SOPHOS

MSP (Managed Service Providers) Perspectives 2024

Un éclairage fourni par 350 MSP sur les outils, les risques, les défis et les opportunités commerciales en matière de cybersécurité.

Un livre blanc Sophos. Mai 2024

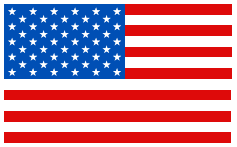
Introduction

Le **rapport MSP (Managed Service Providers) Perspectives 2024** fournit des informations sur cinq domaines clés de l'activité des fournisseurs de services managés (MSP) :

- Outils RMM et PSA
- Gestion de la cybersécurité
- Services MDR
- Défis et risques auxquels font face les MSP et leurs clients
- Impact de la cyberassurance

Les conclusions sont basées sur les résultats d'une enquête indépendante et agnostique menée auprès de 350 MSP aux États-Unis (200), au Royaume-Uni (50), en Allemagne (50) et en Australie (50). L'enquête commandée par Sophos a été réalisée par l'institut de recherche Vanson Bourne en mars 2024.

350 MSP
répartis dans quatre pays



États-Unis
200 répondants

Royaume-Uni
50 répondants

Allemagne
50 répondants

Australie
50 répondants

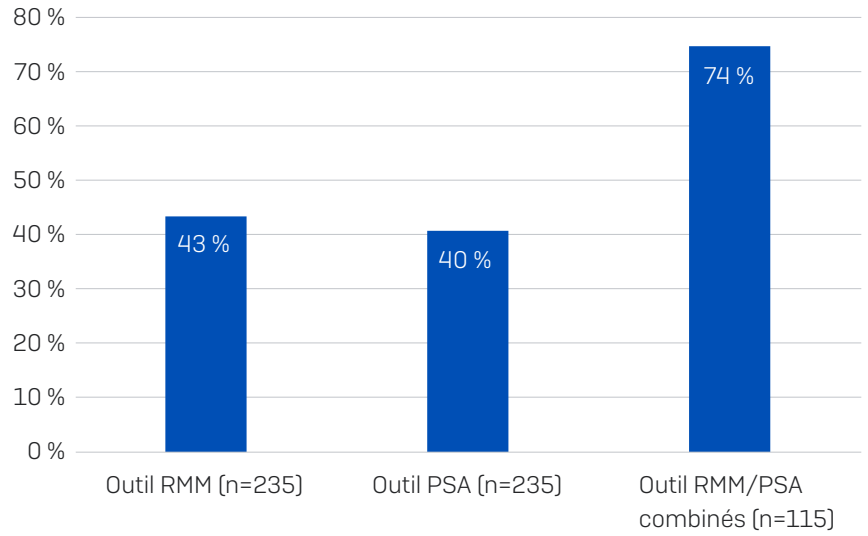
Outils RMM et PSA

Les outils RMM (Remote Monitoring and Management) et PSA (Professional Services Automation) permettent de délivrer des services MSP de manière efficace et optimale tout en rationalisant les frais généraux opérationnels. L'enquête a révélé deux points importants en ce qui concerne ces technologies fondamentales pour les MSP.

Les outils RMM/PSA combinés offrent des niveaux de satisfaction bien plus élevés que chaque outil utilisé séparément.

Près des trois quarts (74 %) des MSP qui utilisent un outil combiné RMM/PSA se déclarent « très satisfaits » de leur solution, contre seulement 43 % des MSP qui utilisent des outils RMM uniquement et 40 % de ceux qui utilisent des outils PSA uniquement.

Répondants « très satisfaits » de leurs outils RMM et PSA existants

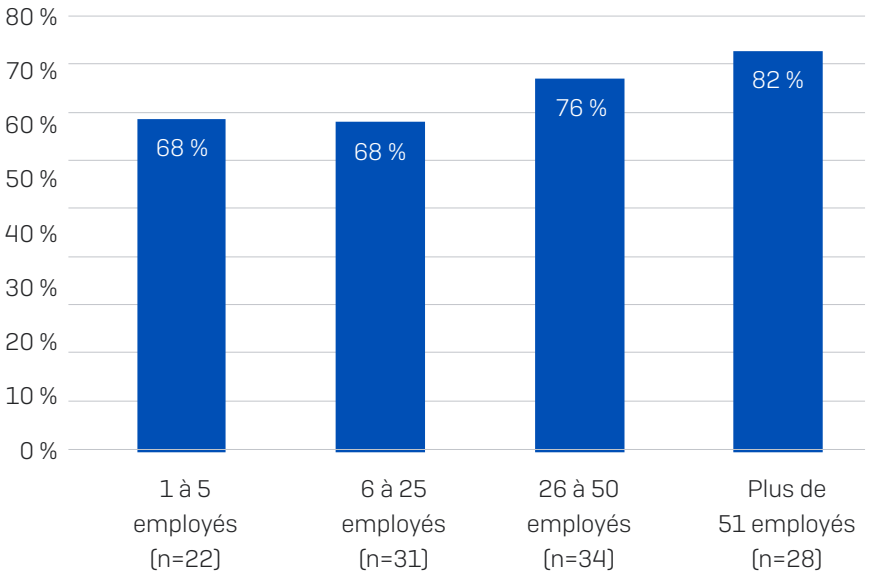


À quel point votre organisation est-elle satisfaite de ses outils RMM et PSA existants ? Chiffres de base dans le graphique.

La satisfaction à l'égard des outils RMM/PSA combinés augmente avec la taille de l'organisation du MSP

Un peu plus des deux tiers (68 %) des MSP comptant jusqu'à 25 employés se disent très satisfaits de leur outil commun RMM/PSA, ce chiffre passant à 76 % pour les MSP comptant entre 26 et 50 employés et à 82 % pour les MSP comptant 51 employés ou plus. Dans la mesure où les grands MSP sont susceptibles de prendre en charge un plus grand nombre de clients, les résultats suggèrent que plus le nombre de clients est important, plus les outils communs RMM/PSA sont bénéfiques.

