Le SOC de demain se réinvente aujourd'hui

5 étapes et 4 piliers pour transformer vos opérations de sécurité afin de contrer les attaques avancées et d'améliorer l'efficacité de votre SOC

Sommaire

Pression inédite sur les SOC

À l'heure où les acteurs malveillants investissent sans compter dans de nouveaux outils comme le machine learning (ML), l'automatisation et l'intelligence artificielle (IA), les menaces évoluent plus rapidement que les technologies de sécurité censées les combattre. Clé de voûte des SOC traditionnels, les systèmes SIEM (gestion des informations et évènements de sécurité) n'ont pas été conçus dans un souci de précision de la détection. Ils sont par exemple incapables d'exploiter la puissance du ML pour garder le rythme face à des campagnes d'attaque de plus en plus sophistiquées, le tout sur fond de transformation numérique et de migration vers le cloud.

Ainsi, les environnements SOC traditionnels présentent plusieurs problèmes :

- Manque de visibilité et de contexte
- Complexité accrue des investigations
- Accoutumance aux alertes et quantité de « déchets » dans les forts volumes de signalements
- Manque d'interopérabilité des systèmes
- Manque d'automatisation et d'orchestration
- Incapacité à collecter, traiter et contextualiser les données CTI
- Environnements SOC souvent déconnectés du cloud

5 étapes vers la création d'un SOC pérenne

Étape 1 : repensez le modèle SOC manuel

Qu'il soit hébergé sur site ou dans le cloud, le modèle SOC manuel considère les analystes comme les premiers référents. C'est ainsi que ces derniers finissent par examiner des centaines d'alertes par jour, en rassemblant eux-mêmes les informations contextuelles permettant de les trier. Ils passent la majeure partie de leur temps à écarter des faux positifs, tout cela manuellement. Face à un volume croissant d'alertes et à des données provenant de systèmes toujours plus divers, cette approche a fait son temps. La solution ? Automatiser au maximum pour permettre aux analystes de se concentrer sur les évènements présentant un risque élevé.

De même que les avions de ligne peuvent être mis en pilotage automatique, un SOC automatisé peut gérer les tâches peu complexes d'alertes, d'analyse et de neutralisation. La plateforme sous-jacente pilote automatiquement le SOC, améliore ses réponses au fil du temps et fournit des informations et recommandations utiles aux analystes. Ces derniers se libèrent ainsi des tâches répétitives pour mieux se concentrer sur les incidents potentiellement les plus impactants pour l'entreprise. Voilà en quoi consiste notre vision du SOC autonome.

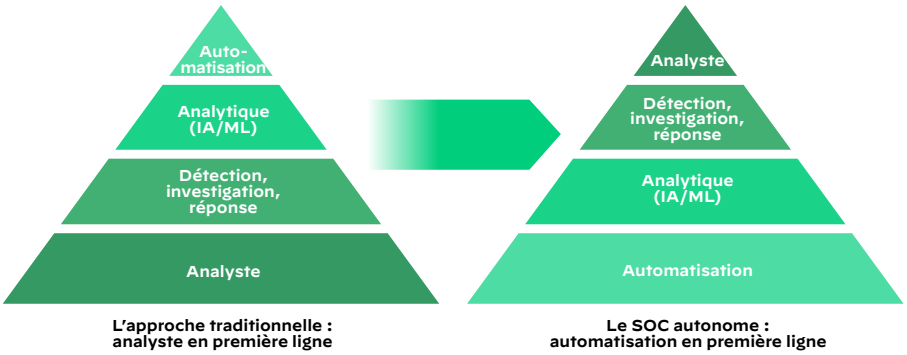

Figure 1. Analyste en première ligne (human-first) vs automatisation en première ligne (machine-first)

Ensemble, les progrès en modélisation et intégration des données et l'automatisation de l'analytique et de la détection libèrent les ingénieurs sécurité du fardeau que représente la création de règles de corrélation personnalisées pour intégrer les données et détecter les menaces. Le SOC moderne applique la data science à d'énormes volumétries de données, en total contraste avec les SecOps d'ancienne génération qui reposaient uniquement sur l'humain et sur des règles dépassées par les nouvelles menaces.

Architectures, utilisation des données, processus… le SOC doit opérer une refonte à tous les niveaux et miser sur une Threat Intelligence actualisée pour neutraliser les nouvelles menaces :

- Intégration, analyse et tri des données élargis et automatisés
- Workflows unifiés qui améliorent la productivité des analystes
- Threat Intelligence intégrée et réponse automatique capables de bloquer les attaques avec une intervention réduite des analystes

Étape 2 : auditez votre environnement pour réduire les risques de sécurité associés à la prolifération d'outils

« La simplicité est la sophistication suprême. » Cette citation attribuée à Léonard de Vinci reste ô combien d'actualité. Entre rachats, fusions et manque de standardisation des produits de sécurité, de nombreuses entreprises doivent composer avec un patchwork de produits de sécurité disparates. En clair, plus il y a d'outils, plus il y a de problèmes. Pour couronner le tout, lorsque les ressources sont hébergées à la fois sur site et dans le cloud, les équipes de sécurité IT sont incapables de protéger l'intégralité de leur surface d'attaque, faute d'un inventaire complet de leurs fournisseurs cloud (CSP), des services fournis par ces derniers ou encore des ressources connectées aux environnements on-prem.

