Cortex – Opérations de sécurité : cap sur la proactivité de bout en bout

Si les centres opérationnels de sécurité (SOC) existent depuis une quinzaine d'années, leur rôle n'est devenu véritablement critique que depuis cinq ans. Face à la nécessité de prévenir les cyberattaques d'une part, et à l'adoption d'opérations de sécurité (SecOps) centralisées d'autre part, les équipes de sécurité se heurtent à bien des défis : manque de personnel qualifié (talents, expertise), contraintes budgétaires, sans parler de l'offre pléthorique de solutions complexes sur le marché.

Quant aux attaques, leur fréquence, leur coût et leur sophistication ne cessent d'augmenter et de progresser avec l'essor des ransomwares. Le problème, c'est que ces compromissions peuvent passer longtemps inaperçues avant d'être détectées, ce qui allonge la durée de présence et retarde les actions d'investigation, d'atténuation ou de remédiation. Bien que l'origine de ces lacunes opérationnelles varie d'une entreprise à l'autre, certaines problématiques, elles, reviennent régulièrement :

- Manque de visibilité sur les appareils, applications, réseaux et systèmes
- Incertitude quant aux ressources à protéger
- Compréhension lacunaire des outils à utiliser et de leur intégration au sein de l'infrastructure existante

Pour rester suffisamment réactives et ne pas perdre pied face à une menace mondialisée, les équipes de sécurité misent de plus en plus sur des solutions complètes en mode cloud. Leurs atouts ? Un contrôle renforcé sur les opérations de sécurité, une vue globale de la posture de sécurité et des services de pointe dans différents domaines : identification des ressources, évaluation des vulnérabilités, détection des menaces, surveillance des comportements, Threat Intelligence et réponse automatisée.

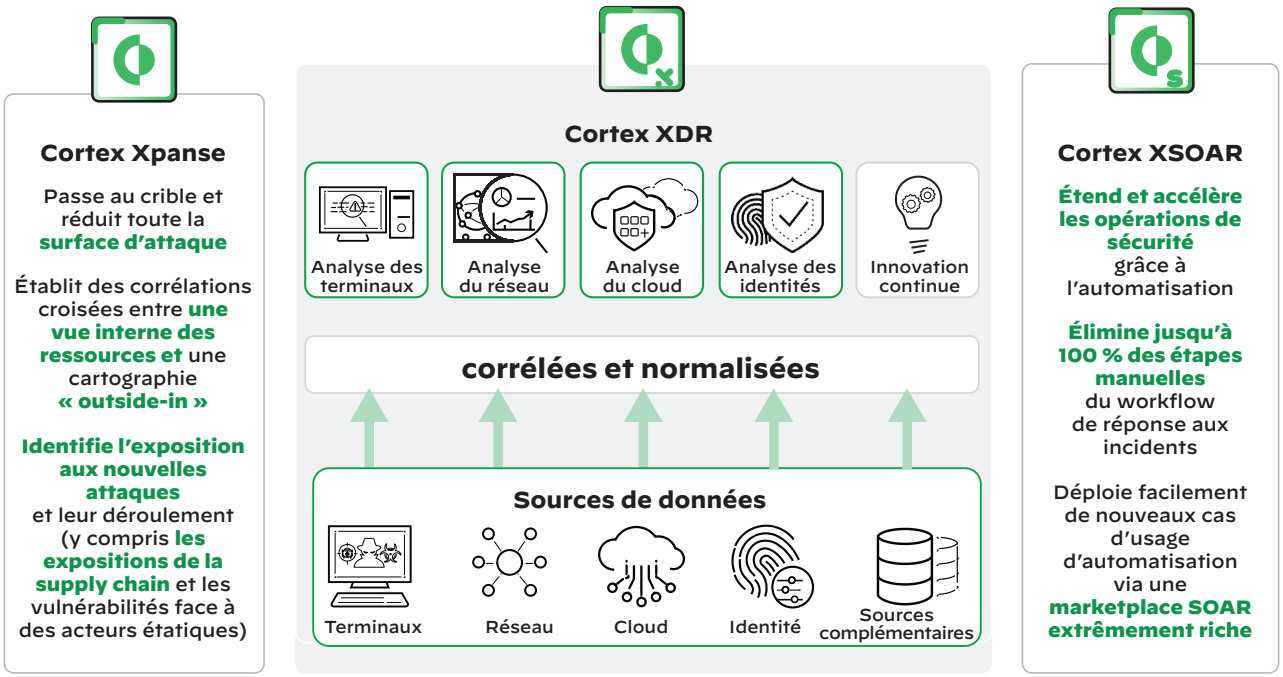

Figure 1 : Automatisation de bout en bout des workflows de sécurité opérationnelle

