SOLUTION BRIEF

PROTEGER LES INFRASTRUCTURES CRITIQUES

Stormshield Network Security + Airbus Cybersecurity Orion Malware

Solution complète on-premise

Protection multi-couches

Outils avancés d'analyse

Les systèmes informatiques des environnements sensibles ne peuvent pas toujours pour des raisons règlementaires être connectés à internet. Dans d'autres cas, la confidentialité des données ne permet pas de transiter via des environnements non-maîtrisés. Ces mesures de protection protègent de certains risques, mais empêchent dans le même temps de bénéficier de solutions de sandboxing, hébergés sur le cloud.

Or, les cyberattaques ciblées qui visent justement les environnements sensibles sont conçues pour contourner les solutions de protection traditionnelles en combinant souvent plusieurs vecteurs y compris hors ligne.

Une solution 100% on-premise contre les cyberattaques complexes

UNE PROTECTION OPTIMALE CONTRE LES ATTAQUES

Pour prévenir, bloquer et se défendre contre les attaques à multiples vecteurs, il est nécessaire d'utiliser des solutions combinant plusieurs technologies et techniques. Pour répondre à cette problèmatique, Stormshield a étendu les capacités de Stormshield Network Security avec Breach Fighter, une technologie de sandboxing en mode cloud, dédiée aux petites et moyennes entreprises. Pour les environnements qui ne peuvent déployer Breach Fighter du fait d'environnements déconnectés, de contexte de données sensibles ou qui ont besoin de flexibilité et d'outils avancés d'analyse, Stormshield permet l'utilisation de la technologie Orion Malware d'Airbus Cybersecurity.

Fort de ses capacités de détection de code malveillant et des menaces inconnues, Orion Malware analyse les fichiers suspects remontés par Stormshield Network Security qui assure aussi la fonction de blocage réseau. Les informations extraites du fichier durant son analyse avec Orion Malware permettent ensuite de passer en phase proactive et de suivre les traces des malwares. Les règles de filtrage réseau peuvent ensuite être adaptées grâce à cette analyse.

Points clés de Stormshield Network Security

- VPN qualifié
- IPS protocolaire avec contrôles applicatifs profonds
- Haute disponibilité
- Disponibilité de matériel durci avec bypass de connexion
- Certification EU restricted, OTAN restricted, EAL4+ et qualification ANSSI

Points clés de Airbus Orion Malware

- Combinaison de multiples techniques d'analyse (signatures, heuristiques, machine learning, sandboxing)
- Modularité : ajout de nouveaux composants d'analyses stastiques, choix de l'OS sandboxé (Windows XP, 7 et 10, Linux, Android)
- Intégration système simple (restfull API, ICAP, SIEM)
- Extraction des IOC pour générer des règles de détection ou réaliser l'analyse
- Made in France

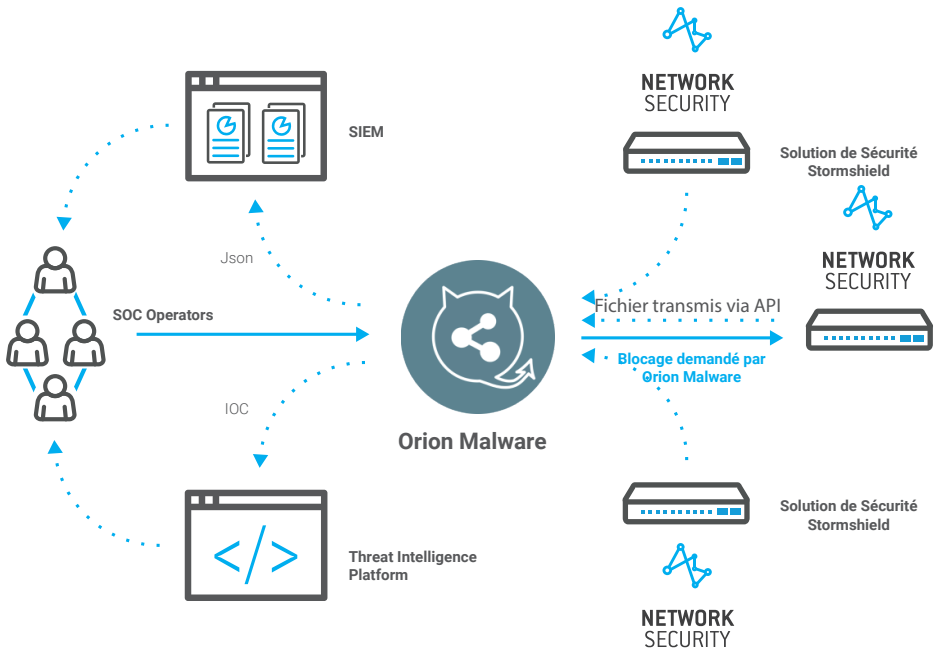
UNE PROTECTION MULTICOUCHES

La solution Stormshield Network Security/Orion Malware est constituée d'équipements réseau capables d'extraire et d'analyser des milliers de fichiers dans un réseau non connecté à Internet. La détection qui est faite repose sur une combinatoire d'analyse protocolaire, de triage sur base de signatures de menaces opportunistes et APT, d'analyse statique, de machine Learning et d'analyse dynamique (sandboxing).

À l'issue de chaque analyse de fichier faite par Orion Malware, un risk assessment est mené et le résultat est communiqué à l'appliance Stormshield Network Security ayant soumis le fichier afin de procéder au blocage si nécessaire. Un résumé de l'analyse de fichiers ainsi qu'un rapport est disponible pour permettre à l'utilisateur de mieux connaitre la menace. L'ensemble des IOC extraits peuvent être exportés automatiquement vers un SIEM (syslog, JSON, API) afin de consolider les connaissances de sécurité.

UNE SOLUTION ON-PREMISE POUR LES ENVIRONNEMENTS SENSIBLES

La solution Stormshield Network Security/Orion Malware est packagée sous forme d'appliances. Elle peut ainsi être déployée facilement dans les environnements sensibles sans nécessité d'échanges avec le cloud.



STORMSHIELD

Stormshield, filiale à 100% d'Airbus CyberSecurity, propose des solutions de sécurité de bout-en-bout innovantes pour protéger les réseaux (Stormshield Network Security), les postes de travail (Stormshield Endpoint Security) et les données (Stormshield Data Security).

www.stormshield.com