Pour certaines, la prolifération d'outils débute avec le simple déploiement d'une solution spécialisée pour résoudre un problème bien particulier. Or, couplée à la gestion d'un grand nombre d'agents, cette approche fragmentée peut (paradoxalement) exposer davantage les réseaux aux menaces, faute d'interopérabilité et de cohérence dans les configurations des différentes solutions.

Pour réduire l'impact de cette prolifération sur la sécurité, les entreprises peuvent commencer par un audit des entités et systèmes protégés.

Éléments de propriété intellectuelle, informations personnelles des clients… elles peuvent identifier précisément ce qui est protégé et contre quelle menace. Cet inventaire des différentes ressources physiques ou logicielles leur permettra de prioriser la protection des données à haut risque et à forte valeur ajoutée.

Une fois que votre entreprise a dressé un bilan complet des éléments protégés, la prochaine étape consiste à identifier les solutions à même de répondre à plusieurs besoins à la fois. D'après une enquête Enterprise Strategy Group (ESG) menée en 2022 auprès de 280 professionnels IT et de la cybersécurité (en Europe, aux États-Unis, au Canada, en Amérique centrale, en Amérique du Sud, en Afrique, en Asie et en Australie) 22 % des entreprises peinent à gérer la multitude d'outils spécialisés qu'elles utilisent et 66 % des répondants indiquent utiliser jusqu'à 25 solutions[1]. De nos jours, il est inutile de recourir à des capteurs et moyens de contrôle à travers différents outils. D'où la nécessité de consolider autant que possible.

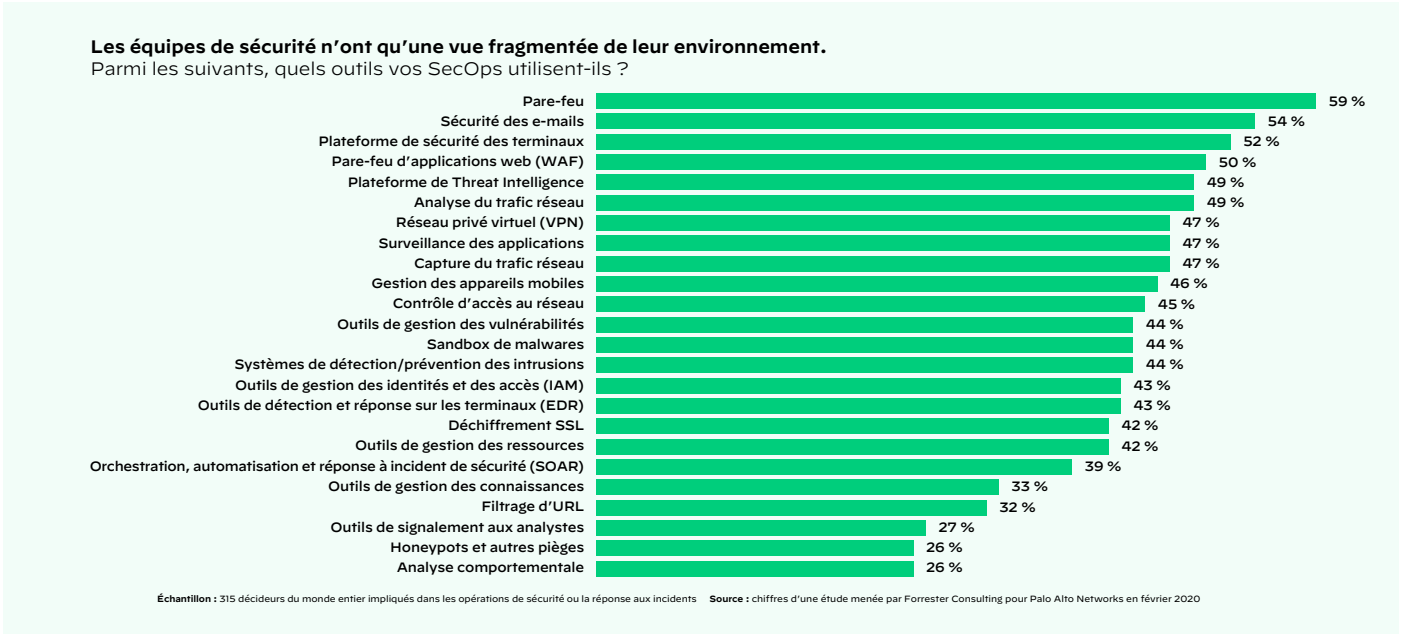

Figure 2. Outils utilisés par les professionnels de la sécurité opérationnelle (données fournies par les sondés dans le cadre d'une étude ESG)

1. « Cybersecurity Process and Technology Survey », ESG, juin 2022, https://research.esg-global.com/reportaction/ESG-ISSACybersecurityProcessAndTechnologySurveyCSR/Toc.

