L'état du SOAR, rapport 2020

Quatrième édition de notre enquête annuelle sur la réponse à incident

Sommaire

Avant-propos

Bienvenue dans cette quatrième édition de notre rapport annuel sur l'état du SOAR. Comme chaque année, nous avons interrogé des centaines de professionnels de la sécurité exerçant au sein de grandes entreprises dans des rôles et des secteurs divers et variés. Ils nous ont fait part de leur point de vue sur la réponse à incident (IR, Incident Response) aujourd'hui et nous ont éclairés sur la place actuelle et future des technologies d'orchestration, d'automatisation et de réponse aux incidents (SOAR) dans leurs stratégies et opérations de sécurité.

Les faits marquants de ce rapport :

- **Les analystes sécurité doivent faire face à des cybermenaces de plus en plus graves**. À l'heure où 63 % des entreprises sont aux prises avec des groupes à la solde d'États, la variété des attaques n'a d'égale que leur ampleur.
- **Le processus IR accable les équipes**. Les analystes doivent surveiller 6,8 flux de Threat Intelligence en moyenne et traiter manuellement un volume excessif d'alertes. La réponse à incident mobilise de nombreux systèmes, avec des workflows transverses à de nombreuses fonctions de l'entreprise.
- **La Covid-19 aggrave la situation**. La pandémie exacerbe les problématiques IR, alors que de nouvelles menaces font leur apparition et que la collaboration entre les membres des équipes SOC se complique. Ainsi, 40 % des sondés estiment que la pandémie de Covid-19 augmente la pression sur leurs ressources.
- **Les analystes savent ce qu'il leur faut pour améliorer la réponse à incident**. Ils veulent :
  - » Davantage d'automatisation pour accélérer la réponse et réduire le stress lié aux opérations manuelles. À cet égard, 65 % des entreprises interrogées feront de l'automatisation IR une priorité absolue au cours des 12 prochains mois.
  - » Une intégration des outils SOC aux systèmes d'autres fournisseurs pour interconnecter facilement d'autres départements et processus IR. En effet, 30 % des sondés souhaitent une plateforme commune pour une réponse à incident transfonctionnelle.
  - » Davantage de playbooks, y compris de sources indépendantes, et une plateforme d'échange communautaire pour bénéficier de l'expertise d'autres équipes. Ainsi, 78 % des personnes interrogées aimeraient s'appuyer sur un cadre et une communauté d'intérêts communs pour le partage de playbooks et d'intégrations.
  - » Intégration de la Threat Intelligence aux outils SecOps pour réduire le nombre de flux à surveiller et se concentrer uniquement sur les menaces graves. À cet égard, 52 % des sondés déclarent que leurs workflows SecOps bénéficieraient d'une meilleure intégration des flux CTI.
- **Les équipes SOC ont besoin de réduire leur accoutumance aux alertes**. Elles attendent un outil capable de diminuer le volume d'alertes ou d'accélérer leur gestion.
- **Le SOAR peut résoudre nombre de ces problématiques**. Cette technologie permet aux équipes SOC de gagner du temps, d'accélérer le tri des alertes et de réduire les étapes du processus IR.
  - » D'après notre enquête, 45 % des équipes SOC utilisent le SOAR pour la détection et la réponse à incident. Parmi les autres cas d'usage actuels, citons la priorisation des vulnérabilités (37 %), le contrôle de conformité (30 %) et les audits de sécurité (30 %).
  - » À l'avenir, les équipes SOC comptent bien appliquer les technologies SOAR à la gestion de l'IoT (23 % des sondés), aux workflows des Red Teams (17 %) et à la sécurité du cloud (38 %).
  - » En outre, 43 % des entreprises interrogées prévoient d'augmenter leurs dépenses consacrées aux outils SOAR en 2020. Elles sont 24 % à vouloir implémenter cette technologie dans les 12 prochains mois.
  - » La pandémie de Covid-19 a conduit 47 % des sondés à recourir davantage aux technologies SOAR.

Introduction

Ce rapport présente les résultats d'une enquête annuelle réalisée auprès de professionnels de la sécurité. Il se penche sur les tendances en matière de réponse à incident (IR) et sur l'intérêt des technologies d'orchestration, d'automatisation et de réponse aux incidents (SOAR) pour le processus IR. Les personnes interrogées occupent différents rôles dans de grandes entreprises de secteurs très variés.

Les centres opérationnels de sécurité (SOC) et leurs analystes sont débordés. Comme le montre la figure 1, ces équipes doivent sans cesse repousser des attaques aussi diverses que variées. Par exemple, 86 % des sondés déclarent avoir fait face à des attaques de phishing au cours des 12 derniers mois. Ils sont par ailleurs 63 % à avoir dû détecter et neutraliser rapidement des attaques par malware. Et ils sont enfin respectivement 51 %, 39 % et 37 % à avoir été aux prises avec des détournements de mots de passe, des attaques par déni de service (DoS) et des ransomwares.

Dans son rapport 2020 sur les grandes tendances de la gestion des risques et de la sécurité, Gartner explique que « les attaquants sont de plus en plus rapides et créatifs. Ils continueront à multiplier les modes opératoires contre des cibles de plus en plus diverses pour atteindre des objectifs de plus en plus variés. D'où la difficulté croissante à anticiper et prévenir les incidents de sécurité. »[1]

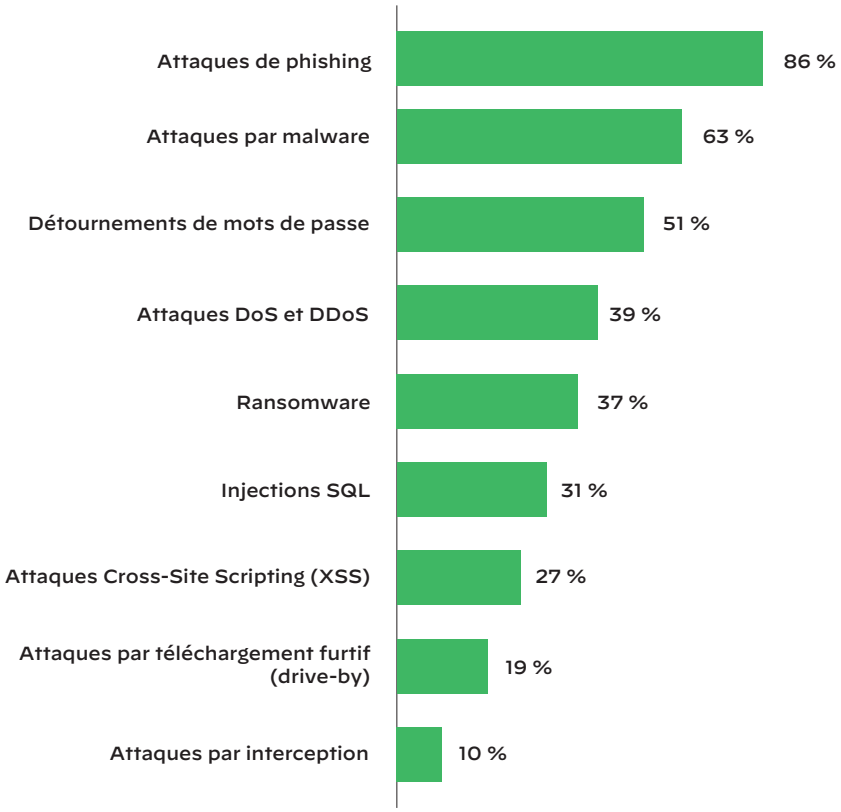

Figure 1 : Attaques subies par les entreprises des sondés ces 12 derniers mois

Au cours des 12 derniers mois, pas moins de 63 % des entreprises interrogées affirment avoir été la cible d'attaquants suspectés d'être en mission commandée pour des États. Pour parvenir à leurs fins, ces groupes disposent d'une puissance de frappe qui va du phishing aux attaques DDoS, en passant par les ransomwares et les injections SQL. La pandémie de Covid-19 aggrave également la situation (cf. « Impact de la Covid-19 sur la réponse à incident »).

Le SOAR en bref

Le SOAR désigne une catégorie de technologies SecOps qui permet aux équipes SOC de gérer plus efficacement le processus IR. La mission première des solutions SOAR est d'automatiser les workflows de réponse à incident, qui restent manuels dans une très grande mesure. Cette technologie s'est également développée pour aider les analystes SOC à orchestrer des processus IR transverses à différents systèmes comme les solutions de gestion des informations et événements de sécurité (SIEM) et les plateformes de gestion des cas.

Les solutions SOAR sont conçues pour accélérer et améliorer l'efficacité de la réponse à incident tout en fournissant des données forensiques détaillées et exploitables. Elles offrent des fonctionnalités essentielles aux équipes SOC :

- **L'orchestration** consiste à relier les fonctions de différents systèmes en vue de servir les objectifs du workflow IR. Généralement basée sur des API standards, elle permet notamment à la solution SOAR de générer des notifications par e-mail, de chercher les menaces et de créer des tickets de service, même si ces fonctions sont assurées par différents systèmes.
- **L'automatisation** consiste à configurer des machines pour leur confier des tâches autrefois manuelles. Dans l'univers du SOAR, elle est surtout vue comme un complément à l'humain, et non comme une alternative. L'automatisation élimine la plupart des tâches répétitives, lassantes et épuisantes pour les analystes SOC, avec à la clé une accélération des investigations et des réponses à incident.
- **Les playbooks** désignent des suites d'actions prédéfinies qu'une équipe SOC peut déployer dans sa solution SOAR afin de neutraliser un type de menace donnée. Par exemple, si l'équipe identifie une vulnérabilité CVE connue et dispose du playbook correspondant, elle peut tout simplement exécuter cette partition plutôt que de devoir partir de zéro. Son processus IR est alors plus rapide et plus efficace.
- **Le reporting et la visualisation de données** dans la solution SOAR permettent aux équipes SOC d'identifier, de corréler, de trier et de documenter les incidents efficacement et de façon intuitive, y compris les étapes du processus IR et ses résultats.

