Collaborateurs, processus, technologies : comment mettre en place un centre opérationnel de sécurité (SOC) réussi

kaspersky BRING ON THE FUTURE

Le boom des SOC

Les organisations se tournent de plus en plus vers les centres opérationnels de sécurité (SOC) pour se protéger des cyberattaques en centralisant le personnel, les outils et l'expertise en un seul département actif 24 h/24. Cette approche présente de nombreux avantages, parmi lesquels la réduction de la fragmentation de la sécurité informatique traditionnelle, mais aussi la transformation de la cybersécurité en centre de coût dont les performances et le retour sur investissement (ROI) peuvent être mesurés.

Toutefois, l'instauration ou l'agrandissement d'un SOC existant peut présenter une avalanche de défis complexes à relever. En premier lieu, citons la difficulté à trouver des collaborateurs qualifiés et à les retenir. La mise en place et l'entretien d'un SOC peuvent également s'avérer onéreux, ce qui nécessite un engagement financier à long terme.

L'une des questions fondamentales est de savoir s'il faut mettre en place ou agrandir les SOC en interne ou plutôt se tourner vers des SOC externalisés et des services administrés. Le marché des services SOC externalisés gagnant rapidement en maturité, un nombre croissant d'organisations combinent ces deux approches dans un souci de flexibilité.

Plusieurs difficultés techniques se posent : intégrer une suite d'outils idoine, obtenir une visibilité sur les systèmes les plus critiques, gérer les alertes par ordre de priorité et mettre en œuvre l'automatisation. Les SOC doivent néanmoins conserver suffisamment de flexibilité pour s'adapter aux nouvelles menaces et être en mesure de croître à mesure que les besoins de l'organisation évoluent.

Ce livre blanc vise à examiner les principaux défis qu'une organisation doit relever lorsqu'elle s'embarque dans l'aventure d'un nouveau projet de SOC.

Qu'est-ce qu'un SOC ?

De nos jours, un SOC typique exécute un nombre croissant de fonctions de sécurité :

- Classer les alertes de sécurité par ordre de priorité, les analyser et y répondre
- Établir le cyberdiagnostic des incidents de sécurité passés
- Surveiller la Threat Intelligence pour détecter des menaces futures
- Générer des rapports à des fins de conformité
- Exécuter en continu des tests de pénétration sur les capacités actuelles
- Recruter des experts aguerris dans la gestion des cyberattaques
- Appliquer une stratégie de gestion orientée risque, notamment par la correction et la gestion des systèmes hérités

La sécurité informatique traditionnelle repose sur un modèle de sécurité réactif qui suppose que la compromission d'un système peut être contenue et que les défenseurs auront le temps d'empêcher les tentatives de se déplacer latéralement au sein des réseaux. Le nombre croissant de signalements de cyberattaques a mis en lumière les failles de cette approche : la détection est faible et la réponse est trop lente.

Le concept de SOC comble ces lacunes de plusieurs manières. Le principal changement consiste à faire de la cybersécurité un département à part entière, distinct de la fonction informatique globale et capable d'appréhender la sécurité de façon unifiée. Composée de spécialistes de la cybersécurité, l'équipe SOC a pour mission de surveiller les menaces 24 h/24 afin d'accélérer la gestion des alertes, la détection des menaces et la réponse aux menaces.