Étape 3 : automatisez les workflows

Avant de commencer, les responsables sécurité doivent se poser plusieurs questions : la configuration ou l'exécution de l'outil nécessite-t-elle une intervention humaine ? Un spécialiste doit-il interpréter ou trier les résultats ? Les tests mobilisent-ils des effectifs ? Ils peuvent alors choisir d'automatiser des tâches de routine répétitives qui, associées au jugement humain, permettent d'accélérer les investigations d'incidents. Si les progrès en machine learning et en intelligence artificielle s'avèrent prometteurs, il demeure crucial de conserver un élément humain pour assurer un transfert de connaissances réciproque, condition sine qua non à une transformation efficace du SOC.

Aujourd'hui, les opérations de sécurité et la réponse aux incidents (IR) reposent sur un trop grand nombre de processus manuels, notamment pour la surveillance d'innombrables flux CTI. En investissant dans des fonctionnalités d'automatisation comme celles des solutions SOAR, vous pouvez faciliter une orchestration transverse à toute la stack de produits pour une IR plus rapide et plus évolutive.

Comment l'automatisation facilite la tâche du SOC (et du NOC)

- **Accélération de la réponse aux incidents** : en automatisant les tâches manuelles de routine, l'automatisation de la sécurité peut diligenter et accroître la précision des réponses aux incidents, tout en améliorant la satisfaction professionnelle des analystes.
- **Standardisation et évolutivité des processus** : grâce à des workflows reproductibles dont les étapes sont clairement définies, l'automatisation de la sécurité peut faciliter la standardisation de l'enrichissement contextuel des incidents et des processus de réponse. Ces derniers gagnent alors non seulement en qualité, mais aussi en évolutivité.
- **Unification des infrastructures de sécurité** : une plateforme SOAR telle que Cortex XSOAR fait office de tissu connectif entre des produits de sécurité auparavant disparates. Les analystes disposent ainsi d'une console centralisée depuis laquelle ils peuvent piloter la réponse aux incidents.
- **Gains de productivité pour les analystes** : avec l'automatisation des tâches de routine et la standardisation des processus, les analystes s'affranchissent des activités rébarbatives pour se recentrer sur des missions plus stratégiques et sur l'amélioration de leur sécurité.
- **Rentabilisation des investissements existants** : grâce à l'automatisation des actions répétitives et à la réduction des allers-retours entre consoles, l'orchestration de la sécurité permet aux équipes de coordonner facilement une multitude de produits et d'extraire davantage de valeur des équipements de sécurité existants.
- **Simplification de la gestion des incidents** : en automatisant le traitement des tickets à l'aide d'intégrations avec des fournisseurs ITSM tels que ServiceNow, Jira et Remedy, ainsi qu'avec des outils de communication comme Slack, les équipes peuvent accélérer la gestion et la résolution des incidents. De plus, les évènements de sécurité peuvent être assignés automatiquement aux acteurs clés concernés sur la base des types d'incidents définis en amont.
- **Renforcement global de la sécurité** : la conjugaison de tous ces avantages se traduit par un renforcement global de la sécurité de l'entreprise et par la baisse correspondante de son exposition au risque.

Automatisation : prévisions sur 1 à 5 ans

Les nouveaux SOC peuvent utiliser l'automatisation immédiatement, tandis que les organisations plus établies devront revoir leurs outils et décider par où commencer. L'objectif pour ces dernières : automatiser 50 % du SOC sur trois ans. Au bout de la cinquième année, la plupart des équipes SOC auront automatisé environ 75 % de leurs activités, mais continueront d'en confier certaines comme la traque des menaces à des ingénieurs.

Étape 4 : renforcez l'efficacité de vos effectifs à l'aide d'une CTI pilotée par ML

Pour transformer le SOC, les équipes de sécurité doivent exploiter tout le potentiel du machine learning en appui et en renfort de leurs moyens humains. L'IA et les outils d'analyse avancée peuvent considérablement accélérer le traitement d'énormes volumes de données dans l'entreprise, avec à la clé des éclairages inestimables sur les évènements de sécurité. En automatisant la détection d'anomalies à travers de multiples sources de données et en ajoutant systématiquement du contexte aux alertes, le machine learning tient aujourd'hui ses promesses d'accélération des investigations et d'élimination des angles morts dans l'entreprise.

À condition cependant d'entraîner les modèles ML à détecter des patterns spécifiques dans les schémas de données, puis de tester et d'optimiser les processus. Les techniques ML permettent de collecter, d'intégrer, d'analyser et d'interroger les données, réduisant considérablement le temps et les connaissances nécessaires à l'humain pour exécuter ces tâches. Le ML facilite également la vie des équipes SOC en les libérant de la recherche de preuves et d'informations contextuelles dans les données générées par de multiples couches de sécurité.

Les techniques de ML supervisé peuvent servir à identifier différents types d'équipements grâce à leurs marqueurs numériques (ordinateurs fixes, serveurs de messagerie, serveurs de fichiers, etc.), puis à profiler leurs comportements spécifiques et à détecter les éventuelles anomalies. De même, le ML permet d'établir des liens de causalité entre différents évènements dans un environnement, laissant au logiciel le soin de décider de la marche à suivre sans aucune intervention humaine. Par exemple, il est possible de signaler des activités comme « malveillantes » sur la base de comportements et d'interactions au sein d'ensembles de données joints, puis de diffuser une décision au reste du réseau avec des instructions explicites (mise en quarantaine, blocage des communications, etc.).

