Enterprise Strategy Group | Obtenir la vérité absolue.MC

Modernisation du SOC et rôle de la XDR

Jon Oltsik, premier analyste principal, boursier ESG
Dave Gruber, analyste principal

JUIN 2022

Objectifs **de la recherche**

Les opérations de sécurité nécessitent une imposante échelle pour recueillir, traiter, analyser des quantités massives de données, et y réagir. Au début, la détection et réponse étendues (XDR) était ancrée à deux sources de données principales : les terminaux et les réseaux. Bien qu'il s'agisse d'une amélioration par rapport aux outils de détection et réponse pour les terminaux (EDR) et de détection et réponse pour les réseaux (NDR) déconnectés, la détection et la gestion des menaces dans les entreprises nécessitent une plus grande ouverture, y compris les charges de travail en nuage, les flux d'informations sur les menaces, les applications de logiciel-service (SaaS) et la visibilité sur la gestion des identités et des accès. En même temps, afin de moderniser les centres des opérations de sécurité (SOC) et de suivre le volume d'alertes de sécurité, les grandes entreprises ont besoin d'analyses sophistiquées pour aider à automatiser les tâches des analystes de premier niveau comme le tri des alertes, la corrélation des alertes avec les indicateurs de compromission (IOC) et la préparation des incidents pour les enquêtes.

Afin de mieux comprendre ces tendances, ESG a interrogé 376 professionnels des TI et de la cybersécurité dans des entreprises en Amérique du Nord (États-Unis et Canada) personnellement responsables de l'évaluation, de l'achat et de l'utilisation des produits et services de détection et de gestion des menaces.

CETTE ÉTUDE VISAIT À :

Examiner les personnes, les processus et les technologies qui prennent en charge la modernisation des opérations de sécurité.

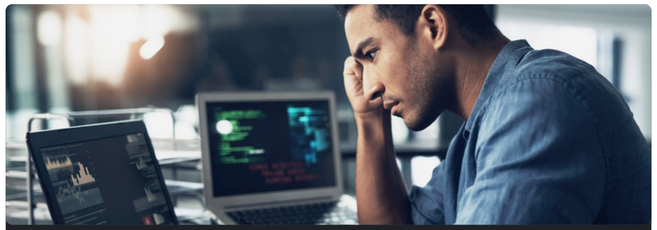
Déterminer la perception actuelle et le rôle de la XDR en tant que composante des efforts de modernisation des opérations de sécurité.

Relever les points de valeur clés, les mesures nécessaires pour soutenir ces points de valeur, et ce qui est attendu des produits et des services gérés pour la modernisation de la XDR et du SOC.

Explorer les stratégies utilisées pour automatiser le triage, accélérer les enquêtes et aider les entreprises à détecter des menaces inconnues.

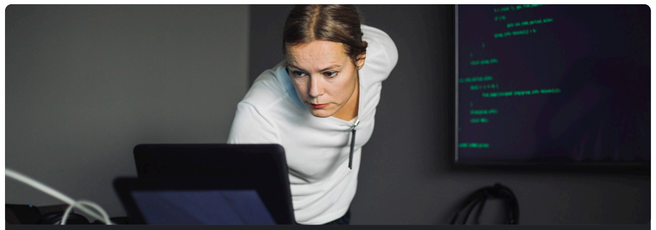
PRINCIPALES CONCLUSIONS

CLIQUEZ POUR SUIVRE



Les opérations de sécurité demeurent difficiles.

L'augmentation de la difficulté est due à la surface d'attaque croissante, au paysage des menaces dangereuses et à l'utilisation croissante de l'informatique en nuage.



Les professionnels de la sécurité veulent plus de données et de meilleures règles de détection.

Malgré l'énorme quantité de données de sécurité utilisées, on en souhaite plus, tout comme de meilleures règles de détection.

Les investissements dans l'automatisation des processus d'opérations de sécurité s'avèrent précieux.

Bien que les stratégies de mise en œuvre varient, la plupart des investissements dans l'automatisation sont payants.

Le cadre MITRE ATT&CK s'avère utile dans la plupart des cas

Cependant, beaucoup sont encore à déterminer comment et où l'appliquer pour qu'il apporte de la valeur.

L'élan de la XDR continue de s'accélérer.

Bien qu'il y ait une certaine confusion sur ce qu'est la XDR, l'investissement dans la prise en charge de la détection des menaces sophistiquées est important.

La MDR est courante et de plus en plus utilisée.

Bien que les scénarios d'utilisation varient, les services de MDR sont largement adoptés dans les entreprises de toutes tailles et de toutes maturités.

Retour au contenu

Les opérations de sécurité demeurent difficiles.

Les opérations de **sécurité** sont devenues plus difficiles dans la plupart des entreprises au cours des dernières années. Plus précisément, plus de la moitié (52 %) des répondants croient que l'environnement des opérations de sécurité de leur entreprise est devenu plus difficile à gérer au cours des deux dernières années. Cela est dû à des facteurs tels que le paysage des menaces de plus en plus dangereuses, une surface d'attaque croissante, le volume et la complexité des alertes de sécurité et la prolifération du nuage public. Étant donné que ces défis ne feront que s'accélérer à l'avenir, de nombreux responsables de la sécurité des systèmes d'information se rendent compte que les stratégies actuelles du centre des opérations de sécurité sont inadéquates. Pour faire face à l'augmentation du volume des menaces et à l'évolutivité et à l'étalement des TI, les entreprises ont lancé plusieurs initiatives axées sur la modernisation du SOC.

52 %

des entreprises pensent que les opérations de sécurité sont plus difficiles aujourd'hui qu'elles ne l'étaient il y a deux ans.

Les opérations de sécurité sont plus difficiles aujourd'hui qu'elles ne l'étaient il y a deux ans, car :

Le paysage des menaces se développe et évolue rapidement,

41 %

La surface d'attaque s'est élargie,

40 %

La surface d'attaque change et évolue continuellement,

39 %

Le volume et la complexité des alertes de sécurité ont augmenté,

37 %

L'utilisation des services de nuage public a augmenté,

34 %

« Les entreprises ont lancé plusieurs initiatives **axées sur la modernisation du SOC. »**

Retour au contenu

Les opérations de sécurité sont touchées par la pénurie mondiale de ressources humaines compétences

En plus des défis généraux liés aux opérations de sécurité, il faut souligner que 81 % des entreprises conviennent que les opérations de sécurité ont été touchées par la pénurie mondiale de ressources humaines compétentes en cybersécurité. En général, cela entraîne une augmentation de la charge de travail du personnel en place, ainsi que l'attrition et l'épuisement professionnel du personnel. Les professionnels de la sécurité soulignent plusieurs domaines où le personnel et les compétences font particulièrement défaut, notamment les architectes en sécurité, les ingénieurs en sécurité, les analystes de troisième niveau, et les analystes de l'évaluation et de la hiérarchisation des vulnérabilités.