1. Peter Firstbrook, Neil MacDonald, Lawrence Orans, Mario de Boer, Katell Thielemann, Bart Willemsen, Akif Khan, et Michael Kranawetter, « Top Security and Risk Management Trends » (ID G00466211), Gartner, 27 février 2020, https://www.gartner.com/en/documents/3981492/top-security-and-risk-management-trends

Réponse à incident : un tissu de compétences, de processus, d'outils et de données

Chaque entreprise interrogée suit ses propres workflows IR. Toutefois, dans l'ensemble, ce processus se divise en quatre volets :

- **Enrichissement et ingestion des incidents** : le SOC collecte des informations détaillées sur un incident de sécurité donné, puis y associe d'autres données pour une meilleure lecture de la situation. Par exemple, si une attaque donnée se rapporte à une CVE particulière, le processus d'enrichissement pourra consister à ajouter des informations sur cette faille, les systèmes qu'elle touche et la manière d'y remédier.
- **Gestion des cas** : chaque incident devient, ou devrait devenir, un cas à gérer par le SOC et d'autres équipes internes (opérations IT (ITOps), opérations réseau (NetOps), service juridique, ressources humaines, etc.)
- **Investigation** : en cas d'incident, les analystes sécurité doivent enquêter pour déterminer la meilleure réponse à apporter et prévenir d'autres attaques du même type à l'avenir. Ce volet repose sur les connaissances et l'expérience des analystes, assistés par des systèmes qui détaillent la cause de l'incident.
- **Réponse et neutralisation** : cette phase de la réponse à incident consiste à implémenter les mesures définies lors de l'investigation.

Tous ces volets se recoupent et se renforcent mutuellement. La phase d'enrichissement facilite l'investigation, qui elle-même sous-tend une réponse effective. Les outils et pratiques de gestion des cas assurent la fluidité du workflow et tiennent tous les acteurs informés, du moins en théorie.

Impact de la Covid-19 sur la réponse à incident

Parmi les sondés, 60 % déclarent que la pandémie a fait émerger de nouveaux modes de travail, y compris le télétravail pour les salariés et les membres de l'équipe SOC. Pour 42 % d'entre eux, cette crise sanitaire a accentué le besoin d'outils de collaboration virtuelle, tandis que 40 % estiment qu'elle intensifie la pression sur les ressources. C'est sans doute pourquoi 24 % affirment que la Covid-19 accentue le besoin d'automatisation, tandis que 23 % citent l'adoption de nouveaux services cloud comme étant directement liée à la pandémie.

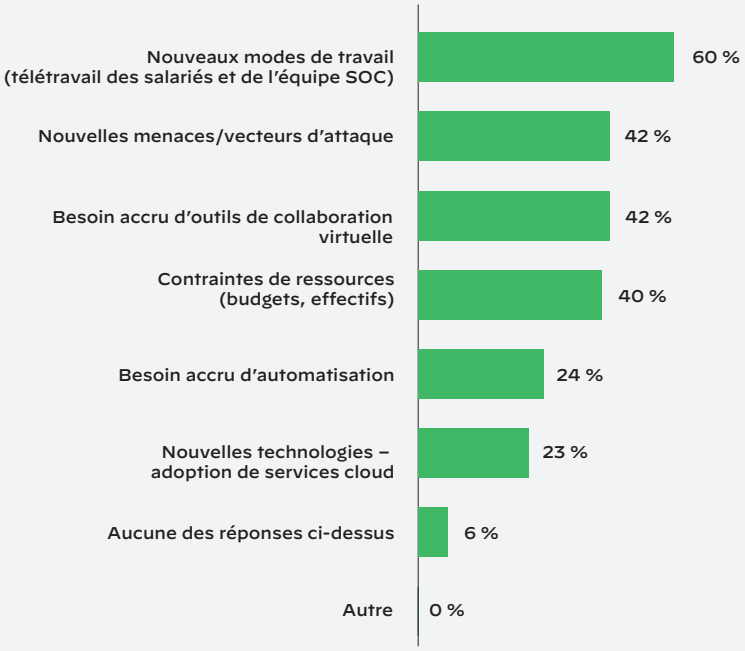

Figure 2 : Résultats d'enquête – Impact de la Covid-19 sur le SOC et les analystes sécurité

Le niveau et les pratiques de sécurité sont également touchés, puisque 42 % des sondés estiment que la pandémie a fait naître de nouvelles menaces et vecteurs d'attaque. Quant à l'adoption du SOAR, elle divise les participants à notre enquête. D'une part, 47 % des sondés dont les entreprises utilisent déjà cette technologie déclarent que la pandémie les incitera à étendre son utilisation et à accélérer son adoption. D'autre part, 47 % estiment aussi que la Covid-19 réduira l'utilisation des outils SOAR et retardera leur déploiement.

Principales conclusions de l'enquête 2020 sur l'état du SOAR

L'enquête SOAR 2020 n'a fait que confirmer certaines des conclusions des années précédentes. Les équipes SOC peinent encore et toujours à gérer l'avalanche d'alertes. Et la pénurie de compétences n'arrange rien. D'après le rapport Gartner 2020 sur les grandes tendances de la gestion des risques et de la sécurité, « l'écart de compétences en sécurité va continuer de s'accroître à mesure que les systèmes IT se complexifient et que les outils de sécurité évoluent pour protéger cette infrastructure en constante mutation ».[2]

Pour alléger la pression, les équipes SOC réclament davantage d'automatisation. De fait, notre enquête révèle un vif intérêt pour l'intégration des systèmes de différents fournisseurs. Même son de cloche du côté des playbooks. Certains plébiscitent même des marketplaces indépendantes et des plateformes de partage communautaires. Les professionnels attendent des solutions, et ils veulent savoir comment leurs pairs font face aux menaces.

La réponse à incident aujourd'hui : un workflow de plus en plus exigeant et complexe

En matière de réponse à incident, chaque entreprise adopte sa propre approche et sa propre constellation d'outils. D'après notre enquête, le point de départ du processus IR diffère selon les structures. Comme le montre la figure 3, plus de la moitié des workflows IR débutent au niveau de la solution SIEM, tandis que 33 % partent de plateformes d'émission de tickets de support comme ServiceNow® et Zendesk®. Seulement 6 % ont un outil de gestion des cas comme première interface, tandis que 2 % préfèrent les solutions SOAR.

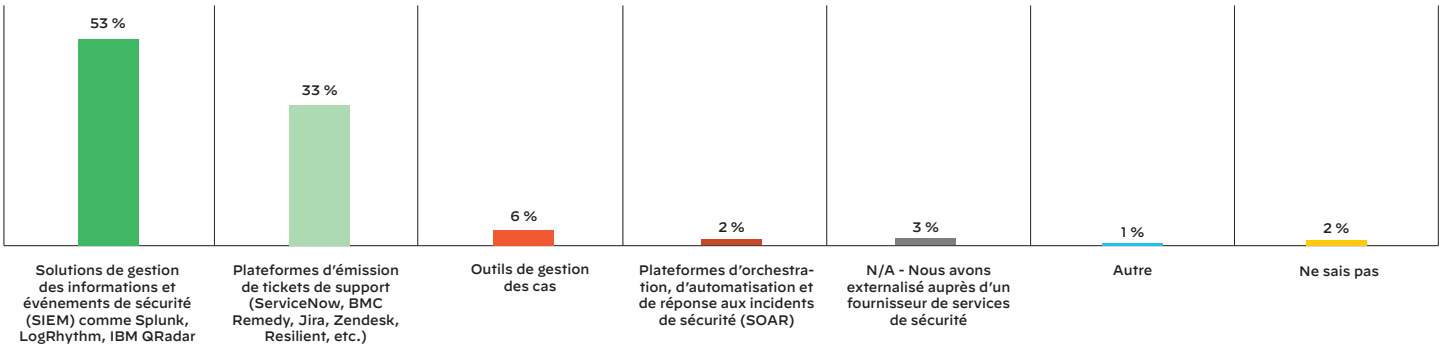

Figure 3 : « Quelle interface sert de principal point de départ pour vos workflows de réponse à incident ? »

D'après la figure 4, une bonne partie de la réponse à incident repose sur des prestataires externes et des processus manuels. En effet, 22 % des workflows IR font intervenir des fournisseurs de services de sécurité managés (MSSP) et des services managés de détection et de réponse (MDR). Puisque des entités externes accomplissent une partie de ces tâches, il est logique que les workflows IR soient en grande partie manuels, sauf si le service MSSP ou MDR choisi s'intègre aux outils d'automatisation de la réponse à incident déployé dans l'entreprise.

Les processus d'investigation sont à 38 % manuels, tandis que les tâches de réponse et de neutralisation le sont à 35 %. Si l'on tient compte des résultats de la figure 3, l'importance des processus manuels n'a rien de surprenant : si 53 % des workflows IR sont enclenchés au niveau des solutions SIEM, qui n'intègrent généralement pas de fonctionnalités IR automatisées, alors un membre de l'équipe SOC devra transférer les données manuellement vers d'autres outils.

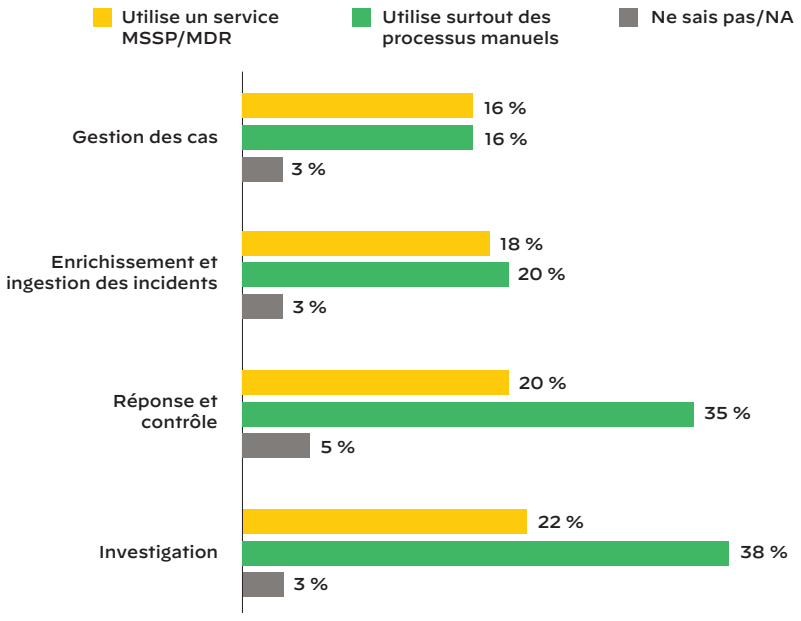

Figure 4 : « Quelles solutions utilisez-vous pour les étapes suivantes de votre réponse à incident ? »

2. « Top Security and Risk Management Trends », Gartner, 27 février 2020

Rapidité et évolutivité : les responsables de la sécurité dans l'impasse

Lorsqu'on les interroge sur leurs processus IR, certains participants laissent à penser qu'ils peinent à accélérer leur réponse à incident et à la déployer à l'échelle. Comme le montre la figure 5, moins de la moitié des sondés ont accès à des tableaux de bord personnalisables. Seuls 40 % bénéficient d'un reporting à intervalles réguliers et en temps réel, tandis que 15 % reçoivent des recommandations par machine learning pour améliorer leurs opérations de sécurité. Ces chiffres sont le reflet d'un environnement SecOps miné par l'inefficacité et les pertes de temps. Lorsque les analystes SOC doivent composer avec des tableaux de bord rigides et inadaptés à leur rôle, et des rapports qui ont toujours un train de retard, la réponse ne peut qu'être ralentie. Et les résultats sont également en demi-teinte. Enfin, malgré l'efficacité reconnue du machine learning, notre enquête montre que seul un SOC sur six en est équipé.