Globalement, les techniques de machine learning couvrent trois grands volets :

- **Intégration** : permettre aux données d'informer sur les évènements.
- **Analyse** : extraire des éclairages sur un sujet donné et établir des prévisions.
- **Automatisation** : accélérer le processus décisionnel humain et automatiser les actions, les workflows et la prise de décision.

Étape 5 : optimisez vos équipes de sécurité

La nécessité d'investir dans des outils et solutions de sécurité ne doit pas faire oublier que l'efficacité d'un SOC passe d'abord et avant tout par le facteur humain. Certes, le machine learning et l'automatisation amélioreront sans aucun doute les temps de réponse, la précision et la remédiation dans son ensemble – surtout du côté des tâches de routine répétitives. Mais toute stratégie de transformation du SOC doit également intégrer le recrutement, la formation et la fidélisation de professionnels de sécurité compétents, notamment des ingénieurs, des analystes et des architectes. En misant sur les technologies d'automatisation, les entreprises peuvent se protéger plus efficacement.

D'après le Bureau of Labor Statistics américain, la population d'actifs salariés dans la cybersécurité devrait augmenter de 31 % entre 2019 et 2029[2] . En outre, selon le National Center for Education Statistics (NCES), le nombre de nouveaux cursus dans cette discipline a augmenté de 33 %, tandis que les offres d'emploi en cybersécurité ont bondi de 94 % ces six dernières années[3].

En plus de pourvoir des postes stratégiques, il est important de sensibiliser les salariés, les sous-traitants voire les partenaires aux enjeux de cybersécurité pour qu'ils contribuent à la prévention des compromissions. Sachant que le vol d'identifiants, le phishing et l'ingénierie sociale jouent sur les faiblesses psychologiques de l'être humain, il est important de sensibiliser tous vos collaborateurs à ces questions pour assurer votre protection sur le long terme. Comme le grand cryptographe et professionnel de la sécurité informatique Bruce Schneier le rappelle : « l'humain représente souvent le maillon faible de la chaîne de sécurité et le principal facteur de défaillance des systèmes de sécurité. »

À chacun son SOC

Pour son SOC, Palo Alto Networks a volontairement choisi de s'affranchir de l'approche à quatre niveaux selon laquelle les analystes de niveau 1 sont chargés de surveiller, de prioriser et d'enquêter sur les alertes SIEM, tandis que les responsables SOC de niveau 4 s'occupent du recrutement, de la stratégie de sécurité et du reporting à la direction. Suivant une démarche plus hybride, l'équipe SOC de Palo Alto Networks applique trois grands principes :

- Maintenir un SOC composé à 80 % de professionnels dotés d'une expérience dans ce type d'environnement
- Former l'équipe SOC dans tous les domaines, y compris le tri des alertes, la réponse aux incidents, le threat hunting, etc.
- Prévoir un budget annuel de formation conséquent pour tous les analystes

Si nous suivons ces principes, c'est pour mieux atteindre nos objectifs :

- Maintenir une équipe agile, capable de jongler entre les responsabilités (et les niveaux de compétences)
- Garantir la continuité d'activité
- Offrir un environnement plus attractif et réduire les risques de burnout
- Promouvoir la formation continue
- Fournir une meilleure couverture à l'aide d'une équipe plus compacte, mais dotée des bonnes technologies

2. « Occupational Outlook Handbook, Information Security Analysts », U.S. Bureau of Labor Statistics, 9 avril 2021, https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.
3. « CISO Benchmark Study », Cisco, mars 2019, https://ebooks.cisco.com/story/anticipating-unknowns/page/6/6.

ASM, SOAR et XDR : les piliers d'un SOC transformé

Pour poser les bases d'un SOC résilient et efficace, vous devez dans un premier temps suivre les cinq étapes que nous venons d'évoquer, puis envisager ces quatre technologies clés pour optimiser votre stratégie opérationnelle de sécurité.

Pilier n° 1 : cernez votre surface d'attaque pour mieux gérer les risques

La transformation du SOC passe notamment par une fonction solide de gestion des risques. Pour établir le contexte d'un plan ou d'une stratégie de gestion du risque, quel que soit son niveau de sophistication, il est logique d'identifier d'abord ce que vous devez protéger contre les attaques. Vous pourrez ainsi prioriser les éléments exposés et déterminer les mesures à prendre afin d'éliminer chaque risque.

Une bonne fonction de gestion des risques, c'est d'abord une capacité à bien cerner sa surface d'attaque. Après tout, on ne peut protéger que ce qu'on voit.

