Cortex XDR

Détection et réponse : brisez les silos de sécurité

Entre les ransomwares, le cyberespionnage, les attaques sans fichier et les compromissions de données sensibles, les équipes de sécurité sont confrontées à un nombre de menaces de plus en plus vertigineux. Pour les analystes sécurité en particulier, cette multiplication des risques se traduit surtout par une augmentation des tâches répétitives, mais néanmoins nécessaires au tri quotidien des incidents et d'un backlog d'alertes qui n'en finit plus.

Dans ce livre blanc, nous passerons en revue les principaux défis que doivent relever les analystes sécurité, à commencer par cette avalanche d'alertes et des processus d'investigation complexes que même les SOC les plus matures peinent à maîtriser. Nous observerons ensuite comment les fonctionnalités de détection et de réponse étendues de Cortex XDR forment un cadre adapté à chaque phase de la sécurité opérationnelle. Face à la prolifération des malwares, des attaques ciblées et des menaces internes, nous verrons enfin qu'un outil tel que Cortex XDR peut constituer une arme essentielle pour éradiquer les menaces et simplifier vos opérations de sécurité.

Des analystes à bout de souffle

À l'heure actuelle, les équipes de sécurité sont doublement submergées par un déluge d'attaques et un torrent d'alertes incessants. De leur côté, les attaquants multiplient les offensives en espérant qu'à force de persévérance, ils parviendront un jour à percer les défenses adverses. Afin de limiter le risque d'intrusion, les équipes sont amenées à déployer plusieurs couches de sécurité qui, en moyenne, génèrent près de 11 000 alertes par semaine[1].

Pour suivre la cadence, les analystes opèrent souvent en mode pompier et s'efforcent de trier au quotidien le plus d'alertes possible. Or, vu que ces données fournissent rarement le contexte nécessaire pour étayer leurs investigations, ils perdent un temps précieux à rechercher des indices complémentaires. Par conséquent, 53 % des équipes de sécurité avouent traiter moins de la moitié des alertes reçues[2], augmentant du même coup le risque de compromission de données.

Une traque mal ciblée

Pour enrayer la recrudescence des attaques, les entreprises de toute taille cherchent à s'équiper de solutions de détection et de réponse. Les acteurs de la sécurité informatique ont donc réagi en introduisant une série d'outils, parmi lesquels l'EDR pour la détection et la réponse sur les terminaux, le NDR pour la détection et la réponse sur le réseau, ou encore l'UBA pour l'analyse des comportements utilisateurs. Mais vu que ces outils fonctionnent en silos, ils n'offrent qu'une visibilité limitée sur l'activité cyber et ne peuvent être pilotés que par des spécialistes chevronnés. De plus, l'implémentation de tels systèmes entraîne un coût non négligeable, puisque leur fonctionnement requiert le déploiement et la maintenance de nouveaux capteurs réseau et d'agents sur tous les terminaux de l'environnement.

D'un autre côté, les entreprises choisissant de faire l'impasse sur les outils de détection et de réponse risquent de s'exposer à des attaques furtives comme les malwares évasifs, les menaces internes ou encore les attaques ciblées. En effet, ces attaques avancées ont en commun de ne laisser transparaître aucun des indicateurs de compromission (IoC) traditionnels (signatures d'attaques, domaines malveillants, etc.). Le seul moyen de les détecter est de scruter l'activité – et non uniquement les alertes – sur la durée et à partir de multiples sources de données via le machine learning et l'analytique.

Les investigations manuelles allongent la durée de présence des attaquants

Une fois qu'une attaque est détectée, la bataille ne fait que commencer puisque les analystes doivent encore procéder à l'investigation des alertes et répondre à plusieurs questions (qui, quoi, quand, pourquoi et comment) avant de pouvoir déterminer leurs prochaines actions. Malheureusement, les outils de sécurité actuels ne présentent les alertes que de façon générique, avec des informations limitées sur les utilisateurs, les terminaux, le réseau, les applications et la CTI. Ces alertes ne fournissent donc pas tout le contexte nécessaire à une investigation et une réponse efficaces. Les analystes doivent par conséquent jongler entre plusieurs interfaces afin de recouper les données et ainsi obtenir le tableau complet d'une attaque. L'investigation d'une alerte réseau peut par exemple exiger une analyse et une corrélation approfondies pour identifier le terminal, l'activité réseau et l'utilisateur associés à chaque incident. Or, les outils de sécurité actuels sont si complexes et cloisonnés que même les experts les plus aguerris ont du mal à suivre le fil d'Ariane.

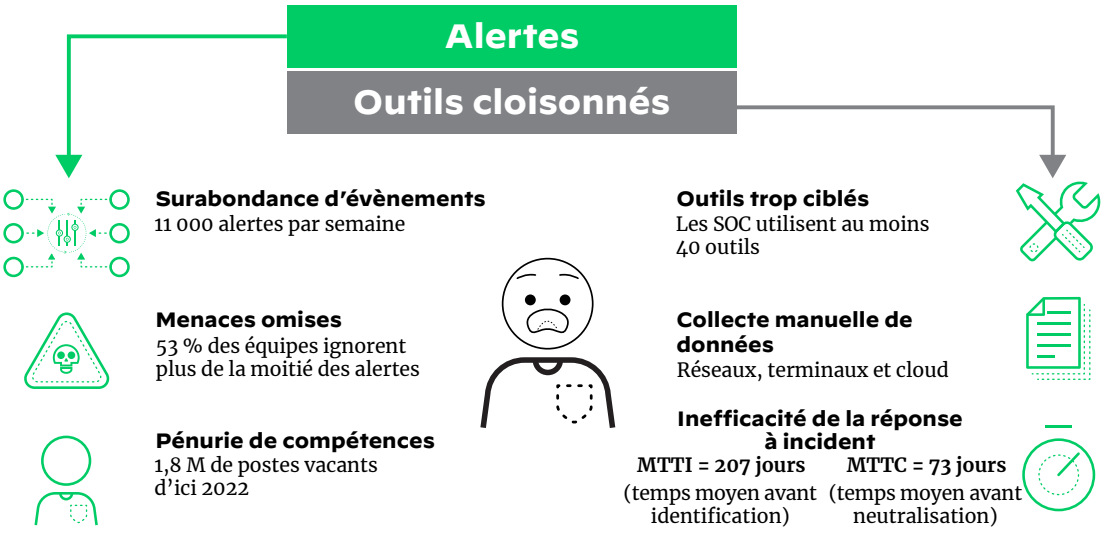
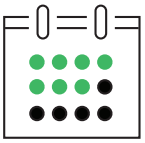


Figure 1 : Les analystes sécurité sont confrontés à de nombreux obstacles

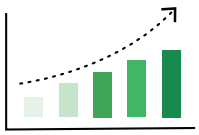
1. « The State of Security Operations Report, 2021 », Forrester, https://www.paloaltonetworks.com/resources/research/state-of-secops-forrester-consulting-study.
2. Ibid.

Étant donné que ces solutions fonctionnent rarement en synergie, les analystes peinent à coordonner leur réponse sur l'ensemble des points de contrôle. Résultat : au lieu de bloquer rapidement une attaque, vos équipes doivent soumettre des tickets ou demander à d'autres collègues de mettre à jour les politiques de sécurité, ce qui peut prendre des jours, voire des semaines. Les chiffres sont d'ailleurs sans équivoque : les entreprises mettent en moyenne 207 jours pour identifier une compromission et 73 jours pour la neutraliser[3]. Dans un contexte de pénurie de compétences en cybersécurité, les équipes doivent se résoudre à briser les silos et simplifier leurs opérations de réponse à incident si elles veulent se donner une chance de contrer efficacement les cyberattaques.



