TEHTRIS SIEM centralizes and organizes management of cybersecurity digital evidences: your systems, applications and network equipment or security’s events and logs. These collected, archived and encrypted elements are constantly analyzed.

This solution collects, archives and processes logs received from sources of events as part of a SIEM (Security Information and Event Management).

Then, a correlation engine continuously analyzes data received to detect risks, suspicious or malicious behaviors: internal and external attacks.

Example: successful login/password brute force attack

Thanks to this solution you are ensured to keep your infrastructure involved systems and applications activities’ digital evidences. In the event of a hack, hackers can no longer delete some traces related to their mischief.

The post-event analysis for archived gross traces in addition to TEHTRIS XDR Platform correlations alerts ease investigations for complex attacks: identities theft, internal smurfing, malicious elements implementation, etc.

TEHTRIS SIEM also exists for Office 365 or Azure in a cloud offer.

More than 450 correlation rules provided detect the suspect elements and report cybersecurity alerts. TEHTRIS solutions conception, research and development are French made. TEHTRIS services and hostings are operated in France by default.

TECHNICAL FEATURES

- Unlimited Event Per Second (EPS)
- Hundreds of correlations rules provided by default for Unix, Windows, Firewalls, routers, switches, antiviruses, proxies, databases, bastions…
- Possibility to add specific correlations rules: business or internal applications
- Windows sources of events agent provided (.MSI)
- Syslog sources of events agent-less (TCP, UDP)
- Other types of sources of events: LEEF, CEF, JSON, CSV…
- GDPR compliant: Security & Privacy by design…
- TEHTRIS fully manages the Solution
- TEHTRIS maintenance and monitoring secured flows from TEHTRIS SIEM VM
- Tickets tools (ISO 27035)
- TEHTRIS SIEM appliance deployed on computer equipment (VMware_ESXi): better hardware costs management (storage, CPU, RAM)