Détection et réponse : optimisez votre ROI

Consolidez vos outils et simplifiez vos opérations pour réduire vos coûts de 44 %

Un programme de sécurité efficace passe d'abord par des outils de détection et de réponse capables d'aider les équipes de sécurité à identifier, investiguer et neutraliser rapidement les menaces.

Pour protéger leurs ressources numériques, beaucoup d'entre elles sont aujourd'hui contraintes de déployer de multiples outils cloisonnés. Et bien que chacun ait ses avantages, ces produits spécialisés obligent les analystes à basculer d'une console à l'autre pour contextualiser les alertes, ce qui ralentit les processus de réponse à incident. Côté opérationnel, ces outils exigent de déployer et maintenir un nombre croissant d'agents logiciels, de capteurs réseau et de serveurs de journaux en interne, mettant un peu plus la pression sur des équipes informatiques déjà surchargées.

Des produits de sécurité silotés, c'est plus de complexité et moins de protection. Pour sortir de cette impasse et bloquer les attaques avancées, Cortex XDR™ offre aux équipes de sécurité la toute première application de détection et de réponse capable d'intégrer nativement les données du réseau, des terminaux et du cloud. Réduction du temps moyen de confinement des menaces, gains de productivité des analystes et amélioration de l'efficacité opérationnelle : Cortex XDR agit sur tous les fronts.

Cortex XDR

- Intègre la protection des terminaux pour bloquer les malwares, ransomwares et attaques sans fichier
- Exploite le machine learning pour détecter les menaces inconnues les plus furtives
- Accélère les investigations pour réduire les délais de réponse à incident
- Confine les menaces susceptibles de provoquer des compromissions coûteuses

Ce livre blanc vous invite à découvrir comment une entreprise de 10 000 utilisateurs peut se prémunir des violations de sécurité tout en réduisant ses coûts de 44 % – soit une moyenne de 889 284 dollars américains – en remplaçant ses outils de détection et de réponse cloisonnés par Cortex XDR.

Les menaces furtives exigent une nouvelle approche de la sécurité

Les hackers ne cessent de développer de nouvelles tactiques pour contourner les systèmes de sécurité. Ils volent des identifiants pour opérer incognito en se faisant passer pour des utilisateurs légitimes. Ensuite, ils se servent d'applications installées sur les terminaux infiltrés pour conduire leurs attaques, allant même jusqu'à passer par des applications de partage d'écran et des connexions VPN légitimes pour se propager au reste de l'organisation.

Bref, pour bloquer les menaces actives (déplacements latéraux d'un attaquant, vol de données en interne, etc.), les équipes de sécurité ont besoin d'outils capables d'identifier facilement les menaces inconnues tout en simplifiant les processus d'investigation et de confinement. Concrètement, cela revient à déployer et gérer plusieurs outils non intégrés :

- **Détection et réponse sur les terminaux (EDR)** pour suivre l'activité des appareils gérés et détecter les éventuelles menaces, fournir du contexte pour les investigations et faciliter les processus de réponse manuels.
- **Analyse du trafic réseau (NTA)** pour surveiller le trafic réseau et détecter les comportements symptomatiques d'une attaque active (communication CnC, déplacement latéral, exfiltration de données, activité malveillante, etc.).
- **Analyse du comportement des utilisateurs et des entités (UEBA)** pour profiler les comportements types des utilisateurs et appareils (ou entités) et détecter les menaces (attaques internes, détournement d'identifiants, etc.).

Selon le cabinet Gartner, ces trois technologies représentent le strict minimum pour « améliorer la priorisation, la visibilité, la détection des menaces et les capacités de réponse à incident ».[1] Or, prise séparément, chacune n'offre qu'une vue étroite basée sur une seule source de données, ce qui oblige les analystes à corréler manuellement les données et nécessite un certain niveau de spécialisation.

Pour ne rien arranger, les EDR, NTA et UEBA imposent chacun un nombre important de capteurs réseau, agents de terminaux et serveurs de journaux que l'entreprise doit ensuite pouvoir gérer.

Détection et réponse : brisez les silos

Cortex XDR est la toute première application cloud de détection et de réponse capable d'intégrer nativement les données du cloud, du réseau et des terminaux pour neutraliser les attaques avancées. À elle seule, elle combine des fonctionnalités EDR, NTA et UEBA pour protéger tout l'environnement et offrir aux équipes de sécurité une visibilité sur toute l'entreprise sans avoir à jongler entre plusieurs écrans. Cortex XDR :

- S'appuie sur Cortex Data Lake, un référentiel cloud évolutif, pour corréler automatiquement les données issues du cloud, du réseau et des terminaux.
- Effectue des analyses comportementales et applique des règles personnalisables pour détecter automatiquement les menaces furtives et inconnues. Les modèles de machine learning analysent les données stockées dans Cortex Data Lake pour identifier les menaces avec une précision incomparable.
- Identifie l'origine et retrace la chronologie d'un incident pour accélérer les processus d'investigation et permettre aux analystes, expérimentés ou non, de vérifier rapidement le niveau de risque.

