TEHTRIS DECEPTIVE ZONE offers different modules: honeypots, inventory. The intrusions on the network are detected thanks to honeypots features. They are automatically alerting and recording video attacks.

TEHTRIS DECEPTIVE ZONE and its honeypots simulate fake machines to deceive attackers who’d believe that they play on real machines, which reveals their presence.

An inventory of the resources of this zone is built thanks to active technics by talking to the customer’s switches and passive technics by listening to network flows.

Statistics for large infrastructures indicate an average of 200 days before the detection of an intruder. With our honeypots strategically positioned, when a scan is starting, an alarm is raised in the TEHTRIS console and reduces drastically the detection time. Our algorithms and our expertise differentiate attacks from legitimate traffic without additional work for the SOC teams.

TEHTRIS DECEPTIVE ZONE and its honeypots simulate fake machines to deceive attackers who’d believe that they play on real machines, which reveals their presence.

An inventory of the resources of this zone is built thanks to active technics by talking to the customer’s switches and passive technics by listening to network flows.

Statistics for large infrastructures indicate an average of 200 days before the detection of an intruder. With our honeypots strategically positioned, when a scan is starting, an alarm is raised in the TEHTRIS console and reduces drastically the detection time. Our algorithms and our expertise differentiate attacks from legitimate traffic without additional work for the SOC teams.

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 customer’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
- Availability in every VLANs (connection on a Trunk port) or on 1 LAN (standard port)
- Integration either on the internal networks or on the external networks (exposed on Internet)
- Passive inventory thanks to network flows analysis
- Active inventory thanks to authorized dialogues with client’s switches
- Cyber Deception (Honeypots) simulating fake services to detect low signals