Le temps moyen avant identification (MTTI) d'une compromission est passé à

207 jours



Le temps moyen avant neutralisation (MTTC) d'une menace est passé à

73 jours

Figure 2 : Allongement du MTTI et du MTTC

La solution

Pour répondre aux enjeux actuels de la sécurité opérationnelle, les équipes doivent adopter une nouvelle approche capable de simplifier chaque étape des opérations de sécurité : de la détection à la réponse, en passant par la traque des menaces, le tri des alertes et l'investigation. Afin de réduire les risques tout en rationalisant les processus, cette nouvelle méthode doit s'articuler autour de trois grands axes :

- **Prévention des menaces :** une prévention efficace dresse le meilleur barrage possible contre plus de 99 % des attaques pouvant être bloquées automatiquement, en temps réel ou quasi-réel, sans aucune vérification manuelle. Vous devez implémenter un système de prévention homogène et coordonné sur l'ensemble de vos ressources numériques.
- **IA et machine learning :** alors que la quantité de données collectées ne cesse de croître, vos analystes ne devraient pas avoir à manuellement analyser ou mettre en corrélation ces informations pour identifier les menaces. Ensemble, le machine learning et l'analytique apprennent à connaître les spécificités de votre entreprise et forment une base de référence comportementale permettant de détecter les attaques avancées.
- **Automatisation :** pour confirmer rapidement qu'une attaque est bien en cours, les analystes ont besoin d'alertes leur livrant tous les détails nécessaires pour engager leurs investigations. La cause racine doit être facilement identifiable, même sans expérience exhaustive.

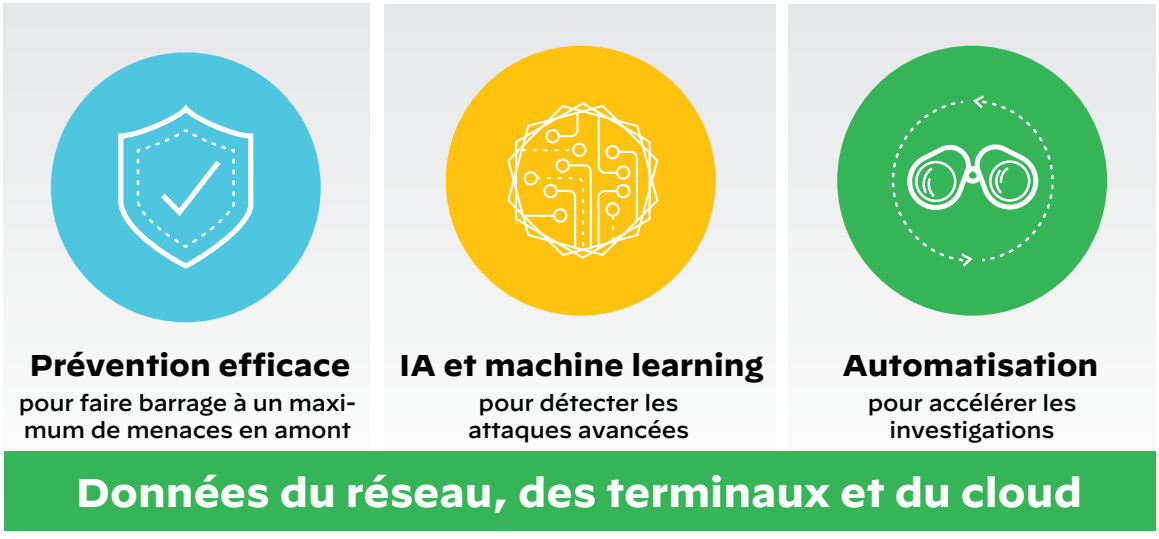


Figure 3 : Fonctionnalités critiques intégrées

En coordonnant ces trois fonctionnalités intégrées sur l'ensemble de vos ressources critiques, y compris votre réseau, vos terminaux et vos infrastructures cloud, vous pourrez déjouer les attaques les plus sophistiquées.

Cortex XDR : détection et réponse étendues

Cortex® XDR™, la première plateforme étendue de détection et de réponse, intègre les données des terminaux, des réseaux, du cloud et de sources tierces pour bloquer les attaques avancées. Cortex XDR a été entièrement conçu dans le but d'aider les entreprises à sécuriser leurs utilisateurs et leurs ressources

3. « 2020 Cost of a Data Breach Study », Ponemon Institute, juillet 2020, https://www.ibm.com/downloads/cas/861MNWN2.

numériques tout en rationalisant les opérations. Grâce à l'analyse comportementale, notre solution identifie les menaces inconnues et hautement évasives qui pèsent sur votre réseau. Le machine learning et les modèles d'IA dévoilent des menaces de n'importe quelle source, y compris des appareils gérés et non gérés.

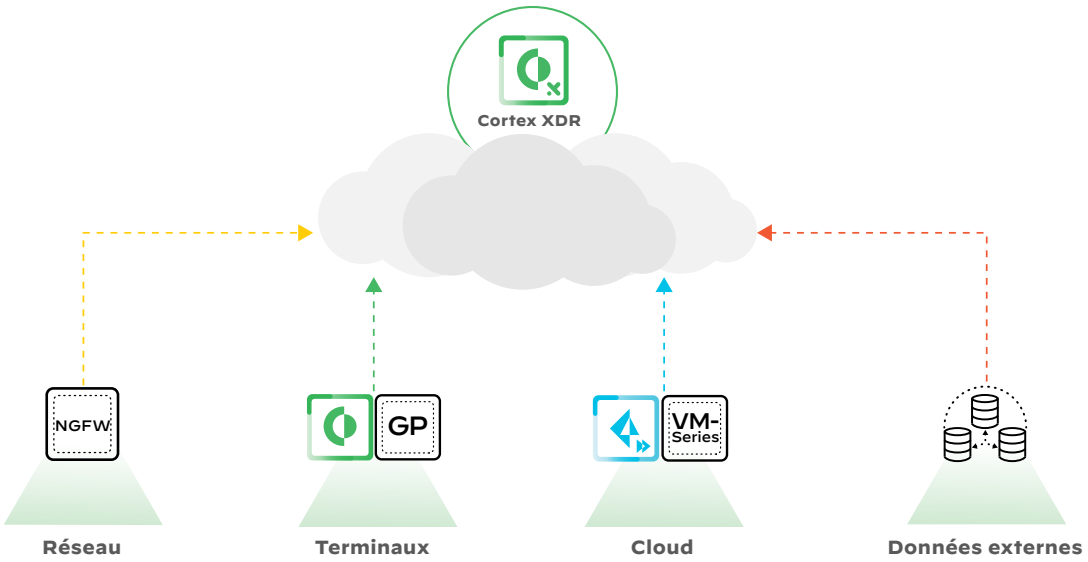


Figure 4 : Analyse de données multisources par Cortex XDR

En accompagnant chaque alerte d'un descriptif détaillé de la menace, Cortex XDR accélère le travail d'investigation. La plateforme rassemble automatiquement différents types de données et révèle les causes racines ainsi que la chronologie des évènements, ce qui permet aux analystes de trier efficacement les alertes, quel que soit leur niveau d'expérience. Enfin, grâce à son intégration étroite aux points de contrôle, vos équipes peuvent répondre aux menaces aux quatre coins de votre environnement ou restaurer facilement les hôtes à un état d'intégrité antérieur.