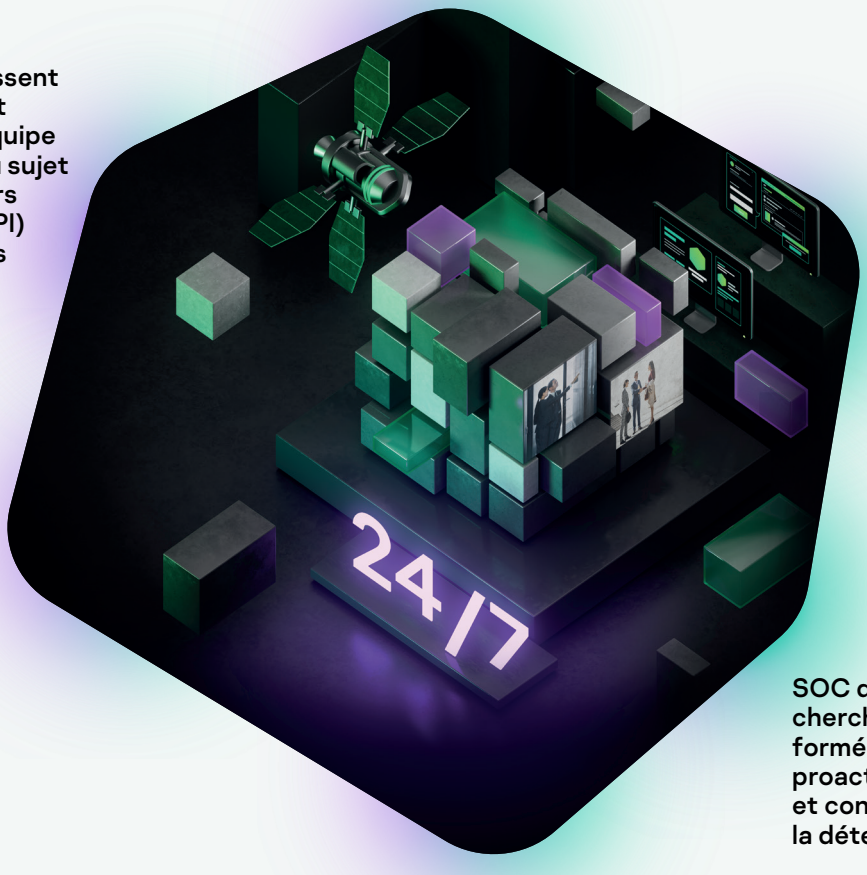
Au fur et à mesure, les SOC ont pris en charge des tâches plus complexes, par exemple en prédisant les menaces en plus d'y répondre.

L'équipe SOC

La mise en place d'un SOC requiert une division logique du travail entre les membres de l'équipe selon leurs compétences. Cela peut inclure :

SOC de niveau 1 : surveillance et tri initial des menaces. Il s'agit de la couche de sécurité chargée de détecter les menaces devant faire l'objet d'un examen attentif, et de les signaler à la hiérarchie si nécessaire.

La direction du SOC : responsables qui établissent la stratégie, planifient et communiquent avec l'équipe de direction générale au sujet du rôle et des indicateurs de performance clés (KPI) permettant d'évaluer les performances du SOC.



SOC de niveau 2 : fonction d'investigation et de réponse qui traite ces alertes, procède à une analyse plus approfondie des programmes malveillants et établit un cyberdiagnostic. Cette fonction se charge d'isoler et de résoudre les menaces avant de transmettre ces mises à jour au système SIEM et à la Threat Intelligence en ajoutant des indicateurs de compromission (IoC).

Les experts juridiques et experts en conformité du SOC.

SOC de niveau 3 : chercheur de menaces formé à la recherche proactive des menaces et contribuant à affiner la détection.

Des analystes spécialisés en programmes malveillants, en cyberdiagnostic et en Threat Intelligence. Les administrateurs du SOC entretiennent et déploient l'infrastructure et les outils du centre de sécurité, ils valident que les capteurs fonctionnent et qu'une infrastructure adaptée alimente les systèmes SIEM en données. Ils sont également chargés de programmer le code personnalisé nécessaire à l'automatisation et aux scripts des outils.

