Le SOAR, vecteur de transformation de la Threat Intelligence

Impossible de nier les avantages de la transformation numérique pour les entreprises. Toutefois, cette transformation apporte aussi son lot de problèmes de sécurité, car elle étend la surface d'attaque et donne aux cybercriminels le choix des armes. Dans un contexte de généralisation du cloud computing, de l'automatisation et de l'intelligence artificielle, les attaquants parviennent à lancer des campagnes d'une sophistication et d'une ampleur sans précédent, quasiment sans intervention humaine. Aujourd'hui, nos ordinateurs subissent leurs assauts toutes les 39 secondes.[1] D'après un rapport de Cybersecurity Ventures, d'ici à 2021, les ransomwares feront une nouvelle victime toutes les 11 secondes parmi les entreprises.[2] Cette intensification redoutable, nous la devons à la puissance des machines utilisées par les attaquants.

1. « Hackers Attack Every 39 Seconds », Security Magazine, 10 février 2017, https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds
2. « Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021 », Cybercrime Magazine, 7 décembre 2018, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021

Comment ne pas sombrer face à un tel déferlement ? Les entreprises ont de plus en plus de difficultés à implémenter et maintenir un bon niveau de sécurité sans impacter leurs activités. C'est là que le centre opérationnel de sécurité (SOC) a un rôle vital à jouer. Sa mission consiste à détecter, investiguer et neutraliser les cybermenaces avancées. Pour tenir la cadence, le SOC allie technologies de sécurité intégrées, processus rationalisés et expertise humaine.

Toutefois, la pénurie de compétences en cybersécurité, l'avalanche d'alertes peu fiables, les innombrables outils de sécurité disparates et le manque de données contextuelles externes finissent par surcharger les équipes de sécurité de toutes tailles et limiter leurs capacités d'action. Pour y remédier, il faut d'abord analyser le fonctionnement interne des SOC afin d'en saisir tous les rouages. Ce travail minutieux est le seul moyen d'évaluer l'ampleur des défis que rencontrent ces équipes et d'implémenter des solutions efficaces.

Dans les plus grandes entreprises, les équipes opérationnelles de sécurité matures obéissent à des organigrammes complexes. Dans ce type de structure, trois grandes fonctions se détachent : analystes SOC, professionnels de la réponse à incident et analystes CTI.

Analystes SOC

Chaque jour, les analystes SOC passent en revue des milliers d'alertes internes déclenchées par des technologies de gestion des évènements et informations de sécurité (SIEM), des systèmes de détection et de réponse (EDR), voire des centaines d'autres outils de sécurité. Ces sentinelles du numérique détectent, investiguent, identifient les causes et répondent rapidement aux incidents de sécurité. Pour ce faire, les analystes SOC surveillent constamment le réseau à l'aide d'outils de détection. En cas de risque avéré, ils doivent également documenter leurs conclusions et partager leurs recommandations avec les autres acteurs de la sécurité.

Toutes ces missions les exposent cependant à un certain nombre de difficultés :

- **Accoutumance aux alertes** – En moyenne, les entreprises reçoivent plus de 11 000 alertes de sécurité par jour[3] et manquent d'effectifs pour les traiter.
- **Manque de temps** –Les tâches administratives, manuelles et répétitives prennent trop de temps. Le manque d'intégration des nombreux outils ralentit chaque étape du processus d'analyse.
- **Contexte limité** – Les investigations et la neutralisation des menaces prennent souvent plusieurs jours. En cause : un manque de contextualisation des alertes et de leur pertinence pour l'environnement ciblé, ce qui contraint les analystes à rassembler toutes ces données manuellement.

Ce dont ils ont besoin pour surmonter ces difficultés :

- **Automatisation** des tâches quotidiennes pour se recentrer sur les alertes critiques.
- **Collaboration en temps réel** avec le reste de l'équipe pour synchroniser leurs actions et apprendre les uns des autres.
- **Threat Intelligence contextualisée** pour mieux comprendre la pertinence et l'impact potentiel des menaces.

