Une protection complète contre les menaces avec un temps de réaction ultrarapide

La solution de cybersécurité Cortex XDR de Palo Alto Networks (PAN) offre une protection des points finaux, du réseau et du cloud sous la forme d'une plateforme complète s'appuyant sur l'IA et avec une automatisation poussée de la détection et réponse aux incidents de sécurité.

Les menaces cybercriminelles sont toujours plus nombreuses et sophistiquées. Les attaques visent généralement les points finaux, qui constituent donc la principale porte d'entrée.

Détection et réponse étendues

Les solutions modernes de protection des points finaux vont bien au-delà des possibilités offertes par les logiciels antivirus conventionnels. Elles fonctionnent sur la base du comportement (UEBA pour user and entity behavior analytics), détectent et analysent les anomalies sur les points finaux et identifient ainsi des menaces jusqu'alors inconnues, dont beaucoup avec le soutien de l'IA et de l'apprentissage automatique. Elles apportent en outre une aide à la résolution des problèmes (alertes/incidents), comme l'isolation des points finaux, l'accès aux points finaux via un terminal et un script, la suppression des fichiers malveillants et les analyses forensiques – toujours de manière aussi automatisée que possible, afin de décharger les spécialistes de la sécurité et de leur permettre de s'occuper des «casse-têtes» nécessitant une intervention humaine. Pour de telles solutions, on parle alors de détection et de réponse aux points finaux (EDR pour endpoint detection and response). Si la solution couvre d'autres domaines comme le réseau et le cloud, il s'agit alors de détection et réponse étendues (XDR pour extended detection and response).

Plateforme XDR leader de la première heure

Le spécialiste de la sécurité Palo Alto Networks (PAN) a été le premier fabricant à lancer en 2019 une plateforme XDR complète – Cortex XDR – qui est toujours considérée comme numéro un.

En moyenne, il ne faut que 10 secondes pour que Cortex XDR détecte une attaque. Sur 133 problèmes détectés, 125 sont résolus de manière entièrement automatique, seules 8 alertes doivent être traitées par des analystes de sécurité – c'est une constatation du Security Operations Center de PAN lui-même. Cela montre que l'équipe de sécurité est considérablement soulagée et peut travailler plus efficacement grâce à l'intelligence et à l'automatisation poussée de la solution.

Cortex XDR est modulaire et regroupe des fonctions telles que: la protection des points finaux (EPP), l'EDR, la détection et la réponse réseau, la détection et la réponse cloud, l'analyse du comportement des utilisateurs dans une plateforme complète avec un fonctionnement unifié et enfin, une visibilité totale sur tous les domaines et toutes les sources de données: points finaux, réseau, identités, données cloud, données sur les menaces collectées par l'agent Cortex XDR de l'entreprise et d'autres clients PAN, et informations sur les menaces provenant d'autres sources. Pour la détection et le traitement des menaces, toutes ces données sont combinées, analysées à l'aide de l'apprentissage automatique et de l'analyse du comportement des points finaux et d'autres systèmes et processus, et les menaces sont signalées ou les problèmes sont automatiquement bloqués et résolus.

BOLL
IT Security Distribution

BOLL Engineering SA
En Budron H15
CH-1052 Le Mont-sur-Lausanne
+41 21 533 01 60,
contact@boll.ch
www.boll.ch