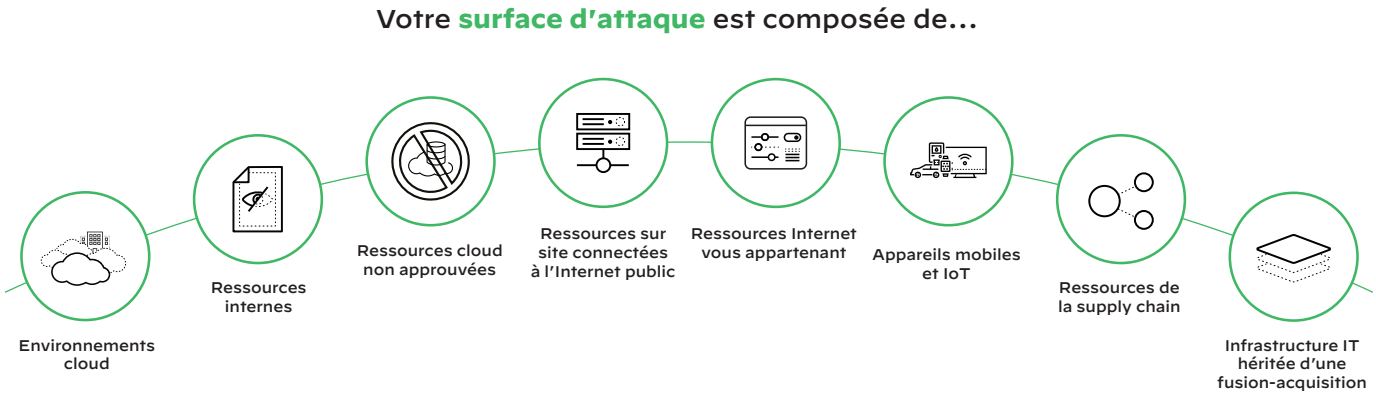

Figure 3. Éléments de la surface d'attaque

Que vous choisissiez de déployer des solutions de gestion de la surface d'attaque (ASM) ou de réaliser des évaluations proactives comme les tests d'intrusion et les analyses de vulnérabilité, une chose est sûre : vous devrez identifier les exigences produits et opérationnelles pour trouver la meilleure option. Parmi ces exigences figurent des fonctionnalités, des capacités et des critères d'évaluation pour vous aider à dresser le cahier des charges de votre outil ou solution ASM.

Dans le *rapport Cortex Xpanse 2021 sur la surface d'attaque*, nous avons présenté les principales conclusions de notre analyse de la surface d'attaque publique de certaines des plus grandes entreprises de la planète. De janvier à mars, l'équipe de recherche Cortex Xpanse a surveillé les scans de plus de 50 millions d'adresses IP rattachées à 50 entreprises mondiales. L'objectif ? Mesurer à quelle vitesse les hackers repèrent les systèmes vulnérables et rapidement exploitables.

D'après ce rapport, près du tiers des vulnérabilités détectées sont dues à des problématiques liées au protocole RDP (Remote Desktop Protocol)[4], dont l'usage a littéralement explosé au début de l'année 2020, avec la migration massive vers le cloud et la généralisation du télétravail provoquées par la pandémie de Covid-19. Mais ce n'est pas tout :

- **Des attaquants toujours à l'œuvre**. Engagés dans un interminable jeu du chat et de la souris, les attaquants effectuent un nouveau scan toutes les heures, tandis que la même opération peut parfois prendre des semaines aux entreprises mondiales[5].
- **De nouvelles vulnérabilités rapidement exploitées**. Entre janvier et mars, les attaquants ont démarré un scan dans les 15 minutes suivant la publication d'une nouvelle CVE (Common Vulnerabilities and Exposures). Ils ont également réagi dans les cinq minutes qui ont suivi la publication du correctif de la vulnérabilité zero-day découverte dans Microsoft Exchange Server[6].

4. « *2021 Cortex Xpanse Attack Surface Threat Report* », Palo Alto Networks, mai 2021, https://www.paloaltonetworks.com/engage/cortex-xpanse-general/xpanse-attack-surface-threat-report-2021.
5. Ibid.
6. Ibid.

- **Une manne de systèmes vulnérables**. Les entreprises mondiales présentent une nouvelle exposition majeure toutes les 12 heures, soit deux fois par jour en moyenne. Accès à distance non sécurisé (RDP, Telnet, SNMP, VNC, etc.), serveurs de base de données mal configurés, exposition à des vulnérabilités zero-day (Microsoft Exchange, équilibreurs de charge F5, etc.)... les cas sont multiples[7].
- **Le cloud en première ligne**. Les environnements cloud représentent 79 % des problématiques de sécurité les plus critiques observées dans les entreprises mondiales (contre 21 % pour les environnements sur site), ce qui souligne encore une fois le risque inhérent aux services basés/hébergés dans le cloud[8].

À retenir : les progrès des technologies de scan permettent aux acteurs malveillants de repérer les vecteurs d'attaque rapidement et facilement, en leur révélant des 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 évalue continuellement la surface d'attaque externe de votre entreprise.

