TEHTRIS
FACE THE UNPREDICTABLE

Endpoint Detection & Response

QUALIFY YOUR DECISION-MAKING WITH OUR AUTOMATIC CORRELATION ENGINE

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.

Gartner

Gartner lists TEHTRIS as a Representative Vendor in the November 2021 Market Guide for Extended Detection and Response.*

afaq ISO 27001 Information Security AFNOR CERTIFICATION 2009/102155

- **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**

Collects, archives, correlates, and alerts 24/7

24/7

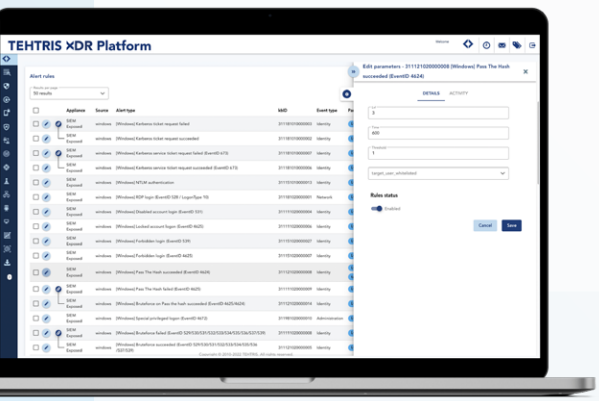
Increasingly frequent and stealthy threats

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...



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

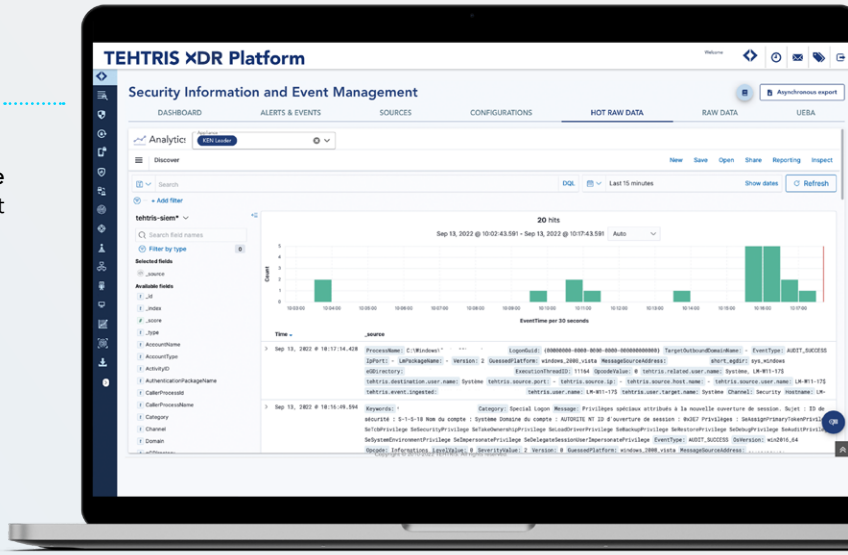
Blacklist or **Whitelist** IoCs to quickly identify suspicious behaviors, customize your IoC databases, and make it easier for your analysts to investigate.

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.).

XDR

TEHTRIS XDR Platform

COLLECTS

ARCHIVES

CORRELATES

ALERTS

KEY FEATURES

- 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®

The GARTNER PEER INSIGHTS Logo is a trademark and service mark of Gartner, Inc. and or its affiliates and is used herein with permission. All rights reserved. « Gartner Peer Insights reviews constitute the subjective opinions of individual end users based on their own experiences and do not represent the views of Gartner or its affiliates »

** Gartner and Market Guide are registered trademarks of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.*

TEHTRIS recognized as a Representative Vendor in the 2021 Market Guide for Extended Detection and Response. Craig Lawson, Peter Firstbrook, Paul Webber, 8 November 2021.

Ask for a demonstration

TEHTRIS XDR Platform

EDR · EPP · MTD · SOAR · SIEM · NTA · Deceptive Response · DNS Firewall · Zero Trust · CWPP · Email Protection · Identity Access Management

CONTACT US

business@tehtris.com
tehtris.com