



XDR/ SIEM

Security Information & Event Management

Events are generated through numerous sources within your organization. **TEHTRIS SIEM** analyzes all the events from your Information System and correlates them to identify possible attacks.

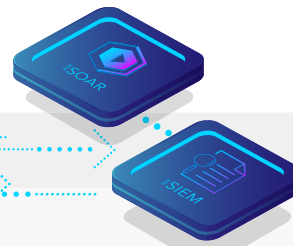


INDUSTRY RECOGNITION

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

Collects, archives, correlates, and alerts 24/7

24/7



Increasingly frequent and stealthy threats

TEHTRIS SIEM collects, processes, and alerts your events to facilitate your decision-making. The solution is integrated into the TEHTRIS XDR Platform and interconnected with our SOAR.

Whatever your sources and their formats (Syslog, Leef, CEF, JSON, CSV, KVP, XML...), TEHTRIS SIEM collects logs thanks to a library of parsers and connectors that are constantly evolving.

Analyze all your events automatically and choose from a catalog of over 2 000 security rules. In addition, take advantage of the behavioral analysis engine (UEBA) to identify unusual activities on your IT assets.

Depending on your security policy, customize your alerting level and define your notification mode (e-mail, SMS...) with the integrated orchestrator: detection window, detection threshold, severity level...

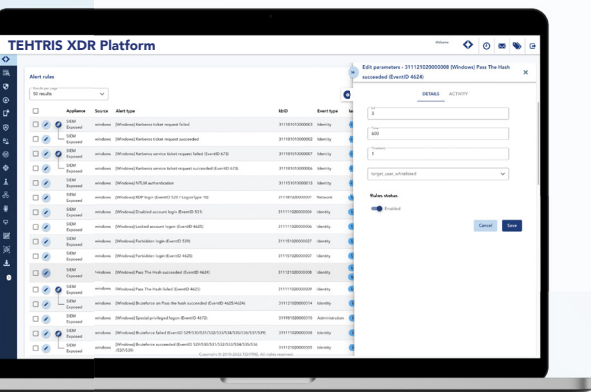
- ↓ Supported sources: AWS, 0365, Proofpoint, Zscaler...
- ↓ All OS supervision
- ↓ Real-time monitoring, detection and alerting of security events
- ↓ Integrated into the TEHTRIS XDR Platform
- ↓ Available in SaaS

Automated investigation and response

TEHTRIS SIEM is integrated into the XDR Platform and benefits from our SOAR's hyperautomation. Create your own playbooks with our SOAR, such as notes and alerts enrichment...

Search and monitor IoCs

Blacklist or Whitelist IoCs to quickly identify suspicious behaviors, customize your IoC databases, and make it easier for your analysts to investigate.