Pilier nº 2 : SOAR – Orchestrez toute votre stack produit pour une réponse efficace aux incidents

Lorsqu'on parle du SOAR, on pense le plus souvent à des solutions qui exécutent un playbook de workflows de réponses automatisées. Pourtant, une stratégie SOAR efficace fait plus que recourir à l'automatisation pour rationaliser et éliminer les tâches manuelles. Il est possible d'orchestrer ces workflows via des intégrations à d'autres technologies et de les automatiser afin d'atteindre les objectifs recherchés. Par exemple :

- Tri des alertes
- Qualification des menaces
- Réponse aux incidents
- Gestion et organisation de la Threat Intelligence
- Suivi et gestion de la conformité

Une solution SOAR complète, qui couvre les moindres aspects de la gestion des incidents, doit proposer des intégrations clé en main aux outils courants des SOC, des playbooks de bonnes pratiques pour faciliter l'automatisation des workflows, ainsi qu'une gestion intégrée des cas et des outils de collaboration en temps réel pour encourager la participation de différentes équipes aux investigations.

Enfin et surtout, cette plateforme doit centraliser la Threat Intelligence (interne et externe) pour permettre une corrélation automatique des indicateurs, des incidents et de la CTI. Ainsi, les analystes sécurité et les équipes de réponse aux incidents auront accès à des informations enrichies sur les attaquants et leurs techniques.

Les solutions SOAR ont vocation à devenir le plan de contrôle de l'environnement SOC de demain, et potentiellement celui de différentes fonctions opérationnelles de sécurité. Dans cette optique, elles commencent à intégrer directement la Threat Intelligence, la gestion des vulnérabilités, etc., et étendent l'automatisation à des cas d'usage hors SOC. De leur côté, les fournisseurs de solutions de sécurité leaders intègrent également des fonctionnalités SOAR et de gestion des incidents à leurs produits, qui sont préprogrammés et optimisés pour cette technologie.

À retenir : une solution SOAR doit pouvoir définir des priorités et créer des workflows rationnels pour les évènements de sécurité nécessitant une intervention humaine minimale. Pour plus d'efficacité, une plateforme SOAR doit automatiser les processus, mais aussi centraliser et orchestrer tous les produits du SOC pour réduire la complexité des investigations en cas d'incident.

7. *Rapport Cortex Xpanse 2021 sur la surface d'attaque*
8. Ibid.

Palo Alto Networks lève le voile sur l'automatisation de sa sécurité

Le SOC de Palo Alto Networks utilise Cortex XSOAR pour réduire les tâches laborieuses et répétitives évoquées dans ce livre blanc. Ci-dessous, vous trouverez un aperçu du temps gagné grâce à l'automatisation pour le mois de février 2021.

Type d'automatisation	Total	Heures gagnées par les analystes sécurité
Enrichissement d'artefacts	2 498	1 457
Déduplication	10 063	821
Utilisateur de messagerie	464	193
Re-imaging de machine	8	4
Réinitialisation de mot de passe	8	4
Workflows 100 % automatisés	57	29
Autres tâches*	*	133

Tâches laborieuses et répétitives qui rebutent les effectifs du SOC

*Métriques PhishMe, tâche liée au flux RSS, tâche de mise à jour de contenu, métriques et missions de traque, création de tickets de surveillance journalière et requête pull de ticket JIRA

Total des heures gagnées en un mois

Le XSOAR automatise la charge de travail de 16,5 ETP

Figure 4. Principaux gains de temps liés à l'automatisation

Pilier n° 3 : XDR – Évolution logique de l'EDR

« XDR », abréviation de « eXtended Detection and Response » (ou « détection et réponse étendues » en français), est un terme utilisé pour la première fois en 2018 par Nir Zuk, CTO et co-fondateur de Palo Alto Networks. La principale mission des plateformes XDR : bloquer les attaques plus efficacement, détecter les techniques et tactiques des attaquants, et aider les équipes SOC à mieux répondre aux menaces qui nécessitent une investigation. Le principe consiste à consolider des données de télémétrie disparates issues de sources multiples (voire complémentaires) comme les systèmes EDR, l'analyse du trafic réseau (NTA), l'analyse du comportement des utilisateurs et des entités (UEBA) et les indicateurs de compromission (IoC).

Le XDR allie des fonctionnalités SIEM d'intégration, de normalisation et de corrélation des alertes à des outils SOAR d'investigation et de remédiation automatisées.

En consolidant des outils cloisonnés, en rationalisant les processus et en améliorant la visibilité pour les investigations et la détection des menaces, le XDR permet aux équipes de sécurité de bloquer les attaques plus efficacement. Ces équipes peuvent éliminer les angles morts, réduire les temps d'investigation et, au bout du compte, améliorer l'issue des incidents de sécurité. Et puisque la plateforme 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 neutraliser les attaques à la racine.

Le XDR séduit par ses visualisations simplifiées d'attaques complexes tout au long de la kill chain, ses automatisations plus robustes, ses fonctions d'analyse avancées et son machine learning. Le besoin de meilleures intégrations aux outils tiers, d'analyses plus pointues et d'une réponse plus rapide vient également renforcer l'attrait de ces plateformes, attrait somme toute logique dans un monde où les entreprises utilisent jusqu'à 45 outils de sécurité en moyenne et doivent jongler entre pas loin de 19 outils pour répondre à un incident[9].

Il ne suffit pas de sécuriser les terminaux. Les entreprises doivent consolider ces données avec celles du réseau et du cloud sur un référentiel centralisé, puis les soumettre à des fonctions d'analyse approfondies.