Avec Cortex XDR, plus besoin d'installer de nouveaux logiciels ou équipements : vos outils de sécurité réseau, terminaux et cloud existants se transforment en capteurs et points de contrôle. Bien qu'une seule source de données suffise pour utiliser Cortex XDR, des sources supplémentaires vous permettront d'exploiter les avantages de la corrélation et de l'analyse croisée. Enfin, vous pouvez tirer un trait sur les contraintes d'une infrastructure de journalisation sur site : toutes vos données sont stockées dans un référentiel cloud sécurisé et évolutif.

Une protection à chaque étape de vos opérations de sécurité

À mesure que les attaquants se perfectionnent, les équipes de sécurité doivent elles aussi hausser leur niveau de jeu. Ceci implique la mise en œuvre d'un processus reproductible visant, d'une part, à neutraliser les attaques en amont via une prévention efficace et, de l'autre, à découvrir et bloquer les menaces actives. Les outils de Cortex XDR vous permettent d'accomplir cette mission en quatre étapes itératives :

1. Prévention automatique des menaces
2. Détection précise
3. Investigation rapide
4. Réponse intelligente

Cette trame pose toutes les bases nécessaires pour protéger votre entreprise contre les menaces actuelles et futures.

Objectif prévention, détection et réponse en boucle fermée

Prévention des menaces connues et inconnues, doublée d'une visibilité complète

Une sécurité à toute épreuve commence par une prévention imparable. C'est pourquoi Cortex XDR bloque en amont les exploits, les malwares, les ransomwares et les attaques sans fichier avec une efficacité incomparable. Spécialement conçu pour minimiser l'impact sur les terminaux, l'agent léger Cortex XDR neutralise les attaques et transmet les données d'évènements à Cortex XDR.

L'agent Cortex XDR propose un arsenal préventif complet, à commencer par le plus large éventail de modules de protection anti-exploit pour bloquer les voies d'infection par malware. Chaque fichier est passé au crible par un moteur local d'analyse par IA qui apprend en permanence pour contrer les nouvelles techniques d'attaque. De son côté, le moteur d'analyses comportementales surveille de multiples processus et établit des interdépendances pour détecter les attaques dès qu'elles se produisent.

En combinant diverses méthodes de prévention, notre antivirus nouvelle génération (NGAV) offre des niveaux de protection des terminaux sans commune mesure. Celui-ci s'intègre à Palo Alto Networks WildFire®, notre service de prévention des malwares, pour analyser les fichiers suspects dans le cloud et coordonner la protection sur l'ensemble des produits de sécurité Palo Alto Networks. Cet agent cloud unifié se déploie rapidement sur vos terminaux pour bloquer instantanément les attaques avancées, tout en collectant des données à des fins de détection et de réponse.

AV-Comparatives classe Cortex XDR au rang de Leader stratégique dans son test EPR (Endpoint Prevention and Response) 2020

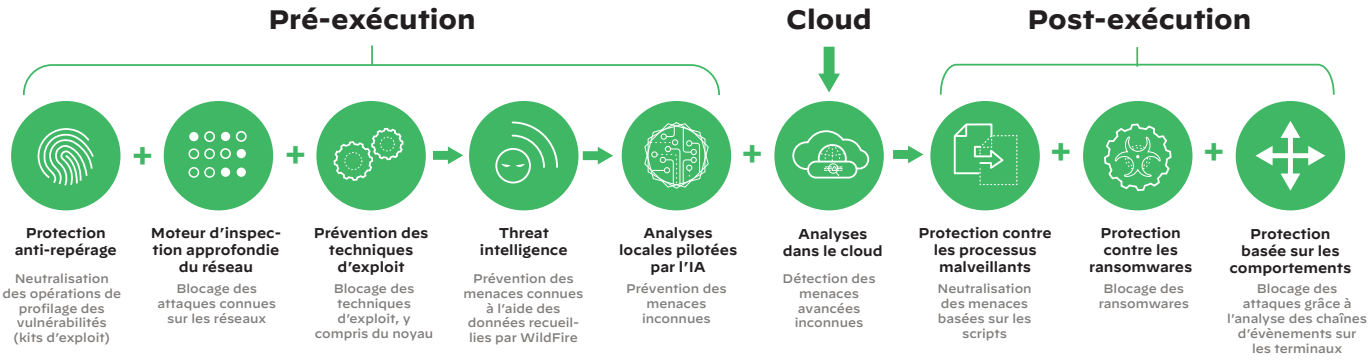


Figure 5 : Protection automatique contre les malwares, les exploits et les attaques sans fichier

Gestion sécurisée des connexions USB

L'utilisation d'équipements USB est certes très pratique, notamment pour la sauvegarde de données ou le raccordement de périphériques. Toutefois, en connectant une clé USB, un clavier ou une webcam infectés à un ordinateur, ou encore en copiant des données confidentielles sur un disque externe, les utilisateurs exposent leur entreprise à des attaques. C'est pourquoi Cortex XDR intègre un puissant module de contrôle des appareils qui permet de sécuriser les accès USB sans devoir installer un agent supplémentaire sur tous vos hôtes. Vous pouvez définir des politiques basées sur un groupe ou une unité organisationnelle d'Active Directory®, restreindre l'utilisation en fonction du type d'appareil et créer des exceptions de lecture seule ou lecture/écriture dans les politiques applicables aux fournisseurs, produits et numéros de série. Avec le module de contrôle des appareils, vous gérez les accès USB facilement et en toute sécurité.

Protection des terminaux à l'aide de pare-feu sur hôte et du chiffrement sur disque

Les fonctionnalités intégrées de pare-feu sur hôte et de chiffrement de disques vous aident à réduire les risques de sécurité et à répondre aux exigences réglementaires. D'une part, le pare-feu sur hôte de Cortex XDR vous permet de contrôler les communications entrantes et sortantes sur vos terminaux Windows® et macOS®. De l'autre, vous pouvez créer des règles et des politiques de (dé)chiffrement de disque afin d'appliquer les chiffrements BitLocker® ou FileVault® sur vos équipements. Cortex XDR offre une visibilité complète sur les terminaux protégés par BitLocker ou FileVault et répertorie tous les lecteurs chiffrés. Ces deux fonctionnalités vous permettent ainsi de centraliser la gestion de vos politiques de sécurité des terminaux dans Cortex XDR.

Visibilité inégalée et accélération des réponses avec Host Insights

La protection de vos terminaux passe par une visibilité complète sur leurs paramètres et leurs contenus, mais aussi par une parfaite compréhension des risques associés. Ensuite, dès lors qu'une menace est identifiée, vous devez la neutraliser rapidement et vérifier que d'autres terminaux n'ont pas été touchés.

Host Insights vous offre toutes ces fonctionnalités, mais pas seulement. Ce module complémentaire de Cortex XDR allie le diagnostic des vulnérabilités à une parfaite visibilité sur les systèmes et applications. Quant à sa fonctionnalité Search and Destroy ultrapuissante, elle facilite la détection et la neutralisation des menaces. En résumé, Host Insights offre une approche complète de la visibilité et de la neutralisation des attaques sur les terminaux, gage d'une réduction de votre exposition aux menaces pour éviter de futures compromissions.