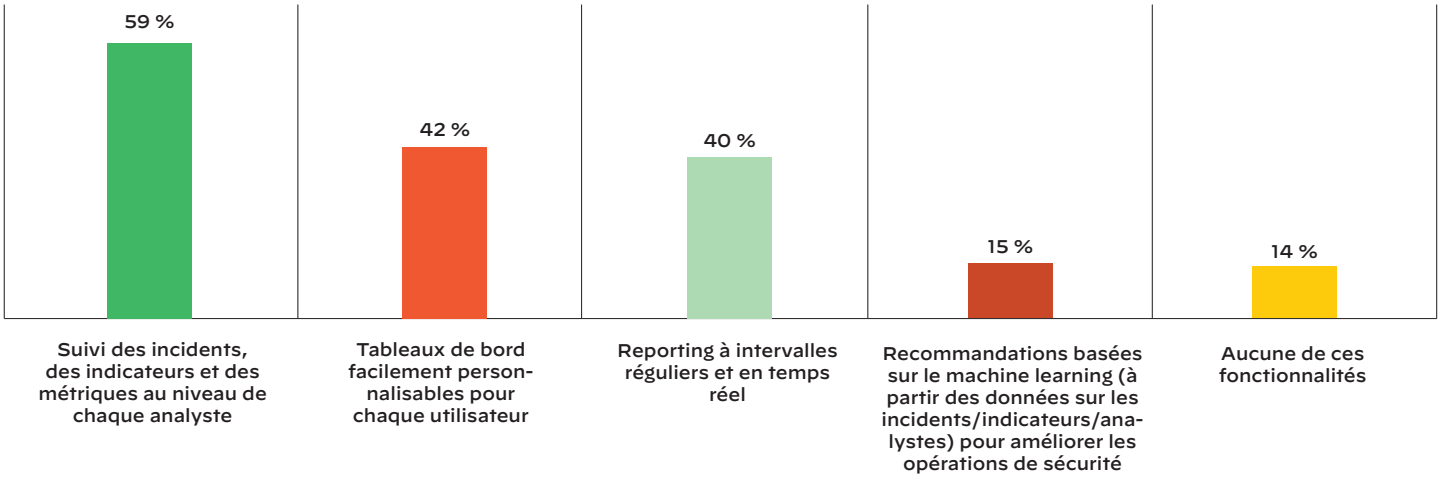

Figure 5 : « De quelles fonctionnalités disposez-vous actuellement pour la réponse à incident et le suivi des performances par des analystes ? » (Plusieurs réponses possibles)

Enjeux des playbooks et des processus automatisés

Notre enquête révèle qu'il est temps de passer à la vitesse supérieure en matière d'automatisation de la réponse à incident. Certes, 44,7 % des processus IR des sondés sont automatisés. Mais cela ne suffit pas. Bien qu'un tel niveau d'automatisation soit un bon début, la prédominance des processus manuels nuit à l'efficacité de la réponse. C'est sans doute pourquoi pas moins de 93 % des équipes SecOps font de l'automatisation une priorité pour leurs processus IR au cours des 12 prochains mois.

Enrichissement et ingestion d'incidents : une automatisation partielle

Au cours de la réponse, l'étape d'enrichissement et d'ingestion des incidents est partiellement automatisée. Comme le montre la figure 6, la moitié des sondés ont automatisé l'ingestion de données multi-sources. La priorisation des alertes est à 46 % automatisée, tout comme la corrélation des alertes aux indicateurs sur différents produits. Mais, quand on sait combien les équipes SOC sont stressées et débordées, une automatisation de 50 % des tâches d'ingestion ne suffit sans doute pas à les soulager. En ce qui concerne l'enrichissement, le pourcentage d'automatisation tombe à 28 % chez nos sondés. Ils sont par ailleurs 30 % à déclarer enrichir manuellement les données d'incident.

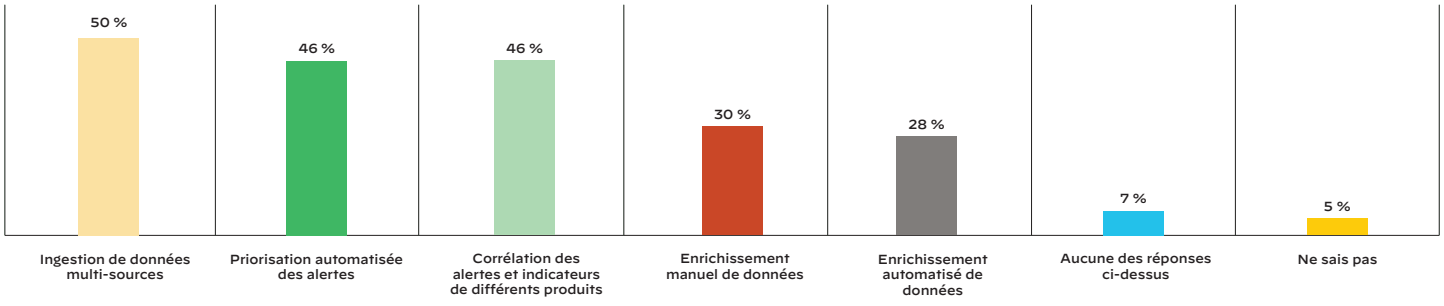

Figure 6 : « De quelles fonctionnalités disposez-vous actuellement pour l'enrichissement et l'ingestion des incidents ? » (Plusieurs réponses possibles)

Implémentation des processus IR : un mélange de workflows automatisés et manuels

L'implémentation des processus IR allie elle aussi l'automatisation à des tâches manuelles. D'après la figure 7, 53 % des implémentations reposent sur un mélange de playbooks, runbooks et processus manuels et automatisés. Seulement 18 % des sondés recourent à des playbooks automatisés, tandis que 6 % n'utilisent aucun playbook. Or, ce sont les playbooks qui permettent aux SOC d'implémenter le processus IR. Et force est de constater qu'ils sont peu automatisés.

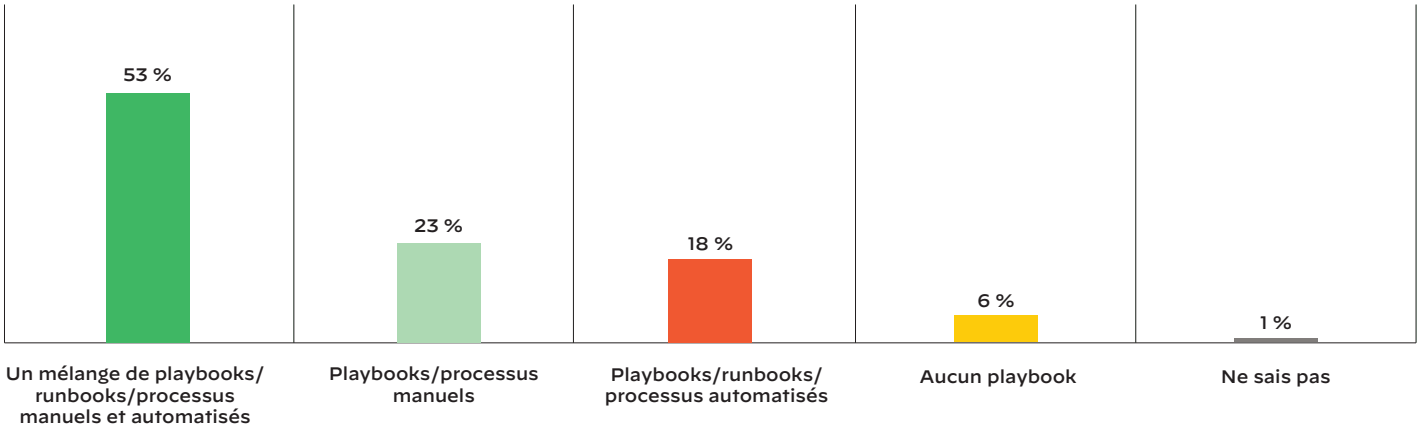

Figure 7 : « Parmi les options suivantes, laquelle décrit le mieux votre implémentation d'un processus de réponse à incident ? »

Automatisation limitée des workflows d'investigation et post-incident

La phase d'investigation affiche également un niveau d'automatisation limité. Tandis que 37 % des outils de sécurité à distance s'exécutent automatiquement, 49 % nécessitent une intervention manuelle. Autre fait important, seulement 18 % des workflows IR intègrent des fonctions de documentation automatique des investigations. Autrement dit, plus de 80 % des analystes documentent leur enquête manuellement, voire pas du tout dans de nombreux cas.

En effet, les membres des équipes SOC sont généralement trop débordés pour se donner cette peine. On ne peut que le déplorer, car ces informations s'avèrent extrêmement utiles lors d'analyses post-incident et pour l'amélioration des processus de réponse à de futures attaques. Un niveau d'automatisation aussi bas ne permet pas de tirer véritablement les leçons des incidents passés. Lorsque la question porte sur les workflows post-incident, seuls 23 % des sondés font état d'une capture automatisée des analyses a posteriori.

Réponse à incident : priorité à l'automatisation

En matière d'automatisation de la réponse à incident, les priorités et les projets des entreprises parlent d'eux-mêmes. Comme le montre la figure 8, 65 % des sondés feront de l'automatisation IR une priorité absolue au cours des 12 prochains mois. Ils sont 58 % à vouloir donner la primauté à la priorisation des menaces, tandis que 46 % affichent cette même ambition pour le reporting et la visibilité transverse aux équipes. Au final, ceux qui ne considèrent pas l'automatisation comme une priorité sont largement minoritaires. Dans le cas de la réponse à incident, cette opinion n'est partagée que par 2 % des sondés.