Le XDR comble les lacunes des outils de détection et de réponse

Jusqu'à l'arrivée des plateformes XDR, la corrélation de données télémétriques des terminaux avec d'autres données d'évènements passait par le filtrage de gros volumes de données et de faux positifs qui encombraient les tableaux de bord des analystes. Laborieuse, la consolidation d'évènements disparates repose en effet sur la capacité d'analystes chevronnés à ne faire remonter que les alertes pertinentes. Ainsi, les équipes SOC perdaient parfois leur temps à vérifier des alertes peu fiables aux dépens des investigations sur des alertes légitimes.

Face à cet incessant « jeu de la taupe » version sécurité, et dans un contexte de sophistication et d'intensification des attaques, certaines équipes de sécurité visionnaires commencent déjà à récolter les fruits d'une approche XDR de l'architecture de sécurité.

À retenir : Cortex XDR s'adapte à diverses configurations d'architecture SecOps. La solution fournit aux entreprises des capacités de prévention, de détection et de réponse incluant des fonctionnalités EDR/EPP, idéales pour les organisations qui n'ont pas besoin de toute la panoplie SIEM. Autre option : Cortex XDR peut également être déployé en complément d'un outil SIEM pour fournir ces mêmes fonctionnalités EDR/EPP, avec en prime des capacités plus ciblées de prévention, de détection et de réponse aux incidents.

9. « *2020 Cyber Resilient Organization Report* », IBM Security, juin 2020 https://www.ibm.com/account/reg/us-en/signup?formid=urx-45839.

Pilier nº 4 : XSIAM – Plateforme SOC pilotée par l'IA qui accélère la réponse et anticipe les menaces

Les solutions SIEM sont conçues pour faciliter la gestion des alertes et des journaux. Le problème, c'est qu'elles dépendent fortement de l'humain et de capacités d'analyse et d'automatisation mal intégrées pour détecter et répondre aux incidents. Des années durant, les SecOps ont continué de recourir à ces outils fortement mobilisateurs en moyens humains, avec un renforcement de la sécurité somme toute marginal. Face à des menaces toujours plus sophistiquées, nous devons repenser de manière radicale la manière dont nous protégeons les entreprises, notamment grâce à l'IA.

Avec Cortex XSIAM, les professionnels de la sécurité délèguent la gestion des informations et des évènements aux outils d'automatisation pilotés par l'IA. Il ouvre ainsi une nouvelle ère où les alertes de sécurité générées par vos systèmes sont organisées et traitées automatiquement.

XSIAM unifie toutes les fonctionnalités au sein d'une solution holistique et automatisée. Il s'inscrit ainsi en complément des outils SIEM et autres produits spécialisés pour devenir le centre névralgique des activités du SOC. Au menu : centralisation des données, corrélation intelligente, détection basée sur les analyses, gestion des incidents, Threat Intelligence, automatisation, gestion de la surface d'attaque… sans oublier une expérience utilisateur intuitive, résolument axée sur l'automatisation.

À retenir : la plateforme « automation-first » Cortex XSIAM exploite toute la puissance du machine learning pour renforcer la sécurité et transformer radicalement les SecOps. Alliée incontournable du SOC de demain, elle permet de consolider différents produits sur une plateforme unique et intégrée, garante d'une diminution des coûts, d'une meilleure productivité et d'une expérience intuitive pour vos analystes.

Cortex XSIAM, Cortex XDR, Cortex XSOAR et Cortex Xpanse

Soyons réalistes. La plupart de nos clients et prospects ne se voient pas jouer aux intégrateurs système. Et ils ne sont pas non plus très friands de tâches manuelles répétitives. Or, la maintenance d'un patchwork d'outils cloisonnés nécessite beaucoup de temps et de moyens. Ces solutions disparates peuvent accroître la complexité et nuire à la visibilité indispensable aux analyses des SOC modernes, ce qui ne peut qu'entraver l'efficacité de la sécurité.

À défaut de pouvoir allonger les journées, nous aidons nos clients à optimiser leur stratégie, à réduire leur TCO et à intégrer plus d'outils tiers que les autres fournisseurs de solutions de sécurité. Au-delà de ces avantages, nous équipons les analystes sécurité des outils dont ils ont besoin pour protéger leurs données et ainsi se concentrer sur leurs priorités, plutôt que sur les tâches de routine.

Pour entamer ou accélérer la transformation de votre SOC, vous pouvez déployer la suite de produits Cortex selon vos besoins. Cortex XSIAM, Cortex XDR, Cortex XSOAR et Cortex Xpanse fonctionnent en synergie pour démultiplier l'efficacité de vos opérations de sécurité. Les avantages sont aussi immédiats que convaincants.