Détection et réponse : des approches multiples et variées

Sachant qu'une compromission de données coûte en moyenne 4,27 millions de dollars en France[2] et 3,86 millions de dollars à l'échelle mondiale[3] (voire 100 millions de dollars pour les violations à grande échelle), chaque entreprise se doit d'investir dans des outils de détection et réponse aux menaces. Le seul problème, c'est que la plupart de ces instruments ont leurs limites (cf. Figure 1). Par conséquent, pour arriver au même niveau de fonctionnalité que Cortex XDR, une entreprise devra acheter, déployer et gérer plusieurs produits non intégrés.

Fonctionnalités	XDR*	EDR	EPP	NTA	UEBA
Détection, investigation et réponse basées sur les terminaux	●	●	◗	○	○
Prévention contre les attaques, les exploits et les malwares sur les terminaux	●	◖	●	○	○
Détection, investigation et réponse sur le réseau	●	○	○	●	○
Analyse du comportement des utilisateurs, détection et réponse	●	○	○	○	●
Corrélation automatique des données issues du cloud, du réseau et des terminaux pour améliorer la détection des menaces et simplifier les investigations	●	○	○	○	◗

* Cortex XDR, Cortex Data Lake et Traps

Figure 1 : Fonctionnalités des principaux outils de sécurité

1. « How to Plan, Design, Operate and Evolve a SOC », Gartner, 6 septembre 2018, https://www.gartner.com/en/documents/3889122/how-to-plan-design-operate-and-evolve-a-soc.
2. « 2018 Cost of a Data Breach Study: Global Overview », Ponemon Institute, juillet 2018, https://www.ibm.com/downloads/cas/861MNWN2.
3. « The 18 biggest data breaches of the 21st century, » CSO Online, 20 décembre 2018, https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

Comparatif du coût total de possession : Cortex XDR vs. outils spécialisés

Le coût total de possession (TCO) est calculé sur la base d'une entreprise de 10 000 utilisateurs (cf. Figures 2 et 3).

Nombre total d'utilisateurs	**10 000**
Nombre total d'appareils gérés et non gérés	**25 000**
Pare-feu	**Pare-feu nouvelle génération Palo Alto Networks**
Système de gestion des pare-feu	**Appliances Panorama™**
Antivirus	**Agent d'antivirus traditionnel**
Objectifs du projet	• **Remplacement de l'antivirus** • **Réduction de 50 % du temps moyen de réponse (MTTR)** • **Renforcement de la visibilité sur les équipements gérés et non gérés** • **Stockage des journaux pendant 30 jours pour Panorama**
Coût d'un analyste en cybersécurité	**107 600 $/an**[4]
Coût d'un administrateur informatique	**81 866 $/an**[5]

Figure 2 : Entreprise modèle

Fonctionnalité	Plateforme Palo Alto Networks (prix catalogue)	Outils de sécurité spécialisés (prix catalogue)
Détection et réponse sur les terminaux (EDR) et protection des terminaux (EPP)	**337 500 $/an** pour Cortex XDR et Traps avec rétention des données des terminaux pendant 30 jours	**450 000 $/an** pour des agents EPP et EDR distincts avec stockage des données pendant 30 jours
Analyse du trafic réseau (NTA)[6]	**246 375 $/an** pour Cortex XDR avec rétention des données du réseau pendant 30 jours	**425 000 $/an** pour des appliances NTA et des TAP réseau ou des générateurs de flux
Analyse du comportement des utilisateurs et des entités (UEBA)	**0 $** (compris dans Cortex XDR)	**250 000 $/an** pour un produit UEBA supplémentaire ou contrat de service SIEM
Tri des alertes et coûts des investigations	**215 200 $/an** pour 2 analystes en cybersécurité	**376 660 $/an** pour 3,5 analystes[7]
Création et optimisation de politiques d'alertes pour les SOC	**53 800 $/an** pour 0,5 analyste en cybersécurité	**107 600 $/an** pour 1 analyste en cybersécurité[8]
Coûts opérationnels liés aux logiciels, aux matériels et aux serveurs de journaux	**122 799 $/an** pour 1,5 administrateur informatique / de postes de travail	**245 598 $/an** pour 3 administrateurs informatique / de postes de travail[9]
Collecte des journaux du réseau	**Avec Cortex**	**Sans Cortex**
Stockage des journaux pour la gestion de la sécurité réseau	**173 000 $/an** pour Cortex Data Lake (support compris)	**133 100 $** pour des appliances Panorama M-600 redondantes en mode « collecte de journaux », avec support premium[10]
Coût total de possession	**1 148 674 $/an**	**2 037 958 $/an**

Figure 3 : Coût total de possession (prix catalogue aux États-Unis)

Méthodologie

Les estimations des coûts opérationnels se fondent sur des entretiens approfondis menés auprès de divers responsables informatique et sécurité. Les économies estimées sont attribuées à plusieurs facteurs : automatisation ; corrélation dynamique des données du cloud, du réseau et des terminaux ; règles prédéfinies et intégrations des réponses ; élimination de la journalisation sur site ; et consolidation des capteurs et des points de contrôle avec des outils de prévention. Remarque :

- Les prix catalogue des outils de sécurité spécialisés varient selon les fournisseurs.
- Les fournisseurs de solutions de sécurité, y compris Palo Alto Networks, peuvent offrir des remises sur le prix catalogue.

