STORMSHIELD

XDR

Améliore l'efficacité opérationnelle cyber de votre infrastructure

Face à la professionnalisation des cyber-criminels et leur *modus operandi*, les entreprises multiplient le déploiement de produits de sécurité. Le constat récurrent de la réussite de ces attaques démontre le manque d'efficacité de cette approche. En effet, la multiplicité des points de protection réseau et terminaux ainsi qu'une politique de sécurité hétérogène induisent une faible réactivité face à ces attaques.

La multiplication des solutions de détection nécessite des configurations toujours plus complexes, provoque des évènements multiples et nombreux avec des comportements difficiles à interpréter et corréler pour les administrateurs. Ce manque de visibilité limite la réactivité qui se traduit dans les faits par une baisse du niveau de protection.

Le XDR **by Stormshield**

Acteur de confiance reconnu dans la cybersécurité, Stormshield propose une nouvelle offre pour :

- Réduire les risques et améliorer la productivité opérationnelle cyber,
- Combler les lacunes inhérentes à l'intégration des solutions de sécurité hétérogènes,
- Proposer une solution complète pour la sécurité de votre infrastructure,
- Corréler les évènements remontés par la protection réseau (SNS) et la protection des postes (SES),
- Alerter en temps réel,
- Piloter les éléments de réponse et de remédiation.

Contrôlez l'ensemble des éléments XDR

Gérez les incidents de sécurité depuis un seul endroit

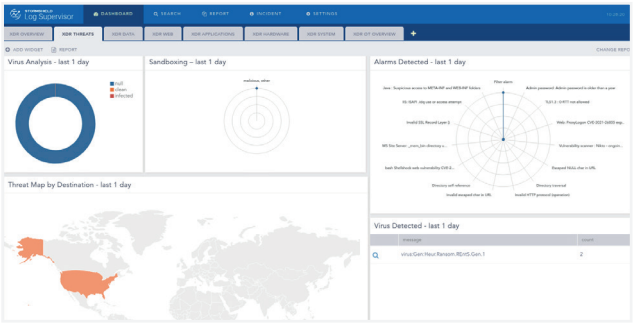
Améliorez la productivité et l'efficacité opérationnelle cyber

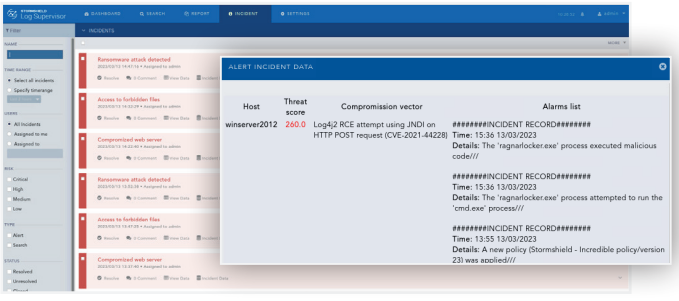
Une offre XDR **complètement intégrée et maîtrisée**

La combinaison idéale de Stormshield Network Security pour **protéger le réseau** et de Stormshield Endpoint Security pour **sécuriser les terminaux**, le tout renforcé par l'expertise Stormshield en Threat Intelligence pour **anticiper la menace**.

L'ensemble orchestré par Stormshield Log Supervisor pour vous **alerter en temps réel** et **piloter une réponse rapide et pérenne** à la fois sur le réseau et sur les terminaux.

En résumé, une solution de protection 100% européenne, 100% de confiance.





Stormshield XDR

MAÎTRISE • PRODUCTIVITÉ • COHÉRENCE

#01
FICHIER MALVEILLANT

Attaque

- Ouverture du fichier malveillant reçu par mail
- Exécution d'un injecteur (dropper)
- Récupération de la charge virale et déclenche l'attaque

Réponse

- Remédiation par isolation réseau du poste
- Arrêt des processus malveillants sur le terminal