Cortex Xpanse : détection des ressources connectées à Internet et réduction des risques associés

Qui dit essor du cloud et du télétravail dit mutation, évolution et complexification constantes de la surface d'attaque. Le problème est d'autant plus inquiétant que les attaquants disposent désormais d'outils capables de scanner facilement et rapidement tout l'Internet pour y repérer des vecteurs d'attaque potentiels (ressources non autorisées, mal configurées ou laissées en déshérence, et susceptibles de servir de backdoor dans le cadre d'une compromission). D'où l'intérêt de déployer une solution ASM qui vous permettra d'évaluer continuellement la surface d'attaque externe de votre entreprise.

Cortex® Xpanse™ dresse un inventaire exhaustif des expositions et des ressources cloud d'entreprise connectées à Internet à l'échelle mondiale. L'objectif ? Cerner, évaluer et diminuer continuellement la surface d'attaque externe, quantifier les risques liés aux fournisseurs, ou encore dresser un bilan de sécurité de sociétés nouvellement rachetées.

Identification de la surface d'attaque – Inventoriez automatiquement l'intégralité des ressources connectées à Internet à la recherche de risques inconnus.

Prévention des ransomwares – Détectez les accès distants exposés avant que vos adversaires ne s'en chargent pour vous.

Gouvernance de l'infrastructure – Assurez un suivi de la sécurité à l'échelle d'environnements fédérés.

Sécurité du cloud – Empêchez la prolifération des instances cloud et centralisez l'application des politiques cloud.

Due diligence des tiers – Cernez les risques induits par vos relations avec des fournisseurs et des sociétés nouvellement acquises.

Cortex XSOAR : orchestration, automatisation et réponse aux incidents de sécurité (SOAR) alliées à la gestion de la Threat Intelligence

La principale fonctionnalité des solutions SOAR est de définir des priorités et de créer des workflows rationnels pour les évènements de sécurité nécessitant une intervention humaine minimale. Pour plus d'efficacité, une plateforme SOAR doit pouvoir automatiser les processus, mais aussi tout centraliser pour simplifier les investigations en cas d'incident.

C'est pourquoi Cortex XSOAR gère de bout en bout les processus de réponse aux incidents et de sécurité opérationnelle. Les entreprises disposent ainsi de toutes les clés pour accélérer leurs opérations de sécurité, l'investigation et la réponse aux menaces. En puisant dans la mine d'intégrations à des solutions tierces et les quelque 725 packs de contenus disponibles sur la marketplace XSOAR, les équipes de sécurité de toute taille ont toutes les cartes en main pour orchestrer, automatiser et accélérer la réponse aux incidents sur n'importe quel workflow SecOps.

Cortex XSOAR, c'est aussi un accès à un référentiel central sur les menaces, provenant d'une variété de sources CTI, tant tactiques (données lisibles par machine) que stratégiques (données issues de rapports). Ainsi, les équipes peuvent non seulement corréler automatiquement les informations sur les menaces aux incidents, mais aussi opérationnaliser la CTI grâce à cette automatisation.

Automatisation et orchestration

Répondez rapidement aux incidents, même à grande échelle :

- Des centaines d'intégrations produits disponibles
- Des milliers d'actions de sécurité exécutables
- Éditeur de playbooks visuel et intuitif

Collaboration en temps réel

Misez sur la collaboration pour des investigations de meilleure qualité :

- Salle des opérations virtuelle pour chaque incident
- ChatOps et actions de sécurité en temps réel
- Documentation automatique des actions effectuées par les playbooks et les analystes

Gestion des cas

Standardisez vos processus à travers différents produits, équipes et cas d'usage :

- ChatOps en temps réel, intégré aux outils de gestion des cas
- Vues personnalisées des types d'incidents
- Rapports et tableaux de bord personnalisables

Gestion de la Threat Intelligence

Maîtrisez vos flux CTI de A à Z :

- Automatisation de la gestion répétitive des indicateurs quotidiens
- Rentabilisation immédiate des flux CTI existants
- Renforcement de la confiance en vos décisions de réponse aux incidents

Cortex XDR : prévention des menaces sur les terminaux, détection et réponse sur les terminaux (EDR), analyse des comportements, services managés de détection et réponse (MDR)

En offrant des fonctions de détection, d'investigation, de réponse et de traque des menaces centrées sur les terminaux, compatibles avec les environnements cloud vers lesquels les entreprises migrent leurs données, Cortex XDR propose une alternative viable aux solutions SIEM. Après avoir bloqué un maximum de menaces sur les terminaux, les fonctions de détection et de réponse de Cortex XDR se concentrent sur les incidents. Elles automatisent la collecte de preuves, groupent les alertes associées, classent ces alertes chronologiquement et identifient les causes racines pour aider les analystes à accélérer le tri et les investigations, quel que soit leur niveau de compétence.