Host Insights comprend ces trois fonctionnalités :

- **Search and Destroy** vous permet de localiser et d'éradiquer immédiatement les menaces sur tous vos terminaux. Cet outil puissant indexe l'ensemble des fichiers de vos terminaux Windows afin de détecter et de supprimer les fichiers malveillants en temps réel, à l'échelle de toute l'entreprise. Ses paramétrages granulaires permettent en outre d'exclure des fichiers et dossiers sélectionnés sur certains hôtes.
- **Host Inventory** identifie les failles de sécurité et améliore vos défenses à l'aide d'une visibilité complète sur les paramètres et fichiers clés de vos hôtes Windows. Vous pouvez ainsi consulter les informations relatives aux utilisateurs, aux groupes, aux applications, aux services, aux pilotes, aux programmes AutoRun, aux partages, aux disques ou encore aux paramètres système. Host Inventory centralise ainsi tous les détails de vos hôtes afin d'identifier rapidement les problèmes de sécurité et d'accélérer les investigations grâce à un contexte approfondi concernant chaque hôte.

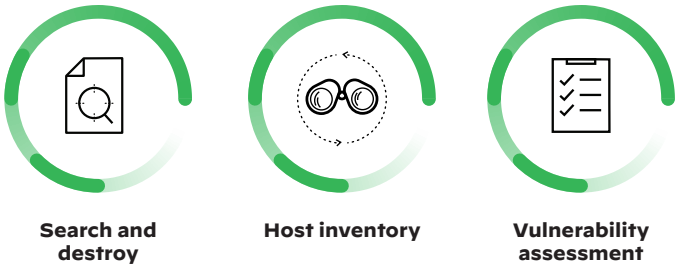


Figure 6 : Module Host Insights

- **Vulnerability Assessment** offre une visibilité en temps réel sur votre exposition aux vulnérabilités et sur les correctifs installés sur vos terminaux afin de définir les priorités de mitigation. Cortex XDR met en lumière les failles sur vos terminaux Linux et Windows grâce aux dernières informations sur les niveaux de gravité fournies par la National Vulnerability Database du NIST et le Centre de réponse aux problèmes de sécurité Microsoft (MSRC). Vous pouvez en outre consulter la liste des mises à jour Windows installées sur vos terminaux dans la base de connaissances de Microsoft.