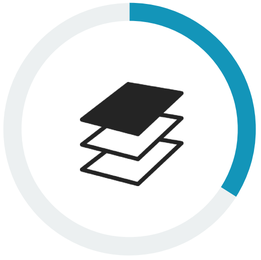
81 %

des entreprises conviennent que leurs opérations de sécurité **ont été touchées par la pénurie de ressources humaines compétentes en cybersécurité.**

Les domaines les plus en sous-effectif des opérations de sécurité.

Architectes en sécurité,
37 %

Ingénieurs en sécurité,
35 %



Analystes de troisième niveau*,
34 %

Analystes de l'évaluation et de la hiérarchisation des vulnérabilités,
33 %

** C'est-à-dire qu'ils sont semblables aux analystes de deuxième niveau, mais qu'ils sont plus expérimentés et se concentrent sur les problèmes complexes ou critiques.*

Retour au contenu

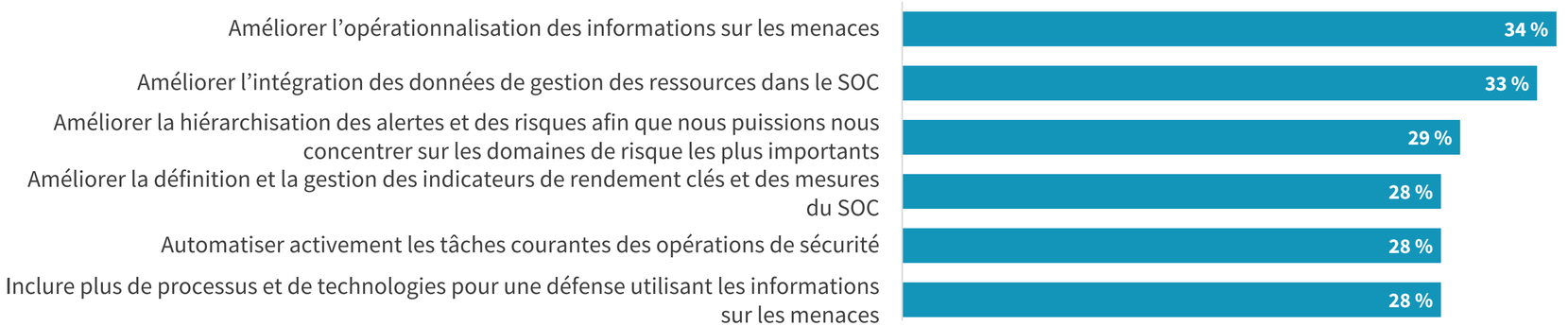
Priorités de modernisation du SOC à court terme

Comment les entreprises prévoient-elles de gérer des environnements opérationnels de sécurité de plus en plus difficiles, y compris des niveaux de dotation insuffisants? La modernisation du SOC est une initiative clé du programme, 88 % des entreprises ayant augmenté leurs dépenses de sécurité cette année. À court terme, les équipes du SOC prévoient de concentrer leurs efforts sur des domaines tels que l'amélioration de l'opérationnalisation des informations sur les menaces, l'amélioration de l'intégration des données de gestion des ressources dans le SOC, l'amélioration de la hiérarchisation des risques et des alertes, l'amélioration de la définition et de la gestion des indicateurs de rendement clés du SOC et l'automatisation des tâches courantes des opérations de sécurité.

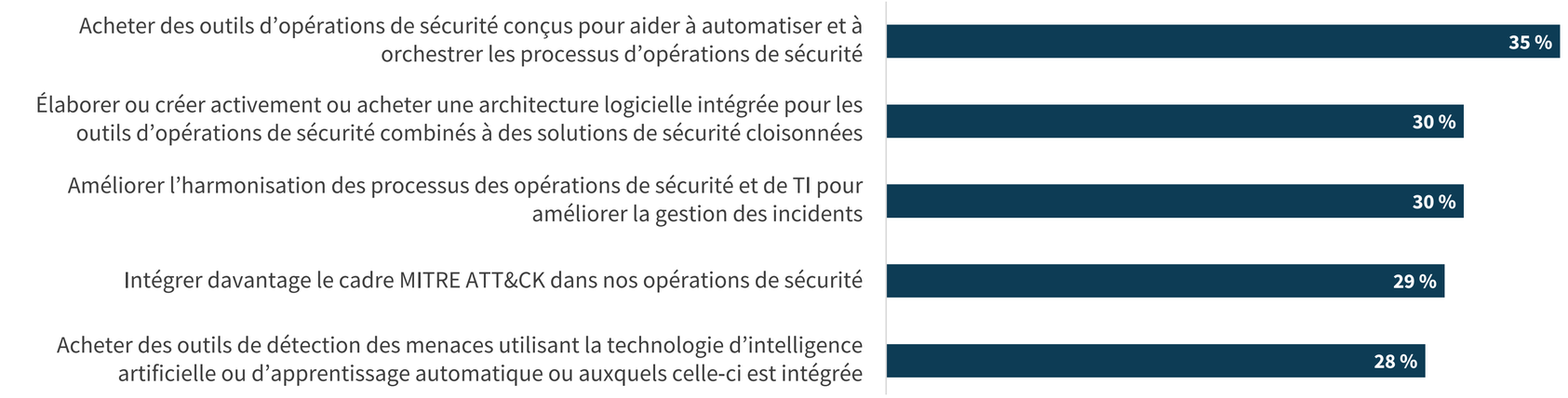
À l'avenir, les entreprises prendront de nombreuses mesures supplémentaires vers la modernisation du centre des opérations de sécurité, comme l'achat d'outils d'automatisation des processus de sécurité, le développement et la création d'une architecture intégrée de plateforme d'analyse et d'opérations de sécurité (SOAPA), l'amélioration de l'harmonisation de la sécurité et des opérations des TI, l'intégration plus poussée du cadre MITRE ATT&CK aux opérations de sécurité et l'achat d'outils d'analyses sophistiquées pour la détection des menaces.

Ces avancées prendront du temps et pourraient nécessiter l'assistance des services de sécurité. Néanmoins, elles doivent être considérées comme des étapes sur le parcours de la modernisation du centre des opérations de sécurité. L'objectif est de créer un SOC qui peut offrir l'évolutivité, le rendement, les informations, l'automatisation et la gérabilité pour prévenir, détecter et gérer les menaces, gérer les risques et soutenir la mission de l'entreprise.

Objectifs axés sur le SOC prévus au cours des 12 prochains mois.



Actions prévues pour améliorer les opérations de sécurité au cours des 12 à 18 prochains mois.



Retour au contenu

Les professionnels de la sécurité veulent plus de données et de meilleures règles de détection

Malgré le passage à la XDR, les données des terminaux sont toujours les plus précieuses

Huit entreprises sur dix recueillent, traitent et analysent les données des opérations de sécurité provenant de plus de dix sources de données. Les professionnels de la sécurité estiment que les sources les plus importantes sont les données de sécurité des terminaux, les flux d'informations sur les menaces, les journaux des appareils de sécurité, les données de gestion de la posture du nuage et les journaux de flux réseau. Bien que cela semble beaucoup de données, les répondants du sondage souhaitent en fait utiliser plus de données pour les opérations de sécurité, d'où le besoin de référentiels de données dorsaux évolutifs, performants et infonuagiques.

