NTA

TEHTRIS NTA est une solution tactique d'analyse de vos flux réseaux en temps réel, utilisant des mécanismes de capture de flux, de métadonnées (NetFlow) et d'audit passif.

CAS D'USAGE

- Détection d'incidents
- Limitation des incidents
- Chasse des menaces
- Investigation de cybersécurité
- Investigation Forensic
- 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

TEHTRIS NTA est une solution tactique d'**analyse de vos flux réseaux en temps réel**, utilisant des mécanismes de **capture de flux de métadonnées (NetFlow) et d'audit passif**.

En fonction de sa position dans votre infrastructure, TEHTRIS NTA pourra autant surveiller les **flux nord/sud** (entrées et sorties d'un périmètre donné) que les **flux est/ouest** (déplacements latéraux). Cette sonde offre la possibilité à une équipe SOC de comprendre ce qui est normal ou non, en termes de trafic.

Plusieurs modules sont présents dans TEHTRIS NTA, avec des **détections basées sur des signatures**, et des techniques basées sur le comportemental. 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 NTA offre la possibilité de remonter dans le temps, en cherchant qui a parlé à qui, quand et comment. Contrairement à de nombreuses solutions, TEHTRIS NTA ne nécessite pas l'usage d'un SIEM pour être utile, puisque la solution est directement intégrée dans la TEHTRIS XDR Platform, afin d'enrichir cet écosystème.

Pour lever des alertes, TEHTRIS NTA n'est pas uniquement limité à des signatures ou à des analyses comportementales. En effet, certains éléments suspicieux pourront être détectés autrement, comme les **déplacements latéraux**, ou les **scans furtifs lents**.

De plus, TEHTRIS NTA est capable de **détecter les vulnérabilités de machines dans le réseau** grâce à un moteur TEHTRIS qui écoute tous les flux qui circulent, qui les étudie, et qui recherche les éléments qui pourraient être utilisés par un pirate. Ce procédé offre la possibilité de **mieux connaître sa surface d'exposition, sans même lancer de scan offensif ou risqué,** ce qui est très apprécié dans certains milieux, comme dans les réseaux OT ou IoT, sachant que TEHTRIS NTA ne se limite pas à ces environnements, puisqu'il est compatible aussi avec les réseaux IT.

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

NTA

Recherche des attaques et des vulnérabilités dans les flux réseaux

FONCTIONNALITÉS CLEFS

- Détection via signatures
- Audit passif de vulnérabilités
- Enregistrements de type NetFlow
- Dashboards et Rapports
- Cloud & On-Premise

PLATEFORMES SUPPORTÉES

- Cloud
- Port Mirroring
- Test Access Port
- TCP/IP
- VMware ESXi
- OT (SCADA/ICS)

FONCTIONNALITÉS

TEHTRIS NTA est une machine virtuelle **facilement déployée** sur le matériel du client (hyperviseur VMware ESXi).

TEHTRIS NTA est **connecté via Internet à sa TEHTRIS XDR Platform** (surveillance des traces et maintenance en mode SaaS).

NIDS : détection des intrusions en temps réel par l'analyse des flux réseaux via des signatures.

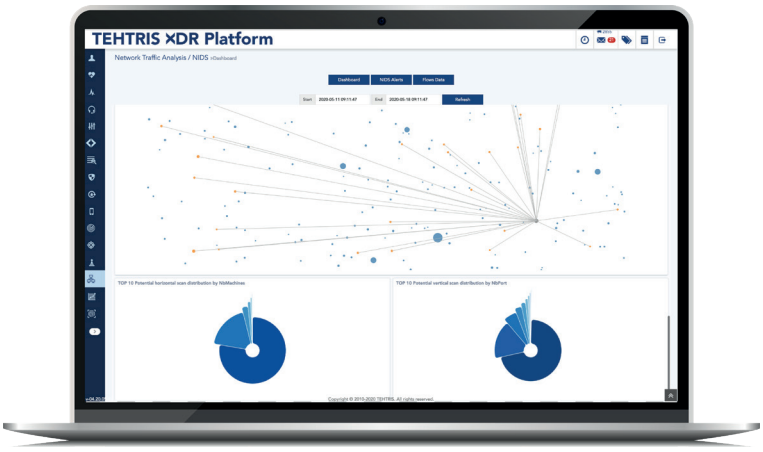
Audit passif : détection des vulnérabilités en écoutant le trafic des machines présentes sur le réseau via un moteur d'analyse, sans qu'il soit nécessaire de scanner ou d'attaquer les cibles.

Network Forensic : autopsie tactique centrée sur les discussions réseaux grâce aux métadonnées des flux enregistrés en continu, pour retrouver qui a parlé à qui, quand et comment.

Mise à jour automatique des signatures.

Identification des pics anormaux d'activité du réseau et **analyse** de certains comportements comme les déplacements latéraux.

Administration à distance par TEHTRIS en mode SaaS.



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

TEHTRIS

FACE THE UNPREDICTABLE