Difficultés de planification du SOC

Si le principe de centralisation de la sécurité au sein d'un SOC ne fait aucun doute quant à son intérêt, la mise en pratique peut s'avérer complexe. La plupart des organisations devront développer leurs capacités à partir d'un département existant, qui avec le temps a peut-être commencé à assumer certains rôles généralement attribués à un centre de sécurité. Pour délaisser cette approche confuse au profit d'une stratégie à même de libérer tout le potentiel d'un SOC, les organisations ont besoin d'une expérience dont elles ne disposent pas toujours.

L'enquête SANS 2021 sur les centres opérationnels de sécurité livre des conclusions concernant certaines de ces difficultés. Elle les classe en deux catégories : les problèmes universels, comme le recrutement de compétences adaptées, et les problèmes opérationnels, comme le fait de s'assurer que les outils et les processus de sécurité soient à la hauteur de la tâche. Les premiers sont les problèmes évidents dont tout concepteur de SOC a conscience, tandis que les seconds se manifestent pendant ou après la mise en œuvre.

L'éternel problème des qualifications

Acquérir des compétences en cybersécurité est devenu un problème enraciné qui n'est pas simple à résoudre. Mentionné par 24 % des sondés dans l'enquête SANS comme leur principal défi à relever, pallier le manque de compétences nécessite de se confronter à un marché vendeur pérenne. Non seulement les organisations doivent trouver des compétences spécifiques, mais l'évolution rapide des compétences nécessaires pour rester à jour dans ce secteur les oblige à constamment former et reformer les équipes existantes. La forte demande de telles compétences en cybersécurité rend le recrutement plus onéreux et entraîne un autre problème : retenir les meilleurs candidats. Kaspersky estime qu'un analyste en cybersécurité reste en moyenne moins de trois ans avec son employeur, il s'agit donc là d'un problème persistant.

Une autre difficulté consiste à comprendre quelles compétences et expériences sont spécifiquement nécessaires au développement d'un SOC, par rapport à un rôle plus généraliste dans le domaine informatique. Il peut s'agir de compétences non techniques, comme une communication claire essentielle à un service client de qualité. Quiconque s'attelant à un projet de SOC doit donc s'attendre à ce que la pénurie de compétences ne soit pas résolue en deux temps trois mouvements, même dans les organisations prêtes à investir du temps et de l'argent dans leur projet de SOC.

SOC interne ou externalisé ?

Malgré leur popularité croissante, les SOC internes demeurent l'exception qui confirme la règle. D'après l'enquête 2020 de Kaspersky sur les risques liés à la sécurité informatique pour les entreprises (ITSRS), menée auprès de 5 266 décideurs dans 31 pays, bien que 52 % des sondés disposent d'un service dédié à la sécurité informatique et que 14 % aient une équipe d'analyse des programmes malveillants, seul un sur cinq est doté d'un SOC interne. En fonction du secteur et de la taille de l'entreprise, cette proportion peut monter à 50 % dans certains cas, mais cela pose tout de même une question importante : les organisations ont-elles toutes besoin d'un SOC interne ?

Les SOC externalisés et les services de sécurité administrés permettent à davantage d'organisations de bénéficier des avantages d'un SOC centralisé sans investissement initial. Leur atout majeur est de résoudre immédiatement la difficulté à trouver et à recruter des collaborateurs compétents. Gartner estime que d'ici 2025, 90 % des SOC auront externalisé au moins la moitié de leurs fonctions de sécurité, pour laisser une part croissante au SOC-as-a-service (SOCaaS). D'autres chercheront à combiner différents éléments de la sécurité interne et externalisée.

D'après l'enquête ITSRS de Kaspersky, 69 % des sondés prévoyaient de faire appel à des fournisseurs de services administrés dans les 12 mois, principalement pour accéder à l'expertise dont manque leur organisation. Bien qu'il puisse sembler intéressant d'externaliser ces services pour combler la pénurie de compétences, les organisations doivent malgré tout évaluer les conséquences du recours à une tierce partie en termes de sécurité des données et de conformité. Le niveau de maturité des fournisseurs est variable et l'externalisation de la sécurité s'accompagne de son propre lot de difficultés.