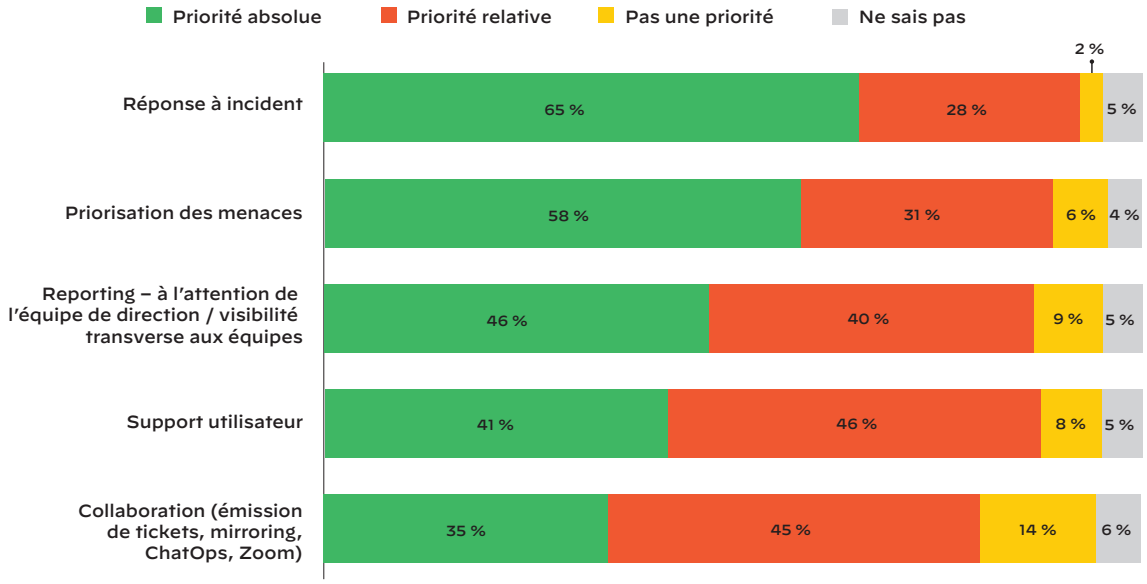

Figure 8 : « Au cours des 12 prochains mois, dans quelle mesure l'automatisation des processus SecOps suivants sera-t-elle une priorité ? »

Besoin de simplification et d'intégration de la Threat Intelligence aux workflows IR

Dans un contexte de multiplication des menaces dans le monde entier, les équipes SOC doivent impérativement pouvoir compter sur une Threat Intelligence toujours à jour. Preuve de cette importance, 81 % des participants à notre enquête qualifient la CTI de primordiale pour leur processus IR. Pour s'informer sur les menaces, les entreprises s'abonnent à 6,8 flux CTI en moyenne. Toutefois, sans une gestion cohérente et intégrée de ces flux de données, des menaces potentiellement graves peuvent vite échapper à l'attention des analystes. Pour 62 % des sondés, l'utilisation de la Threat Intelligence est un processus qu'ils qualifient de chronophage.

C'est sans doute pourquoi l'intégration de la CTI figure parmi les principaux critères de choix d'un nouvel outil de sécurité. Comme le montre la figure 9, 50 % des personnes interrogées déclarent que leurs workflows SecOps bénéficieraient grandement d'une meilleure intégration des flux CTI. Si l'on ajoute à cela les 46 % de sondés pour lesquels les workflows IR en bénéficieraient « quelque peu », ce sont pas moins de 96 % de professionnels de la sécurité qui plébiscitent une telle intégration.

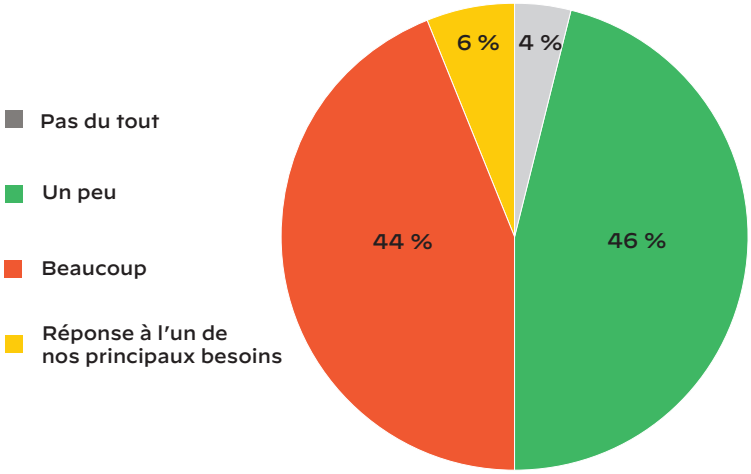

Figure 9 : « Dans quelle mesure vos workflows SecOps bénéficieraient-ils d'une meilleure intégration de la Threat Intelligence ? »

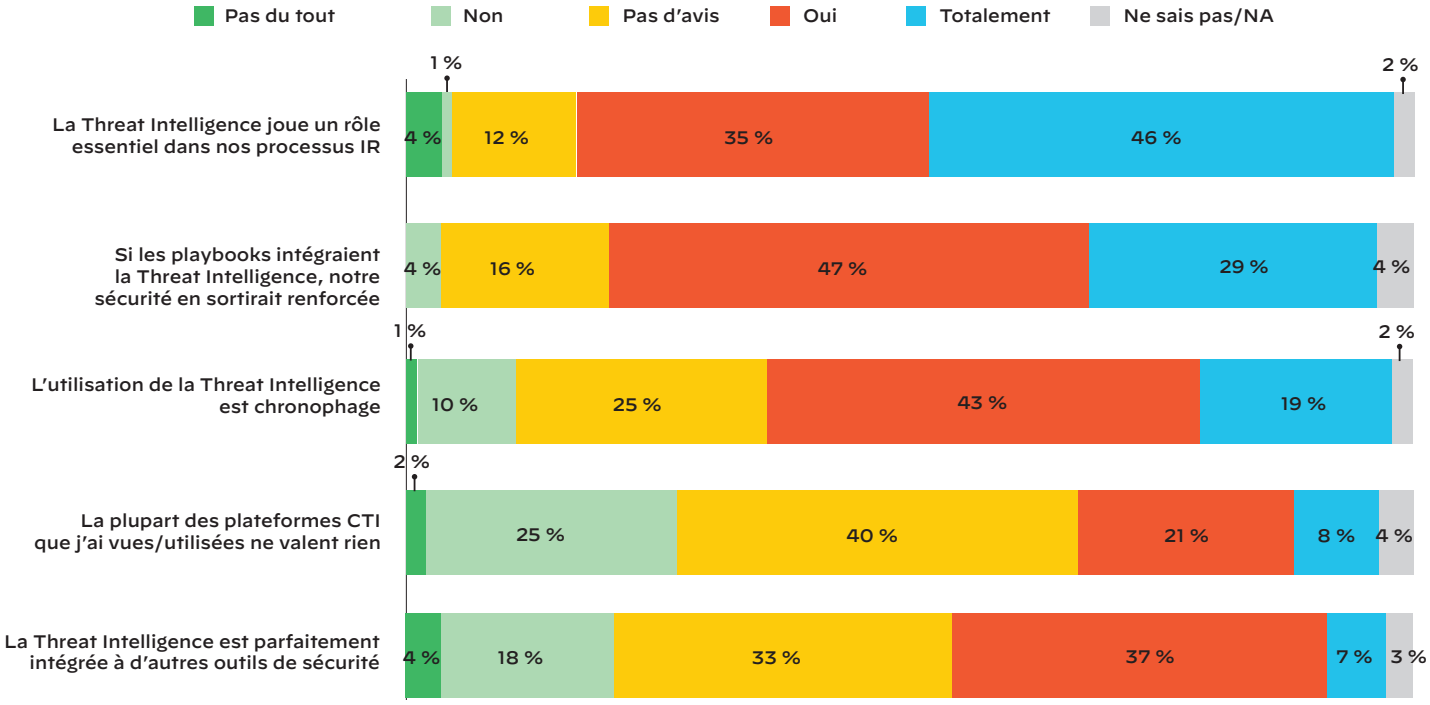

Figure 10 : « Quel est votre avis sur les affirmations suivantes concernant la Threat Intelligence ? »

Ceci étant dit, le taux d'intégration réel s'avère relativement bas, puisque seulement 43 % des personnes interrogées s'accordent sur le fait que « la Threat Intelligence est parfaitement intégrée à d'autres outils de sécurité ». En outre, seulement 28 % des processus d'investigation sont renseignés par des sources CTI.

Un certain nombre d'éléments de notre enquête expliquent cet écart entre la volonté d'intégrer la Threat Intelligence et son taux d'intégration réel. Pour commencer, la gestion de la CTI fait intervenir un grand nombre de collaborateurs différents. D'après la figure 11, elle concerne tant les équipes SecOps que les équipes de sécurité de l'entreprise, les équipes ITOps, voire les équipes de Threat Intelligence. La qualité perçue des plateformes CTI pourrait elle aussi contribuer à cet écart. En effet, 29 % des sondés s'accordent à dire que « la plupart des plateformes de Threat Intelligence qu'ils ont vues et/ou utilisées ne valent rien ».

D'après la figure 12, le processus CTI lui-même repose sur pas moins de 12 systèmes différents. Les collaborateurs cités à la figure 11 utilisent des solutions SIEM, des outils d'analyse du trafic réseau, des solutions de prévention/détection des intrusions, et d'autres encore. En clair, trop de gens et trop d'outils, le tout sans intégration ou presque. Rien d'étonnant à ce que nos sondés attendent mieux.

Enjeux de la réduction des alertes pour les équipes SecOps

Les analystes SOC peinent à faire face à l'avalanche d'alertes qui déferlent sur eux tous les jours. On voit alors apparaître un phénomène d'accoutumance aux alertes, avec ses corollaires que sont le burnout et le turnover. C'est ainsi que des menaces graves finissent parfois par passer à travers les mailles du filet. Sans compter que la pandémie n'arrange rien. D'après notre enquête, 47 % des entreprises font état d'une hausse du nombre d'alertes depuis le début de la crise sanitaire, avec un bond de 34,2 % du volume d'alertes en moyenne.

