

CAS D'USAGE

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

AVANTAGES

- Réduction du MTTD (Mean time to detect)
- Réduction du MTTR (Mean time to respond)
- Multiples modules XDR compatibles
- Gestion centralisée et à distance (SaaS)
- Facile à déployer et à utiliser

TEHTRIS XDR Platform répond à plusieurs besoins essentiels. Elle utilise son **réseau de capteurs efficaces**, comme les composants TEHTRIS EDR, **pour améliorer les capacités de protection, de détection et de réaction face à une attaque du réseau** où elle est positionnée. Avec la TEHTRIS XDR Platform, vous serez prêts, prêts à faire face à l'imprévisible.

TEHTRIS XDR Platform est **paramétrable de manière centralisée**, avec un **système intuitif pour construire ses propres arbres de décision** sur la conduite à tenir en cas d'agression.

Le fait d'avoir une **vision holistique centralisée**, dans la **console unifiée** de la TEHTRIS XDR Platform, autorise les analystes de cybersécurité à mixer différentes visions, sans jamais subir d'angle mort. On passera à souhait d'une vision orientée sur des signaux faibles, par exemple produits par les honeypots d'une appliance TEHTRIS Deceptive Response, à une autre interface, par exemple sur la partie antivirus nouvelle génération TEHTRIS EPP, ou sur les analyses d'APT trouvées par TEHTRIS EDR, pour comprendre pourquoi le Windows d'un employé s'est mis à scanner un honeypot interne de TEHTRIS.

L'unification des composants de la TEHTRIS XDR Platform se fait aussi au travers de nombreuses briques TEHTRIS : EDR, EPP, MTD, SIEM, Honeypots, NTA, DNS Firewall, Zero Trust Response, etc. Une **dynamique de partage entre les composants** est possible grâce aux relations entre les produits, avec des **automatisations via le SOAR intégré**, et des requêtes liées à du **renseignement technique** vers TEHTRIS CTI (Cyber Threat Intelligence).

SERVICES

TEHTRIS XDR PLATFORM



SIEM



DNS
FW



EDR



EPP



MTD



ZTR



NTA



DECEPTIVE
RESPONSE



CLOUD



SYSTEMS



NETWORKS

EN SAVOIR PLUS SUR LES SOLUTIONS TEHTRIS

Testez nos produits et contactez-nous
<https://tehtris.com>
business@tehtris.com

FONCTIONNALITÉS CLEFS

- Data Science, Dashboards
- Automatisation, SOAR
- Intelligence Artificielle
- Cyber Threat Intelligence
- Conformité, Audits

PLATEFORMES SUPPORTÉES

- Cloud
- Endpoints (Windows, Unix)
- On-Premise
- Mobile, IoT
- Networks
- OT (SCADA/ICS)

FONCTIONNALITÉS

Instrumentation de l'infrastructure du client avec des capteurs de TEHTRIS (EDR, EPP, Honeybots, etc.) pour obtenir des informations précises

Centralisation des données remontées depuis le terrain, de manière normalisée, dans un data lake dédié à l'écosystème TEHTRIS

Capacité d'analyse manuelle ou automatique, de data science, de hunting, d'audit et de corrélation entre les données de sécurité, les alertes et les incidents

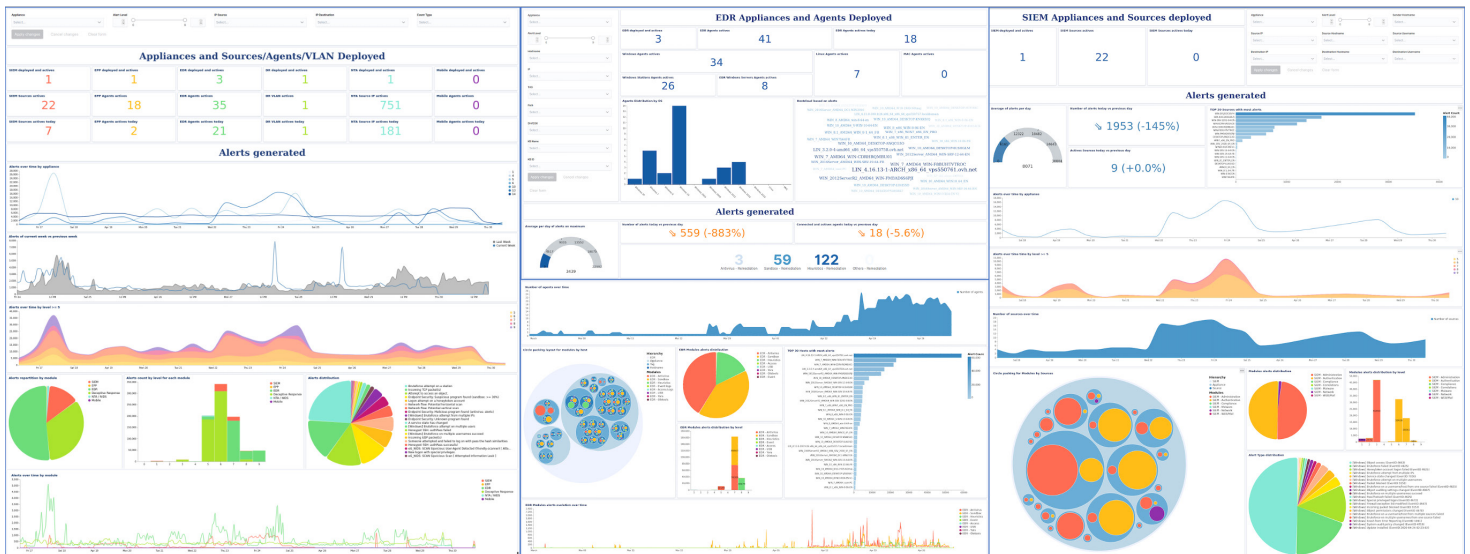
Capacité centralisée de réaction automatique aux incidents avec un **SOAR** intégré à la TEHTRIS XDR Platform, capable d'agir en retour vers différents produits de sécurité, en fonction d'une politique de sécurité prédéfinie

API internes privées et natives permettant de relier tous les composants de la XDR via des actions automatiques diverses

Simplicité et rapidité d'intégration de ces solutions y compris dans des infrastructures larges, hétérogènes et distribuées

Résultats immédiats grâce aux politiques de détection existantes fournies par défaut contre des millions de menaces déjà référencées dans les briques **TEHTRIS Cyber Threat Intelligence**

Sécurité efficiente avec des coûts maîtrisés et des outils réellement utiles sur le court et long terme



EN SAVOIR PLUS SUR LES SOLUTIONS TEHTRIS

Testez nos produits et contactez-nous
<https://tehtris.com>
business@tehtris.com

< TEHTRIS >

FACE THE UNPREDICTABLE