XDR PLATFORM

The XDR infrastructure brings together multiple security solutions into one coherent platform capable of security incident detection and response, investigation and reporting.

USE CASES

- Detection of incidents
- Containment of incidents
- Threat Hunting
- Cybersecurity Investigation
- Remote Remediation
- Attack Surface Reduction
- Reporting

ALL BENEFITS

- Faster MTTD (Mean time to detect)
- Faster MTTR (Mean time to respond)
- Multiple XDR-compatible modules
- Open XDR through in & out APIs
- Remote & Centralized Management (SaaS)
- Easy to deploy and easy to use
- Customized or industrialized offer

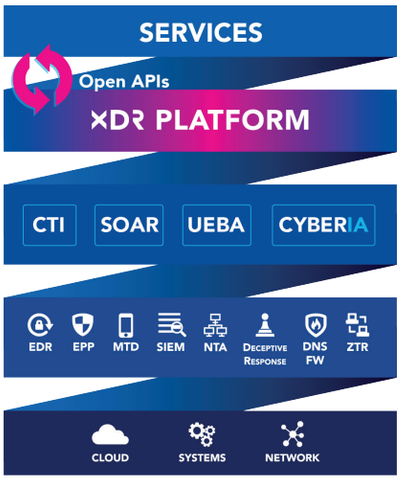
TEHTRIS XDR Platform meets several key needs. It uses its **network of efficient sensors**, such as TEHTRIS EDR/EPP or TEHTRIS DNS FW components, **to improve protection, detection and response capabilities to an attack on the network where it is positioned**. As an OPEN XDR, it allows you to interface with your existing security solutions, centralize alerts and facilitate team decision-making. With the TEHTRIS XDR Platform, you'll be ready to face the unpredictable.

TEHTRIS XDR Platform **is fully customizable**, the construction of decision trees to define the behavior in case of aggression is done via an intuitive, dedicated and centralized system. Certain actions such as **remediation or playbook activation can be automated**, thanks to the integrated SOAR and the synergy between **the different modules, TEHTRIS or external.**

Through **the console and its centralized holistic view**, cybersecurity analysts are invited to mix different analysis views, so that they never experience a blind spot.

The user can switch between an interface displaying weak signals, for example from the honeypots of a TEHTRIS Deceptive Response appliance, and an interface aggregating the APT analyses found by TEHTRIS EDR to understand why an employee's Windows started scanning an internal TEHTRIS honeypot. Depending on his or her needs, he or she can then go to the TEHTRIS EPP next-generation antivirus or to the TEHTRIS SOAR configuration page to activate playbooks, etc.

The unification of the components of the TEHTRIS XDR Platform is also done through numerous TEHTRIS bricks, such as EDR/EPP, SIEM, NTA, Honeypots, DNSFW etc. **Dynamic sharing between components is possible** thanks to relationships between products, **with automation via the integrated SOAR**, and requests related to technical intelligence to **TEHTRIS CTI (Cyber Threat Intelligence)**. Seamlessly integrated with partner ecosystems through its APIs, the TEHTRIS XDR Platform provides the ability to create a variety of analytical reports to continuously improve customer fleet security.



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

XDR

TEHTRIS XDR PLATFORM

Holistic Incident Detection and Response Platform

KEY FEATURES

- Data Science, Dashboards
- Automation, SOAR
- Artificial Intelligence
- Cyber Threat Intelligence, Hunting
- Compliance, Audit
- Mutualized and Multi-tenancy XDR platforms available

SUPPORTED PLATFORMS

- Cloud
- Endpoints (Windows, Unix)
- On-Premise
- Mobile, IoT
- Networks
- OT (SCADA/ICS)

FEATURES

Instrumentation of the customer's infrastructure with TEHTRIS sensors (EDR, EPP, Honeypots, etc.), to gather accurate information.

Centralization of data collected from the field, in a standardized way, in a datalake dedicated to the TEHTRIS ecosystem.

Capacity for manual or automatic analysis, data science, hunting, auditing and correlation of safety data, alerts and incidents.

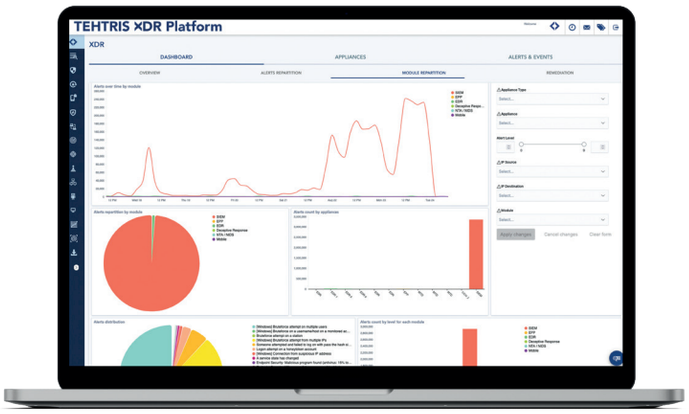
Centralized automatic incident response capability with a SOAR integrated into the TEHTRIS XDR Platform, capable of responding to different security products, according to a predefined security policy.

Native and private internal APIs to link all XDR components via various automatic actions.

Simple and fast integration of these solutions, including in large, heterogeneous and distributed infrastructures.

Immediate results through existing detection policies provided by default against millions of threats already referenced in TEHTRIS Cyber Threat Intelligence bricks.

Efficient security with controlled costs and highly useful tools in the short and long term.



LEARN MORE
ABOUT TEHTRIS SOLUTION
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