80 %

des entreprises utilisent plus de dix sources de données dans le cadre de leurs opérations de sécurité.

« Les répondants veulent en fait utiliser **plus de données pour les opérations de sécurité.** »

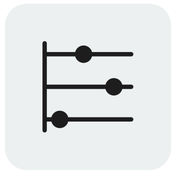
Les sources de données les plus importantes pour les opérations de sécurité.

24 %

Données sur la sécurité des terminaux

21 %

Flux d'information sur les menaces



20 %

Données des journaux des appareils de sécurité

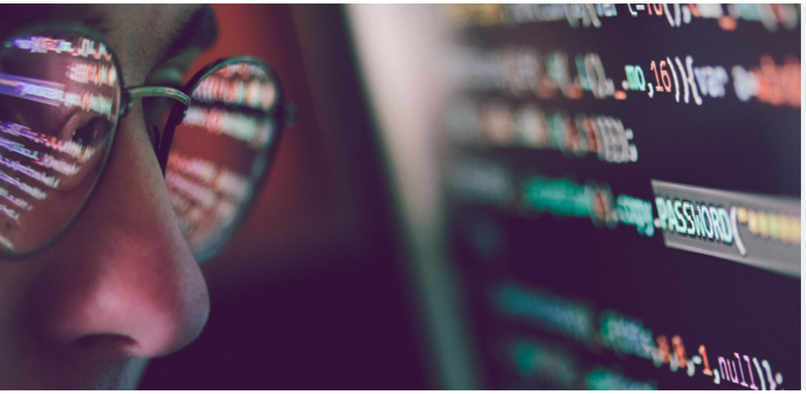
20 %

Systèmes de gestion de la posture de sécurité dans le nuage

18 %

Données NetFlow et/ou IPFIX, et/ou journaux de flux VPC

Retour au contenu

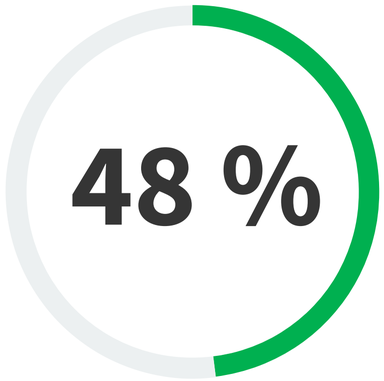


La plupart des entreprises élaborent leurs propres règles de détection personnalisées

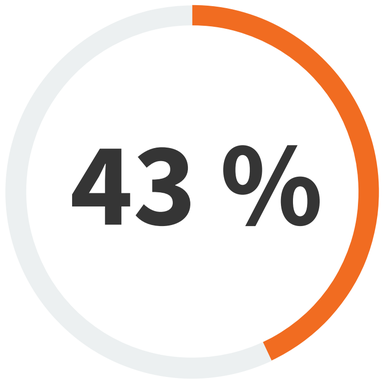
Bien que les fournisseurs fournissent des volumes croissants de contenu prêt à l'emploi pour la détection des menaces, 91 % des entreprises complètent ces efforts avec leur propre ingénierie de détection. En fait, les équipes du SOC recueillent, traitent et analysent diverses données de télémétrie de sécurité pour les aider à déterminer les faiblesses de détection où des règles personnalisées sont nécessaires. Les équipes de sécurité personnalisent les ensembles de règles des fournisseurs pour répondre à leurs besoins et élaborent des règles personnalisées pour détecter les menaces ciblant leur secteur ou leur organisation. Pour soutenir cette tendance, les fournisseurs doivent faciliter la collaboration du réseau d'utilisateurs tout en adoptant des normes ouvertes telles que Sigma et YARA avec un soutien établi du secteur.

Étendue des règles de détection des menaces personnalisées.

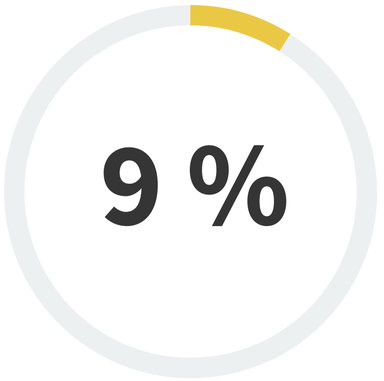
Mon entreprise élabore un nombre important de règles personnalisées pour compléter les règles de détection fournies par les fournisseurs.



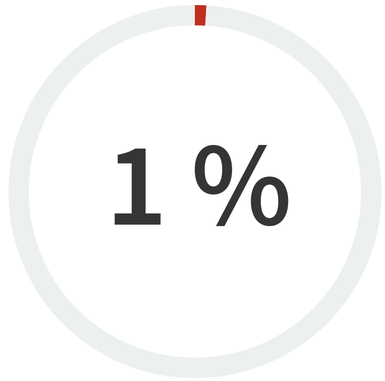
Mon entreprise élabore plusieurs règles personnalisées pour compléter les règles de détection fournies par les fournisseurs.



Mon entreprise peut élaborer quelques règles de détection personnalisées, mais elle s'appuie principalement sur celles fournies par les fournisseurs.



Mon entreprise n'élabore pas de règles de détection personnalisées et s'appuie entièrement sur celles fournies par les fournisseurs.



Retour au contenu

Les investissements dans l’automatisation des processus d’opérations de sécurité s’avèrent précieux

De nombreuses entreprises ont tiré parti des avantages de l'automatisation des processus de sécurité, mais des défis persistent.

L'automatisation des processus de sécurité est populaire, comme en témoignent les 90 % des entreprises qui automatisent actuellement leurs processus d'opérations de sécurité, 46 % qualifiant leurs efforts d'automatisation d'importants. Ceux qui participent à l'automatisation des processus de sécurité font état d'avantages tels que l'amélioration de la détection des menaces à l'aide de guides, du délai moyen de résolution (MTTR) et de la hiérarchisation des incidents, ainsi que la possibilité d'isoler plus rapidement les ressources infectées. Compte tenu des défis liés aux opérations de sécurité, comme la surface d'attaque croissante, les tempêtes d'alertes et le paysage des menaces dangereuses, l'automatisation des processus de sécurité se poursuivra et fusionnera probablement avec l'automatisation des processus informatiques pour améliorer l'efficacité des TI et de la sécurité.

Bien que l'automatisation des processus de sécurité demeure populaire et bénéfique, elle s'accompagne de certains défis. Près de deux entreprises sur cinq (39 %) affirment que leur équipe des opérations de sécurité n'a pas les compétences de programmation adéquates pour développer des cahiers d'exploitation et des flux de travail dans les outils de SOAR, tandis que 21 % affirment que leurs processus d'opérations de sécurité ne sont pas matures et doivent être repensés avant de pouvoir être automatisés. Dans ces cas, les entreprises doivent évaluer davantage les flux de travail des processus, en recherchant les goulots d'étranglement avant de passer à l'automatisation. Les personnes ayant des compétences limitées en programmation doivent étudier les options de SOAR avec peu ou pas de code, ou utiliser la fonctionnalité d'automatisation des processus intégrée dans d'autres outils d'exploitation.