Figure 1 : Difficultés rencontrées par les analystes SOC

Experts IR

Les experts de la réponse à incident (IR, Incident Responders) ont pour mission de limiter les dégâts. Ils traquent les éventuelles compromissions et, le cas échéant, ouvrent une investigation et stoppent leur propagation. Compte tenu du caractère sensible des compromissions, il est essentiel de rassembler toutes les preuves et de les partager avec tous les acteurs de la sécurité. Les experts IR ont accès à des outils d'endiguement des menaces, comme les outils EDR qui neutralisent l'hôte infecté. Ils confient aux administrateurs de pare-feu le déploiement de politiques destinées à stopper la propagation de la menace sur le réseau. Ils s'appuient également beaucoup sur la Threat Intelligence externe pour se familiariser avec les profils et modes opératoires courants des attaquants, de façon à mieux les combattre le moment venu.

Dans toutes ces missions, les experts IR sont confrontés aux défis suivants :

- **Transfert de connaissances** – Le manque de collaboration entre les équipes fait émerger des failles de sécurité.
- **Gestion des cas** – Dans l'univers de la sécurité, une gestion des cas trop générique se solde par un manque d'efficacité et une documentation trop vague.
- **Manque de Threat Intelligence** – Nombre d'experts IR doivent s'appuyer sur des processus manuels faillibles pour contextualiser les menaces externes, avec pour conséquence des accumulations de retards et une augmentation des risques.

Ce dont les experts IR ont besoin :

- **Gestion complète des cas** pour détailler leurs conclusions et collaborer en temps réel avec les autres acteurs de la sécurité, mais aussi déployer des mesures préventives et de mise en quarantaine à travers toute l'entreprise.
- **Threat Intelligence** pour mieux connaître les attaquants et leurs motivations.

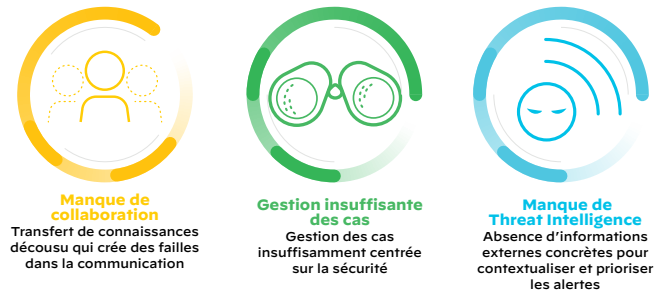

Figure 2 : Difficultés rencontrées par les professionnels IR

3. D'après une étude menée par Forrester Consulting pour Palo Alto Networks en février 2020. À la date de publication de ce document, le rapport n'a pas encore été officiellement publié.

Analystes/Programmes de Threat Intelligence

Les analystes CTI identifient des risques potentiels qui n'ont encore jamais été observés sur le réseau de leur entreprise. Pour contextualiser ces menaces, ils étayent leur propre jugement par des flux de Threat Intelligence de multiples sources externes. D'après une enquête récente du SANS Institute, 49,5 % des entreprises possèdent une équipe ou un programme de Threat Intelligence doté de son propre budget et de ses propres effectifs.[4] Ce chiffre montre l'importance croissante des analystes CTI pour identifier et profiler les attaquants (motivations et modes opératoires). Les équipes de Threat Intelligence transmettent leurs conclusions sur des attaques données, ainsi que des rapports plus généraux sur le champ des menaces, aux équipes SOC et de réponse à incident. Ils aident ainsi à renforcer les capacités de prévention.

Les analystes CTI sont confrontés à plusieurs obstacles :

- **Manque de contrôle** sur les flux de Threat Intelligence, ce qui les oblige à ajuster et évaluer eux-mêmes les indicateurs de compromission (IoC) par rapport à leur environnement.
- **Workflows cloisonnés** causant des dysfonctionnements dans les communications et les intégrations entre outils, équipes et processus de réponse à incident et de Threat Intelligence.
- **Passage à l'action trop lent** car il est tributaire de nombreuses tâches manuelles et doit faire intervenir d'autres équipes.

Ce dont ils ont besoin :

- **Contrôle complet** sur les indicateurs des flux de Threat Intelligence afin de développer leur propre logique et leur propre contrôle de fiabilité en fonction de leur environnement et des besoins de leur entreprise.
- **Collaboration** avec les autres équipes pour leur transmettre rapidement des données contextuelles détaillées et les résultats de leurs dernières recherches.
- **Documentation robuste** pour rassembler leurs conclusions.

