



Network Traffic Analysis
**SURVEILLEZ ET DÉTECTEZ
 LES INTRUSIONS RÉSEAU
 EN TEMPS RÉEL**



XDR/NTA

Network Traffic Analysis

Les activités malveillantes laissent des traces importantes sur les réseaux qui sont souvent sous-exploitées. Seule une supervision accrue permet de circonscrire les attaques. Avec **XDR/NTA**, vous surveillez vos réseaux : la détection des activités anormales au sein du trafic renforce votre capacité de réaction.

INDUSTRY RECOGNITION

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

Réactivité augmentée face aux attaques avec la surveillance et détection 24/7 de vos réseaux

24/7



Basé sur la capture de flux, XDR/NTA surveille les flux entrants et sortants d'un périmètre donné, ainsi que les mouvements latéraux qui pourraient s'y produire.

Grâce à une base de données de plus de 60 000 règles qualifiées, XDR/NTA détecte les activités anormales du trafic 24/7 en utilisant l'analyse des signatures réseaux et l'analyse comportementale (Intelligence Artificielle Cyberia).

Adapté à des environnements à la fois IT et OT, notre solution renforce la cybersécurité sur des appareils souvent oubliés (imprimantes, automates industriels...). Aucun processus supplémentaire de déploiement et de maintenance n'est requis de votre part.

Intégré à la TEHTRIS XDR Platform, les alertes NTA enrichissent vos contextes d'investigation lorsqu'une anomalie ou une activité suspecte (scan, exploit...) est repérée sur vos réseaux.

- ↓ Surveillance des signatures réseaux
- ↓ Détection des anomalies
- ↓ Accès à la TEHTRIS XDR Platform et à sa technologie augmentée (SOAR, CTI, Cyberia)
- ↓ Couverture complète des réseaux IT et OT

Intégration rapide

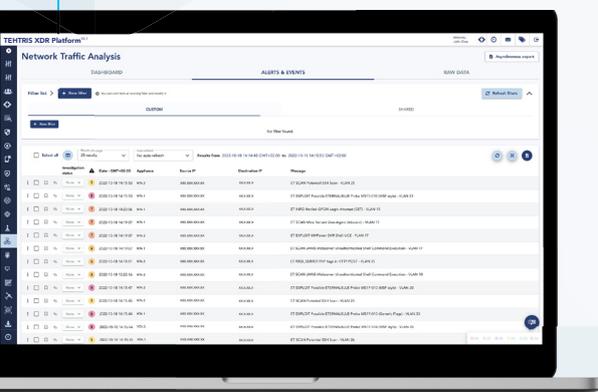
XDR/NTA s'intègre facilement dans votre environnement en y ajoutant des points de collecte passifs. Les systèmes en production et les éléments déjà en place ne sont pas modifiés.

Placement stratégique des sondes NTA

Déployez les sondes NTA sur les parties les plus critiques de votre réseau, pour cibler votre surveillance en accord avec votre politique de sécurité.