Les avantages les plus couramment obtenus de l'automatisation des processus des opérations de sécurité.

Amélioration de la détection des menaces à l'aide de guides

51 %

Amélioration du délai moyen de réponse

49 %

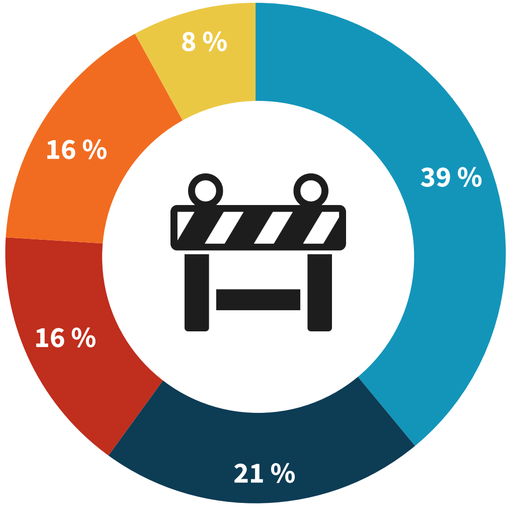
Amélioration de la hiérarchisation des incidents

44 %

Isolation plus rapide des ressources infectées

44 %

Les plus grands obstacles à l'automatisation des processus des opérations de sécurité.



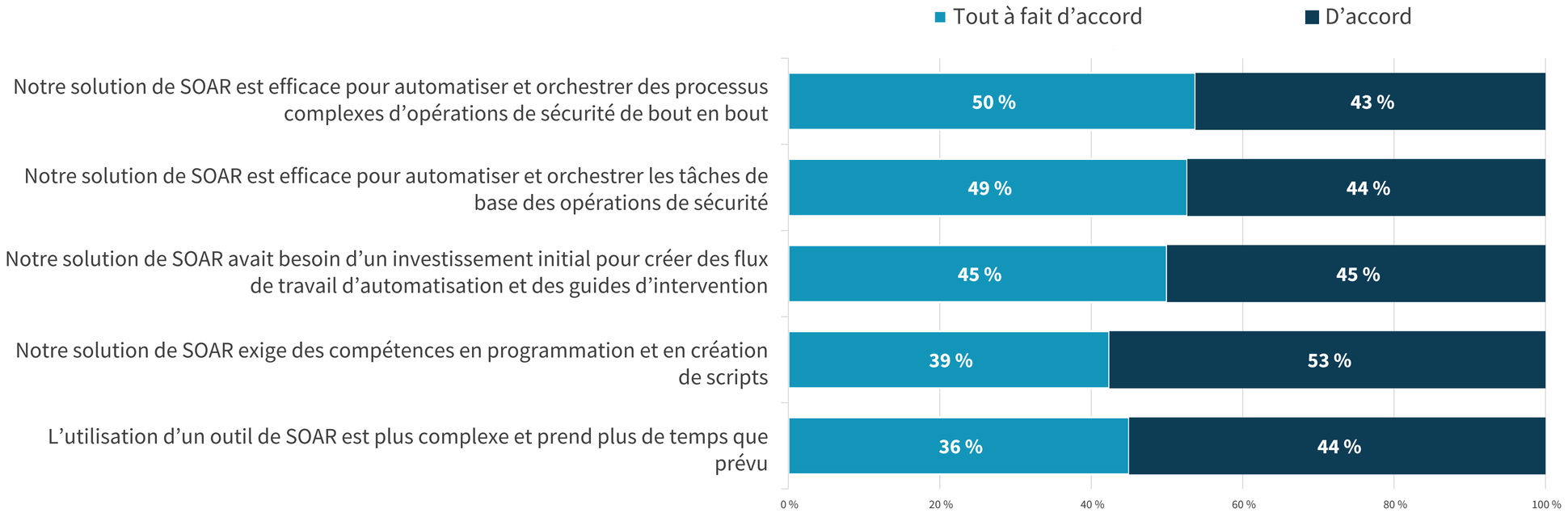
- Compétences en développement de logiciels : Notre équipe des opérations de sécurité n'a pas les compétences en programmation nécessaires pour développer des dossiers d'exploitation ou des flux de travail
- Immaturité des processus : Nos processus d'opérations de sécurité sont relativement immatures, nous devrons donc vraiment les remanier avant de procéder à l'automatisation des processus
- Temps : L'équipe de sécurité n'a pas suffisamment de temps pour travailler sur l'automatisation des processus
- Outils : Notre entreprise ne dispose pas des technologies, comme le SOAR, nécessaires pour l'automatisation des processus de sécurité
- Aucun obstacle

Retour au contenu

Les outils de SOAR peuvent produire des résultats avec les bons investissements initiaux et les bonnes attentes

Plus d'un quart (29 %) des entreprises utilisent un type d'outil d'orchestration, d'automatisation et de réponse de sécurité (SOAR) pour l'automatisation des processus. L'utilisation de SOAR peut être bénéfique : 93 % des professionnels de la sécurité conviennent que leur solution de SOAR est efficace pour automatiser les processus complexes d'opérations de sécurité de bout en bout et pour automatiser ou orchestrer les tâches d'opérations de sécurité de base. Cependant, SOAR n'est pas sans frais. La réussite dépend d'une planification initiale, d'investissements et des compétences adéquates. Par exemple, 90 % des professionnels de la sécurité affirment que SOAR avait besoin d'un investissement initial pour créer des flux de travail d'automatisation et des guides de réponse, 92 % conviennent que SOAR exige des compétences en programmation et en écriture de scripts, et 80 % conviennent que l'utilisation d'un outil de SOAR est plus complexe et prend plus de temps que prévu. Sur la base de ces données, les entreprises doivent reconnaître que SOAR doit être considéré comme un projet, et non comme une panacée. Les avantages de SOAR ne peuvent être obtenus qu'avec le bon niveau de planification, de formation et de gestion de projet.

Outils d'orchestration, d'automatisation et de réponse de sécurité (SOAR)



« L'utilisation de SOAR peut être bénéfique. »

Retour au contenu

Le cadre MITRE ATT&CK s’avère utile dans la plupart des cas

La plupart des entreprises utilisent et voient la valeur du cadre MITRE ATT&CK pour les opérations de sécurité

Le cadre MITRE ATT&CK a gagné en popularité au point que près de neuf entreprises sur dix l'utilisent dans une certaine mesure aujourd'hui. À mesure que les responsables du SOC se tournent vers l'avenir, ils constatent une utilisation encore plus grande de MITRE. En fait, 97 % des professionnels de la sécurité croient que MITRE ATT&CK (et les projets dérivés) seront essentiels, très importants ou importants pour la stratégie des opérations de sécurité de leur entreprise.

Utilisation du cadre MITRE ATT&CK pour les opérations de sécurité.

Les entreprises utilisent-elles le cadre MITRE ATT&CK pour les opérations de sécurité?

Importance du cadre MITRE ATT&CK pour les opérations de sécurité.