Figure 3 : Difficultés rencontrées par les analystes CTI

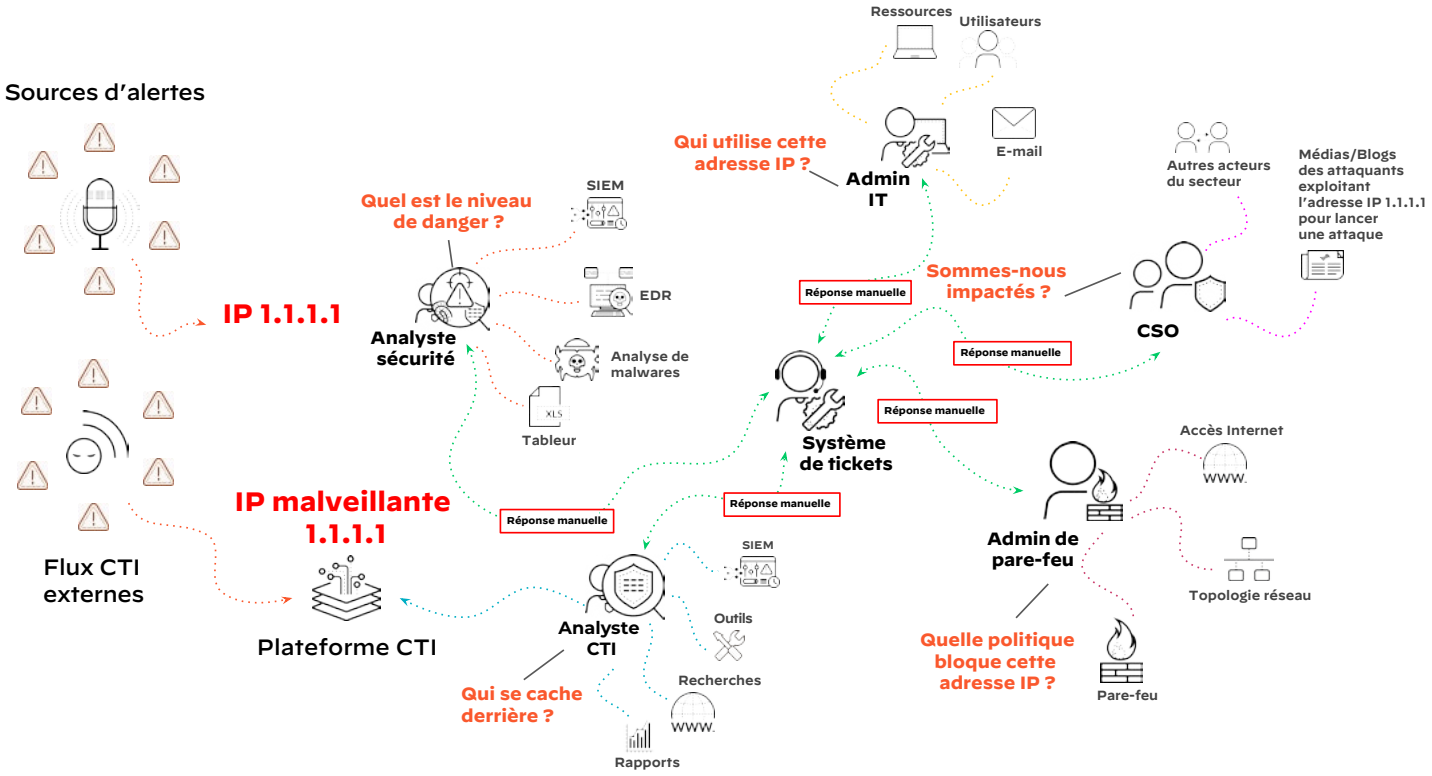

Figure 4 : Vue schématique de la journée type d'un SOC

4. « 2020 SANS Cyber Threat Intelligence (CTI) Survey », SANS Institute, 11 février 2020, https://www.sans.org/reading-room/whitepapers/threats/paper/39395

Le SOAR en renfort

Automatisation, gestion des cas, collaboration en temps réel, intégration de la Threat Intelligence... Les besoins des différentes équipes de sécurité se recoupent. Certes, de nombreux SOC utilisent des plateformes d'orchestration, d'automatisation et de réponse aux incidents de sécurité (SOAR) pour gérer les alertes multi-sources, standardiser leurs processus à l'aide de playbooks et automatiser la réponse face à de multiples scénarios. Mais leur gestion de la Threat Intelligence laisse encore à désirer.

