TEHTRIS ZTR
Zero Trust Response

La première offre mondiale de ZTNA avec réponse automatique contre les attaques

CAS D'USAGE

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

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

TEHTRIS ZTR est une solution tactique de type Zero Trust Network Access qui **protège en temps réel tous les flux réseaux** des machines clientes, et qui propose une surveillance basée sur des **mécanismes de capture de flux de métadonnées** (NetFlow) et d'autres dispositifs de protection comme des **réponses automatiques à incidents**, et de la **protection DNS.**

TEHTRIS ZTR s'inscrit dans le principe de sécurité **Zero Trust**, ce qui nous permet de vous proposer une **cyber surveillance complète**, tant à l'extérieur qu'à l'intérieur même de votre système d'information. Avec un positionnement optimisé dans votre réseau, TEHTRIS ZTR pourra surveiller autant les flux nord/sud (entrées et sorties d'un périmètre) que les flux est/ouest (déplacements latéraux).

La partie **détection** de TEHTRIS ZTR permet à votre centre opérationnel de sécurité d'**identifier les éléments normaux ou anormaux**, en termes de trafic. Doté de plusieurs modules, TEHTRIS ZTR base ses détections sur les signatures, et axe ses techniques sur les données comportementales, mais pas seulement : en effet notre outil est également à même de détecter des éléments suspicieux extrêmement variés, comme les scans furtifs lents. L'ensemble des flux est appris en continu pour pouvoir effectuer des analyses avancées et détecter des anomalies réseaux.

Grâce à l'**enregistrement des métadonnées**, en mode NetFlow, TEHTRIS ZTR offre la possibilité de créer des puits de logs, et d'effectuer, dès que cela s'avèrera nécessaire, des investigations de type Forensic.

De plus, TEHTRIS ZTR est capable de **réagir** grâce à un moteur de **réponse à incidents automatique** : en effet, TEHTRIS ZTR est la **première solution au monde à intégrer du SOAR dans un outil ZTNA**. Là où de nombreuses solutions ZTNA/SASE nécessitent l'usage d'un SIEM pour être pleinement efficaces, TEHTRIS ZTR, de part son intégration native à la TEHTRIS XDR Platform, vous permet d'accéder directement à une véritable **synergie entre vos solutions de sécurité**, ainsi qu'à des **capacités surpuissantes d'automatisation.** De ce fait, si TEHTRIS ZTR écoute les flux qui circulent, les étudie et recherche les éléments qui pourraient être utilisés par un cyberattaquant, il peut également mettre en place des actions automatiques proportionnées, comme l'isolation des machines, la redirection vers des leurres informatiques (honeypots), le blocage de certains flux, etc. Ce procédé offre la possibilité de limiter votre surface d'attaque, de manière mandataire, sans même lancer d'opération sur les machines concernées, ce qui est très pratique pour tous les environnements qui ne peuvent pas avoir d'agent ou de Firewall local comme dans les réseaux OT ou IoT.

Optez pour une cybersécurité globale et rigoureuse, pensez TEHTRIS Zero Trust Response.

EN SAVOIR PLUS
SUR LES SOLUTIONS TEHTRIS

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

TEHTRIS ZTR
Zero Trust Response

La première offre mondiale de ZTNA avec réponse automatique contre les attaques

FONCTIONNALITÉS CLEFS

- ZTNA, VPN
- FWaaS (FireWall as a Service
- Protection DNS
- Détection via signatures
- Network Forensic
- SOAR intégré

PLATEFORMES SUPPORTÉES

- Cloud & On-Premise
- Windows
- Linux
- MacOS
- iPhone/iPad
- Android
- IT/OT

FONCTIONNALITÉS

TEHTRIS ZTR vous propose des fonctionnalités de **protection DNS**, comme de l'anti-phishing, de l'anti-spyware, de l'anti-malware ou de l'anti-backdoor

TEHTRIS ZTR inclut une **protection VPN** et une solution **FireWall as a Service**

TEHTRIS ZTR vous permet de **détecter des intrusions en temps réel** par l'analyse des flux réseaux via des signatures et les analyses comportementales (NIDS)

TEHTRIS ZTR vous permet de mener à bien des **investigations Forensic** en effectuant des autopsies tactiques centrées sur les discussions réseaux grâce aux métadonnées des flux enregistrés en continu, pour retrouver qui a parlé à qui, quand et comment

TEHTRIS ZTR permet l'**identification des pics anormaux d'activité** du réseau et l'analyse de certains comportements comme les déplacements latéraux

TEHTRIS ZTR est **facile à maintenir** : les bases de données sur les signatures et les menaces via notre **CTI** (Cyber Threat Intelligence) sont mises à jour automatiquement et continuellement

TEHTRIS ZTR est une **machine virtuelle facilement déployée** sur le matériel du client (hyperviseur VMware ESXi), ou dans le Cloud de TEHTRIS

TEHTRIS ZTR est connecté via Internet à sa **TEHTRIS XDR Platform** (centralisation et surveillance des traces) et est **administrable à distance** par TEHTRIS en mode SaaS

TEHTRIS ZTR peut être au choix en mode **on-premise**, en mode **cloud**, ou en mode **hybride**

EN SAVOIR PLUS
SUR LES SOLUTIONS TEHTRIS

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

FACE THE UNPREDICTABLE

https://tehtris.com
@tehtris