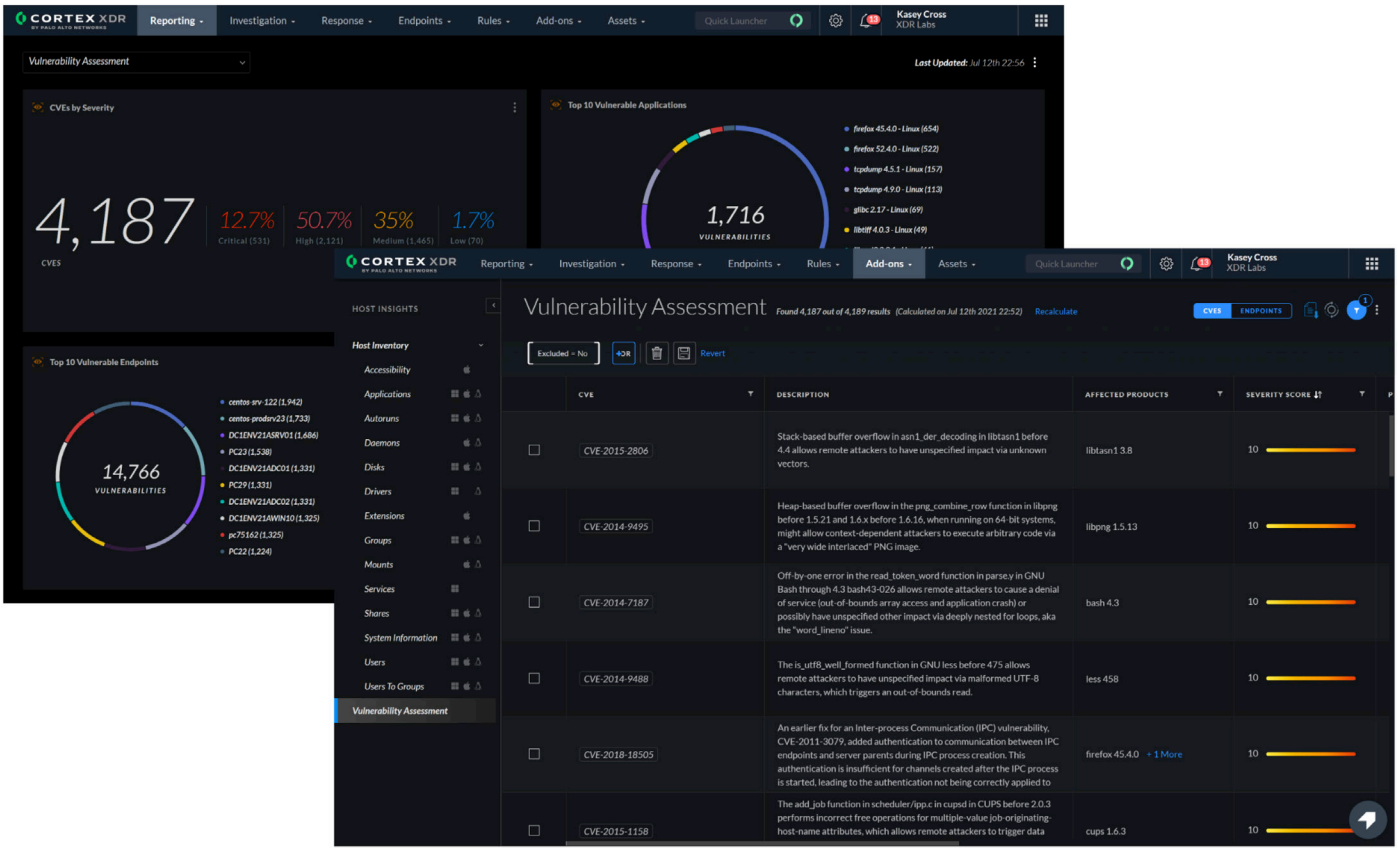


Figure 7 : Tableau des vulnérabilités avec les dernières données CVE

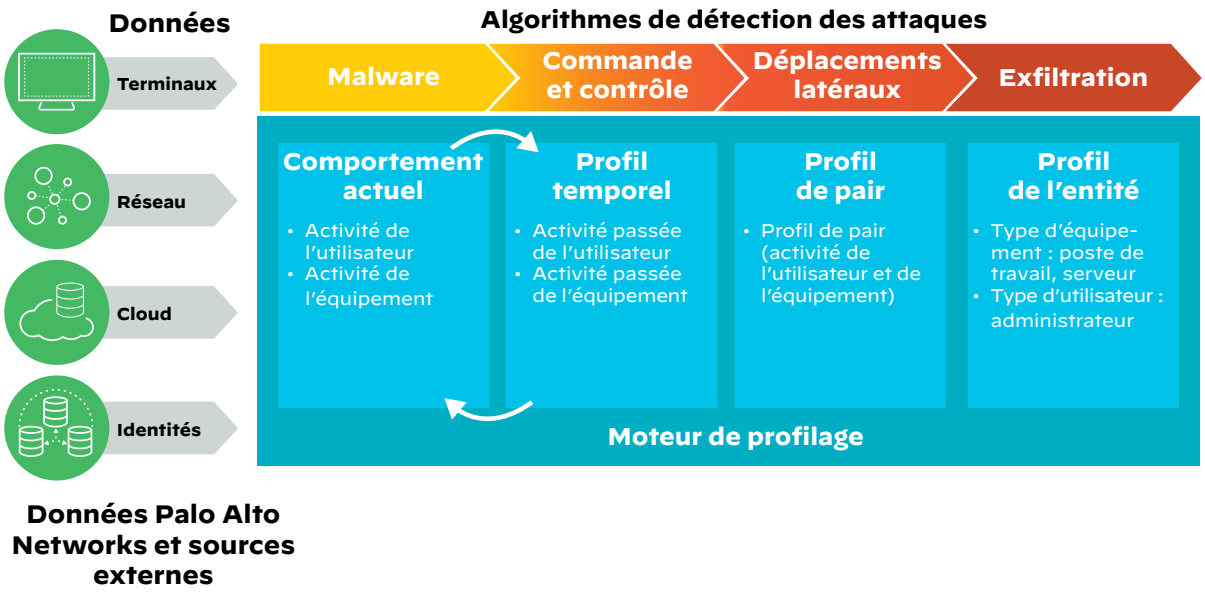


Figure 8 : Architecture d'analyses comportementales de Cortex XDR

Détection automatique des attaques via les analyses comportementales et l'IA

En s'appuyant sur l'analytique et le machine learning, Cortex XDR révèle les attaques furtives et vous permet de réduire la durée de présence des menaces en les neutralisant rapidement. Pour commencer, Cortex XDR analyse les données enrichies recueillies depuis toutes les sources disponibles, avec à la clé une visibilité complète et sans angle mort. Les données issues de vos réseaux, terminaux et ressources cloud sont ainsi corrélées pour détecter avec précision les attaques et faciliter le travail d'investigation.

Cortex XDR surveille plus d'un millier de variables comportementales, dont des attributs pratiquement impossibles à évaluer à partir des journaux de menaces traditionnels. L'intelligence artificielle effectue ensuite un profilage comportemental des utilisateurs et des terminaux grâce à deux modèles de machine learning :

- **Apprentissage non supervisé :** Cortex XDR définit le modèle comportemental de base des utilisateurs et des terminaux, lance des analyses par groupe de pairs et classifie les équipements en fonction de catégories comportementales. À partir de ces profils, Cortex XDR détecte les écarts avec les comportements individuels et collectifs antérieurs afin de mettre en lumière les activités malveillantes (malwares, C&C, latéralisation, exfiltration, etc.).
- **Apprentissage supervisé :** Cortex XDR surveille de multiples caractéristiques du trafic réseau afin de classifier les équipements par type (PC Windows, iPhone®, outils d'analyse de vulnérabilités…). Cortex XDR distingue également les utilisateurs finaux des administrateurs informatiques. Grâce au machine learning supervisé, Cortex XDR identifie les divergences par rapport au comportement attendu selon le type d'utilisateur ou d'équipement afin de réduire les faux positifs.

Détection des menaces basées sur les utilisateurs avec Identity Analytics

Le module complémentaire Identity Analytics de Cortex XDR permet à votre équipe de dépister les comportements d'utilisateurs risqués et malveillants qui échappent à la surveillance des outils traditionnels. Cette fonctionnalité dresse le profil comportemental des utilisateurs en examinant l'évolution de données variées (authentification, terminaux, réseaux, cloud, journaux des menaces, etc.) au fil du temps. En comparant le comportement présent de l'utilisateur à une base de référence antérieure, Identity Analytics est capable de détecter les vols d'identifiants, les attaques par force brute ou encore les déplacements impossibles avec une précision inédite. Ses algorithmes de détection sont en outre constamment affinés à partir de métriques et d'analyses dans le cloud afin de toujours garder un temps d'avance sur les attaquants. Les alertes Identity Analytics sont automatiquement groupées avec les autres alertes pour fournir une analyse des attaques étape par étape.

Identification des menaces furtives avec des règles personnalisées

Votre équipe de sécurité peut établir des règles personnalisées afin d'identifier des menaces spécifiques ainsi que les attaques visant vos ressources les plus sensibles. En plus des alertes de Cortex XDR basées sur les IoC (p. ex. les hachages de malwares), les règles personnalisées permettent d'exposer les modes opératoires des attaquants à partir d'indicateurs comportementaux de compromission (BIoC). En ce qui concerne la détection avancée, des règles de corrélation aident à mettre au jour les combinaisons de comportements complexes d'un ou plusieurs ensembles de données à l'aide du puissant langage de requête XQL de Cortex XDR. Ces règles de corrélation peuvent identifier les abus liés aux systèmes et aux applications, ainsi que les attaques zero-day employant des techniques de contournement. Les menaces seront ainsi mises en évidence même en cas de manipulation des noms de malwares, de hachages ou d'adresses IP.

Vos analystes peuvent définir des règles basées sur des dizaines de paramètres différents, y compris les informations liées aux processus, aux fichiers, au réseau ou encore au registre. Plus de 500 règles prédéfinies permettent de détecter immédiatement des menaces de types très divers : persistance, falsification, élévation de privilèges, latéralisation, etc. Pour encore plus de sécurité et de sérénité, ces fonctionnalités de détection sont opérationnelles 24 h/7 j.

Données inspectées par Cortex XDR

Cortex XDR analyse les métadonnées de protocoles des journaux applicatifs, de trafic et de menaces collectés par Prisma Access® et les pare-feu nouvelle génération (NGFW) de Palo Alto Networks. Notre plateforme étendue de détection et de réponse inspecte également les données recueillies par les agents Cortex XDR, les journaux et les alertes d'outils tiers. En créant des profils basés sur des centaines de variables comportementales (fréquence des connexions, source et destination du trafic, protocoles utilisés, etc.), Cortex XDR se familiarise avec les comportements attendus des utilisateurs et des équipements. Il surveille également le trafic interne et le trafic sortant des clients et serveurs vers Internet.

Données de session

Les journaux de trafic de pare-feu fournissent les métadonnées nécessaires au profilage des comportements des utilisateurs et équipements :

- Ports et adresses IP sources et cibles
- Octets envoyés et reçus
- Durée de la connexion
- Journaux applicatifs avancés, avec données transaction-nelles sur les protocoles DNS, HTTP, DHCP, RPC, ARP, ICMP, etc.
- Données applicatives d'App-ID™

Données utilisateurs

Cortex XDR analyse le trafic réseau et les données des terminaux pour en extraire des informations contextuelles sur l'utilisateur :

- Utilisateur connecté
- Utilisateur habituel d'une machine donnée
- Utilisateur créateur du processus à l'origine de la communication
- Groupe d'utilisateurs et unité organisationnelle via Directory Sync
- Évènements d'authentification des journaux Okta, Azure Active Directory, PingOne, PingFederate, Kerberos et Windows

Données cloud

Cortex XDR recueille les journaux détaillés du cloud :

- Prisma Access et VM-Series
- Google Cloud Platform et Google Kubernetes Engine (GKE)
- Amazon CloudWatch et AWS CloudTrail
- Amazon Elastic Kubernetes Service (EKS)
- Azure Kubernetes Service (AKS)

Données terminaux

Cortex XDR analyse l'activité complète des terminaux :

