TEHTRIS NTA detects network intrusions with signatures, flow’s analysis, makes Network Forensics via study of the Netflow metadata and passive audits seeking for vulnerabilities.

This solution is connected by the client to a port mirroring or to a Test Access Port (TAP) linked to network flows that will be analyzed. Then, this appliance is able to read these flows and to apply multiple security controls.

The list of flows to analyze and the addresses to consider, internal, external or any other essential information of the client can be shared with TEHTRIS in order to optimize the settings during remote deployment and improve efficiency.

TEHTRIS NTA is doing network flows monitoring missions to carry out passive audits, signature intrusion detection and network Forensics.

TEHTRIS solutions conception, research and development are French made. TEHTRIS services and hostings are operated in France by default.

**TECHNICAL FEATURES**

- TEHTRIS Virtual Machine deployed on client’s hardware (hypervisor VMware ESXi)
- This VM talks over the internet to the hardened TEHTRIS Cloud (monitoring and maintenance)
- This solution is fully managed on TEHTRIS side
- Passive audit: analysis of network flows, to continuously discover security flaws, without launching dangerous scans: non-intrusive and permanent audit style
- NIDS: Network Intrusion Detection System based on signatures
- Flow analysis (Netflow style): metadata study, alerts and Network Forensics