GROUPE
SAPHELEC
Simplyo MICOM

CYBER

LEXIQUE

ENDPOINT PROTECTION PLATFORM

L'EPP est une solution de sécurité des endpoints issue du monde des antivirus de nouvelle génération.

Il permet de prévenir les attaques et possède des fonctionnalités spécifiques contre de nombreux problèmes de sécurité tels que le phishing, l'exploitation 0-day, les attaques de réseau.

ENDPOINT DETECTION & RESPONSE

L'EDR est une solution qui vient compléter l'EPP, en permettant de détecter des attaques inconnues et de lancer des correctifs automatiques contre ces menaces, avec des fonctionnalités avancées pour effectuer des investigations à distance.

EXTENDED DETECTION & RESPONSE

L'XDR est une version plus complète de l'EDR qui va surveiller également les actions réseaux notamment les mails, le Cloud et ainsi fournir une visibilité et une corrélation plus grandes entre toutes ces infrastructures.

La solution va pouvoir agir en mode monitoring, mais peut également proposer des capacités de mise en quarantaine, du sandboxing afin d'apporter des capacités de réponses supplémentaires face aux menaces.

MOBILE THREAT DEFENSE

Le MTD est une protection dynamique et sophistiquée contre les cybermenaces visant les appareils mobiles.

LES TECHNOLOGIES SIEM ...

... Regroupent les données des journaux de votre réseau informatique, les alertes de sécurité et tous les évènements qui surviennent dans une plateforme centralisée pour fournir une analyse en temps réel pour la surveillance de la sécurité.

... Assurent une surveillance plus ou moins complète d'un réseau informatique.

LES TECHNOLOGIES SIEM ...

... Collectent des données au niveau des périphériques réseau *(le concentrateur ou hub réseau, le commutateur, le routeur réseau, la passerelle, le répéteur, le point d'accès...)*, des serveurs *(web, proxy, messagerie, FTP...)*, des dispositifs de sécurité réseau *(pare-feux, antivirus, filtrage de contenu, EDR...)* ainsi qu'au niveau des applications sur le réseau.

Ces données collectées sont ensuite analysées et corrélées, permettant à la solution SIEM de détecter les menaces avec des règles préréglées pour réduire la fatigue liée aux alertes et de mener des enquêtes pour identifier les éventuelles intrusions.

SOC : CENTRE DES OPÉRATIONS DE SÉCURITÉ

Le SOC est un emplacement centralisé en local depuis lequel une équipe d'opérations de sécurité (SecOps) surveille, analyse et répond en permanence aux incidents de sécurité qui menacent l'entreprise.

Pour y parvenir le SOC utilise divers dispositifs de cybersécurité, dont font partie les solutions EDR, XDR et aussi SIEM que nous avons vues précédemment.

SOC : CENTRE DES OPÉRATIONS DE SÉCURITÉ

Les fonctions d'un centre des opérations de sécurité incluent la surveillance proactive des intrusions, des menaces et des vulnérabilités, la réponse aux incidents et récupération, les activités de remédiation ou encore s'assurer que la sécurité du réseau soit conforme aux normes de sécurité externes telles que l'ISO 27001, le NIST Cyber Security Framework (CSF) ou encore le RGPDF.

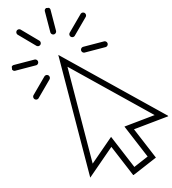
GROUPE SAPHELEC

Simplyo MCOM

Bloque les pirates avant qu'ils ne te bloquent !

Rendez vous sur notre site internet pour découvrir comment protéger votre entreprise des cyberattaques !

saphelec.fr



SAPHELEC, simplifions la technologie !