Convaincre les dirigeants réticents

On dit souvent que la direction n'investit dans la cybersécurité qu'après les faits, lorsqu'il est déjà trop tard. Les dépenses nécessaires au développement et à l'entretien d'un centre de sécurité devraient donc être rédhibitoires. Pourtant, la popularité des SOC ne cesse d'augmenter. Pour les responsables de la sécurité informatiques, les arguments en faveur de l'investissement sont au nombre de trois. Le premier consiste à expliquer que la cybersécurité est une question d'évaluation et d'atténuation des risques. Cet argument sera davantage compris par les dirigeants qui n'ont pas un profil technique, car il ouvre la porte à des indicateurs de performance clés mesurables. Un deuxième argument avance que l'informatique traditionnelle fragmente la détection et la réponse. La cybersécurité est plus efficace lorsqu'elle est centralisée et mise en œuvre à plus grande échelle, ce que permet précisément le centre de sécurité.

Enfin, la cybersécurité représente aujourd'hui un avantage concurrentiel. Selon une enquête de Kaspersky datant de 2019, l'estimation de l'impact financier d'une cyberattaque était deux fois plus faible chez les organisations disposant d'un SOC interne que chez celles qui n'en avaient pas. La conclusion est claire : les organisations qui investissent dans un centre de sécurité subissent moins de répercussions financières sur le long terme.

Coût d'un projet de SOC

Les avantages de la mise en place et de l'exploitation d'un SOC interne sont universellement reconnus, mais naturellement les coûts varient d'une organisation à l'autre.

Cela étant dit, il peut être très utile d'avoir une idée, même vague, de l'investissement à prévoir avant de se lancer dans un changement de stratégie radical. Cela s'applique entre autres à la mise en place d'une SOC interne. Ce livre blanc vous indique un ordre de grandeur du coût des collaborateurs, des processus et des technologies dont votre entreprise aura besoin pour profiter entièrement du potentiel de défense révolutionnaire que seul un centre de sécurité interne peut vous apporter. Tous les chiffres sont des montants annuels en dollars américains et s'appliquent aux entreprises possédant plus de 1 000 terminaux.

Votre plus grande dépense concernera vos **collaborateurs**, notamment le directeur du SOC, mais aussi les analystes, les ingénieurs et la formation. Les frais de personnel s'élèvent généralement à environ 721 000 $.

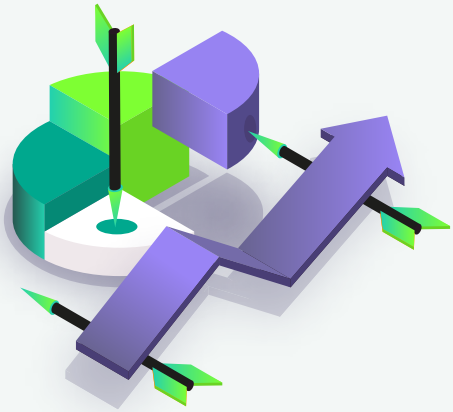
En ce qui concerne les frais liés aux **processus** courants, aux services de conseil pour les études de cas, aux manuels stratégiques et au reporting, vous pouvez tabler sur un montant d'environ 200 000 $.

Quant aux **technologies** en elles-mêmes, le coût s'élève généralement autour de 409 000 $; cela inclut les solutions EDR, le système SIEM, la détection des intrusions réseau, la Threat Intelligence, le système de tickets, la surveillance et le support.