- Création, suppression et modification de fichiers
- Hachage de fichiers
- Chemin d'accès aux fichiers
- Nom de processus
- Modification du registre
- Arguments CLI, appels RPC et injection de code
- Évènements matériels (connexions USB, etc.)
- Manipulation des journaux d'évènements
- Alertes de sécurité de l'agent Cortex XDR
- Verdict d'analyse de malware par WildFire

Données hôtes

Cortex XDR identifie les machines à l'aide des données suivantes :

Nom d'hôte

- Adresse MAC
- Système d'exploitation

Conservation des données

- 30 derniers jours au minimum

Traque des menaces et recherche d'IoC

Que ce soit dans le cadre d'une recherche isolée ou d'une investigation à grande échelle, la traque des menaces joue un rôle essentiel dans la sécurité opérationnelle. À partir de simples requêtes, vos analystes peuvent détecter des activités suspectes en effectuant des recherches des hôtes, des fichiers, des processus, des clés de registre et des connexions spécifiques. La demande peut être précise (p. ex. : « Quels changements ont été apportés au fichier [x] par le processus [y] sur l'hôte [z] ») ou ouverte (ex. : « Afficher tous les processus exécutés dans le domaine »). Votre équipe peut donc rechercher certains comportements symptomatiques d'une attaque ainsi que les IoC traditionnels, sans devoir apprendre un nouveau langage de requête. Les analystes peuvent filtrer les résultats afin de réduire le nombre d'évènements à inspecter et de ne révéler que les menaces latentes. Pour traquer les menaces avancées, il est possible d'exécuter des requêtes complexes contenant des caractères génériques et des expressions régulières, d'agréger et de visualiser les résultats et d'effectuer une recherche complète des données avec XQL Search. En intégrant la Threat Intelligence à un ensemble complet de données (réseau, terminaux, cloud), votre équipe de sécurité dispose de tous les éléments pour découvrir en quelques secondes des incidents antérieurs ou en cours.

Investigations huit fois plus rapides grâce à l'intégration et l'automatisation des données

Pour accélérer le tri des alertes, l'analyse des menaces et, in fine, la réponse à incident, votre équipe doit pouvoir mener ses investigations à l'aide d'informations contextualisées. Cortex XDR répond à tous ces impératifs par plusieurs fonctionnalités clés. Une console de gestion des incidents rassemble les alertes connexes afin de proposer une vue intégrale de l'attaque. Votre équipe peut ainsi consulter les hôtes et utilisateurs affectés, la CTI détaillée et les principaux artefacts tels que les domaines, les adresses IP et les processus impliqués dans l'incident. Le regroupement et la déduplication permettent de réduire à hauteur de 98 % le volume d'alertes à inspecter, limitant du même coup le phénomène d'accoutumance. D'autre part, le scoring des incidents vous aide à classer et prioriser les évènements présentant un risque élevé. Votre équipe peut aussi trier, filtrer ou exporter les incidents et les alertes. D'un simple clic, les analystes démarrent une investigation – quelle que soit la source de l'alerte – et obtiennent les détails nécessaires afin de déterminer la cause racine, la réputation et la séquence des évènements : plus besoin d'expérience exhaustive pour vérifier une menace.

Les analyses suivantes répondent aux différentes interrogations que soulèvent les alertes :

- **Analyse des causes racines :** ce moteur d'analyse breveté passe au crible des milliards d'évènements de sécurité pour identifier, visualiser et détailler la chaîne de causalité de chaque menace, rendant ainsi les attaques complexes beaucoup plus lisibles. Vos analystes peuvent identifier les processus de terminaux à l'origine des alertes de sécurité cloud ou réseau, le tout sans devoir établir une corrélation manuelle des évènements ni jongler entre plusieurs consoles.

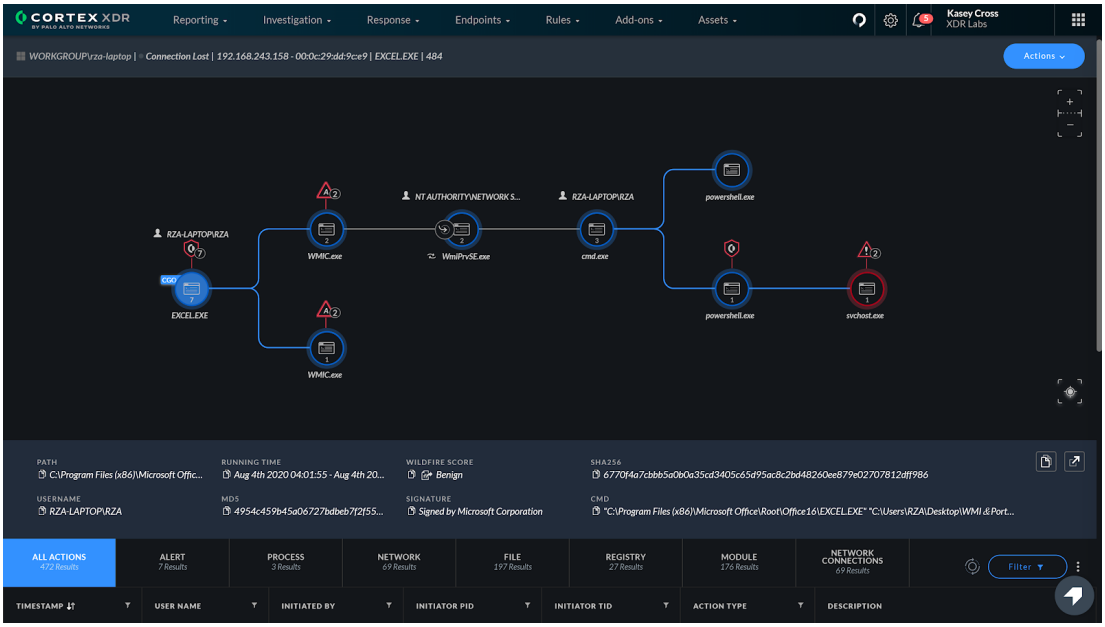


Figure 9 : Cortex XDR affiche la cause racine des alertes et les artefacts clés

- **Analyse de la chronologie :** une chronologie forensique de l'attaque fournit des éléments essentiels aux investigations d'incidents, permettant aux analystes de déterminer en quelques secondes l'ampleur de l'attaque, son impact et les étapes à suivre pour la neutraliser. Les informations contenues dans les alertes facilitent la compréhension des évènements complexes, tandis que la visualisation du framework MITRE ATT&CK® indique toutes les tactiques et les techniques d'attaque observées au cours d'un incident.

Cortex XDR soulage les équipes submergées par un déluge d'alertes et d'analyses complexes et chronophages. Grâce à ses outils intuitifs, visuels et contextuels, il simplifie le tri des alertes et l'investigation d'incidents. Des analyses qui, autrefois, nécessitaient des compétences pointues et des heures, des jours, voire des semaines de travail s'exécutent désormais facilement en quelques secondes ou minutes.

Réponse et adaptation aux menaces

Dès lors qu'une menace est identifiée dans votre environnement, tout doit être fait pour la neutraliser le plus rapidement possible. Cortex XDR permet à votre équipe de sécurité d'éliminer instantanément les menaces sur le réseau, les terminaux et le cloud depuis une seule et même console. Votre équipe peut ainsi rapidement stopper la propagation des malwares et restreindre l'activité réseau entrante ou sortante des appareils, mais aussi mettre à jour les listes de prévention des menaces (domaines malveillants, etc.) grâce à une parfaite intégration aux points de contrôle.

