



FACE THE UNPREDICTABLE

Deceptive Response  
DECEIVE POTENTIAL INTRUDERS



# Deceptive Response

TEHTRIS Deceptive Response and its honeypots simulate fake machines and services in order to fool intruders.

TEHTRIS Deceptive Response provides an effective alarm system in real-time, adding a complementary view to the security of your systems and infrastructures. By adding false resources to your network, these sensors lure attackers and provide you with reports and event dashboards.

The associated analysis allows you to gain a new perspective alongside your existing assets without modifying them. It also allows you to keep a complete record of attacks and explorations of your infrastructure.

Integrated with TEHTRIS XDR Platform, TEHTRIS Deceptive Response enables detection, incident response and automation of SOC services. As a result, you get insightful overviews and alerts, making it easier for your SOC incident response teams to work together.

Unlike products that have to shuffle through billions of data with the risk of generating false alarms, TEHTRIS Deceptive Response will

only be solicited when it is being interacted with. No one is usually supposed to play with or attack these fake machines that are not officially present on the network for production purposes.

Cybersecurity teams, such as the SOC, will then be able to deal more easily with the alerts obtained, resulting in technical certainty that is immediately useful to surveillance teams.

TEHTRIS Deceptive Response makes it possible to easily deploy honeypots anywhere, while reducing the cost and associated complexity, unlike many other solutions of this type. We allow you to increase the probability of catching attackers, while keeping your budget under control.

When hackers target a network secured by TEHTRIS Deceptive Response, they may fall on the fake machines, also called decoys, triggering an alarm. It will complicate the attackers' internal exploration sessions and their lateral movements.

## USE CASES

- ▶ Protect your network areas for which an endpoint agent cannot be installed
- ▶ Protect a DMZ exposed to Internet
- ▶ Monitor targeted attacks on your organization

## ALL BENEFITS

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



TEHTRIS Deceptive Response allows to gain a new vision alongside the assets in place.

## FEATURES

- ▶ Honeypots simulating **fake services** to detect potential intrusions.
- ▶ **Videos of command lines** typed by attackers.
- ▶ Passive network flow analysis.
- ▶ Simplified log analysis.
- ▶ TEHTRIS Deceptive Response virtual machine **easily deployed** on the customer's hardware (VMware hypervisor).
- ▶ **Availability of honeypot services in all VLANs** via a trunk port connection, or on a single LAN via standard port.



**MITRE** |  
**ATT&CK**

TEHTRIS XDR Platform  
is 100% compatible  
with MITRE ATTACK

Ask for a free  
demonstration

TEHTRIS XDR Platform

CONTACT US