Technologies SecOps : une intégration indispensable à d'autres solutions

Comme le montre la figure 13, les workflows IR sont enclenchés à partir d'outils divers et variés. Tout au long du processus, ils passent par de multiples solutions et départements. C'est pourquoi l'intégration des outils IR et des autres solutions peut contribuer à la productivité des équipes SOC et à l'efficacité des réponses à incident. Ainsi, 30 % des participants à notre enquête réclament une plateforme commune pour une réponse à incident transfonctionnelle, tandis que seulement 32 % disposent déjà d'une telle plateforme.

Pour prendre la mesure du problème, rappelez-vous que les équipes SOC utilisent une grande variété d'outils à chacun des quatre stades du workflow IR. D'après la figure 13, les solutions SIEM dominent puisqu'elles sous-tendent 69 % des processus d'enrichissement et d'ingestion des incidents, et un peu moins de la moitié des étapes de gestion des cas et des investigations. D'autre part, 20 % des processus de réponse et de neutralisation et 22 % des investigations reposent sur des plateformes SOAR. Moins courantes, les plateformes de Threat Intelligence (TIP) couvrent moins de 20 % des processus sur les quatre stades.

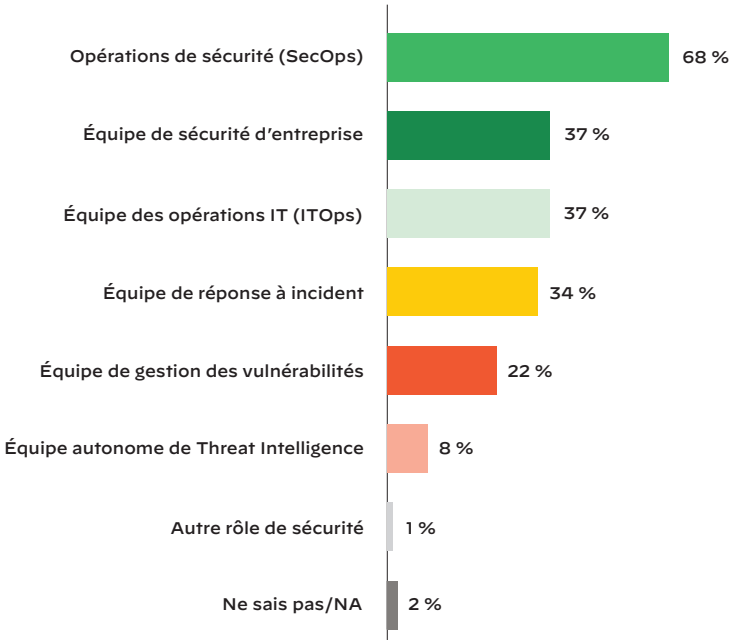

Figure 11 : « Dans votre entreprise, qui est chargé de gérer la Threat Intelligence ? »

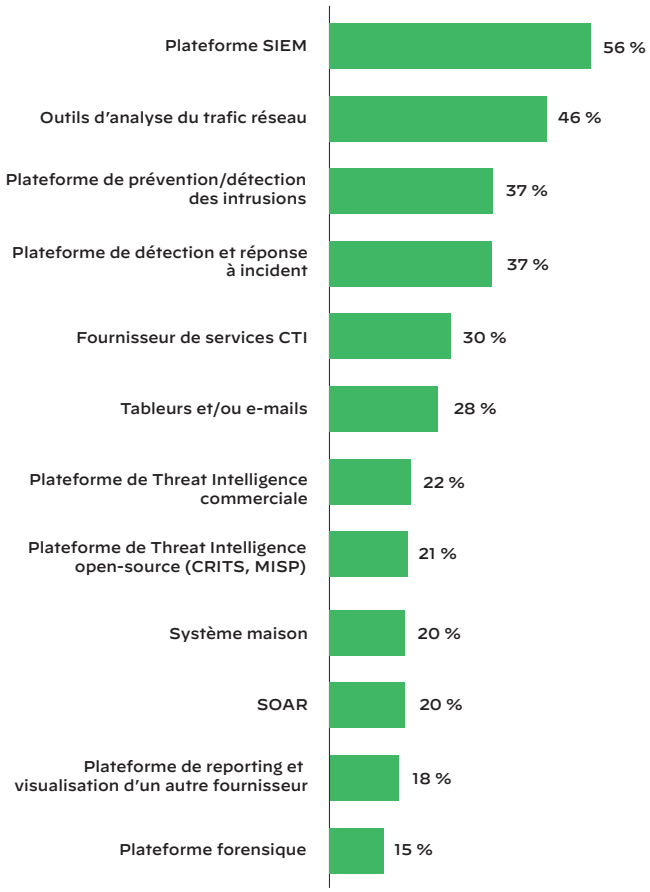

Figure 12 : « Quels types d'outils et/ou de fonctionnalités de gestion utilisez-vous pour agréger, analyser et/ou diffuser la Threat Intelligence ? » (Plusieurs réponses possibles)

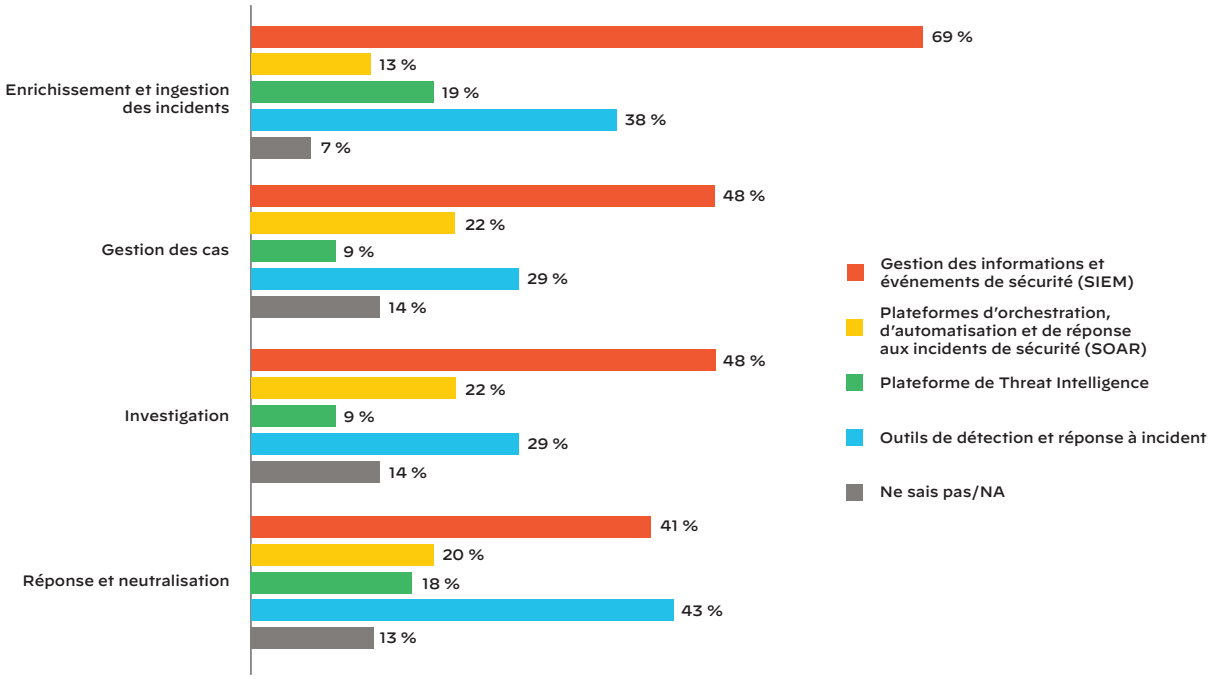

Figure 13 : « Quelles solutions utilisez-vous pour les étapes suivantes de votre réponse à incident ? » (Plusieurs réponses possibles)

Par ailleurs, les workflows IR font intervenir de nombreux départements dont les systèmes sont toutefois très peu intégrés. Comme le montre la figure 14, ce sont les outils des équipes IT qui sont les mieux intégrés aux solutions de réponse à incident puisque 23 % de ces systèmes et processus sont qualifiés « d'étroitement intégrés ». Ce taux descend à 16 % pour les équipes chargées d'exploiter le réseau (NetOps). Quant au département RH, ses systèmes et processus fonctionnent en silo dans 50 % des cas. Dans la même veine, 48 % des services juridiques et 30 % des équipes de conformité opèrent en vase clos.

Des équipes partagent « certains systèmes et processus » seulement : 51 % des équipes de conformité, 56 % des équipes IT et 52 % des équipes NetOps. Dans les autres services, cette pratique reste minoritaire. C'est dans les départements juridiques que l'on enregistre le plus bas taux d'intégration à la réponse à incident, avec un maigre 7 % de systèmes et processus étroitement intégrés. Ce chiffre est peut-être dû à l'utilisation de systèmes spécialisés pour la gestion des cas et des dossiers. Bien que tous les incidents de sécurité ne concernent pas le département juridique, ce manque d'intégration risque de coûter cher et de faire perdre du temps aux équipes IR et juridiques qui devront coordonner leurs workflows manuellement.

