< TEHTRIS >
FACE THE UNPREDICTABLE

Deceptive Response
DECEIVE POTENTIAL INTRUDERS

afaq ISO 27001 Information Security AFNOR CERTIFICATION 2009/102155

Honeypots

Deceptive Response

Simulation of fake machines, fake services... Position decoys with **Honeypots** to increase your detection capabilities and deflect 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.

Integrated with TEHTRIS XDR AI 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.

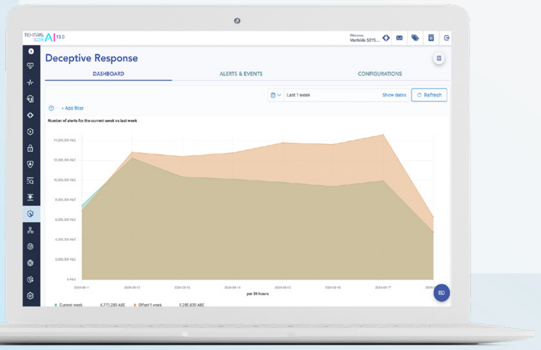
24/7

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 AI PLATFORM
- Remote & Centralized Management
- Easy to deploy



Deceptive Response

Number of alerts for the current week vs last week

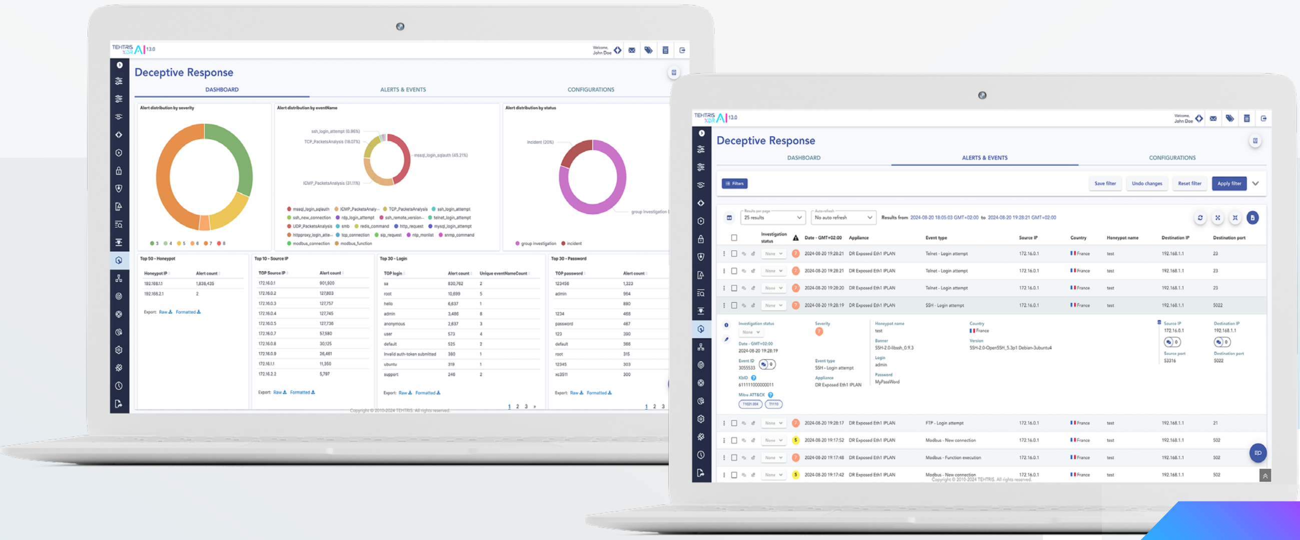
Current week 4,773,289 A&E
Offset 1 week 6,295,829 A&E

Honeypots
Deceptive Response

TEHTRIS DECEPTIVE RESPONSE allows to gain a new vision alongside the assets in place.

FEATURES

- Honeypots simulating **fake services** to detect potential intrusions.
- **Ready-to-use personalities** (OS, Network devices, web servers, databases, or other systems).
- Passive network flow analysis.
- Simplified log analysis.
- **TEHTRIS Deceptive Response** is easy to deploy in every kind of environment to meet the customer's needs.
- **Availability of honeypot services in all VLANs** via a trunk port connection, or on a single LAN via standard port.



TEHTRIS XDR AI PLATFORM
is 100% compatible
with

MITRE
ATT&CK®

Ask for a free demonstration

TEHTRIS XDR AI PLATFORM

EDR
MTD
SIEM
NTA
Honeypots
Deceptive Response
eGuardian
Threat Intel
SOAR
Zero Trust
Email Protection
Identity Access Management

CONTACT US

business@tehtris.com
tehtris.com