Difficultés opérationnelles du SOC

Automatisation et orchestration

Point de tension crucial dans tout SOC, le besoin d'automatisation a été qualifié de problématique par 23 % des sondés dans l'enquête SANS. Le manque d'automatisation risque de surcharger le personnel et de faire perdre un temps précieux. De la même manière, la lutte contre les cyberattaques requiert généralement des mesures et une orchestration automatisées que seul le Machine Learning peut permettre de mettre en œuvre. Avec le temps, ce besoin d'automatisation et d'orchestration a augmenté, obligeant les entreprises à trouver des moyens d'application moins évidents mais innovants. SANS cite l'exemple d'une entreprise qui se sert de l'automatisation afin de consolider des données issues de plusieurs divisions pour alimenter un seul et même portail. Cela a réduit certains temps de réponse de 25 %. Ce n'est pas une exigence facile : la planification et la mise en œuvre de procédures d'automatisation est un projet complexe à long terme qui exige des trésors de réflexion et d'anticipation.



Migration et intégration des outils

Tout l'enjeu d'un SOC consiste à fournir une vue d'ensemble centralisée et unifiée de la sécurité d'une organisation. Il n'est pas toujours évident de rassembler les outils logiciels nécessaires pour y parvenir. Les organisations qui bâtissent un SOC en partant de zéro disposent généralement d'une collection hétéroclite d'outils de sécurité de diverses générations, ayant chacun une console et des paramètres opérationnels qui lui sont propres. Or, d'après les estimations, les centres de sécurité utilisent jusqu'à 20 outils en moyenne. Cela peut donc entraîner une fragmentation qui risque de ralentir la détection et la réponse. Dans certains cas, ces outils devront être rationalisés ou leur nombre devra être réduit. Le problème ne réside pas seulement dans le fait de posséder trop de consoles, dont tout le monde ne sait pas se servir. Ces systèmes génèrent par nature un volume de données considérable qui, avec le temps, noiera votre centre de sécurité sous cette masse de données.

Nombre excessif d'alertes (et faux positifs)

Depuis l'invention des systèmes de détection des intrusions à la fin des années 90, les systèmes de sécurité sont régulièrement décriés pour le volume d'alertes qu'ils génèrent. L'ajout d'une nouvelle génération d'application grâce à la technologie SIEM n'a fait qu'aggraver la situation. Un afflux d'alertes risque de surcharger les analystes de travail, d'affecter le temps de résolution moyen (MTTR) voire d'entraîner une indifférence totale aux alertes. De plus, les faux positifs génèrent du bruit et offrent aux attaquants une cachette idéale pour gagner du temps. Dans des cas extrêmes, cela peut signifier que les alertes sont purement et simplement ignorées, comme l'ont signalé 3 % des sondés dans l'enquête SANS. La principale raison citée était le manque de corrélation entre les alertes générées par différents systèmes.

Manque de visibilité sur les systèmes d'entreprise et les terminaux

Étonnamment, une surcharge d'alertes peut au contraire avoir pour conséquence un manque de visibilité sur les systèmes d'entreprise. Certains SOC excluent parfois les alertes SIEM provenant des systèmes « bruyants » tels que les terminaux qui génèrent trop de faux positifs. C'est une interprétation erronée de la théorie du « Less is more », un problème signalé à SANS par 15 % des sondés.

La détection des terminaux peut s'avérer complexe, mais limiter son champ d'action aggrave le problème, car il s'agit de cibles de choix pour une grande majorité des attaques connues. La compromission des terminaux a pris une telle importance aux yeux des cybercriminels, précisément parce que ces appareils et leurs utilisateurs sont plus difficiles à protéger. Cela concerne non seulement les PC et les appareils mobiles, mais aussi les objets connectés (IoT) et les périphériques tels que les imprimantes-scanners, qui ont souvent un contrôle d'accès permissif et dont peu disposent de solutions de sécurité. Par ailleurs, les attaques APT analysent de plus en plus les couches de niveau inférieur telles que les firmwares, rarement surveillées en temps réel par les logiciels de sécurité actuels.

