TEHTRIS
FACE THE UNPREDICTABLE

Deceptive Response
DÉJOUEZ LES PLANS
DES ATTAQUANTS

Honeypots

Deceptive Response

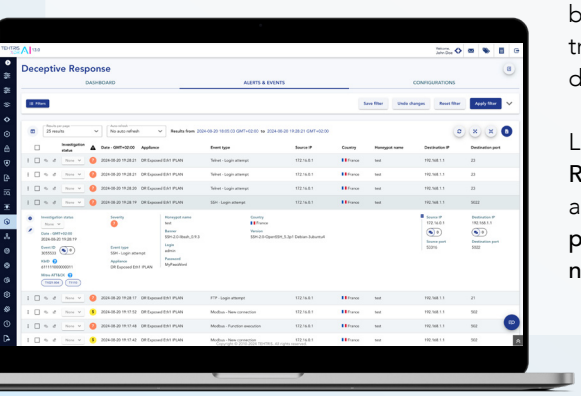
Simulations de fausses machines, de faux services...
Positionnez des leurres avec **Honeypots** pour augmenter vos capacités de détections et dévier les intrusions.

afaq ISO 27001 Information Security
AFNOR CERTIFICATION
2009/102155

TEHTRIS Deceptive Response constitue un système d'alertes en temps réel qui donne une vision complémentaire pour assurer la sécurité de vos infrastructures. En ajoutant de fausses ressources à votre réseau, les attaquants sont leurrés et concentrent leurs attaques sur des ressources qui vous permettront d'analyser l'intrusion : des rapports et des tableaux de bord d'événements sont consultables directement sur la TEHTRIS XDR AI Platform.

De nouvelles capacités de détection sont offertes grâce aux ressources fictives déployées aux côtés de vos machines existantes, sans impact sur votre système.

Lorsque des attaquants ciblent un réseau sécurisé par **TEHTRIS Deceptive Response**, les tentatives d'exploration furtives et les mouvements latéraux sont autant de faux pas possibles qui signaleront leur présence. Intégré à la TEHTRIS XDR AI Platform, **TEHTRIS Deceptive Response permet la détection, facilite la réponse aux incidents et l'automatisation des services SOC.**



24/7

Ainsi, les alertes apportent des informations utiles qui simplifient le travail des équipes de sécurité.
C'est un gain de temps pour l'investigation et la prise de décision !

Pas de faux positif, TEHTRIS Deceptive Response n'est sollicité que lorsqu'il y a une interaction avec lui. Toute interaction avec des assets qui ne sont pas inhérents à votre activité ou à des fins de production doit systématiquement être considérée comme suspicieuse. Le faible niveau de bruit des alertes générées permet un traitement directement qualifié au sein de la TEHTRIS XDR Platform.

Le déploiement de **TEHTRIS Deceptive Response** représente un impact maîtrisé au sein de votre environnement et **vous permet d'assurer l'intégration d'un nouvel allié sans risque.**

USE CASES

- Protection des zones de votre réseau dans lesquelles un agent de surveillance des terminaux ne peut pas être installé
- Protection d'une DMZ exposée à internet
- Surveillance des attaques ciblées contre votre organisation

AVANTAGES

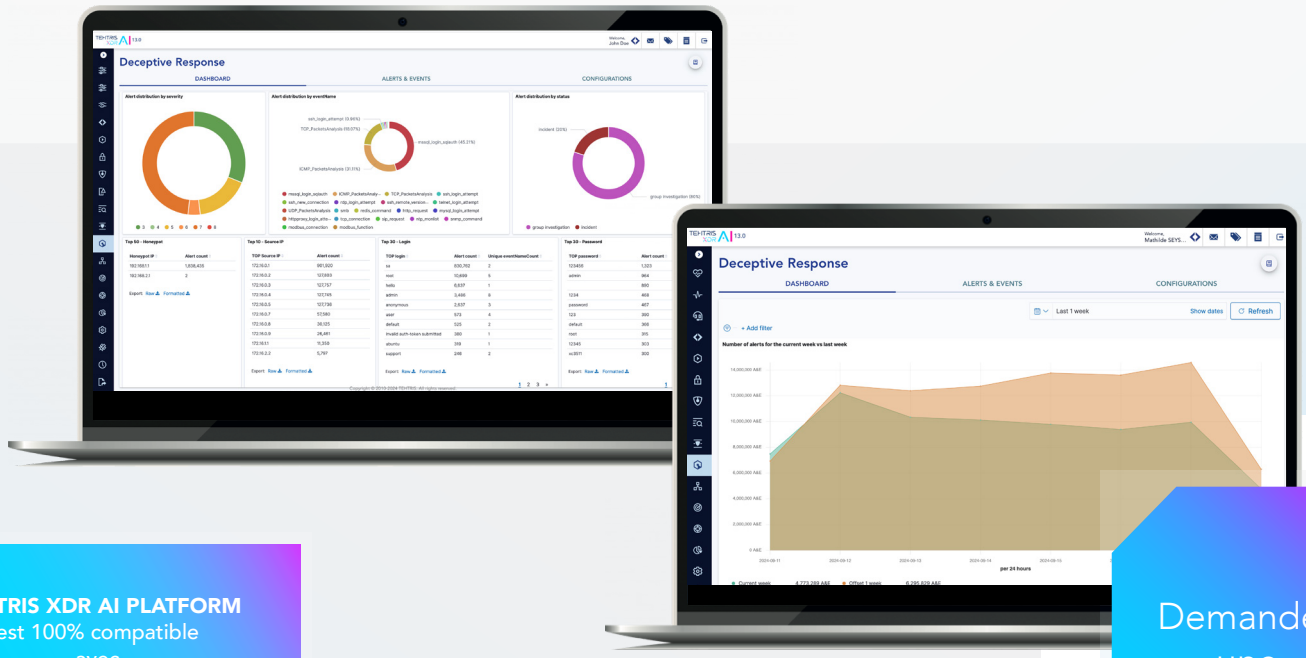
- Temps moyen de détection plus rapide (MTTD)
- Temps moyen de réponse plus rapide (MTTR)
- Intégré à la TEHTRIS XDR AI Platform
- Gestion à distance et centralisée
- Facile à déployer

Honeypots
Deceptive Response

TEHTRIS DECEPTIVE RESPONSE permet d'obtenir une nouvelle vision des menaces au sein de votre organisation

FONCTIONNALITÉS

- Honeypots simulant de **faux services** pour détecter des intrusions potentielles
- **Des personnalités simulées prêtes à l'emploi** (OS, système réseau, serveurs web, base de données, et d'autres systèmes).
- Analyse passive du flux réseau
- Analyse simplifiée des logs
- **TEHTRIS Deceptive Response** est facile à déployer dans différents types d'environnement pour s'adapter à tous les besoins.
- Disponibilté des **services Honeypots dans l'ensemble des VLANs** via une connexion sur un port trunk, ou sur un seul LAN via un port standard.



TEHTRIS XDR AI PLATFORM
est 100% compatible
avec

MITRE ATT&CK®

Demandez une démonstration

TEHTRIS XDR AI PLATFORM

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

CONTACTEZ-NOUS

business@tehtris.com
tehtris.com

Oct.2024 - V_13