4. Basé sur un salaire moyen de 79 738 $ majoré de 135 % pour les impôts, avantages, primes et frais de bureau. Informations salariales obtenues sur le site Glassdoor.com le 20 juin 2019.

5. Basé sur un salaire moyen de 60 642 $ majoré de 135 % pour les impôts, avantages, primes et frais de bureau. Informations salariales obtenues sur le site Glassdoor.com le 20 juin 2019.

6. Cortex XDR intègre des fonctions d'analyse du trafic réseau, mais les clients doivent eux-mêmes collecter les journaux du trafic réseau, ce qui augmente les exigences de stockage et, par conséquent, les coûts du contrat.

7. Des outils cloisonnés pèsent sur la productivité, mobilisent davantage de main d'œuvre et augmentent les coûts d'investigation et de tri des alertes.

8. Cortex XDR comprend près de 200 règles BIOC (Behavioral Indicator Of Compromise) prédéfinies ainsi que des algorithmes de détection prêts à l'emploi. L'analyse de métriques cloud anonymisées contribue au développement de règles prédéfinies et appliquées aux mises à jour des produits, ce qui réduit les coûts d'optimisation des politiques.

9. Les outils cloisonnés génèrent des dépenses supplémentaires pour la gestion et la maintenance des agents EPP et EDR. Ils exigent également des capteurs NTA et des serveurs sur site de gestion, analyse et stockage des journaux.

10. Adossé à un système de gestion centralisé comme Panorama, Cortex Data Lake élimine le besoin de stocker tous les journaux sur une appliance dédiée. Panorama s'intègre à Cortex Data Lake pour afficher les journaux de pare-feu dans son interface utilisateur.

Réduire le coût total de possession avec Cortex XDR

Chaque jour, les responsables de la sécurité doivent trouver un juste équilibre entre leurs stratégies de défense et les réalités budgétaires. Face à l'escalade des menaces, il leur faut investir dans des technologies capables de s'adapter rapidement pour contrer les attaquants sans avoir à déployer un énième outil spécialisé.

Cortex XDR s'impose comme le choix par excellence pour bloquer les attaques sophistiquées, tout en réduisant les coûts opérationnels et la prolifération d'équipements sur votre réseau. Au menu :

- **Réduction des coûts d'installation et de maintenance.** Cortex XDR est une application cloud, ce qui signifie que vous pouvez tirer un trait sur les logiciels, matériels et systèmes de stockage des journaux sur site, réduisant ainsi les dépenses d'investissement (CapEx) et d'exploitation (OpEx). Avec Cortex XDR, les produits Palo Alto Networks existants font office de capteurs et points de contrôle afin de simplifier les déploiements et la gestion. Les données de sécurité sont quant à elles stockées dans Cortex Data Lake, un référentiel cloud évolutif qui en simplifie la gestion.
- **Simplification des investigations pour une réduction des coûts opérationnels.** Cortex XDR corrèle dynamiquement les données du cloud, du réseau et des terminaux, donnant ainsi aux analystes les moyens d'investiguer les alertes sans jongler entre plusieurs consoles ou effectuer des analyses manuelles.
- **Détection automatique par machine learning pour réduire les coûts de la traque des menaces.** Cortex XDR profile le comportement des utilisateurs et des équipements pour identifier avec précision les menaces propres à chaque environnement client, ce qui élimine le besoin d'analyse manuelle des modes opératoires des attaquants. Lors d'un test au banc d'essai MITRE ATT&CK™, Cortex XDR s'est imposé devant 10 autres solutions sur le plan de la couverture. Les responsables sécurité peuvent donc être confiants dans sa capacité à détecter automatiquement les menaces furtives.
- **Élimination des coûts d'optimisation des politiques et des prestations de conseil.** Cortex XDR intègre des fonctions de détection des menaces prêtes à l'emploi, y compris des algorithmes de détection pour les analyses comportementales et près de 200 règles comportementales prédéfinies. Il est donc inutile de créer vos propres politiques de détection. Contrairement à la plupart des outils UEBA qui imposent l'intervention de consultants, Cortex XDR est immédiatement opérationnel.

Cortex XDR permet aux équipes de sécurité de consolider plusieurs produits de détection et réponse au sein d'une seule et même plateforme, migrer la gestion des données dans le cloud et baisser les coûts de gestion des journaux. À la clé : une **réduction de 44 % du coût total de possession pour votre système de détection et de réponse aux menaces**. Pour renforcer votre sécurité et optimiser votre efficacité opérationnelle, votre arme secrète tient en deux mots : Cortex XDR.

CORTEX XDR™
BY PALO ALTO NETWORKS

Oval Tower, De Entrée 99 - 197
1101HE Amsterdam, Pays-Bas
+31 20 888 1883
www.paloaltonetworks.fr

maximize-the-roi-of-detection-and-response-wp-091119-fr