Absence de contexte des alertes de menace

Même lorsqu'une anomalie est détectée, l'absence de contexte peut limiter son utilité pour un SOC. Par exemple, la détection des adresses URL suspectes est commune à tous les systèmes de sécurité et l'on peut compter plusieurs milliers de détections en une seule journée. Encore faut-il savoir quelle cyberattaque ou quel programme malveillant est associé(e) à cette URL, car cela donne aux centres de sécurité une longueur d'avance concernant la potentielle compromission à chercher ainsi que les outils, les tactiques et les procédures (TTP) à employer. Combler cette lacune nécessite une Threat Intelligence précise, un autre angle mort de la sécurité. Dans l'enquête SANS, 12 % des sondés ont affirmé que l'absence d'informations contextuelles sur les menaces constituait leur principale préoccupation.

Résoudre les problèmes

Trouver les compétences

Les organisations qui souhaitent attirer ou retenir les meilleurs collaborateurs au sein de leur SOC finissent souvent par augmenter les salaires de départ, qui ont atteint 125 000 $ aux États-Unis pour un analyste de base. Si cela peut fonctionner dans un premier temps, le problème fréquemment signalé de turnover élevé parmi le personnel suggère que cela ne suffit pas toujours à améliorer la rétention des talents à long terme. Une hausse des salaires de la direction risque également de modifier la perception qu'ont les hauts dirigeants du retour sur investissement (ROI) d'un SOC, ce qui pourrait avoir un impact sur les investissements futurs. L'efficacité d'un SOC peut être mesurée à l'aide de différents indicateurs, mais cela ne doit pas peser excessivement sur les ressources.

Paradoxalement, la surperformance des SOC pourrait finir par poser problème. L'exploitation d'un centre de sécurité constitue toujours un environnement exigeant, qui augmente la probabilité de burnout parmi les effectifs. Bien qu'il s'agisse d'un besoin opérationnel, le temps alloué à la formation du personnel peut se trouver réduit en raison de la pression des délais et des contraintes budgétaires. La rotation fréquente des effectifs finit par dégrader les SOC, qui perdent constamment des collaborateurs une fois que ceux-ci ont fait le tour du fonctionnement interne de l'entreprise.

Pour éviter cela, les centres de sécurité peuvent faire tourner le personnel sur différents postes, en particulier entre les niveaux 1 à 3. Cela augmente l'intérêt que les équipes portent à leur travail au sein du SOC, tout en réduisant la probabilité que les collaborateurs situés à l'échelon le plus bas, le niveau 1, ne deviennent surqualifiés pour leur poste après un an ou deux. Cette stratégie doit s'accompagner d'un programme de formation structuré permettant de décrocher des certifications telles que la GIAC (Global Information Assurance Certification). Dans certaines entreprises, les salaires de départ sont également échelonnés de manière à recevoir des augmentations au bout d'un, deux ou trois ans de travail.

Trouver des partenaires

Pour résoudre la pénurie de compétences, une solution de plus en plus plébiscitée consiste à externaliser certaines fonctions du SOC à un fournisseur de services administrés tiers. Cela évite d'avoir à trouver ou à retenir le personnel, puisque celui-ci fait partie intégrante du service fourni. Il n'est plus nécessaire non plus d'investir régulièrement dans la mise à niveau des équipements et des outils. La cybersécurité ne représente donc plus un coût d'investissement, mais un coût d'exploitation.

Les petites organisations sont de plus en plus nombreuses à avoir recours à des services administrés, car elles manquent d'expérience et de ressources financières pour mettre en place un centre de sécurité en partant de zéro. En ce qui concerne les moyennes et grandes entreprises, la balance bénéfice-risque est plus complexe à déterminer. Cela étant dit, les SOC tiers et les services administrés reviennent cher. En outre, cette solution présente d'autres difficultés telles que la gestion des contrats de niveau de services (SLA) et la définition des mesures de signalement, d'atténuation et de résolution des événements de sécurité gérés par le prestataire de services.