97 %

des professionnels de la sécurité croient que MITRE ATT&CK (et les projets dérivés) seront essentiels, très importants ou importants pour la stratégie des opérations de sécurité de leur entreprise.

Retour au contenu

Les scénarios d'utilisation de MITRE ATT&CK sont nombreux

MITRE ATT&CK est également devenu essentiel dans une panoplie de processus d'opérations de sécurité. Parmi les entreprises qui adoptent le cadre MITRE ATT&CK, 38 % l'utilisent pour les aider à utiliser les informations sur les menaces dans leur processus de triage des alertes ou d'enquête, 37 % l'utilisent comme ligne directrice pour l'ingénierie de sécurité, 35 % utilisent MITRE pour mieux comprendre les tactiques, les techniques, et les procédures des cyberadversaires, et 34 % utilisent le cadre pour les aider à comprendre plus rapidement l'étendue des attaques.

De cette manière, les entreprises opérationnalisent MITRE ATT&CK pour la prévention, la détection et la gestion des menaces.

Façons dont les entreprises utilisent le cadre MITRE ATT&CK.

Pour nous aider à mieux utiliser les informations sur les menaces dans nos processus de triage des alertes ou d'enquête,

38 %

En tant que ligne directrice pour l'ingénierie de sécurité,

37 %

Pour mieux comprendre les tactiques, les techniques et les procédures des cyberadversaires,

35 %

Pour aider les entreprises à comprendre plus rapidement l'étendue des attaques,

34 %

Pour nous assurer que nous recueillons les bonnes données à partir des bonnes sources de données,

33 %

« MITRE ATT&CK est également devenu **essentiel dans une panoplie de processus d'opérations de sécurité. »**

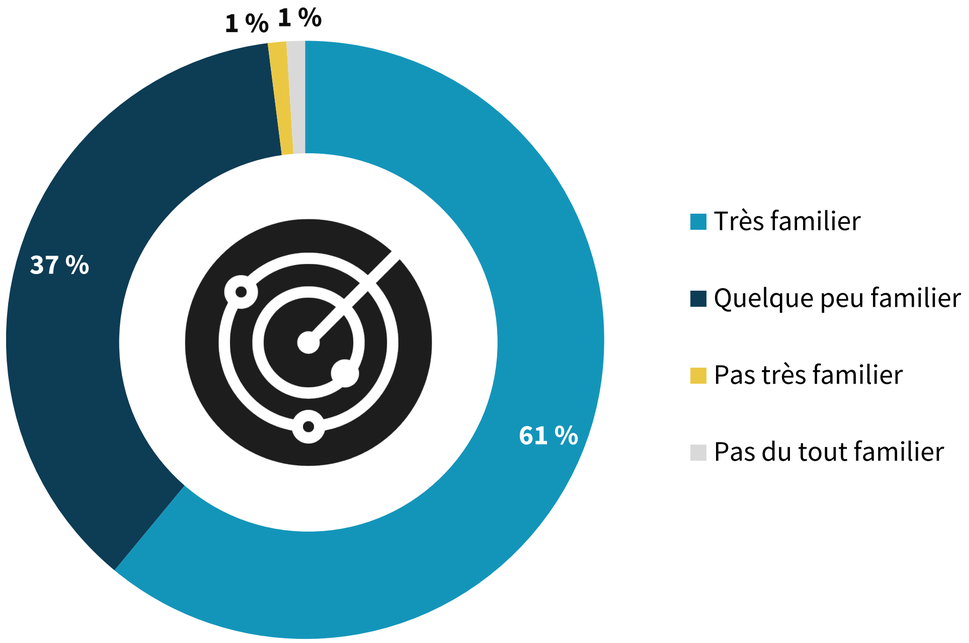
Retour au contenu

L’élan de la XDR continue de s’accélérer.

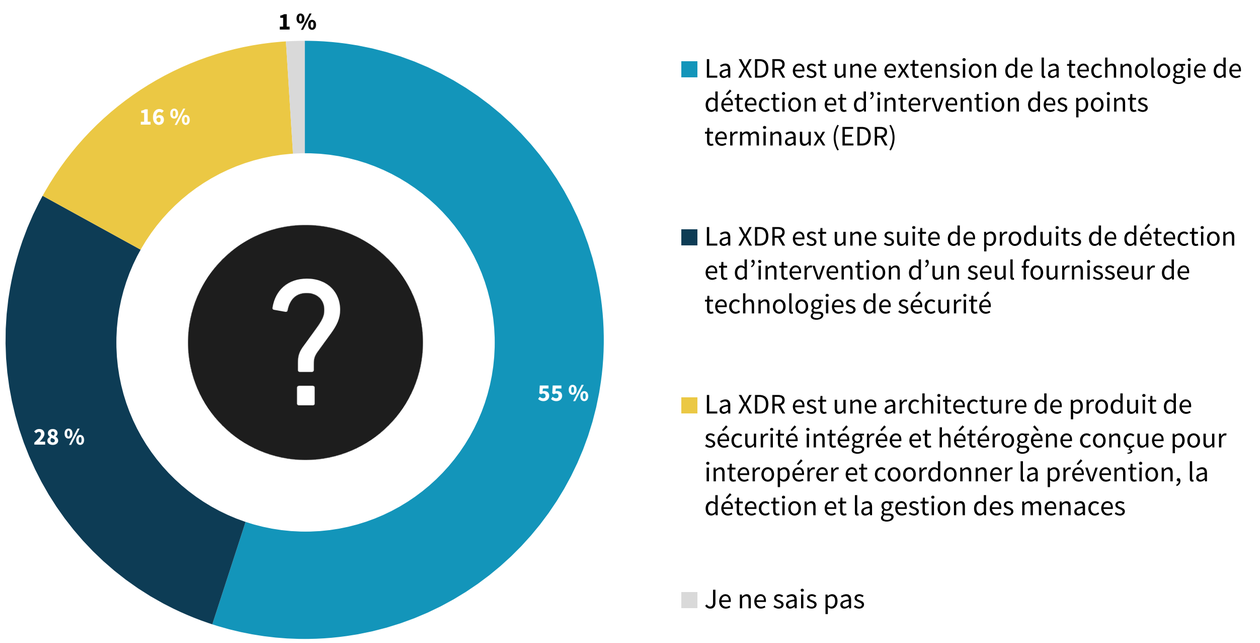
La notoriété de la XDR continue de croître, bien que la plupart constatent que la XDR s'ajoute aux technologies du SOC ou les consolide.

Bien que la technologie de XDR ait attiré l'attention du secteur, elle demeure un concept vague avec différentes composantes et définitions. Cela se reflète dans le fait que 61 % des professionnels de la sécurité affirment connaître très bien la technologie de XDR. Bien qu'il s'agisse d'une amélioration par rapport à la recherche d'ESG de 2020 (alors que seulement 24 % des professionnels de la sécurité connaissaient très bien la XDR), 39 % sont encore quelque peu familiers, pas très familiers ou pas du tout familiers avec la XDR. Les utilisateurs sont également confus au sujet de ce qu'est la XDR. Tandis que 55 % des répondants affirment que la XDR est une extension de l'EDR, 44 % pensent que la XDR est un produit de détection et d'intervention provenant d'un fournisseur de technologies de sécurité unique ou d'une architecture de produit de sécurité intégrée et hétérogène conçue pour interopérer et coordonner la prévention, la détection et la gestion des menaces. Il est prudent de dire que la XDR n'est pas encore inachevée.