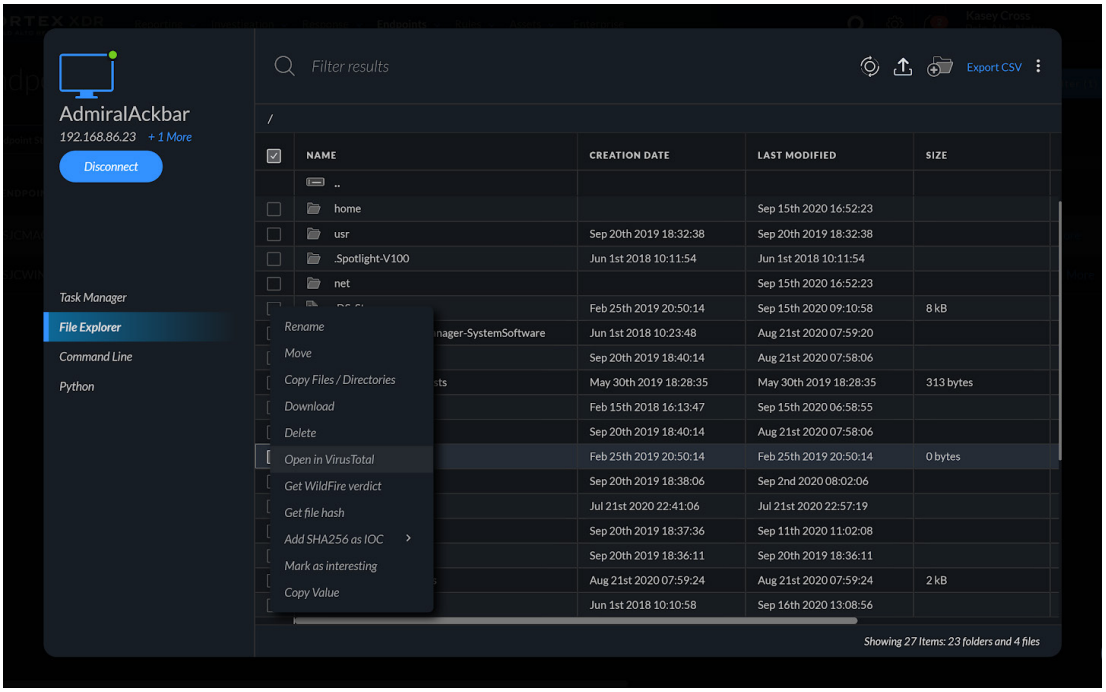


Figure 10 : Gestionnaire des tâches de Cortex XDR Live Terminal

Éliminez rapidement les menaces à l'aide de plusieurs options flexibles :

- **Isolez les terminaux compromis** en bloquant tout accès au réseau, excepté pour le trafic à destination de la console de gestion Cortex XDR. Ce confinement empêche ainsi la contamination d'autres terminaux.
- **Interrompez les processus** pour cesser toute activité des malwares sur le terminal.
- **Bloquez toute autre exécution** d'un fichier incriminé en le plaçant sur liste de blocage.
- **Mettez les fichiers malveillants en quarantaine** et supprimez-les de leur répertoire de travail, si Cortex XDR ne s'en est pas déjà occupé.
- **Récupérez des fichiers spécifiques** sur des terminaux en cours d'investigation pour des analyses complémentaires.
- **Accédez directement aux terminaux** depuis Live Terminal et bénéficiez des processus de réponse les plus flexibles du marché pour exécuter Python®, PowerShell® ou des commandes ou scripts systèmes ; évaluer et gérer les processus actifs ; ou encore voir, supprimer, déplacer ou télécharger des fichiers. Vos équipes peuvent aussi interrompre et supprimer des processus dans un environnement de production sur n'importe quel hôte, tout en exécutant parallèlement un audit complet. Les menaces sont donc éliminées pendant que vos utilisateurs continuent de travailler, sans aucune perturbation de leur activité ni temps d'arrêt.
- **Utilisez des API ouvertes** pour permettre l'intégration d'outils de gestion tiers, appliquer des politiques et collecter les données des agents depuis n'importe quel emplacement.
- **Misez sur l'intégration à Cortex XSOAR** pour vos besoins d'orchestration, d'automatisation et de réponse. Vos équipes de sécurité peuvent alimenter Cortex XSOAR en données d'incident pour engager une réponse automatique pilotée par playbook, un procédé qui couvre plus de 450 outils tiers. Les playbooks de Cortex XSOAR peuvent ingérer automatiquement les incidents de Cortex XDR, recouvrer les alertes correspondantes et actualiser les champs d'incident dans Cortex XDR sous forme de tâches de playbook.
- **Exécutez des scripts Python** depuis la console de gestion Cortex XDR ou des outils d'orchestration tels que Cortex XSOAR. Des scripts prêts à l'emploi sont disponibles afin d'exploiter facilement les avantages de cette puissante fonctionnalité.
- **Localisez et supprimez rapidement des fichiers** au sein de votre environnement avec la fonction Search and Destroy, qui indexe le contenu de vos terminaux.
- **Restaurez les hôtes à un état d'intégrité antérieur** basé sur les suggestions de remédiation. Ces recommandations de réponse étape par étape vous permettent de résoudre facilement tous les problèmes identifiés au cours d'un incident. Pour un retour rapide à la normale après une attaque, supprimez les fichiers et les clés de registre malveillants, et restaurez les fichiers et les clés de registre endommagés, le tout sans devoir réimager vos terminaux ni développer de scripts personnalisés.

Centralisation de la gestion, du reporting, du tri et de la réponse à incident

La plateforme Cortex XDR offre à vos équipes une expérience homogène en rassemblant au sein d'une même console web la gestion des politiques des terminaux, la détection des menaces, l'investigation et la réponse à incident. Des tableaux de bord personnalisables vous permettent d'évaluer l'état de sécurité des terminaux et de dresser le bilan des incidents. Vous disposez aussi de rapports graphiques spontanés ou programmés à intervalles réguliers pour synthétiser visuellement les incidents et les tendances de sécurité. Le déploiement et la mise à jour des agents Cortex XDR peuvent en outre être gérés depuis la même interface.

La solution évolue constamment afin d'anticiper les menaces et contrecarrer les futures attaques. Son intégration à WildFire, le service d'analyse des malwares le plus complet du marché, permet d'identifier les programmes malveillants. Cortex XDR est une application cloud-native, ce qui lui permet d'intégrer rapidement les découvertes de notre communauté afin de mettre en lumière les dernières tactiques d'attaque tout en améliorant la précision de ses fonctionnalités de détection.

MITRE | ATT&CK®

Cortex XDR a obtenu les meilleurs résultats de protection et détection combinées lors de la phase 3 de l'évaluation MITRE ATT&CK, avec 100 % de prévention des menaces et 97 % de visibilité.

Accélération de la réponse à incident avec Forensics

Cortex XDR Forensics est une solution efficace de tri et d'investigation vous permettant d'examiner les indices, de traquer les menaces et de diagnostiquer les compromissions à partir d'une même console. Ce module complémentaire recueille des données approfondies et offre un accès immédiat à plusieurs artefacts forensiques afin de déterminer plus facilement la source et l'ampleur d'une attaque. Cortex XDR Forensics est une solution de bout en bout intervenant à chaque phase de la réponse à incident, de la collecte de données à la remédiation, en passant par l'analyse et la traque des menaces. Le module Forensics a été spécialement mis au point par et pour des experts de la réponse à incident. Il simplifie les investigations, détecte les moindres faits et gestes de l'attaquant et neutralise rapidement les menaces depuis la console Cortex XDR : plus besoin de jongler entre plusieurs outils de sécurité.

