Une protection des terminaux hors pair

La protection classique des terminaux a fait son temps. Aujourd'hui, XDR est le mot d'ordre lorsqu'il s'agit de détecter et de se défendre contre les cyberattaques. Explication avec Rolf Bamert, sales engineer chez le distributeur de sécurité informatique BOLL, qui prend pour exemple la solution XDR de Palo Alto Networks.

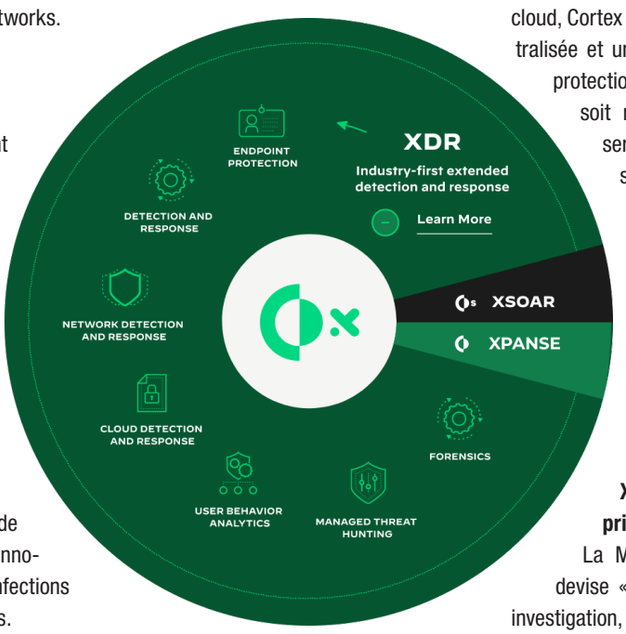
Que signifie XDR?
XDR est un acronyme de l'anglais «extended detection and response» – synonyme de solutions de protection complètes qui collectent et traitent les informations de sécurité sur les terminaux, dans le réseau et dans le cloud afin de stopper les attaques complexes. XDR réunit la prévention, la détection, l'analyse et la réaction aux cyberattaques sur une seule et même plateforme – gage d'une sécurité et d'une efficacité opérationnelle sans précédent.

Comment se présente le marché des solutions XDR?
Il existe toute une série de fournisseurs de cybersécurité qui proposent des produits sous le label XDR. Mais toutes les solutions n'offrent pas la même protection, comme le montre le test comparatif de MITRE ATT&CK lors de la phase 3 de l'évaluation effectué en 2021. Les meilleurs scores de détection et de protection combinés ont été obtenu par Cortex XDR de Palo Alto Networks.

Comment fonctionne Cortex XDR?
Avec un seul et même agent qui protège de manière fiable les terminaux contre les ransomwares, les logiciels malveillants, les exploits et les attaques sans fichier, grâce à une protection basée sur le comportement et une analyse locale pilotée par IA. L'agent déploie tout un arsenal préventif doté de mécanismes de protection innovants pour empêcher les infections par des logiciels malveillants.

Comment l'intelligence artificielle entre-t-elle en jeu?
A titre d'exemple, les fichiers sont examinés et évalués par un moteur d'analyse local autoapprenant afin de se prémunir également contre les nouvelles techniques d'attaque inconnues. Grâce à l'apprentissage automatique, Cortex XDR établit en permanence le profil des utilisateurs et du comportement des terminaux afin de découvrir les activités inhabituelles et de détecter rapidement les attaques.

Un aspect important de la cybersécurité est la visibilité complète de tous les risques. Comment Cortex relève-t-il ce défi?
Cortex XDR collecte et traite des données provenant de n'importe quelle source. Les données relatives aux terminaux, au réseau, au cloud et aux identités sont automatiquement combinées pour détecter avec précision les attaques et simplifier les investigations.



Comme l'ensemble de l'environnement est intégré, il n'y a pas non plus d'angles morts. Les alertes provenant de tiers sont intégrées de manière dynamique pour élargir le champ de vision.

Et comment la solution facilite-t-elle la réponse aux cyberincidents?
Tout d'abord, en réduisant le nombre d'incidents à contrôler: Cortex XDR relie les différentes alarmes en les résumant intelligemment en événements. Les analystes peuvent ainsi se concentrer sur les incidents vraiment importants, malgré des ressources en personnel généralement limitées. Chaque incident est enrichi d'artefacts importants et de données intégrées sur les menaces. Ce qui permet d'obtenir une image complète de la séquence des événements et de leur cause.

Cortex XDR est une plateforme basée sur le cloud. Qu'est-ce que cela signifie pour les utilisateurs?
En étant basé sur une plateforme en cloud, Cortex XDR offre une gestion centralisée et un déploiement facile de la protection des terminaux, sans qu'il soit nécessaire d'installer des serveurs, des logiciels de gestion ou des sondes réseau sur place. Les données sont collectées dans le Cortex Data Lake, un référentiel cloud évolutif et efficace.

Palo Alto Networks a récemment publié la version 3.0 de Cortex XDR. Quelles sont les principales nouveautés?
La Major Release 3.0 a pour devise «deeper detection, broader investigation, faster response». Ainsi, la nouvelle version offre une intégration avec les données des systèmes RH et permet une évaluation des risques pour les utilisateurs individuels. L'agent a été complété par un module forensique intégré et collecte des données provenant de solutions tierces supplémentaires. Quant à la gestion des incidents, elle est dotée d'une nouvelle interface, présente une cartographie MITRE-ATT&CK des preuves et des artefacts des menaces et offre un tableau de bord SOC Manager.


Rolf Bamert, sales engineer, BOLL.

BOLL
IT Security Distribution

BOLL Engineering SA
En Budron H15 | 1052 Le Mont-sur-Lausanne
Tél. 021 533 01 60 | vente@boll.ch
www.boll.ch