Connaissance de la technologie de XDR.



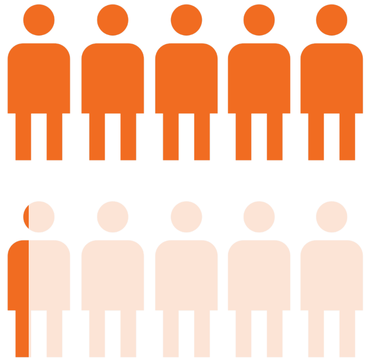
Définitions organisationnelles de la technologie de XDR.



Retour au contenu

La plupart voient la XDR s’ajouter aux technologies du SOC ou les consolider

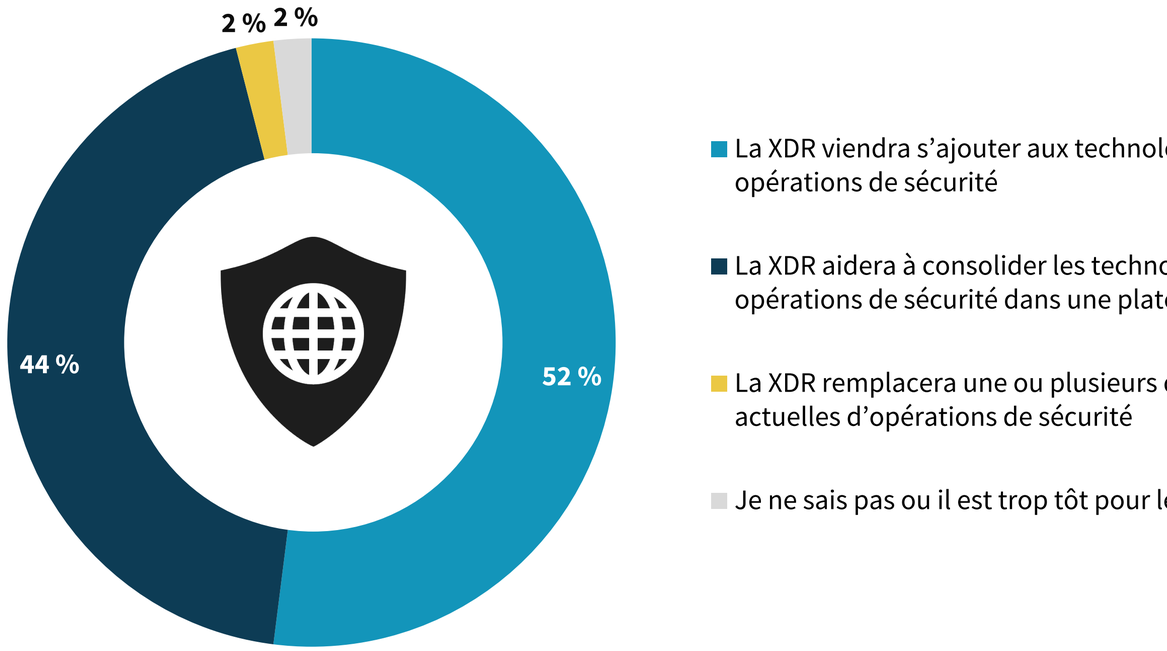
Dans cette optique, à ce stade, la XDR n’est pas considérée comme un remplacement potentiel pour les technologies du SOC comme la SIEM, le SOAR et la TIP. Plutôt, plus de la moitié (52 %) des professionnels de la sécurité croient que la XDR s’ajoutera aux technologies d’opérations de sécurité existantes, tandis que 44 % considèrent que la XDR regroupe les technologies d’opérations de sécurité actuelles en une plateforme commune. Seulement 2 % croient que XDR remplacera toutes les technologies actuelles d’opérations de sécurité.



PLUS DE LA MOITIÉ

des professionnels de la sécurité pensent que **la XDR viendra s’ajouter aux technologies d’opérations de sécurité existantes.**

Incidence prévue de la XDR sur les environnements d’opérations de sécurité.



Retour au contenu

Les utilisateurs veulent que la XDR réponde aux défis courants de détection et de gestion des menaces

Quelle que soit la définition de la XDR, les professionnels de la sécurité souhaitent utiliser la XDR pour les aider à relever plusieurs défis en matière de détection et de gestion des menaces. La XDR semble être une option attrayante, car les outils actuels ont du mal à détecter et à analyser les menaces sophistiquées, nécessitent des compétences spécialisées et ne sont pas efficaces pour corréler les alertes. En résumé, les responsables de la sécurité des systèmes d'information (RSSI) veulent des outils de XDR qui peuvent améliorer l'efficacité de la sécurité, en particulier en ce qui concerne la détection des menaces sophistiquées. En outre, ils veulent que la XDR simplifie les opérations de sécurité et renforce la productivité du personnel.

Les professionnels de la sécurité semblent avoir à l'esprit un certain nombre de scénarios courants de la XDR. Par exemple, 26 % des professionnels de la sécurité veulent que la XDR aide à hiérarchiser les alertes en fonction des risques, 26 % cherchent à améliorer la détection des menaces sophistiquées, 25 % veulent des enquêtes sur les menaces et des analyses plus efficaces, 25 % souhaitent un ajout par couches aux outils de détection des menaces existants, et 25 % pensent que la technologie de XDR pourrait améliorer la détection des menaces afin de renforcer les contrôles de sécurité et de prévenir de futures attaques semblables. De toute évidence, les utilisateurs veulent que la XDR comble les lacunes de la pile de sécurité tout en améliorant l'efficacité et l'efficience de la détection et de la gestion des menaces.

Les cinq défis les plus courants qui stimulent l'intérêt pour la XDR.

51 %

Les outils actuels peinent à détecter et à analyser les menaces sophistiquées

38 %

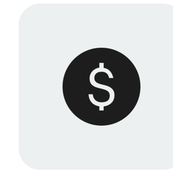
Les outils actuels nécessitent trop de compétences spécialisées

36 %

Les outils actuels ne sont pas efficaces pour corréler les alertes

35 %

Lacunes précises dans les capacités de détection et de gestion en nuage



32 %

L'approche actuelle des outils est trop dispendieuse

Les cinq scénarios de XDR les plus prioritaires.

