TEHTRIS EDR (Endpoint Detection and Response) automatically detects and neutralizes in real-time sophisticated and unknown attacks on each equipment, station or server, where it is deployed.

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

TEHTRIS EDR agent automatically detects in real time sophisticated or unknown threats thanks to its learning system, heuristic technologies, sandboxes, Artificial Intelligence, threat bases, tactical SIEM.

This “Next-Gen” agent monitors activities of system to discover suspicious and malicious behaviors. It protects Windows, Mac OS and Unix workstations and servers.
The installation binary, MSI can be used with SCCM (remote deployment for the whole park).

Key real-time actions with no human intervention are carried out: unknown virus neutralization and quarantine, ransomwares detection and neutralization, sandbox tests for unknown binaries with technical diagnosis that can lead to remediation.

This service is managed from a centralized console where detection, protection and incident response policies can be adapted, “on-premise” or “Cloud”.

TEHTRIS EDR Windows and Unix agent
“Cloud” and “on-premise” provision
Security between EDR agents and Management VM
Security audits on agents (~10 000 rules)
Tactical SIEM on stations (local logs)
Executed processus monitoring
Behavior analysis, migrations tracking
Threats bases (white/black lists)
Persisting elements monitoring (reboot…)
Artificial Intelligence and Antivirus
Sandboxes
Process memory analysis
Remote machines post-event investigations
Protection against Office attacks
USB security
Advanced analysis (privilege escalation…)
Networks attacks (lateral movements…)
Anti-ransomwares techniques