NTA

TEHTRIS NTA is a tactical solution to analyze your network flows in real time, using flow capture, metadata (NetFlow) and passive audit mechanisms.

USE CASES

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

ALL BENEFITS

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

TEHTRIS NTA **is a tactical solution to analyze your network flows in real time**, using flow capture, metadata (Netflow) and passive audit mechanisms.

Depending on its position in your infrastructure, TEHTRIS NTA **can monitor both north/south flows (entry and exit of a given perimeter) and east/west flows (lateral movements)**. This probe offers the possibility for a SOC team to understand what is normal or not, in terms of traffic.

Several modules are available in TEHTRIS NTA, with signature-based detections and behavioral-based techniques. TEHTRIS NTA continuously learns and examines all flows to perform advanced analysis and detect network anomalies. By recording metadata in Netflow mode, TEHTRIS NTA offers the ability to go back in time, finding out who spoke to whom, when and how. Unlike many solutions, **TEHTRIS NTA does not require a SIEM to be useful**, since the tool is directly integrated into the TEHTRIS XDR Platform.

Moreover, TEHTRIS NTA is not limited to signature or behavioral analysis to raise alerts. Indeed, some suspicious elements, like lateral movements or slow stealth scans, may be detected in other ways, such as lateral movements, or slow stealth scans.

TEHTRIS NTA **can detect device vulnerabilities in the network**, thanks to a TEHTRIS engine that listens to all the flows. This engine searches for elements that could be used by hackers. This solution enables you to better understand your surface of exposure, without even lauching an offensive or risky scan. This is highly appreciated in specific environments like OT or IoT networks. That being said, TEHTRIS NTA is not limited to these environments; it is also compatible with IT networks.

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

NTA

Tracking threats and vulnerabilities from network traffic

KEY FEATURES

- Signature-based Detection
- Passive audit of vulnerabilities
- Netflow-based features
- Dashboards & Reporting
- Cloud & On-Premise

SUPPORTED PLATFORMS

- Cloud
- Port Mirroring
- Test Access Port
- TCP/IP
- VMware ESXi
- OT (SCADA/ICS)

FEATURES

TEHTRIS NTA virtual machine can **easily be deployed** on client hardware (VMware ESXi hypervisor).

TEHTRIS NTA virtual machine can be **connected via the Internet to its TEHTRIS XDR Platform**.

NIDS: Real-time intrusion detection by analyzing network flows via signatures.

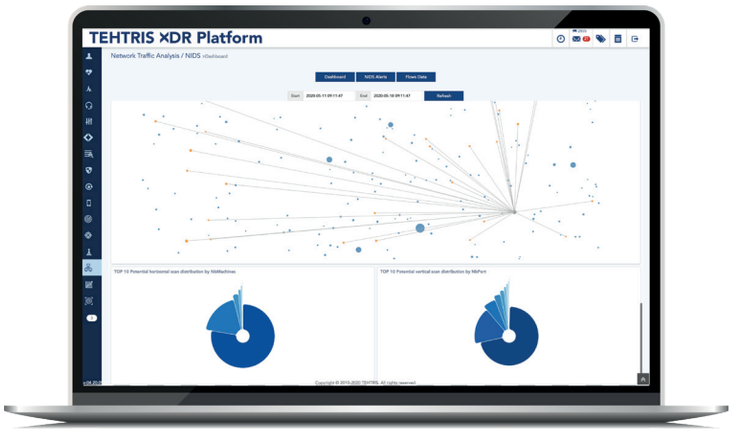
Passive Audit: Detection of vulnerabilities by listening to the traffic of the current devices on the network via a TEHTRIS engine, without having to actively scan or attack targets.

Network Forensic: Tactical forensics focused on network discussions using metadata from streams to find out who talked to whom, when and how.

Automatic regular signature updates.

Identification of abnormal peaks of network activity and analysis of certain behaviors such as lateral movements.

Remote administration by TEHTRIS in SaaS mode.



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