FACE THE UNPREDICTABLE

Domain Name System Firewall

PROTÉGEZ VOTRE TRAFIC DNS

afaq ISO 27001 Information Security AFNOR CERTIFICATION 2009/102155

XDR/ DNS Firewall

DNS Firewall

Face aux attaques toujours plus nombreuses et sophistiquées exploitant les résolutions DNS, XDR/ DNS FireWall protège vos utilisateurs des domaines malicieux.

Industry Recognition

TEHTRIS recognized as a Representative Vendor in the 2022 Gartner® Market Guide for Network Detection and Response.*

Empêchez l'exfiltration de données en interceptant les résolutions DNS potentiellement malveillantes 24/7

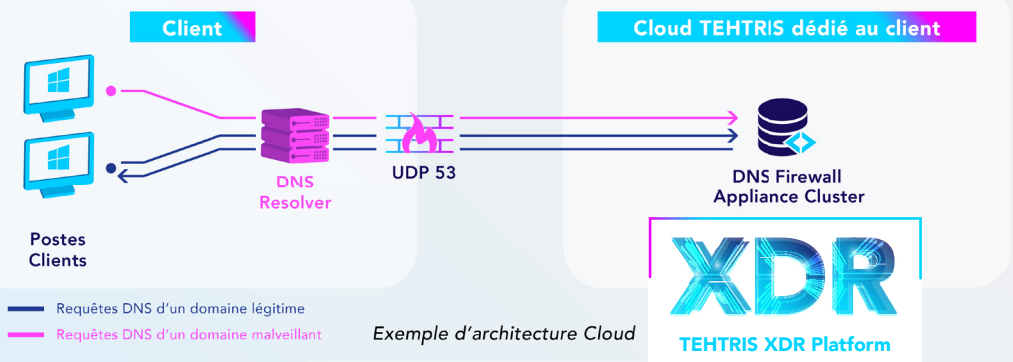
XDR/ DNS FireWall détecte et **bloque** les domaines de logiciels malveillants en supervisant les demandes de résolution DNS avant que votre système d'information ne soit infecté.

En associant sa base de connaissances des menaces à ses capacités de filtrage de requêtes DNS, et grâce aux analyses de Cyberia (Intelligence Artificielle), **XDR/ DNS FireWall** permet l'identification rapide des activités suspectes en temps réel, comme les tentatives de phishing.

La réponse aux requêtes DNS douteuses est adaptée à leur nature. Les control lists sont personnalisables et vous permettent d'assurer une surveillance en accord avec votre propre politique de sécurité.

Intégré à la **TEHTRIS XDR Platform**, les alertes DNS FireWall enrichissent vos contextes d'investigation lorsqu'une requête DNS est effectuée.

- Prévention des menaces : phishing, malware, command & control, cryptominer...
- Détection des DGA basée sur l'Intelligence Artificielle (Deep Learning)
- Remédiation paramétrable (blocage et/ou alerting)
- Analyse forensic à partir des Raw Data
- Accès à la TEHTRIS XDR Platform et à sa technologie augmentée (SOAR, Intelligence Artificielle Cyberia...)
- Disponible en cloud & on-premise



Exemple d'architecture Cloud

Intégration rapide sans installation supplémentaire

XDR/ DNS FireWall protège vos environnements sensibles (IoT & BYOD compliance) sans la complexité de la gestion d'un déploiement d'agent.

Les appliances peuvent être déployées **on-premise** ou en mode **cloud**.

BÉNÉFICES

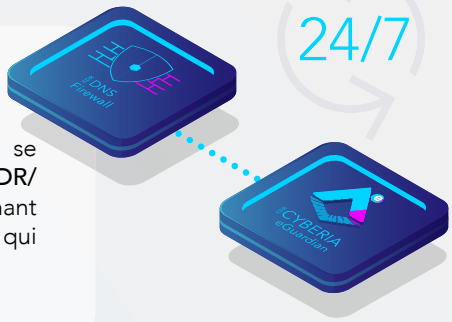
- **Protection de vos usagers :** blocage d'accès aux sites malveillants
- **Limitation des incidents :** blocage des tentatives d'exfiltration et détection de malware
- **Investigations en cas d'incidents :** journalisation des évènements
- **Intégration et défense des environnements sensibles :** pas de nécessité de déploiement d'agent

Utilisez les blacklists TEHTRIS intégrées

Avec **XDR/ DNS FireWall** vous bénéficiez des bases de connaissances de menaces qui s'étendent à de nombreuses catégories comme celles dédiées aux malware, C2, phishing, cryptominer. Une comparaison des requêtes est systématiquement effectuée : si une correspondance est établie, la demande est bloquée ou une alerte est levée. Les bases de données sont mises à jour automatiquement et continuellement.