26 %

Une solution de XDR qui pourrait aider à hiérarchiser les alertes en fonction des risques

26 %

Détection améliorée des menaces sophistiquées

25 %

Enquêtes sur les menaces et analyses plus efficaces

25 %

Ajout par couches aux outils de détection des menaces existants, visant à détecter les menaces sophistiquées ou plus complexes

25 %

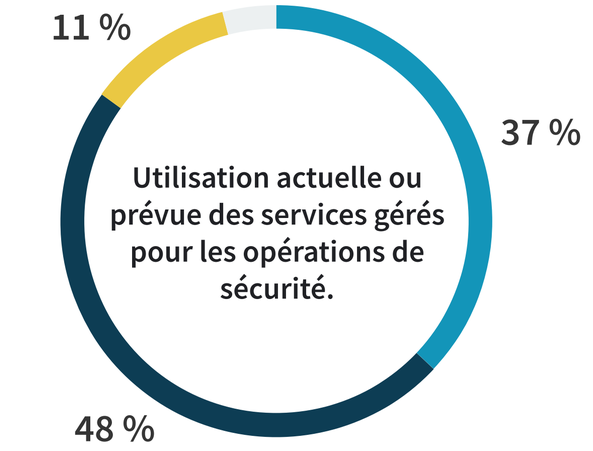
Utilisation de la détection améliorée des menaces pour renforcer les contrôles de sécurité et prévenir de futures attaques semblables

Retour au contenu

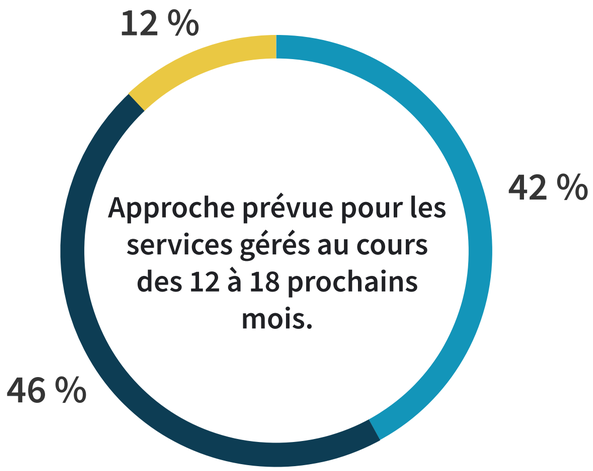
La MDR est courante et de plus en plus utilisée

La MDR est courante et de plus en plus utilisée

Quelles que soient les définitions technologiques ou les stratégies de mise en œuvre, les données d'ESG démontrent une vérité presque universelle : les entreprises ont besoin de l'aide des fournisseurs de services pour les opérations de sécurité. Aujourd'hui, 85 % des entreprises utilisent des services gérés pour une partie ou la majorité de leurs opérations de sécurité. Et parmi ceux qui utilisent des services de sécurité gérés, 88 % augmenteront l'utilisation des services gérés pour les opérations de sécurité à l'avenir.



- Nous utilisons des services gérés pour la majorité de nos opérations de sécurité.
- Nous utilisons des services gérés pour une partie de nos opérations de sécurité.
- Nous utilisons des services gérés pour les opérations de sécurité dans une capacité limitée.



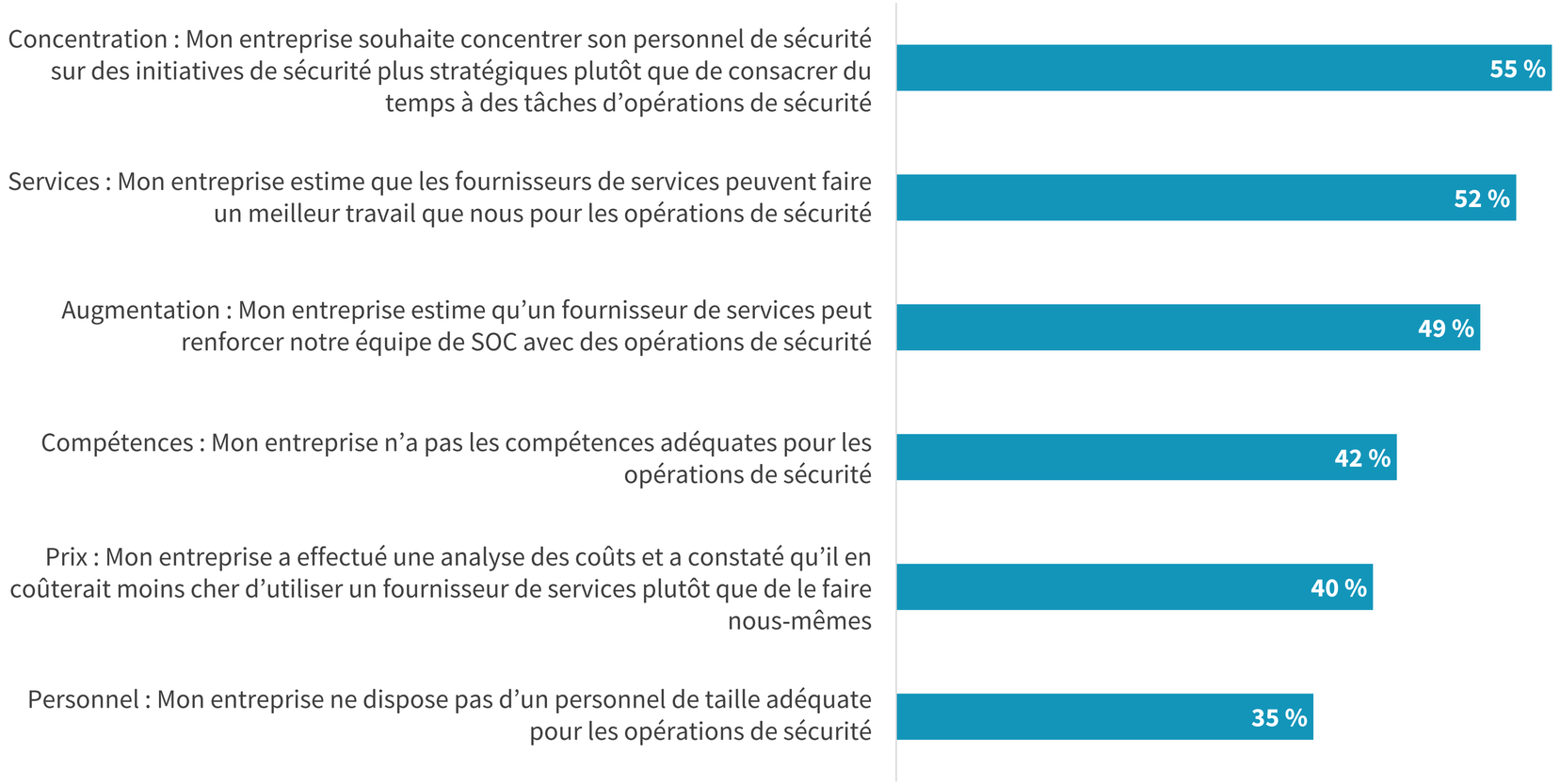
- Nous augmenterons considérablement notre utilisation des services gérés pour les opérations de sécurité.
- Nous augmenterons légèrement notre utilisation des services gérés pour les opérations de sécurité.
- Nous maintiendrons notre utilisation actuelle des services gérés pour les opérations de sécurité.