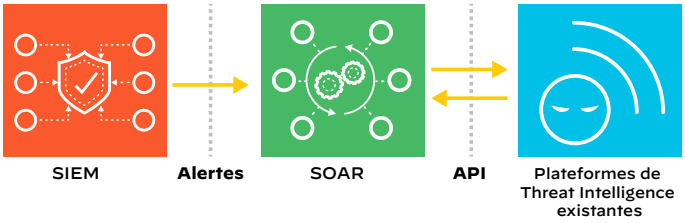

Figure 5 : Cas typique de déploiement cloisonné de plateformes SOAR et TIP

Pour obtenir de la visibilité sur les menaces externes, les équipes de sécurité s'appuient encore sur des plateformes de Threat Intelligence (TIP) cloisonnées. Or, ce manque de coordination des flux CTI les empêche d'automatiser leur réponse. Conscients du problème, les spécialistes plaident pour une convergence des plateformes SOAR et TIP. En effet, les plateformes de Threat Intelligence ne font qu'accroître la complexité dans la mesure où elles agrègent des sources CTI sans les mettre en contexte et sans fournir les fonctions d'automatisation nécessaires pour répondre rapidement à la menace. Il est grand temps que les choses changent.

Besoin d'une plateforme SOAR étendue

Avec sa fonctionnalité Threat Intel Management intégrée, Cortex™ XSOAR s'impose comme la solution. Cette fonctionnalité de gestion de la Threat Intelligence instaure une nouvelle approche en alliant l'agrégation, la notation et le partage d'informations CTI à l'automatisation basée sur des playbooks. Elle offre Ainsi

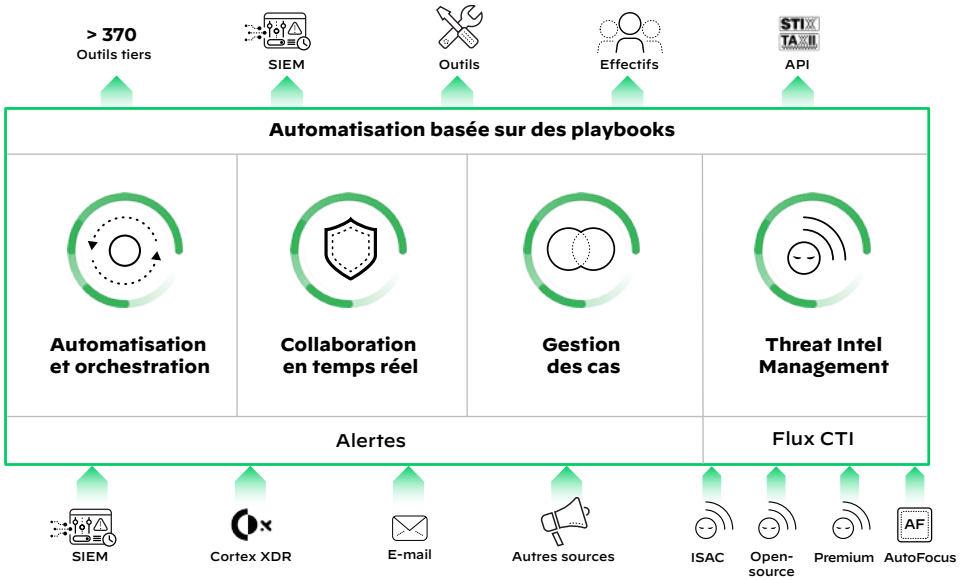

Figure 6 : Automatisation pilotée par des playbooks avec Cortex XSOAR

aux responsables de la sécurité une visibilité instantanée sur les menaces les plus graves pour une réponse adaptée dans toute l'entreprise.

Figure 7 : Avantages de Threat Intel Management

Pour cela, elle unifie la gestion des cas, l'automatisation, la collaboration en temps réel et la gestion CTI native dans la toute première offre SOAR (Security Orchestration, Automation and Response) étendue du marché.

Les avantages de Cortex XSOAR :

- **Fin des tâches manuelles** – Misez sur des playbooks automatisés pour agréger, analyser, éliminer les doublons et gérer des millions d'indicateurs à travers de multiples flux CTI au quotidien. Élargissez et modifiez facilement les systèmes de notation des IoC. Trouvez des fournisseurs dont les indicateurs sont les plus en phase avec votre environnement.
- **Identification des menaces les plus dangereuses** – Intégrez la CTI de sources externes à vos propres incidents afin de prioriser les alertes et de mieux répondre en cas d'attaque. Pour accélérer vos investigations, le service Palo Alto Networks AutoFocus™ vous offre une Threat Intelligence haute-fidélité intégrée. Alimentez vos outils de détection, de surveillance et de réponse en données contextuelles issues de flux CTI méticuleusement sélectionnés.
- **Automatisation de la réponse** – Neutralisez instantanément les menaces sur l'ensemble de votre entreprise. Pour élargir le champ de vos investigations, facilitez le partage des données de Threat Intelligence entre vos équipes internes et avec des organisations externes de confiance.