Managed Threat Hunting, votre assurance sérénité

Cortex XDR Managed Threat Hunting, c'est une surveillance 24 h/7 j assurée par des analystes chevronnés grâce au premier service de traque des menaces intégrant les données des terminaux, des réseaux et du cloud. Nos experts Unit 42™ agissent en votre nom pour découvrir les menaces avancées (cybercriminels, groupes à la solde d'États, malfaiteurs internes, malwares, etc.). Pour détecter les attaquants infiltrés dans votre entreprise, nos analystes passent au peigne fin un ensemble complet de données issues des solutions de sécurité de Palo Alto Networks et d'autres fournisseurs.

Des rapports détaillés mettent en lumière les outils, les étapes et l'ampleur des attaques pour contrer rapidement les cybercriminels, tandis que les rapports d'impact vous aident à garder une longueur d'avance sur les menaces émergentes.

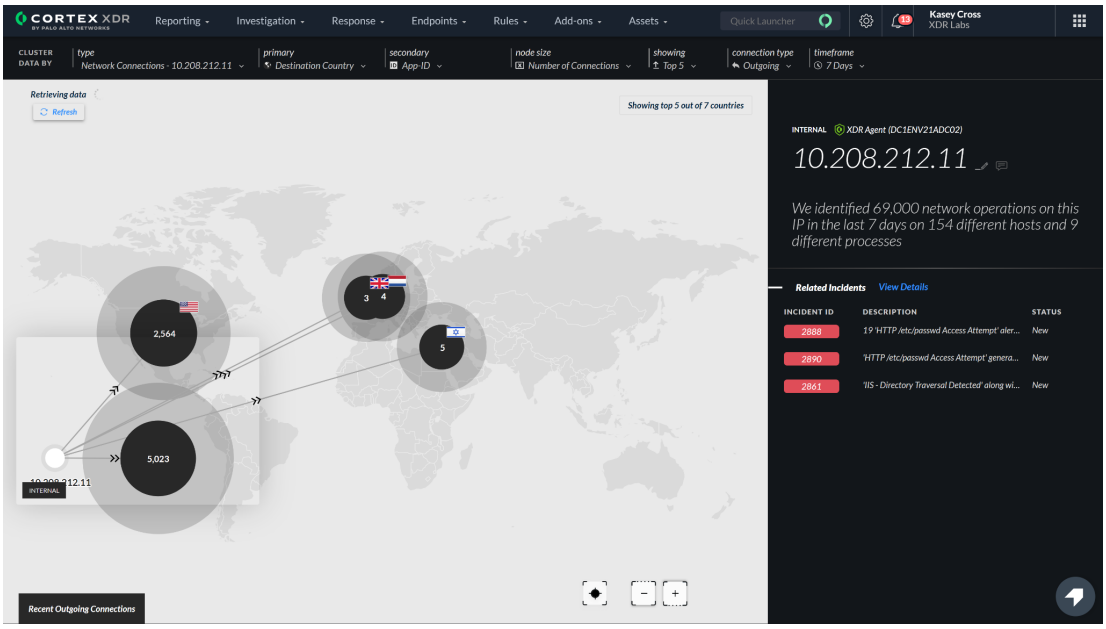


Figure 11 : L'affichage en mode IP fournit des informations exploitables et contextuelles sur les adresses IP

L'éclaircie venue du cloud

Le modèle cloud-native de Cortex XDR rationalise le déploiement en évitant toute installation de nouveaux logiciels ou équipements sur site. Vos produits Palo Alto Networks – y compris l'agent Cortex XDR – se transforment en capteurs et points de contrôle afin de simplifier vos opérations de sécurité. Les données ainsi recueillies sont stockées au sein de la plateforme Cortex XDR, qui offre un système de journalisation évolutif pour absorber toutes les données essentielles à la détection et la réponse. Grâce au déploiement rapide de la solution, vous ne perdez plus de temps à configurer de nouveaux équipements.

L'agent Cortex XDR s'installe facilement et sans redémarrage sur l'ensemble de vos terminaux Windows, macOS, Linux, Chrome® OS et Android®. Parfaitement adapté aux serveurs physiques, aux machines virtuelles (VM) et aux containers, l'agent Cortex XDR protège toutes vos ressources numériques, des appareils mobiles aux environnements privés, publics, hybrides et multicloud. Côté containers, Cortex XDR se synchronise parfaitement avec Kubernetes pour que votre sécurité évolue parallèlement à vos workloads cloud.

En centralisant le stockage des données issues des pare-feu nouvelle génération de Palo Alto Networks, de Prisma Access, Prisma Cloud, Cortex Xpanse et du reste de votre infrastructure de sécurité, vous réduisez les coûts liés à la gestion des journaux et aux systèmes SIEM. De même, en éliminant la journalisation sur site ainsi que l'installation de nouveaux capteurs et points de contrôle locaux, Cortex XDR baisse de 44 % le coût total de possession (CTP) par rapport aux outils cloisonnés. Cortex XDR booste également la productivité de votre équipe SecOps en détectant les attaques avec précision et en accélérant les investigations.

Renforcez votre sécurité avec Cortex XDR

De nos jours, être analyste sécurité n'est pas un métier de tout repos. Face à un volume de menaces qui ne cesse de s'amplifier, les entreprises déploient de plus en plus d'outils cloisonnés qui génèrent une avalanche d'alertes tant incomplètes qu'imprécises. Au lieu d'utiliser des systèmes cloud de machine learning pour détecter plus facilement les attaques furtives, les systèmes de gestion des informations et des évènements de sécurité (SIEM) se bornent à agréger des alertes déjà identifiées et bloquées par l'infrastructure de sécurité. Côté détection et réponse, les outils cloisonnés imposent le déploiement de logiciels et d'équipements additionnels, mais n'offrent en retour qu'une visibilité étroite et limitée sur les menaces, tant et si bien que les analystes finissent par perdre un temps précieux à recueillir et corréler eux-mêmes les données issues de plateformes disparates.

Avec Cortex XDR, vos équipes disposent d'une arme redoutablement efficace pour éradiquer les menaces furtives en corrélant toutes les données issues des réseaux, des terminaux et du cloud. Les avantages parlent d'eux-mêmes :

- Prévention des malwares avancés, des exploits et des attaques sans fichier à l'aide d'un seul agent léger
- Détection automatique des menaces furtives avec le machine learning et l'analytique
- Accélération du tri des alertes et des investigations pour aller droit à la cause racine d'une alerte et ainsi améliorer la productivité des analystes sécurité
- Neutralisation rapide des menaces via une réponse coordonnée sur tous les points de contrôle
- Simplification des opérations, évolutivité et agilité accrues grâce au déploiement cloud-native

En choisissant Cortex XDR, vous obtenez une visibilité complète sur vos réseaux, vos terminaux et vos ressources cloud tout en garantissant la sécurité de vos utilisateurs et de vos données.

paloalto® NETWORKS | Cybersecurity Partner of Choice

Oval Tower, De Entrée 99 – 197
1101HE Amsterdam
Pays-Bas

+31 20 888 1883
www.paloaltonetworks.fr

cortex_wp_cortex-xdr_082321-fr