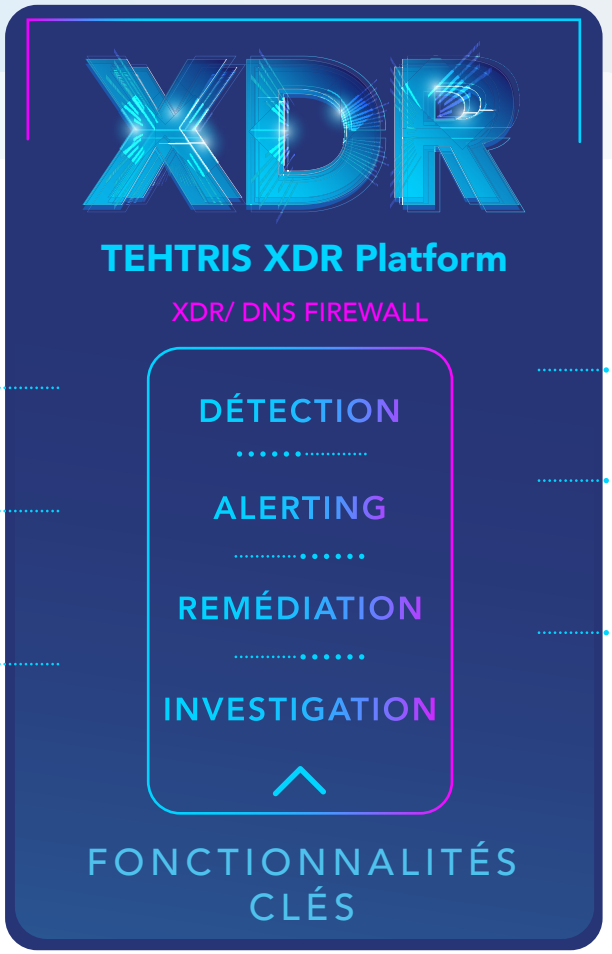
Identifiez les DGA grâce au Deep Learning

Les domaines issus d'algorithmes de génération de noms de domaines (DGA) hébergent et délivrent des malwares en contournant les mécanismes de filtrage de domaine. Pour une détection efficace des DGA, le **Machine Learning** et le **Deep Learning**, plus particulièrement, se sont avérés être la meilleure solution. **XDR/ DNS FireWall** intègre un module provenant de l'Intelligence Artificielle **Cyberia** qui détecte les DGA.



Bloquez les domaines récemment créés

Une source de menaces souvent ignorée est constituée par des domaines nouvellement enregistrés. Pour éviter une contamination du réseau par malware, les tentatives de fraudes par phishing ou une exfiltration de données, **XDR/ DNS FireWall** permet de bloquer les accès aux domaines fraîchement créés.



- Blacklists **TEHTRIS** intégrées
- Whitelists/Blacklists personnalisables selon votre politique de sécurité
- Modèle de Deep Learning **Cyberia** détectant les DGA
- Remédiation paramétrable
- Investigations approfondies grâce aux Raw Data
- Dashboards personnalisables

TEHTRIS XDR Platform est 100% compatible avec **MITRE ATT&CK®**

Gartner, Market Guide for Mobile Threat Defense, January 2023, Market Guide for Network Detection and Response, December 2022, Hype Cycle for Endpoint Security, 2023, August 2023. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and HYPE CYCLE is a registered trademark of Gartner, Inc. and/or its affiliates and are used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Demandez une démonstration

TEHTRIS XDR Platform

EDR · MTD · SIEM · NTA · Honeypots · CYBERIA eGuardian · CTI · SOAR · Zero Trust · Email Protection · Identity Access Management

CONTACTEZ-NOUS

business@tehtris.com
tehtris.com

Déc. 2023 - V_11