Retour au contenu

La MDR aide les entreprises à cibler leurs efforts de sécurité et à remédier aux pénuries de compétences et de personnel

Pourquoi les entreprises ont-elles besoin de services gérés pour les opérations de sécurité? Plus de la moitié (55 %) veulent des services de sécurité afin de pouvoir concentrer le personnel de sécurité sur les initiatives de sécurité stratégiques. D'autres croient que les fournisseurs de services gérés peuvent accomplir des choses que leur entreprise ne peut tout simplement pas faire, avec 52 % d'entre eux estimant que les fournisseurs de services peuvent fournir de meilleures opérations de sécurité que leur entreprise, 49 % indiquant qu'un fournisseur de services gérés peut renforcer leur équipe de SOC et 42 % admettant que leur entreprise n'a pas les compétences adéquates pour les opérations de sécurité.

Principales raisons expliquant l'utilisation ou les plans des services gérés pour les opérations de sécurité.



Retour au contenu

cisco SECURE

Une chose est claire : la XDR jouera un rôle essentiel dans la modernisation du SOC. La définition de la façon dont elle aidera votre équipe de sécurité et les partenaires avec lesquels vous travaillez à mesure que vous élaborez votre approche de XDR détermineront votre niveau de réussite. Ne vous contentez pas de recueillir plus de données, cherchez une solution qui peut vous aider à les transformer en meilleures données exploitables avec contexte. L'automatisation peut aider à combler les lacunes en matière de compétences, en réduisant le temps nécessaire pour détecter, examiner et résoudre les incidents afin que la responsabilité puisse être transférée à des analystes moins expérimentés, ce qui permet aux entreprises de réaffecter le temps des analystes principaux de la sécurité à la maturation de leurs opérations de sécurité. Et ne sous-estimez jamais l'importance d'un partenaire de confiance.

De la sécurité du réseau à la sécurité des terminaux, de la sécurité de la messagerie électronique à celle dans le nuage, la gamme Cisco Secure relie les détections à des réponses fiables grâce à des fonctionnalités intégrées dans chaque point de contrôle, ce qui permet d'obtenir la XDR la plus vaste du secteur. Notre approche à la XDR transforme votre infrastructure d'une série de solutions incohérentes en un écosystème entièrement intégré, empêchant ainsi les menaces de contourner les équipes de sécurité débordées. Et comme plus de 300 000 clients dans le monde peuvent en témoigner, Cisco offre une expertise en laquelle les RSSI peuvent avoir confiance. Discutons aujourd'hui.

EN SAVOIR PLUS

À PROPOS D'ESG

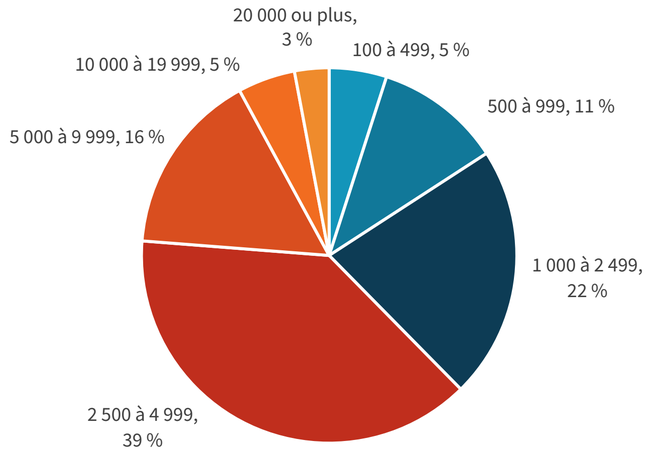
Enterprise Strategy Group est une société intégrée d'analyse, de recherche et de stratégie technologique qui fournit des informations sur le marché, des informations exploitables et des services de contenu de mise en marché à la communauté technologique mondiale.

Méthodologie de recherche

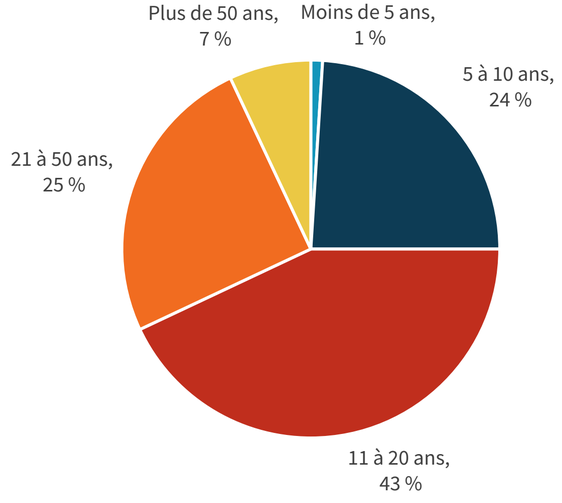
Pour recueillir des données pour ce rapport, ESG a mené un sondage en ligne complet auprès des professionnels des TI et de la cybersécurité des entreprises des secteurs privé et public en Amérique du Nord entre le 4 avril 2022 et le 15 avril 2022. Pour être admissibles à ce sondage, les répondants devaient être des professionnels des TI ou de la cybersécurité responsables de l'évaluation, de l'achat et de l'utilisation de produits et de services de détection et de gestion des menaces. Tous les répondants ont reçu un incitatif pour répondre au sondage sous forme de récompenses en espèces ou d'équivalents en espèces.

Après avoir filtré les répondants inadmissibles, supprimé les réponses en double et examiné les réponses remplies restantes (sur un certain nombre de critères) pour l'intégrité des données, nous nous sommes retrouvés avec un échantillon total final de 376 professionnels des TI et de la cybersécurité.

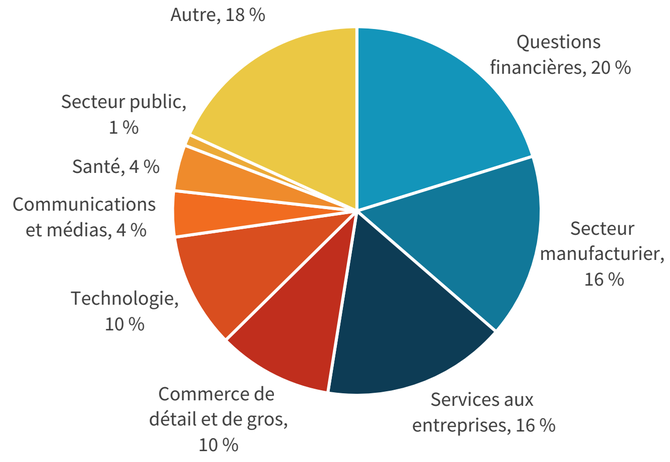
RÉPONDANTS SELON LE NOMBRE D'EMPLOYÉS DE L'ENTREPRISE



RÉPONDANTS SELON L'ÂGE DE L'ENTREPRISE



RÉPONDANTS SELON LE SECTEUR



Retour au contenu

Enterprise Strategy Group est une société intégrée d'analyse, de recherche et de stratégie technologique qui fournit des informations sur le marché, des informations exploitables et des services de contenu de mise en marché à la communauté technologique mondiale.