SIEM

Centralize and organize the management of all the logs in your environment: events from systems, applications, network or security devices.

USE CASES

- Detection of incidents
- Threat Hunting
- Cybersecurity
- Investigations
- Forensic Investigations
- Attack Surface Reduction
- Behavorial Analysis

TEHTRIS SIEM (Security Information and Event Management) provides an effective alerting tool to monitor the security of your systems and applications through reports and event dashboards powered by a correlation engine fed by threat intelligence from the extensive TEHTRIS XDR Platform.

The resulting analysis allows you to keep an eye on the security health of your systems while your assets are under control through real-time data aggregation. This keeps track of abnormal behavior and also provides data retention for further forensic analysis that will allow you to hunt down threats at a higher level for better compliance with common standards.

Integrated with the TEHTRIS XDR Platform, TEHTRIS SIEM **enables real-time incident detection and response and automation of Security Operations Center (SOC) services** to provide insights and smart alerts, making the job of your SOC response team easier.

ALL BENEFITS

- Faster MTTR (Mean time to respond)
- Integrated with TEHTRIS XDR Platform
- Remote & Centralized Management (SaaS)
- Easy to deploy and easy to use
- Smooth consumption model

LEARN MORE
ABOUT TEHTRIS SOLUTION
Test our products or contact us
https://tehtris.com
business@tehtris.com

SIEM

Full cybersecurity accountability with correlations

KEY FEATURES

- Log centralization
- Monitoring, Correlation & Analysis
- Dashboards & Reporting
- Historical data / Forensic & Threat hunting
- Cloud & On-Premise and Hybrid
- SIEM Cluster
- UEBA & behavioral analytics

SUPPORTED PLATFORMS

- 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)

FEATURES

Easy and flexible integration with On-Premise, or Cloud, or Hybrid mode.

Possibility to build source-based offerings for unlimited number of EPSs.

Agent-based and agentless **log collection**.

Monitoring of all your IT and OT equipment.

Compatible with :

- all operating systems (Unix, Windows...)
- all the components of your infrastructure (Routers, Firewalls, Proxies, Switches, Bastions hosts...)
- all your applications to be monitored (Antiviruses, Databases, SAP...)
- cloud sources (e.g. Azure Active Directory / Office 365, Salesforce, etc.)

All formats are accepted : LEEF, CEF, JSON, CSV...
All standard protocols are accepted: Syslog TCP, Syslog UDP...

Ultra-secure solution running on appliances containing a hardened kernel (anti 0-day) with a fully encrypted hard drive.

Simplified and scalable integration of TEHTRIS SIEM appliances in your VMware ESXi environments. The hardware can be scaled over time to keep up with the developments of your SIEM solution (more CPU, RAM or disk).

Several hundred alert rules supplied by default, to detect all attacks recognized by TEHTRIS and gathered on your SIEM to be operational from day one.

Possibility to add alert rules through the correlation rule creation interface.

Unified management of large amounts of data thanks to the SIEM Cluster.

Behavioral analysis based on a UEBA module allowing anomaly detection and report creation.

LEARN MORE
ABOUT TEHTRIS SOLUTIONS
Test our products or contact us
https://tehtris.com
business@tehtris.com


TEHTRIS
FACE THE UNPREDICTABLE
CYBERIA
EDR
EDR
EDR
EDR
EDR
MTD
MTD
SIEM
DNS
FW