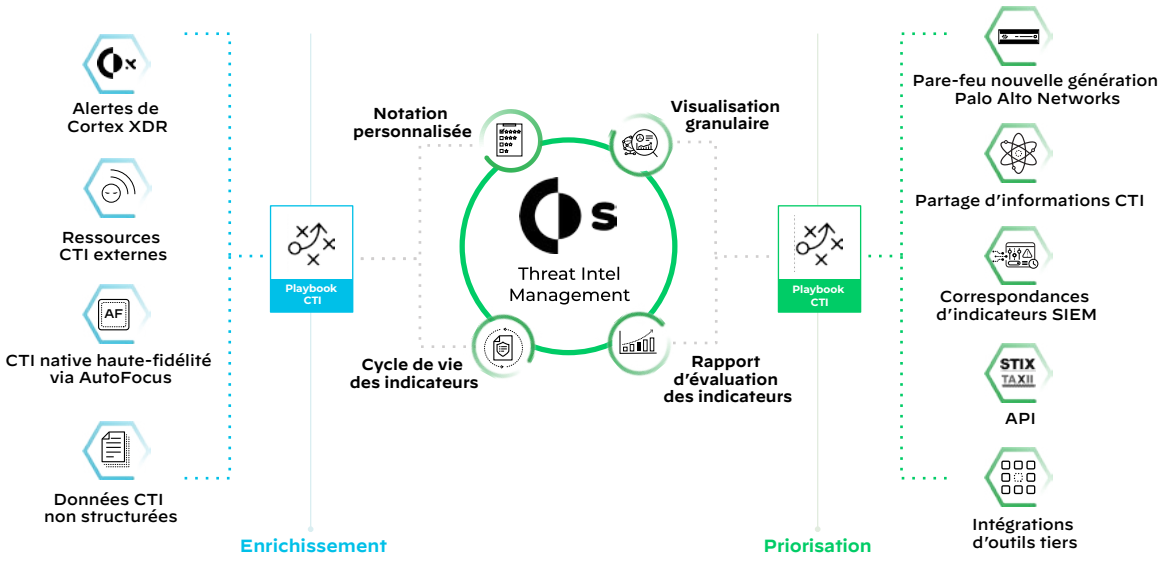

Figure 8 : Enrichissement des données et priorisation de la Threat Intelligence

Cas d'usage : Priorisation des incidents

Les analystes en sécurité traitent des millions d'indicateurs issus de centaines de flux CTI multi-sources. Le problème, c'est que ces indicateurs ne fournissent pas le contexte nécessaire pour prendre les bonnes décisions et agir de façon sûre et ciblée. Quant aux outils à la disposition des analystes, ils sont incapables de traiter les volumes colossaux d'indicateurs générés. Il incombe donc aux analystes d'établir eux-mêmes les priorités en fonction des spécificités de leur environnement. Avec sa fonctionnalité Threat Intel Management intégrée, Cortex XSOAR leur offre une flexibilité et un contrôle complets sur la logique métier qui sous-tend leur système de notation des IoC. L'intégration de plus de 370 outils d'autres fournisseurs permet aux analystes de réagir en temps réel, au fur et à mesure de la transmission des indicateurs.

