'appareil
- ▶ Blocklist et Allowlist
- ▶ Localisation GPS
- ▶ Liste des réseaux Wi-Fi utilisés

REMÉDIATION AUTOMATIQUE

- ▶ Désinstallation des applications via MDM
- ▶ Blocklist des applications et noms de domaine
- ▶ Isolation DNS ciblée

DASHBOARD & REPORTING

Console unifiée pour une visibilité totale 24/7

- ▶ Mobiles Rootés / Jailbreakés
- ▶ Mobiles compromis
- ▶ Mobiles non conformes
- ▶ Indicateur déploiement XDR/ MTD
- ▶ Cartographie des OS

Raw Data : Historisation des données de sécurité pour une meilleure traçabilité

- ▶ DNS
- ▶ Géolocalisation
- ▶ Historique des scans de sécurité

Security Checks

- ▶ Rapports d'analyses de bas niveau
- ▶ Rapports systèmes d'exploitation

ALERTES

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



XDR/ MTD nous a sauvé la mise face à une attaque sur un appareil Jailbreak. L'attaque a tout de suite été stoppée et tous les portables ont continué à fonctionner sans qu'il y ait d'interruption. Au jour le jour, notre travail est simplifié. La gestion centrale des mobiles est devenue incontournable pour l'équipe.



RSSI secteur industriel, client TEHTRIS



Dès
Android 8.0



Dès
iOS / iPadOS 15

**MITRE
ATT&CK®**

TEHTRIS XDR Platform
est 100% compatible
avec MITRE ATTACK

Gartner, Market Guide for Mobile Threat Defense, January 2023, Market Guide for Network Detection and Response, December 2022, Hype Cycle for Endpoint Security, 2023, August 2023. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and HYPE CYCLE is a registered trademark of Gartner, Inc. and/or its affiliates and are used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Demandez une
démonstration

TEHTRIS XDR Platform

CONTACTEZ-NOUS

business@tehtris.com
tehtris.com