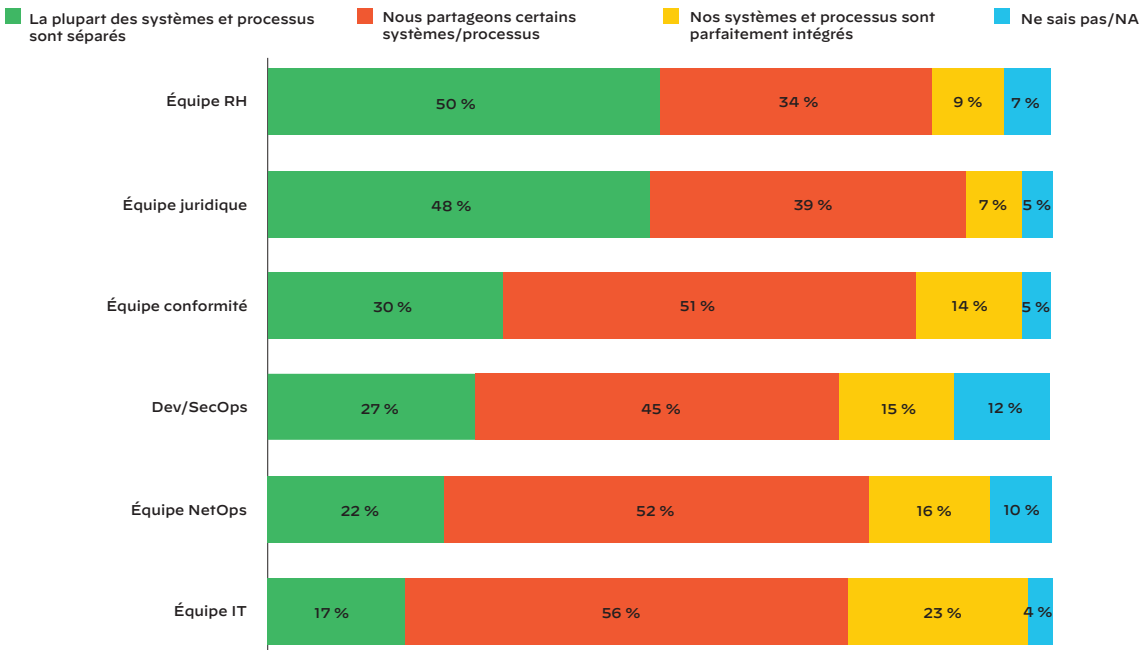

Figure 14 : « Dans quelle mesure partagez-vous vos outils, processus, systèmes et flux de données avec les équipes suivantes ? »

Engouement pour les marketplaces indépendantes et les plateformes communautaires

Il existe une longue tradition dans l'univers de la cybersécurité qui consiste à mettre la force du collectif au service de la sécurité de tous. Il faut dire que de nombreux outils informatiques et de sécurité nous viennent de l'open-source et qu'un grand nombre de professionnels cyber ont d'abord exercé dans l'armée ou la police, deux corporations dans lesquelles le partage d'informations fait partie des usages. Si, dans les faits, cet idéal n'est pas toujours atteint, il existe néanmoins un véritable engouement pour le partage d'informations et de bonnes pratiques selon un modèle communautaire.

En témoignent les 78 % de participants à notre enquête qui appellent de leurs vœux un cadre commun et une communauté de partage de playbooks et d'intégrations. Seuls 42 % des sondés estiment qu'ils obtiennent de meilleurs résultats en créant eux-mêmes leurs propres playbooks. Outre leur sens du collectif, les personnes interrogées montrent un certain intérêt pour les marketplaces indépendantes. En effet, 52 % d'entre elles sont enclines à investir dans des intégrations à des outils d'autres fournisseurs. La figure 15 reflète parfaitement cet engouement pour les cadres communs, les communautés de partage et les marketplaces indépendantes.

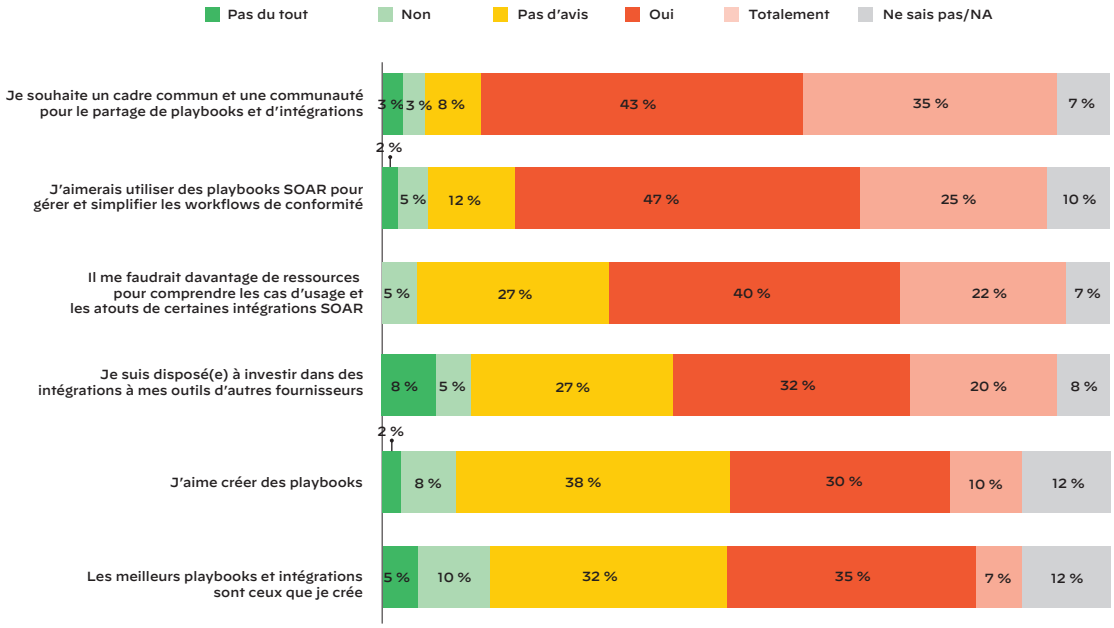

Figure 15 : « Dans quelle mesure partagez-vous vos outils, processus, systèmes et flux de données avec les équipes suivantes ? »*

Reste donc à savoir qui les professionnels de la sécurité plébiscitent pour leurs playbooks. D'après la figure 16, ils font davantage confiance aux fournisseurs de solutions SOAR puisque 53 % des sondés disent préférer opter pour des playbooks certifiés par ces spécialistes. Viennent ensuite les playbooks développés en interne (47 %), ceux créés – mais non certifiés – par leur fournisseur de solutions SOAR (44 %), et enfin par un prestataire MSSP ou un autre partenaire de sécurité (35 %).

Fait intéressant, si près de 8 sondés sur 10 souhaitent voir l'émergence d'une communauté de partage, seuls 20 % sont davantage susceptibles de faire confiance aux playbooks créés par ses membres. Cette contradiction apparente prend tout son sens lorsqu'on se souvient que 53 % des personnes interrogées préfèrent s'en remettre aux playbooks certifiés par leur fournisseur. Ces résultats montrent donc l'importance de la certification.

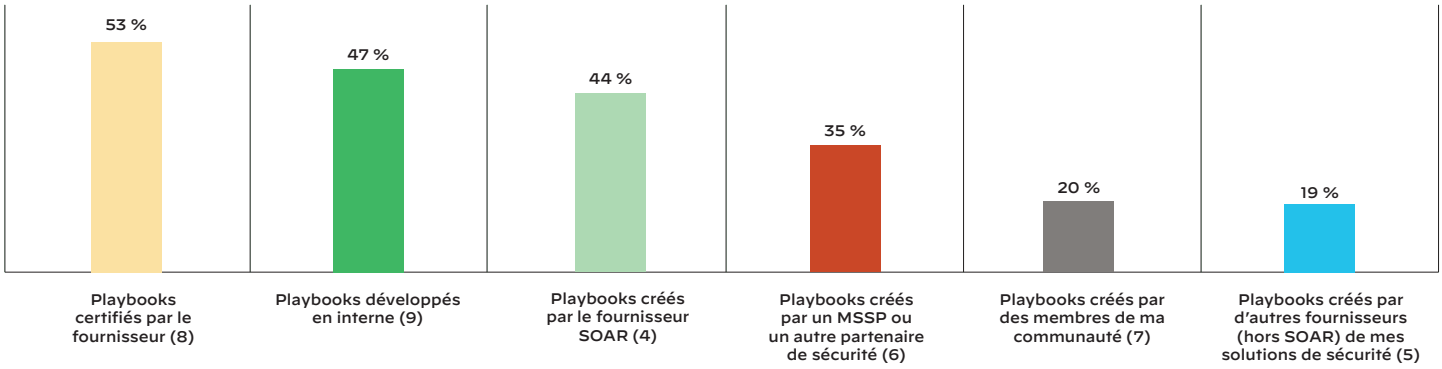

Figure 16 : « Parmi ces sources de playbooks SOAR, lesquelles sont le plus susceptibles de vous inspirer confiance ? » (Plusieurs réponses possibles)

* Les chiffres étant arrondis, le total des pourcentages dépasse 100.

L'état du SOAR

Le SOAR répond à de nombreuses problématiques mises en lumière par notre enquête, notamment par davantage d'automatisation et par une réduction de l'accoutumance aux alertes. C'est sans doute pour cela que les personnes interrogées manifestent beaucoup d'intérêt pour cette technologie. Cet engouement se reflète dans la proportion impressionnante de sondés qui ont déjà adopté le SOAR ou qui envisagent de le faire dans les 12 prochains mois. Cette technologie joue déjà un rôle croissant dans la réponse à incident et l'environnement SecOps, et devrait continuer à gagner du terrain l'an prochain.

Multiplication des cas d'usage SOAR

Les équipes SOC font confiance au SOAR pour une multitude de cas d'usage. D'après la figure 17, les entreprises l'utilisent surtout pour la détection et la réponse à incident (45 %), la priorisation des vulnérabilités (37 %), les contrôles de conformité (30 %) et les audits de sécurité (30 %).

