(Endpoint Detection & Response)

EDR

LA PROTECTION INDISPENSABLE POUR VOS ENDPOINTS

CAS D'USAGE

- Détection d'incidents
- Limitation des incidents
- Chasse des menaces
- Investigation de cybersécurité
- Remédiation automatique
- Réduction de la surface d'attaque

TOUS LES AVANTAGES

- Réduction du MTTD (Mean time to detect)
- Réduction du MTTR (Mean time to respond)
- Intégration à TEHTRIS XDR Platform
- Gestion centralisée et à distance (SaaS)
- Facile à déployer et à utiliser (accompagnement /MSSP) en SaaS, On-Premise ou hybride.

TEHTRIS EDR, **l'EDR souverain hyper automatisé depuis 2013**, embarque de nombreux moteurs de détection et de neutralisation capables d'analyser les menaces très avancées du moment : **il détecte et neutralise automatiquement les menaces connues ou inconnues en temps réel et sans action humaine.**

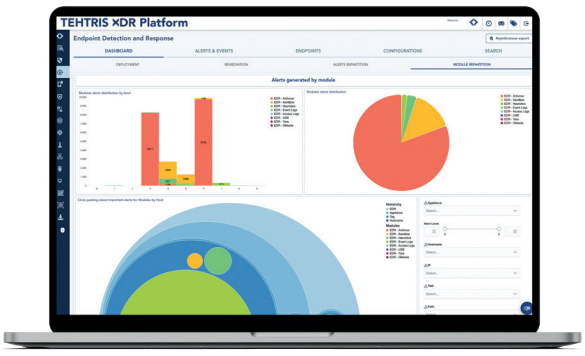
Un coup d'arrêt à votre dette technologique de cybersécurité.

TEHTRIS EDR fait partie des pionniers et créateurs de la technologie EDR. La technologie TEHTRIS, conçue pour **lutter et se défendre efficacement de façon autonome**, est en capacité d'installer des milliers d'agents EDR en moins de 24h, **de détecter des opérations d'espionnage furtif sans arme et sans malware**, de reconnaître les techniques utilisées par les pirates et **de construire en autonomie les réponses en avance de phase...**

TEHTRIS EDR est une solution fournie en mode SaaS, via le cloud, avec une volonté de **prévoir, prévenir, détecter et réagir au niveau cybersécurité.**

Nous croyons en la convergence des technologies EDR et EPP : complétez les fonctionnalités de détection de votre EPP avec la puissance de TEHTRIS EDR. L'EPP bloque les signatures connues et identifiées, tandis que l'EDR neutralise les nouvelles cyberattaques et comportements malveillants ou inconnus. **Bloquez instantanément toutes les attaques complexes qui échapperont à l'EPP** : l'installation du module EPP peut dès à présent se faire en totale autonomie depuis TEHTRIS EDR. **La solution bundle TEHTRIS EDR/EPP** peut se configurer selon les besoins de chaque client et s'adapter à tous les environnements.

TEHTRIS EDR est compatible avec tous les OS de votre parc informatique.



≤ 1 jour
pour déployer TEHTRIS EDR

+20k
EDR déployés dans le cloud en moins de 24 heures

Compatible avec tous les OS

EN SAVOIR PLUS
SUR LES SOLUTIONS TEHTRIS
Testez nos produits et contactez-nous
https://tehtris.com
business@tehtris.com

Bon pour la planète, léger pour vos ressources :

TEHTRIS EDR utilise seulement 1% de CPU et 90 Mo RAM, pour un stockage de <100Mo/agent*

**pour une machine standard Windows 10 avec 4 CPU et 8 Go de RAM*

EDR

DÉTECTION ET RÉPONSE À INCIDENT DANS LES SYSTÈMES D'EXPLOITATION

FONCTIONNALITÉS CLÉS

- Anti-Ransomware
- Anti-Spying
- Anti-Backdoors
- Remote Forensics
- Security Assessments
- Bundle TEHTRIS EDR/EPP
- Cloud & On-Premise

PLATEFORMES SUPPORTÉES

- Cloud Workload
- Windows Workstation
- Windows Server
- macOS
- Linux (Red Hat, Ubuntu, CentOs...)
- OT (SCADA/ICS)

Gartner peerinsights™

Au 31 Août 2021, TEHTRIS a obtenu la note globale de 5 sur 5 sur le marché des Endpoints Detection and Response, basée sur 13 revues.

FONCTIONNALITÉS

Intelligence artificielle CYBERIA intégrée : TEHTRIS EDR analyse les binaires et répond aux menaces inconnues en temps réel grâce au Machine Learning et au Deep Learning. La surveillance bas niveau permet d'obtenir des connaissances sur les comportements normaux pour distinguer les attaquants, leurs outils et leurs méthodes.

Protection contre les ransomware : TEHTRIS EDR contient des modules de détection et d'alerte face aux attaques de type ransomware, qui vont tenter de détruire les fichiers accessibles lors d'une contamination.

Produits tiers : TEHTRIS EDR comprend les méthodes de lancement d'interpréteurs de scripts ou d'autres fichiers externes afin de les analyser et stopper les tentatives modernes de contournement.

PowerShell : TEHTRIS EDR analyse les actions et les lignes de commande lancées depuis PowerShell, déclenchant en direct (au choix) des alertes et/ou des blocages, notamment pour toutes les gammes d'attaques modernes sans fichier.

Analyse mémoire : TEHTRIS EDR détecte les codes malveillants injectés dans la mémoire des processus, pour éviter les intrusions furtives modernes associées.

Audit de vulnérabilité : fonctionnalité unique à TEHTRIS EDR, capable d'inspecter les vulnérabilités connues (CVE) dans votre parc afin de réduire la surface d'exposition tout en respectant vos politiques de conformité face aux risques. 12 000 règles de points de contrôle sont inclues dans le moteur.

Mécanismes de liste blanche et de liste noire : TEHTRIS EDR peut imposer votre propre politique de sécurité afin de n'autoriser que les programmes choisis, ou interdire certaines menaces contraires à vos critères d'aversion au risque.

Politique avancée sur les applications : Créez et personnalisez vos règles techniques de cybersécurité pour bénéficier d'alertes / neutralisations / mises en quarantaine automatiques en fonction de vos préférences.

Shadow IT : TEHTRIS EDR détecte les éléments du parc non protégés.

Une efficacité renforcée avec TEHTRIS UES : TEHTRIS UES est la console qui unifie et renforce l'efficacité des solutions EDR, EPP et MTD. Dotée d'outils Front-End surpuissants et simples d'usage, la console UES vous permettra d'acquérir des capacités d'action de cybersécurité renforcées, pour une opération temporaire de crise comme de la surveillance régulière.

Sans Backdoors

Développé et hébergé en France et en Europe

Solutions natives

EN SAVOIR PLUS
SUR LES SOLUTIONS TEHTRIS
Testez nos produits et contactez-nous
https://tehtris.com
business@tehtris.com

TEHTRIS

FACE THE UNPREDICTABLE