Les entreprises plus grandes engagent des SOC externes pour accéder à une expertise spécifique ou pour libérer les équipes internes afin de les affecter à d'autres projets de développement. Elles s'en servent de soupape. Elles comprennent par ailleurs qu'aussi mature que puisse être leur SOC interne, les attaquants finissent toujours par parvenir à pénétrer même les meilleures défenses. Lorsque cela arrive, pouvoir faire appel à l'expérience d'un partenaire peut faire toute la différence.

L'avenir des SOC

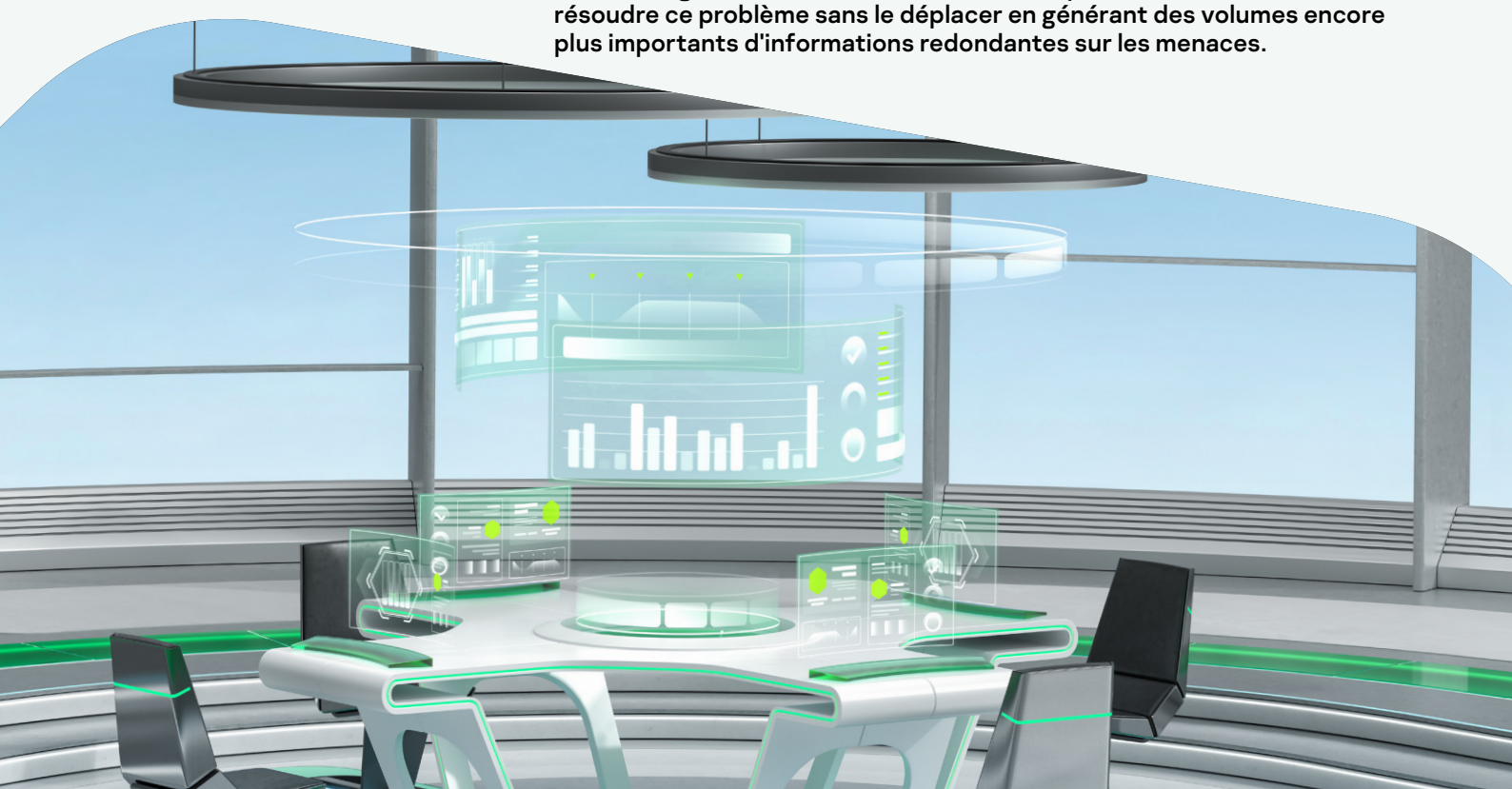
Comment l'essor des SOC pourrait influencer la cybersécurité dans les cinq prochaines années ?