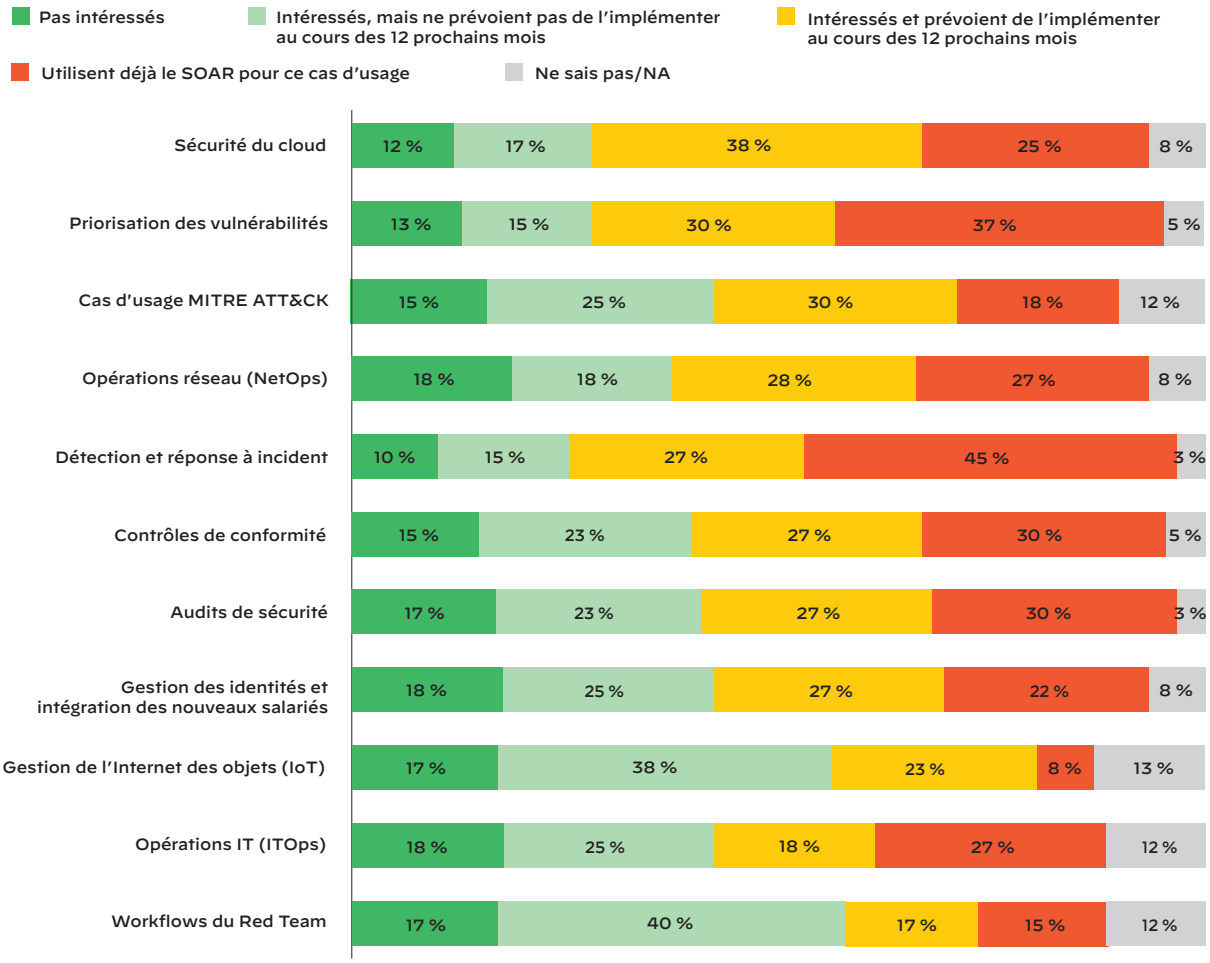

Figure 17 : « Dans quelle mesure prévoyez-vous d'étendre votre utilisation du SOAR aux cas d'usage suivants ? »

Si les taux d'adoption du SOAR sont plus bas pour les autres cas d'usage de notre enquête, la technologie n'en reste pas moins utilisée, fut-ce à un degré moindre. Les équipes de sécurité ont ainsi recours au SOAR pour les workflows Red Team (15 %), les opérations IT (27 %) et de sécurité (27 %) et les cas d'usage MITRE ATT&CK® (18 %). Ces résultats laissent à penser qu'elles s'intéressent au SOAR, mais qu'elles restent relativement lentes à l'implémenter.

Généralisation des technologies SOAR

D'après notre enquête, le SOAR s'impose peu à peu au SOC. En effet, presque la moitié des personnes interrogées (46 %) utilisent déjà cette technologie ou prévoient de l'adopter au cours des 12 prochains mois. Toutefois, le SOAR reste une discipline jeune puisque seuls 7 % des sondés y ont recours depuis plus de deux ans. La figure 18 répartit les participants en fonction de leur usage du SOAR. Fait intéressant, 41 % connaissent cette technologie sans pour autant prévoir de l'implémenter au cours des 12 prochains mois. Ils sont aussi 12 % à n'avoir jamais entendu parler du SOAR. Est-ce parce que les professionnels parlaient plutôt de SAO jusque récemment ?

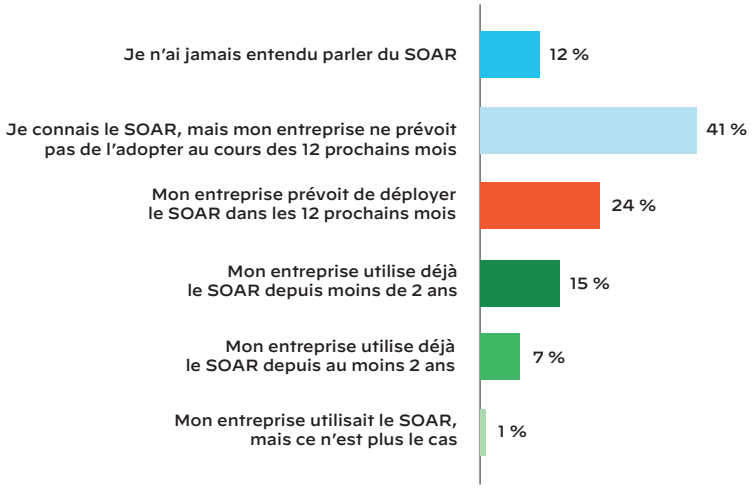

Figure 18 : « Laquelle des affirmations suivantes décrit le mieux votre intérêt pour le SOAR, ainsi que votre utilisation et votre maîtrise de ces outils ? »

Impact positif du SOAR sur les équipes SecOps et la réponse à incident

Si le SOAR bénéficie aux SecOps et à la réponse à incident à bien des égards, c'est peut-être parce qu'il permet d'en automatiser les opérations. D'après Gartner, « les technologies SOAR émergentes promettent d'automatiser, d'homogénéiser et d'améliorer l'efficacité des opérations de sécurité bien au-delà de ce que permettent les solutions SIEM d'aujourd'hui ».[3]

Parmi les sondés qui utilisent le SOAR depuis au moins deux ans, 54 % affirment qu'il leur permet d'agir plus vite en cas d'incident. Les autres avantages cités sont des délais de neutralisation plus courts (51 %), une réduction du temps moyen passé sur chaque incident (47 %) et une accélération du tri (44 %). Ils sont également 37 % pour qui le SOAR a réduit le nombre d'étapes nécessaires à la réponse à incident.

La figure 19 illustre parfaitement l'impact du SOAR sur les performances du SOC pour ce groupe de sondés :

- Processus mieux définis (79 %)
- Meilleure communication avec les équipes hors SecOps (53 %)
- Réduction voire élimination des étapes inutiles (47 %)
- Structure organisationnelle horizontale grâce à l'amélioration des compétences des analystes (42 %)
- Capacité à gérer des cas d'usage plus complexes (42 %)
- Structure organisationnelle horizontale grâce à l'automatisation des processus (37 %)

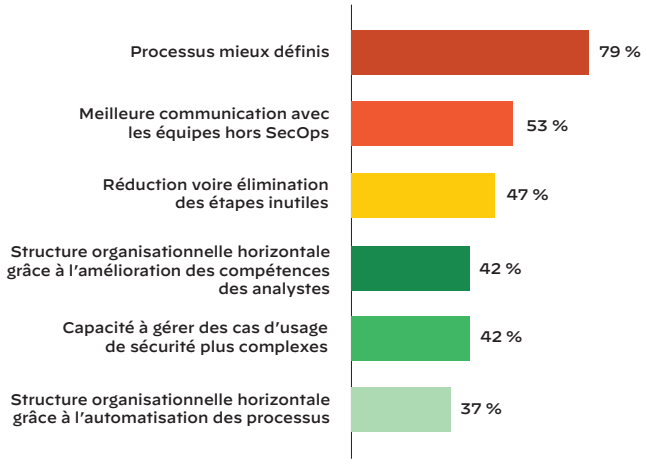

Figure 19 : « Comment votre implémentation des technologies SOAR a-t-elle changé vos workflows ? » (Plusieurs réponses possibles) Remarque : N=19

Ces résultats suggèrent que le SOAR offre une bonne solution aux problématiques actuelles des équipes SOC. L'amélioration des communications transverses vient contrecarrer le problème soulevé à la figure 14, à savoir le manque de coordination avec les équipes IT, RH, juridiques et autres. En réduisant le temps consacré à la gestion et à la résolution des incidents, le SOAR a le pouvoir d'alléger la pression liée à la surabondance d'alertes et de flux CTI. Qui dit tri plus rapide et équipes SOC plus productives, dit aussi recentrage sur les incidents les plus complexes.

3. « Top Security and Risk Management Trends », Gartner, 27 février 2020

Engouement et intentions d'achat

Nous avons également interrogé les responsables sécurité sur leurs plans en matière de SOAR. Résultat : qu'ils l'aient déjà adoptée ou non, 43 % des participants à notre enquête ont l'intention d'augmenter leurs dépenses dans les outils SOAR l'année prochaine.

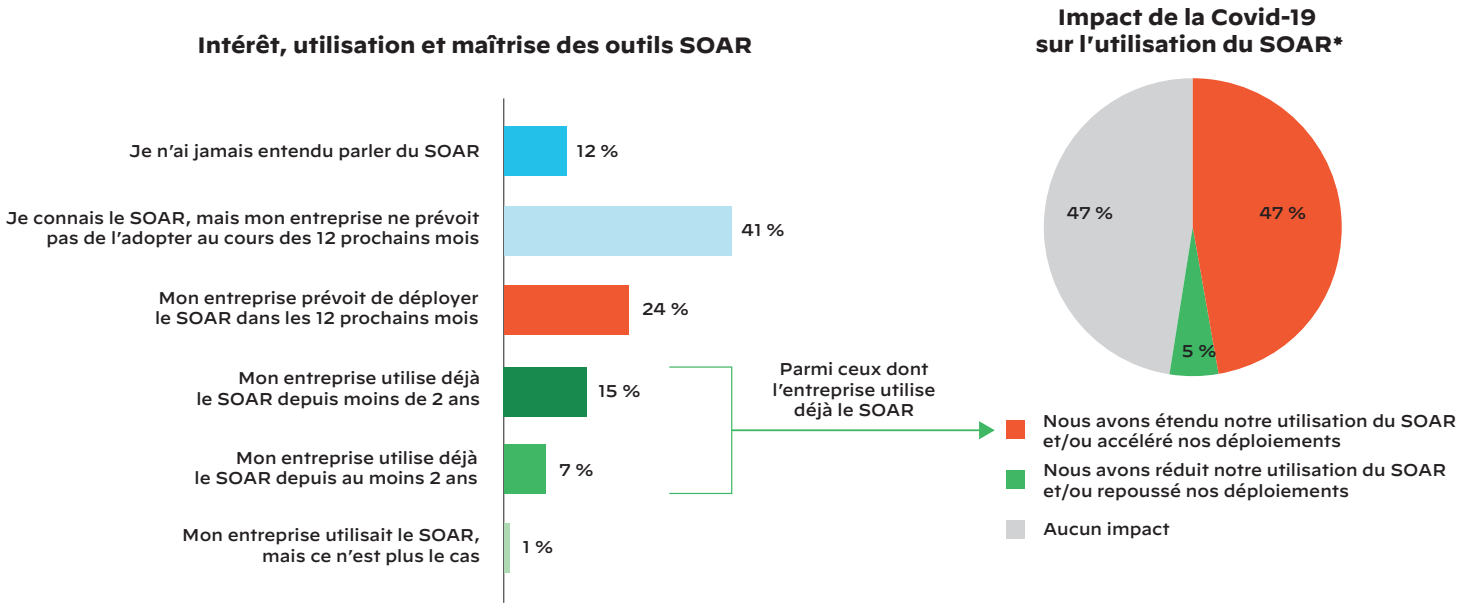

Figure 20 : « Quel impact la pandémie de Covid-19 a-t-elle eu sur l'utilisation (présente et future) du SOAR dans votre entreprise ? » Remarque : N=19