Cortex XDR stoppe les attaques sur les hôtes et les terminaux à l'aide d'un système EDR leader pour les hôtes Linux et Windows® reposant sur :

- Des analyses locales pilotées par IA et des analyses comportementales par ML régulièrement actualisées
- Une série de fonctionnalités de protection des terminaux : contrôle des appareils, pare-feu sur hôte, chiffrement de disque, etc.
- Un éventail de modules de protection contre les exploits de pré- et post-exécution

De meilleures intégrations aux outils tiers, des analyses plus pertinentes et une réponse plus rapide… le triptyque de Cortex XDR s'avère indispensable dans un monde où les entreprises utilisent jusqu'à 45 outils de sécurité en moyenne pour répondre à un incident[1].

En misant sur cette solution, les équipes de sécurité peuvent bloquer les attaques plus efficacement, éliminer les angles morts, réduire les temps d'investigation et, au bout du compte, améliorer l'issue des incidents de sécurité. Et puisque Cortex XDR peut intervenir à des stades critiques d'une attaque comme l'exécution (avant que les techniques de persistance n'entrent en action pour permettre une latéralisation de la menace), les équipes de sécurité disposent enfin d'une solution pour tuer les attaques dans l'œuf.

Détection des attaques avancées – Dépistez les menaces grâce à l'intelligence artificielle, l'analyse comportementale et les règles de détection personnalisées.

Priorité aux incidents plutôt qu'aux alertes – Évitez l'accoutumance aux alertes grâce à un moteur d'incident unifié et intelligent qui regroupe les alertes ayant un lien entre elles.

Investigations huit fois plus rapides – Allez directement au cœur des causes racines pour obtenir une vue complète et vérifier plus rapidement les attaques.

Blocage des attaques sans compromis sur la performance – Assurez la protection la plus efficace des terminaux grâce à un agent léger.

Augmentation du retour sur investissement – Réduisez vos coûts de 44 % en exploitant l'infrastructure existante pour la collecte et le contrôle des données.

1. 2020 *Cyber Resilient Organization Report*, Ponemon Institute, 30 juin 2020 https://www.ibm.com/account/reg/us-en/signup?formid=urx-45839.

L'union fait la force

Cortex, c'est une gamme de solutions de sécurité de bout en bout qui couvre chaque étape de vos opérations.

En premier lieu, Cortex Xpanse s'assure que votre entreprise dispose d'une vue complète et actualisée sur l'intégralité de sa surface d'attaque et des risques associés. Outre les expositions éventuelles, elle identifie en un clin d'œil les ressources protégées et non protégées par Cortex XDR. Autre avantage de Cortex Xpanse, l'exploitation de données issues de Cortex XDR pour vous livrer des informations essentielles sur les environnements de vos utilisateurs distants.

À mesure que de nouveaux risques et dangers sont détectés par Xpanse et Cortex XDR, Cortex XSOAR déleste vos équipes des tâches manuelles destinées à réduire ces risques et à répondre aux menaces. Ainsi, en cas de détection d'une nouvelle ressource ou exposition, Cortex XSOAR se charge de notifier automatiquement et exclusivement l'équipe ou le collaborateur responsable de la gestion de ce type de problème.

Cortex s'impose comme le portefeuille de produits le plus complet du marché pour vos opérations de sécurité. Munies de ses solutions de bout en bout, vos équipes passent d'une posture purement réactive à une approche résolument proactive. Première étape, la gestion de la surface d'attaque pour une visibilité totale sur vos ressources et les risques associés. Place ensuite à une solution de pointe de prévention, détection et réponse sur les terminaux dotée de capacités puissantes d'automatisation pour faciliter le travail de votre SOC. Opter pour un portefeuille de solutions intégrées, c'est offrir à vos équipes une protection en continu et une gestion des risques ininterrompue.

Détection et prévention des menaces, gestion de la surface d'attaque, automatisation de la sécurité… pour en savoir plus sur les fonctionnalités leaders de la suite de produits Cortex, téléchargez nos livres blancs :

Cap sur une plateforme SOC virtuelle avec Cortex

Le SOC de demain se réinvente aujourd'hui

Consultez nos pages produits :

Cortex Xpanse

Cortex XSOAR

Cortex XDR

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