TEHTRIS
FACE THE UNPREDICTABLE

QUALIFIEZ VOTRE PRISE DE DECISION AVEC NOTRE MOTEUR AUTOMATIQUE DE CORRELATION

afaq ISO 27001 Information Security
AFNOR CERTIFICATION
2009/102155

XDR/ SIEM

Security Information & Event Management

Les sources qui émettent des évènements sont souvent très nombreuses au sein d'une organisation. XDR/ **SIEM** analyse l'ensemble des événements de votre Système d'Information et les corrèle pour identifier tous types d'attaques.

Industry Recognition

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

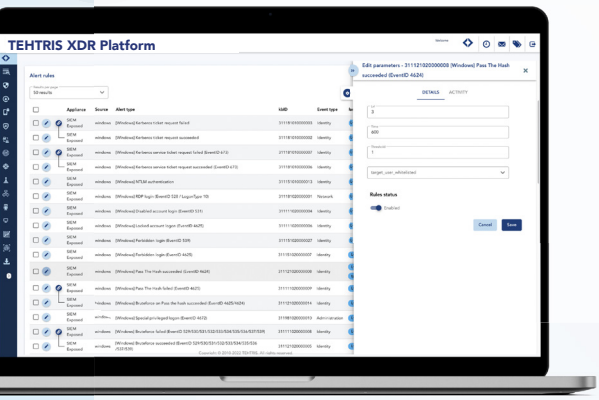
- **Sources supportées :** AWS, 0365, Proofpoint, Zscaler...
- **Supervision sur l'ensemble des OS**
- **Surveillance, détection** et **alerte** des évènements de séurité **en temps réel**
- Intégré à la **TEHTRIS XDR Platform**
- Disponible en **Cloud**

Collecte, archive, corrèle et alerte en 24/7

24/7

Des menaces de plus en plus fréquentes et furtives

Intégré à la **TEHTRIS XDR Platform** et interconnecté avec le **SOAR**, **XDR/ SIEM** collecte, traite et alerte pour faciliter la prise de décision.



Quelles que soient vos sources et leurs formats (Syslog, Leef, CEF, JSON, CSV, KVP, XML...), **XDR/ SIEM** collecte les logs grâce à une bibliothèque de parsers et connecteurs en constante évolution.

Analysez automatiquement l'ensemble de vos évènements en choisissant parmi un catalogue de plus de **2 000 règles de sécurité**. En complément, bénéficiez du moteur d'analyse comportementale (UEBA) pour identifier les activités inhabituelles sur votre parc.

En fonction de votre politique de sécurité, personnalisez votre niveau d'alerting et définissez votre mode de notification (e-mail, SMS...) avec l'orchestrateur intégré : fenêtre de détection, seuil de détection, niveau de sévérité...

Investigation et réponse automatisée

TEHTRIS SIEM bénéficie de l'**hyperautomatisation et du SOAR intégré de la XDR Platform** permettant la création de playbooks supplémentaires, comme l'enrichissement de notes et d'alertes...

Recherche et mise sous surveillance d'IoC

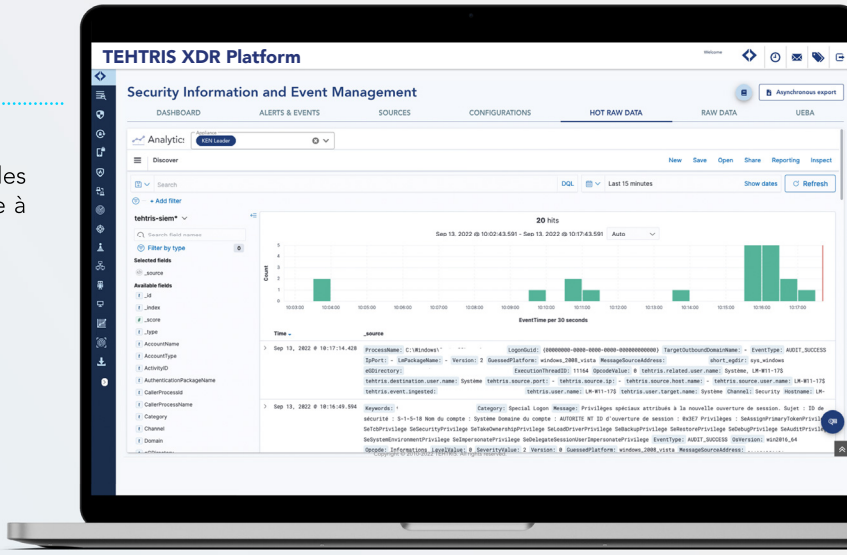
Blacklistez ou **Whitelistez** les IoC pour rapidement identifier des comportements suspects, personnalisez vos bases d'IoC et facilitez le travail d'investigation de vos analystes.

BÉNÉFICES

- Facilité d'installation et d'utilisation
- Bibliothèque de sources et de règles en constante évolution
- Création et gestion des règles en autonomie
- Vision à 360° sur l'ensemble de votre infrastructure
- Surveillance complète du réseau 24/7
- Automatisation des actions du SOC

Hot Raw data configurable

Tout en restant conforme à la RGPD et aux protocoles de sécurité, optimisez votre recherche forensic grâce à la **rétention personnalisable** des Hot Raw data.



Supervisez la cybersécurité de votre parc

Créez vos **propres tableaux de bords** et surveillez les fonctions vitales de votre infrastructure en temps réel (indicateurs de volumétrie des logs, de sources actives...).

XDR

TEHTRIS XDR Platform

- Surveillance en temps réel de tous les équipements IT
- Compatibilité avec tous les composants de vos infrastructures, serveurs, appareils, équipements réseaux ou de sécurité
- Acceptation de tous les formats et protocoles
- Plus de 2 000 règles de sécurité disponibles à activer ou désactiver
- Création et gestion des règles en autonomie

COLLECTE

ARCHIVAGE

CORRELATION

ALERTES

FONCTIONNALITÉS CLÉS

- Hyperautomatisation grâce au XDR/ SOAR
- Moteur d'analyse comportementale (UEBA)
- Création de tableaux de bords personnalisables
- Recherche et mise sous surveillance d'IoC
- Forensic dans les Hot Raw data
- Architecture Cloud

TEHTRIS XDR Platform est 100% compatible avec

MITRE ATT&CK®

Demandez une démonstration

TEHTRIS XDR Platform

EDR · MTD · SIEM · NTA · Honeypots · CYBERIA eGuardian · CTI · SOAR · Zero Trust · Email Protection · Identity Access Management

CONTACTEZ-NOUS

business@tehtris.com
tehtris.com

Déc. 2023 - V_11