SOAR : l'avenir pour la sécurité IoT, le framework MITRE et les Red Teams

Les utilisateurs du SOAR envisagent de l'appliquer à des workloads bien précis pour les années à venir. Le tableau 1 synthétise leurs réponses à la question « Dans quelle mesure prévoyez-vous d'étendre votre utilisation de la technologie SOAR aux cas d'usage suivants ? ». Parmi les entreprises qui ont déjà recours à cette technologie, 38 % prévoient de l'appliquer à la gestion de l'Internet des objets (IoT) dans les 12 prochains mois. Elles sont également 23 % à s'intéresser à ce cas d'usage sans prévoir de l'implémenter au cours de l'année prochaine. Si l'on ajoute à cela les entreprises qui utilisent déjà le SOAR pour la gestion de leur IoT (8 %), ce sont pas moins de 69 % d'utilisateurs de cette technologie qui y voient un élément de leur stratégie IoT.

Les workflows des Red Teams (57 %), la sécurité du cloud (55 %) et les cas d'usage MITRE ATT&CK® (55 %) ont eux aussi de fortes chances de figurer dans les plans SOAR à l'avenir, si ce n'est déjà le cas. Même les cas d'usage qui suscitent moins d'intérêt – priorisation des vulnérabilités (45 %), opérations IT (43 %) et détection et réponse (42 %) – se situent dans une fourchette relativement élevée.

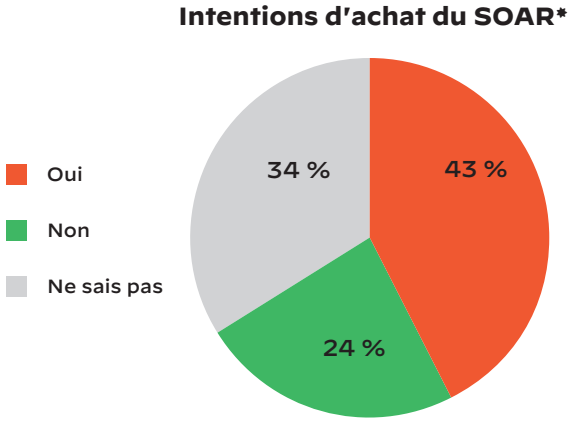

Figure 21 : « Votre entreprise prévoit-elle d'accroître ses dépenses consacrées aux outils SOAR en 2020 ? »

* Les chiffres étant arrondis, le total des pourcentages dépasse 100.

Tableau 1 : Réponses à la question « Dans quelle mesure prévoyez-vous d'étendre votre utilisation de la technologie SOAR aux cas d'usage suivants ? »		
	Intéressés et prévoient de l'implémenter au cours des 12 prochains mois	Utilisent déjà le SOAR pour ce cas d'usage
Gestion de l'IoT	38 %	8 %
Workflows des Red Teams	40 %	15 %
Sécurité du cloud	17 %	25 %
Cas d'usage MITRE ATT&CK	25 %	18 %
Gestion des identités et intégration des nouveaux salariés	25 %	22 %
Contrôles de conformité	23 %	30 %
Audits de sécurité	23 %	30 %
Opérations réseau (NetOps)	18 %	27 %
Priorisation des vulnérabilités	15 %	37 %
Opérations IT (ITOps)	25 %	27 %
Détection et réponse à incident	15 %	45 %
Moyennes	24 %	26 %

Avantages de Cortex XSOAR

Cortex™ XSOAR de Palo Alto Networks offre une seule et même plateforme d'orchestration de tous vos produits de sécurité pour une réponse à incident plus rapide et plus évolutive. Pour rationaliser les processus IR, elle interconnecte des outils disparates et automatise les tâches manuelles répétitives qui ne nécessitent pas d'intervention humaine. Cortex XSOAR est la première solution SecOps du marché à intégrer nativement la Threat Intelligence et des fonctions de collaboration, de gestion des incidents, d'orchestration et d'automatisation de la sécurité.

Comme le montre le tableau 2, Cortex XSOAR aide à résoudre les problématiques IR soulevées par les participants à notre enquête.

Tableau 2 : Cortex XSOAR, la solution aux problématiques IR		
Problème/souhait	Solution attendue	Avec Cortex XSOAR
Trop de processus IR manuels	Davantage d'automatisation pour accélérer la réponse et réduire le stress lié aux opérations manuelles	Automatisation des actions répétitives grâce à des playbooks qui coordonnent les processus à travers tous les produits de sécurité
Manque d'intégration aux autres solutions	Intégration des outils SOC aux systèmes d'autres fournisseurs pour interconnecter facilement d'autres départements et processus IR	Plus de 450 intégrations de produits tiers pour coordonner et automatiser les opérations de sécurité
Partage de playbooks créés par des pairs/une communauté	Davantage de playbooks, y compris de sources externes, et une plateforme d'échange communautaire pour bénéficier de l'expertise d'autres équipes	Communauté DFIR (Digital Forensics and Incident Response) ouverte pour partager vos bonnes pratiques avec plus de 15 000 autres membres
Trop de flux CTI à surveiller	Intégration de la Threat Intelligence aux outils SecOps pour réduire le nombre de flux à surveiller et se concentrer sur les menaces graves	Automatisation basée sur des playbooks éprouvés pour unifier l'agrégation, la notation et le partage de la Threat Intelligence et ainsi permettre au SOC de reprendre le contrôle de sa gestion CTI
Trop d'alertes à traiter	Baisse du volume d'alertes	Jusqu'à 95 % de réduction des alertes exigeant une validation humaine

Conclusion

Cette quatrième édition de notre rapport sur l'état du SOAR souligne l'évolution rapide de la cybersécurité. Les SOC sont aujourd'hui confrontés à des attaques de plus en plus graves et sophistiquées, souvent perpétrées par des groupes agissant pour le compte d'États. Dans ce contexte et malgré certains progrès réalisés sur le champ des SecOps, les analystes sont encore et toujours dépassés par le processus global de réponse à incident. Les alertes à traiter et les flux CTI à surveiller sont trop nombreux. Il en va de même pour les processus manuels qui ralentissent les interventions et empêchent de se concentrer sur les alertes vraiment importantes.

Les analystes sécurité savent ce dont ils ont besoin pour sortir de cette impasse. Ils réclament davantage d'automatisation des processus IR et une réduction du nombre d'alertes. Les outils SOC doivent quant à eux s'intégrer aux systèmes d'autres fournisseurs. Un choix plus large de playbooks, surtout ceux certifiés par des fournisseurs de solutions, contribuera à l'efficacité des SOC. Enfin, la Threat Intelligence doit elle aussi mieux s'intégrer aux outils SecOps.

Le SOAR peut résoudre nombre de ces problématiques. Des plateformes comme Cortex XSOAR permettent aux équipes SOC de gagner du temps, d'accélérer le tri des alertes et de réduire les étapes du processus IR. D'après notre enquête, à l'initiative des équipes SOC, cette technologie devrait s'étendre à de nouveaux cas d'usage innovants dans les 12 prochains mois. À l'heure où la Covid-19 accentue la pression sur les opérations de sécurité, le SOAR apparaît plus que jamais comme un vecteur d'efficacité et de productivité.

Annexe : données démographiques de l'enquête

Tous les participants à notre enquête sont membres de la communauté Virtual Intelligence Briefings qui réunit plus de 150 000 professionnels de la sécurité. La figure 22 illustre la taille des entreprises représentées et la proportion de chaque tranche parmi les sondés. Toutes les personnes interrogées occupent des postes dans les domaines de la sécurité et de la conformité.

Nous avons exclu les profils suivants de notre échantillon :

- Collaborateurs d'une entreprise de moins de 1 000 salariés ou qui externalise la totalité de sa sécurité
- Professionnels qui ignorent si leur sécurité est externalisée en tout ou partie
- Collaborateurs qui ne supervisent pas ou ne travaillent pas pour la fonction sécurité

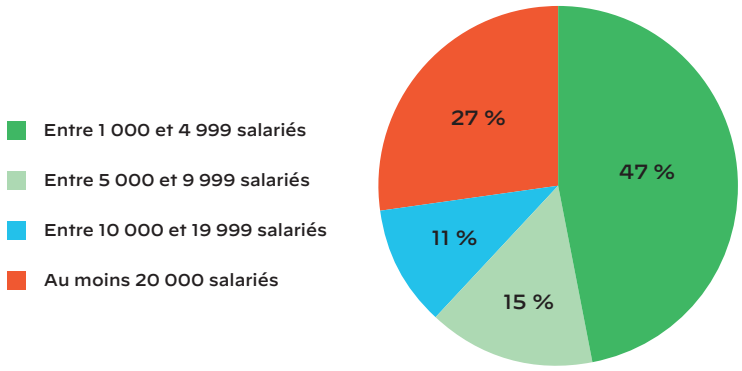

Figure 22 : Répartition des sondés par taille d'entreprise

Les secteurs représentés vont des services financiers (17 %) aux technologies et/ou services technologiques (15 %), en passant par la santé (13 %), le commerce de détail et d'autres industries dans une moindre mesure. Aucun secteur ne représente plus de 20 % de sondés. En termes de rôles, 24 % des personnes interrogées sont des analystes/ingénieurs sécurité. Les responsables d'une fonction de cybersécurité représentent 17 % des sondés, tandis 14 % sont des architectes sécurité.

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