SIEM

Centralisez et organisez la gestion de tous les logs de votre environnement : les évènements des systèmes, des applications, des équipements réseau ou de sécurité.

CAS D'USAGE

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

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
- Modèle souple de consommation

TEHTRIS SIEM (Security Information and Event Management) fournit un outil d'alerte efficace pour **surveiller la sécurité de vos systèmes et applications**, par le biais de **rapports et de tableaux de bord d'évènements**, propulsés par un **moteur de corrélations** alimenté par des renseignements sur les menaces grâce à la vaste TEHTRIS XDR Platform.

L'analyse associée vous permet de garder un œil sur la santé de vos systèmes pendant que **vos actifs sont sous contrôle** grâce à une **agrégation de données en temps réel.**

Celle-ci garde une **trace des comportements anormaux** et offre également une rétention de données pour une **analyse Forensic plus poussée** qui favorisera une **chasse aux menaces à un niveau supérieur** pour une meilleure conformité avec les normes communes.

Intégré à la TEHTRIS XDR Platform, le TEHTRIS SIEM permet une **détection en temps réel des incidents et une automatisation des services SOC**. Il fournit une vue d'ensemble perspicace et des alertes intelligentes, facilitant la tâche de l'équipe de réponse de votre centre d'opérations de sécurité.

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

SIEM

Traçabilité complète et alertes de cybersécurité.

FONCTIONNALITÉS CLEFS

- Centralisation des logs
- Surveillance, Corrélation & Analyse
- Dashboards & Rapports
- Historique des données
- Cloud & On-Premise Hybride
- SIEM Cluster
- UEBA & analyse comportementale

SOURCES SUPPORTÉES

- Cloud (App, Workload, etc.)
- OS (Windows, Linux, etc.)
- Network Equipment (Firewalls, Proxy, Router, etc.)
- Security Protection (Antivirus, EDR, etc.)
- Authentication Services
- Databases
- Applications
- OT (SCADA/ICS)

FONCTIONNALITÉS

Souplesse et simplicité d'intégration avec les modes on-premise, cloud, ou hybride.

Possibilité de construire des offres à la source pour être en nombre d'EPS illimité.

Collecte des logs avec agent et sans agent.

Surveillance de tous vos équipements IT et OT.

Compatible avec :

- tous les composants de vos infrastructures (routeurs, firewalls, proxies, switches, bastions...)
- tous les systèmes d'exploitation (UNIX, Windows...)
- toutes vos applications à surveiller (antivirus, bases de données, SAP...)
- les sources dans le cloud (Azure Active Directory / Office 365, Salesforce...)

Acceptation de :

- tous les formats : LEEF, CEF, JSON, CSV…
- tous les protocoles classiques : Syslog TCP, Syslog UDP...

Solution ultra sécurisée installée dans des appliances contenant un kernel blindé contre les 0-days et avec un disque dur totalement chiffré.

Intégration simplifiée des VM métiers dans vos environnements VMware ESXi avec la possibilité de faire grandir le hardware dans le temps pour suivre vos évolutions SIEM (plus de CPU, de RAM, de disque).

Fourniture par défaut de plus de 1000 règles d'alerte qui détectent l'ensemble de toutes les attaques reconnues par TEHTRIS et rassemblées sur votre SIEM pour être opérationnel dès le premier jour.

Possibilité de faire ajouter des règles d'alerte au travers de l'interface de création de règles de corrélation.

Gestion unifiée des quantités de données Cloud grâce au SIEM Cluster par : Support de volumétrie importante et scalabilité grâce au SIEM Cloud Cluster.

Analyse comportementale basée sur un module UEBA permettant la détection d'anomalies et la création de rapports.

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

TEHTRIS

FACE THE UNPREDICTABLE