Une possibilité serait qu'à mesure que les services SOC tiers deviennent de plus en plus sophistiqués, le SOCaaS se banalise, non seulement parmi les grandes entreprises mais aussi dans les organisations plus petites. Cela dépendra de la maturité des outils proposés ainsi que de la sophistication de l'offre de services. Les systèmes de sécurité actuels ont été conçus en premier lieu pour les départements informatiques internes, bien qu'ils aient été nombreux à s'adapter à une utilisation au sein d'un SOC. De plus en plus de fournisseurs conçoivent des outils de nouvelle génération spécifiquement dédiés aux environnements SOC. Ceux-ci seront optimisés pour gérer le flux de travail d'un SOC en termes de détection de menaces complexes et de réponse aux incidents, tout en prenant en charge des environnements exigeants tels que le télétravail et le cloud.

Cela pourrait favoriser un cercle vertueux grâce auquel les systèmes de sécurité seraient conçus et actualisés plus rapidement de manière à gérer la détection et la réponse aux menaces réelles, plutôt que des menaces généralisées. Les ransomwares sont un bon exemple de ce phénomène, car ils influencent à présent la conception de nombreux outils, des systèmes d'exploitation aux systèmes de sauvegarde en passant par les plateformes complètes de réponse aux incidents.

L'automatisation est une autre tendance inexorable dont l'influence se fait déjà sentir dans la surveillance et l'analyse des menaces de niveau 1. L'augmentation de l'automatisation est désormais un levier essentiel de l'évolution des SOC. Il n'y aura jamais assez d'analystes formés pour prendre le temps de passer au crible et de corréler la chaîne de frappe d'une attaque parmi un fatras de données de journal. Les éditeurs de solutions de sécurité capables de fournir des outils d'automatisation en mesure d'exécuter ces tâches seront très demandés.

Toutefois, l'avenir des SOC ne dépend pas simplement de l'accélération de la détection en déléguant plus de travail aux machines. Les centres de sécurité traitent et génèrent des quantités potentiellement astronomiques de données. En théorie, l'automatisation peut aider à réduire les besoins en stockage de données en identifiant les schémas de données importants et ceux qui sont secondaires. Les systèmes de sécurité sont souvent accusés de surcharger les défenseurs de données superflues, et les SOC doivent résoudre ce problème sans le déplacer en générant des volumes encore plus importants d'informations redondantes sur les menaces.



Comment Kaspersky peut vous aider

Nous comprenons les difficultés que représentent la mise en place et l'exploitation d'un SOC interne, et nous sommes fiers des grands progrès réalisés par les grandes entreprises internationales dans leur lutte contre les APT et autres menaces similaires en décidant de mener ce combat en interne.

Forts de plus de 20 années de recherche permanente de menaces, de technologies de protection leaders du marché, d'une expertise reconnue et d'une expérience éprouvée dans les projets de cybersécurité complexes, nous sommes à même de vous aider à libérer le potentiel de votre SOC pour gagner en efficacité à tous les niveaux afin de vous protéger contre des cybermenaces de plus en plus sophistiquées.

Contactez-nous

Recommandations de lecture :

Gérer la complexité croissante de l'informatique

Rapport analytique concernant les réponses aux incidents

Éviter l'épuisement de votre équipe de cybersécurité en cinq étapes

www.kaspersky.fr