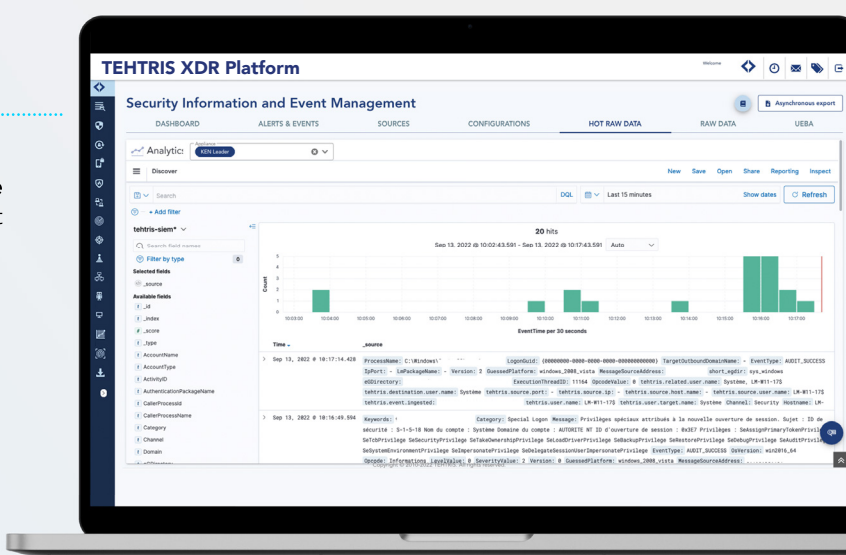


BENEFITS

- ▶ Easy to install and to use
- ▶ Constantly evolving library of sources and rules
- ▶ Autonomy in the creation of the rules and their management
- ▶ Complete view of your infrastructure (360°)
- ▶ Full network monitoring 24/7
- ▶ SOC actions automation

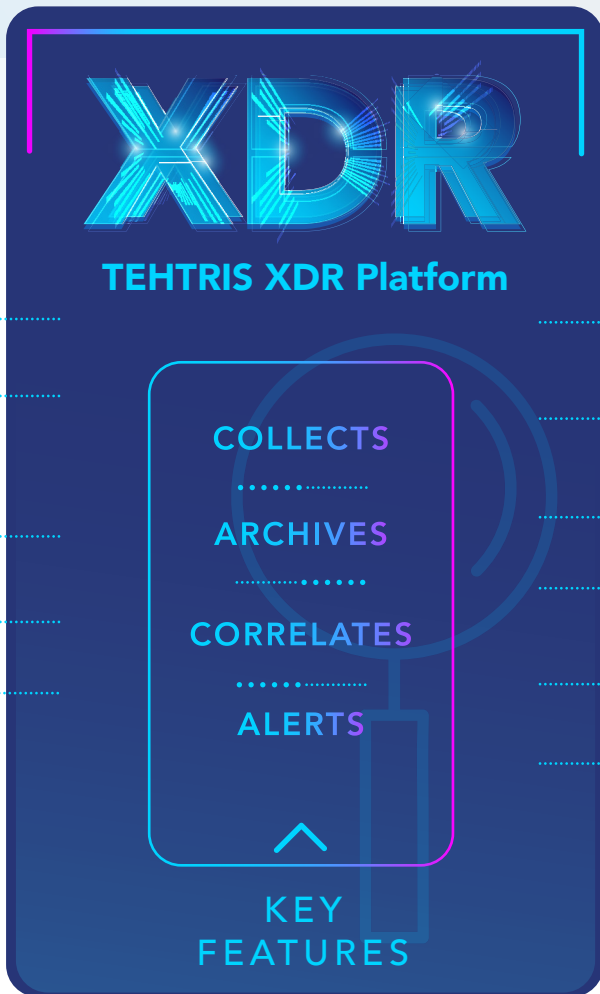
Hot Raw data configurable

Optimize your forensic research with the customizable retention of your Hot Raw Data and stay compliant with GDPR and security protocols.



Supervise the cybersecurity of your infrastructure

Create your own dashboards and monitor your infrastructure's vital functions in real time (log volume indicators, active sources, etc.).



Real-time monitoring of all your IT assets

Compatibility with all parts of your infrastructures, servers, devices, networks, or security equipment

All formats and protocols accepted

+ 2 000 security rules available

Autonomy in the creation of the rules and their management

Hyperautomation thanks to TEHTRIS SOAR

Behavioral analysis engine (UEBA)

Customizable dashboards

Forensic in your Hot Raw Data

IoCs search and monitoring

Cloud architecture

TEHTRIS XDR Platform is 100% compatible with

MITRE ATT&CK®

Gartner, Market Guide for Mobile Threat Defense, January 2023, Market Guide for Network Detection and Response, December 2022, Hype Cycle for Endpoint Security, 2023, August 2023. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and HYPE CYCLE is a registered trademark of Gartner, Inc. and/or its affiliates and are used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Ask for a demonstration

TEHTRIS XDR Platform

CONTACT US



business@tehtris.com
tehtris.com