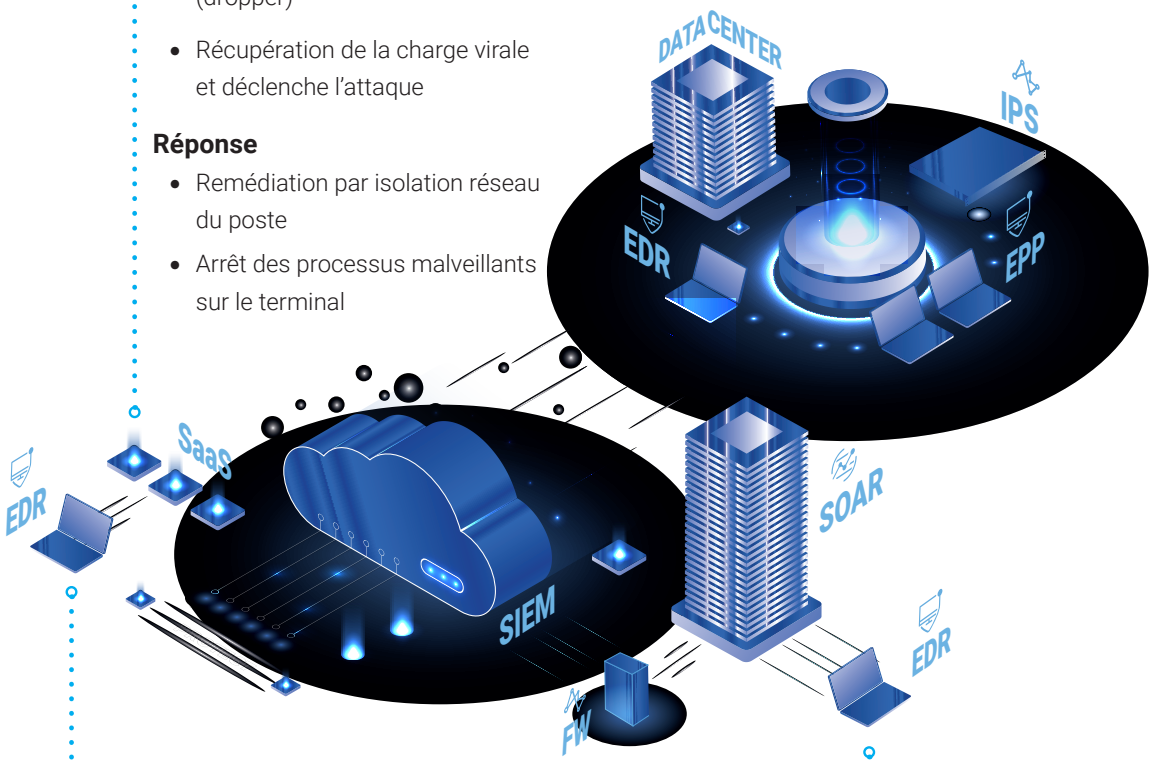
#02
SERVEUR WEB SUBISSANT UNE ATTAQUE DDoS

Attaque

- Envoi d'une multitude de connexions qui sature le serveur

Réponse

- Restriction aux seules connexions de confiance
- Activation de la limitation de connexion sur le serveur pour protéger son intégrité



#03
CLÉ USB MALVEILLANTE

Attaque

- Dépôt d'un injecteur (dropper) sur le PC
- Connexion à un serveur de Command & Control (C2)
- Récupération de la charge virale depuis le serveur
- Tentative de compromission du poste et début de la latéralisation de l'attaque

Réponse

- Arrêt du processus malveillant sur le terminal
- Remédiation par isolation réseau du poste
- Blocage de la clé USB sur les autres postes
- Blocage de l'IP de C2 sur la protection réseau

#04
DÉCOUVERTE DU RÉSEAU INTERNE PAR L'ATTAQUANT

Attaque

- Scan du réseau interne
- Découverte du réseau et de ses vulnérabilités
- Test des exploits connus sur les serveurs critiques (AD ou Exchange)
- Tentative de prise de contrôle des ressources critiques

Réponse

- Isolation du poste compromis
- Activation de l'IPS sur les connexions critiques

Solution souveraine

Acteur français de la cybersécurité, nous proposons des solutions qui respectent les exigences légales européennes.

Certifications

Nos technologies certifiées au plus haut niveau européen vous garantissent une protection adaptée pour les informations stratégiques ou les plus sensibles de votre organisation.

Écosystème

Nous collaborons avec d'autres acteurs dans le but de développer des solutions conjointes, de mutualiser des informations sur les menaces et d'améliorer collectivement les défenses de nos clients.

www.stormshield.com

Stormshield, retrouvez nos lignes produits :

Cybersécurité des réseaux et infrastructures IT

Avec leurs fonctionnalités essentielles, les solutions Stormshield Network Security vous garantissent une sécurité complète et de hautes performances en termes de protection des réseaux. **Optez pour une sécurité performante et évolutive**.

Cybersécurité des postes de travail

Stormshield Endpoint Security est capable de modifier de manière **dynamique ses opérations de sécurité en fonction de son environnement** et d'analyser dans le même temps l'accès aux applications et aux ressources de l'entreprise selon l'emplacement du poste.

Cybersécurité des données sensibles

Fondée sur le chiffrement des données de bout en bout, notre solution Stormshield Data Security se positionne comme une offre complète pour **contrôler les données sensibles au sein de votre organisation et la confidentialité** des courriers électroniques.