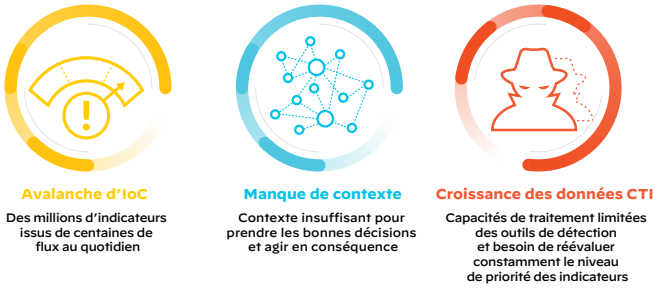

Figure 9 : Problématiques des outils CTI disparates

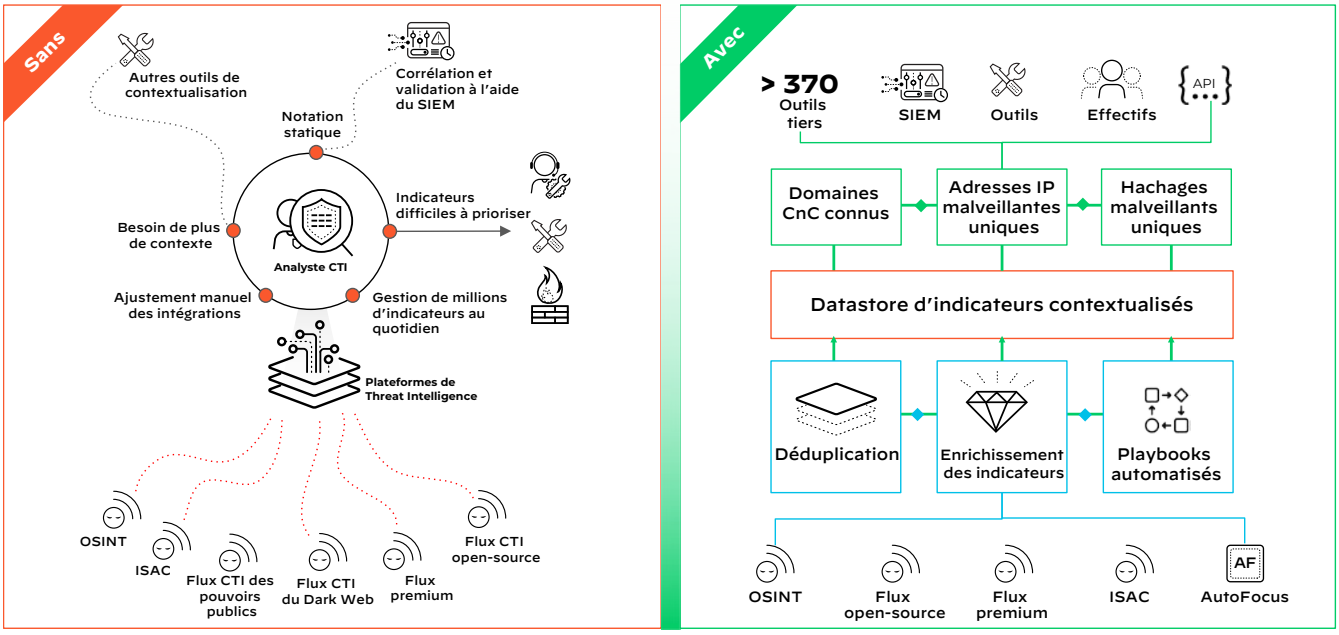

Figure 10 : Gestion CTI avec et sans Cortex XSOAR

Figure 11 : Avantages de Cortex XSOAR pour tout le SOC

Cortex XSOAR : une multitude de cas d'usage

Ouverte et extensible, la plateforme Cortex XSOAR répond à un large éventail de cas d'usage, y compris dans des domaines sortant du champ de compétences des SOC et des équipes de réponse à incident. Les cas d'usage les plus courants figurent le phishing, les opérations de sécurité, le traitement des alertes, l'orchestration de la sécurité du cloud, la gestion des vulnérabilités et la traque des menaces.

À l'avenir, les plateformes SOAR devront intégrer la gestion CTI en natif pour permettre aux équipes de décloisonner les opérations de sécurité et les fonctions de Threat Intelligence. Forts d'une communication plus fluide, d'une hausse de l'efficacité et d'un meilleur accès à l'information, les analystes SOC, les experts IR et les équipes CTI pourront unir leurs efforts pour lutter ensemble contre les menaces avancées.

Toute première plateforme SOAR étendue du marché, Cortex XSOAR redéfinit l'orchestration, l'automatisation et la réponse à incident. Collaboration en temps réel, gestion des cas, Threat Intel Management… elle permet aux équipes de sécurité de mieux tenir le rythme face aux attaquants, aujourd'hui et pour longtemps.

Pour en savoir plus sur Cortex XSOAR, rendez-vous sur notre site web.

paloalto NETWORKS

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

© 2021 Palo Alto Networks, Inc. Palo Alto Networks est une marque déposée de Palo Alto Networks. La liste de nos marques est disponible à la page https://www.paloaltonetworks.com/company/trademarks.html. Toutes les autres marques mentionnées dans le présent document appartiennent à leurs propriétaires respectifs. how-cortex-is-transforming-threat-intelligence-wp-100121-fr