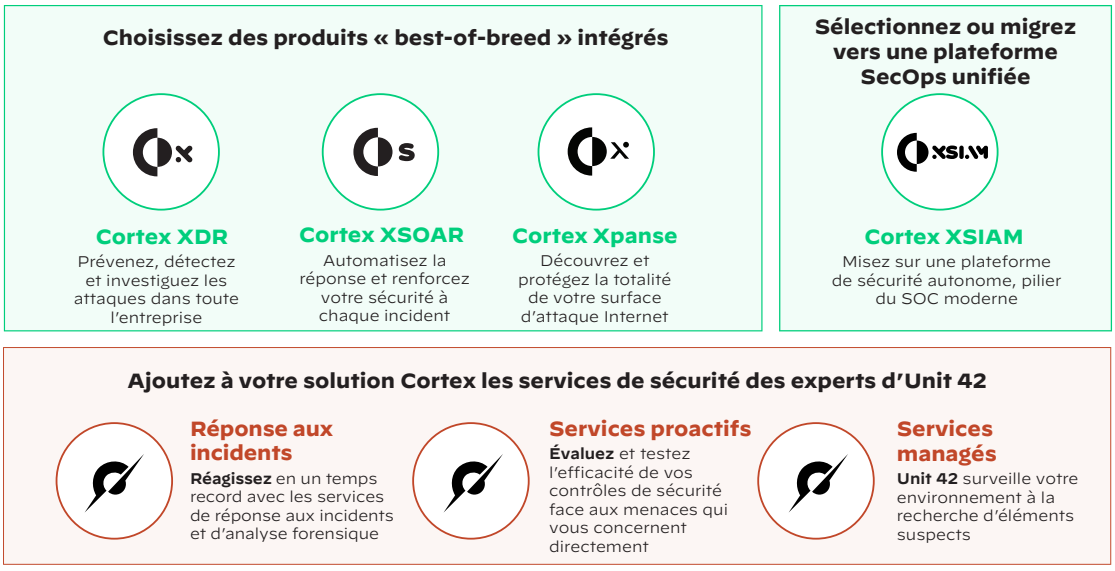

Figure 5. Les solutions Palo Alto Networks vous aident à créer un SOC pérenne

Cortex XSIAM

Cortex® XSIAM™ intègre en natif des capacités XDR, SOAR, CTI, ASM et SIEM pour un SOC plus autonome. Cet outil de gestion étendue de l'automatisation et des informations de sécurité permet de consolider différents produits sur une plateforme unique et intégrée, garante d'une diminution des coûts, d'une meilleure productivité et d'une expérience intuitive pour vos analystes.

Cortex XDR

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, grâce à des fonctions de détection et de réponse qui 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 XSOAR

Cortex® XSOAR™ intègre une plateforme centralisée pour la gestion de bout en bout du cycle de vie des processus opérationnels de sécurité et des incidents. Les équipes de sécurité de toutes tailles peuvent bénéficier de plus de 900 packs de contenu d'intégration préconfigurés, d'une gestion robuste des cas centrée sur la sécurité et d'outils de collaboration en temps réel pour orchestrer, automatiser et accélérer la réponse aux incidents et tout workflow ou processus de sécurité dans leur environnement. En outre, grâce à une gestion intégrée de la Threat Intelligence, ces équipes ont accès à un référentiel central sur les menaces. Elles peuvent non seulement corréler automatiquement les informations sur les menaces aux incidents, mais aussi opérationnaliser la CTI grâce à cette automatisation.

Cortex Xpanse

Cortex® Xpanse™ dresse un inventaire exhaustif des erreurs de configuration et des ressources cloud d'entreprise connectées à Internet à l'échelle mondiale pour cerner, évaluer et diminuer continuellement votre surface d'attaque externe, signaler les communications suspectes, évaluer les risques liés aux fournisseurs, ou encore déterminer le niveau de sécurité d'une cible de rachat.

Intégration et interopérabilité de bout en bout

Les synergies permanentes à travers l'écosystème Cortex permettent aux équipes SOC de neutraliser plus facilement les menaces :

- Cortex XSIAM unifie les fonctions essentielles du SOC (EDR, XDR, SOAR, ASM, UEBA, TIP, ITDR et SIEM). Grâce à un modèle data axé sur la sécurité et à ses capacités de machine learning, il automatise l'intégration, l'analyse et le tri des données pour répondre à la plupart des alertes. Les analystes peuvent ainsi se consacrer aux missions qui nécessitent une intervention humaine.
- Cortex XDR et Cortex Xpanse fournissent des outils de détection et une visibilité optimale sur la surface d'attaque Internet, les terminaux, le cloud et le réseau.
- Cortex XDR et Cortex Xpanse exploitent les fonctionnalités d'orchestration, d'automatisation et de réponse de Cortex XSOAR.
- Cortex XSOAR utilise Cortex XDR et Cortex Xpanse pour piloter les workflows orchestrés à l'aide de fonctionnalités de détection et d'alertes ultrafiables.

Cortex réinvente les SecOps pour neutraliser les attaques

Fidèle à ses missions d'innovation au service de la protection des ressources stratégiques de ses clients, Palo Alto Networks s'engage à mettre sur le marché les solutions de sécurité les plus avancées. N'attendez pas pour les découvrir et n'hésitez pas à nous contacter pour échanger. Nous serons ravis de vous accompagner sur la voie de la transformation de votre SOC.

Pour en savoir plus, lisez nos pages produits :

- Cortex Xpanse
- Cortex XSOAR
- Cortex XDR
- Cortex XSIAM
- Unit 42

Une démo vous intéresse ? Prenez rendez-vous dès aujourd'hui.

paloalto NETWORKS

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