BÉNÉFICES

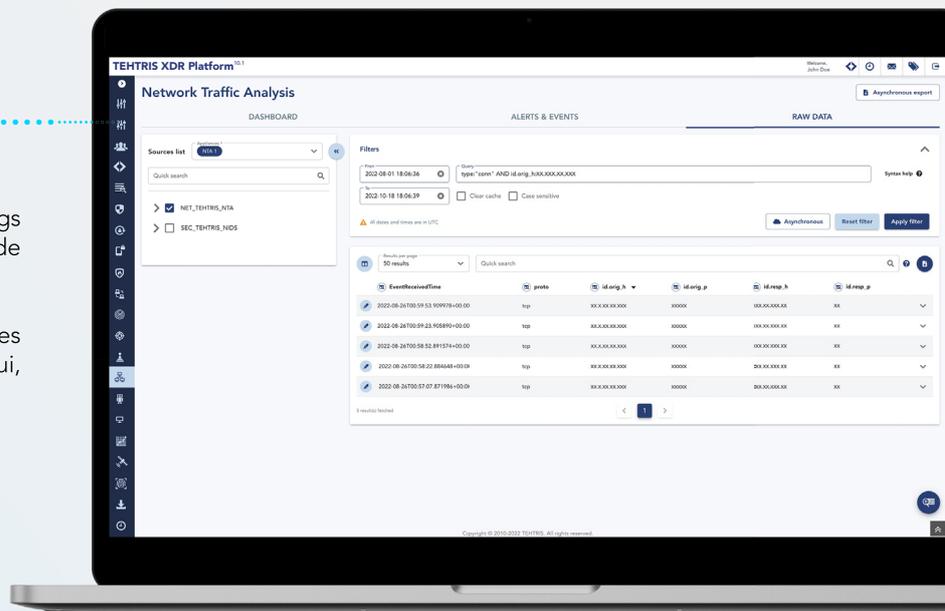
- ▶ Déploiement et intégration rapide
- ▶ Surveillance des flux de toutes les machines connectées à vos réseaux, internes et externes (prestataires, visiteurs,...)
- ▶ + 60 000 règles compatibles MITRE mise à jour en continu
- ▶ + 40 catégories d'alertes
- ▶ Analyses Forensic à partir des Raw Data



Des investigations plus précises avec l'historique XDR/ NTA

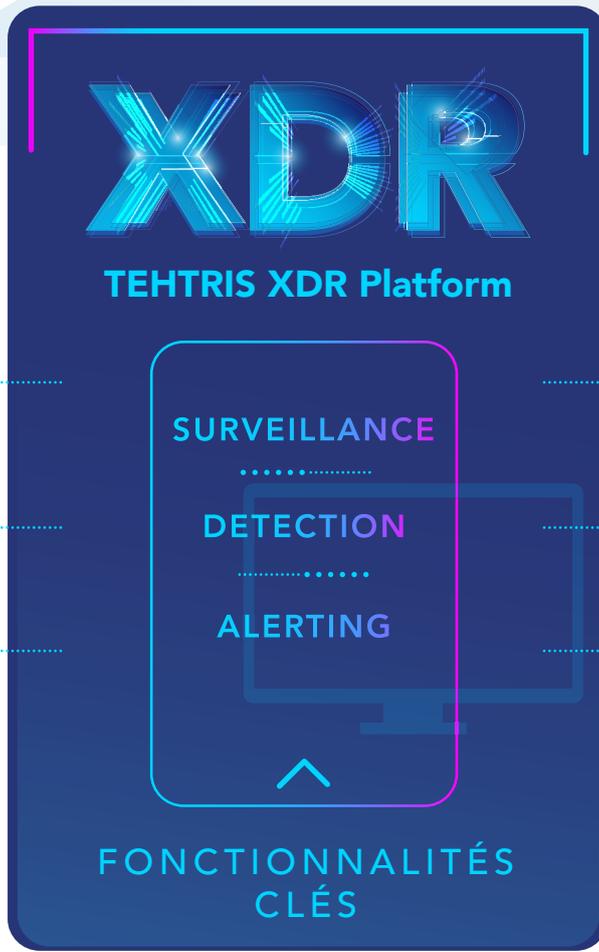
La vue Raw Data synthétise l'ensemble des logs réseaux collectés par XDR/ NTA et vous permet de mener des investigations en profondeur.

Obtenez un historique des connexions effectuées entre les machines pour savoir qui a parlé à qui, quand et comment.



Suivi en temps réel de l'activité sur le réseau

Surveillez vos alertes en temps réel et créez vos propres **tableaux de bord personnalisés**, en définissant les critères adaptés à vos besoins : degré de sévérité, source IP ou encore la destination IP.



Compatible sur tous les environnements IT et OT

Surveillance des flux réseaux en temps réel

Détection des activités suspectes grâce à l'analyse de signatures et l'analyse comportementale

Analyse des flux basée sur + 60 000 règles de sécurité compatibles MITRE et actualisées en continu

Investigations approfondies grâce aux Raw Data

Dashboards personnalisables

TEHTRIS XDR Platform est 100% compatible avec

MITRE ATT&CK®

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