Répondants « très satisfaits » de leur outil commun RMM/PSA



À quel point votre organisation est-elle satisfaite de ses outils RMM et PSA existants ? Chiffres de base dans le graphique.
* Le nombre de répondants dans ce segment étant faible, il faut considérer les résultats comme des indications plutôt que comme statistiquement significatifs.

Recommandation : Les MSP qui utilisent des outils RMM/PSA séparés peuvent envisager de passer à une solution RMM/PSA combinée afin d'accroître leur satisfaction, en particulier s'ils prévoient d'élargir leur clientèle.

Gestion de la cybersécurité

Partenariats avec les éditeurs de cybersécurité

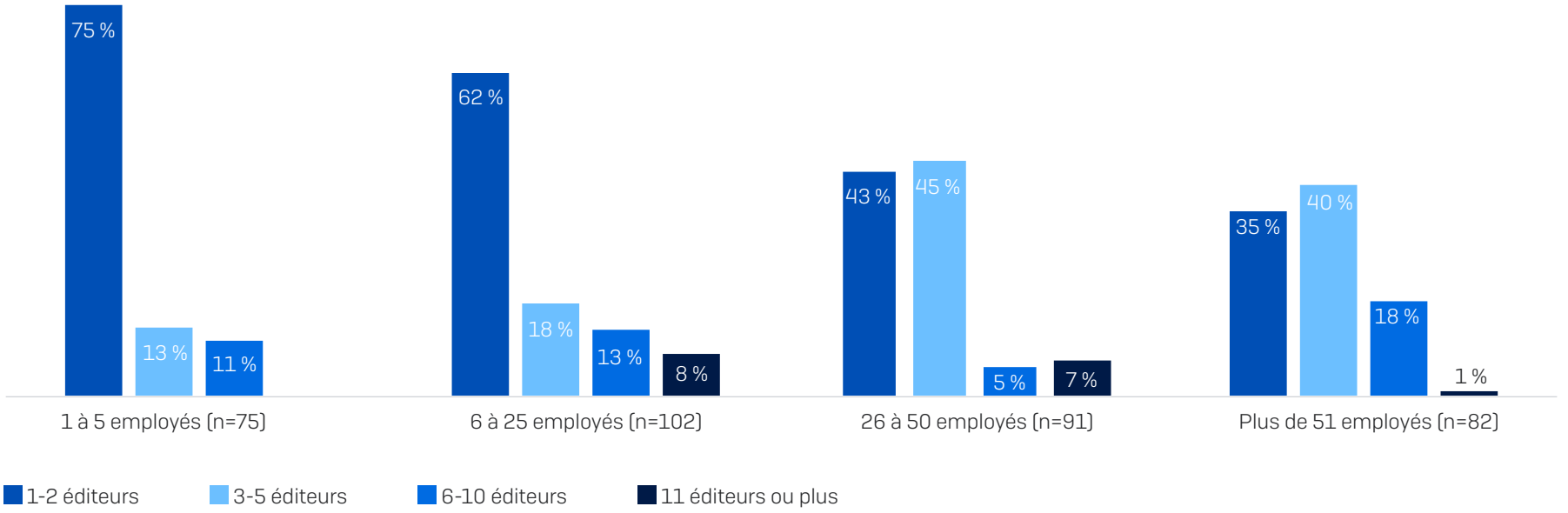
La cybersécurité est une prestation de base pour la plupart des MSP. L'étude a révélé que les MSP travaillent généralement avec un petit nombre d'éditeurs de solutions de cybersécurité pour protéger leurs clients :

- 53 % travaillent avec un ou deux éditeurs
- 83 % travaillent avec un à cinq éditeurs
- 4 % travaillent avec 11 éditeurs ou plus

Les données montrent également que le nombre d'éditeurs de solutions de cybersécurité utilisés augmente généralement avec la taille de l'organisation du MSP. 75 % des plus petits MSP (1 à 5 employés) travaillent avec un ou deux éditeurs de cybersécurité, contre seulement 35 % des MSP de 51 employés ou plus.

À l'inverse, les plus grands MSP sont presque deux fois plus susceptibles de travailler avec six éditeurs ou plus que les plus petits (environ 20 % contre 11 %). Si travailler avec un plus grand nombre d'éditeurs de solutions de cybersécurité permet d'élargir la gamme des services offerts, il est aussi probable que cela augmente les frais généraux de gestion des éditeurs et les difficultés liées à l'intégration de technologies disparates.

Nombre d'éditeurs de cybersécurité utilisés pour protéger les clients



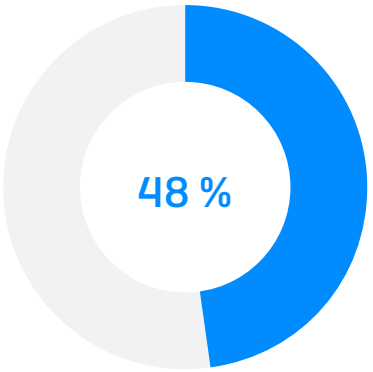
À combien d'éditeurs de cybersécurité votre organisation fait-elle actuellement appel pour protéger ses clients ? n=350. Chiffres de base dans le graphique. À l'exclusion des réponses « Ne sait pas ».

Consolidation des plateformes de cybersécurité

L'enquête révèle qu'il existe un formidable potentiel d'amélioration de l'efficacité et de réduction des frais généraux pour les MSP grâce à la consolidation des plateformes de cybersécurité.

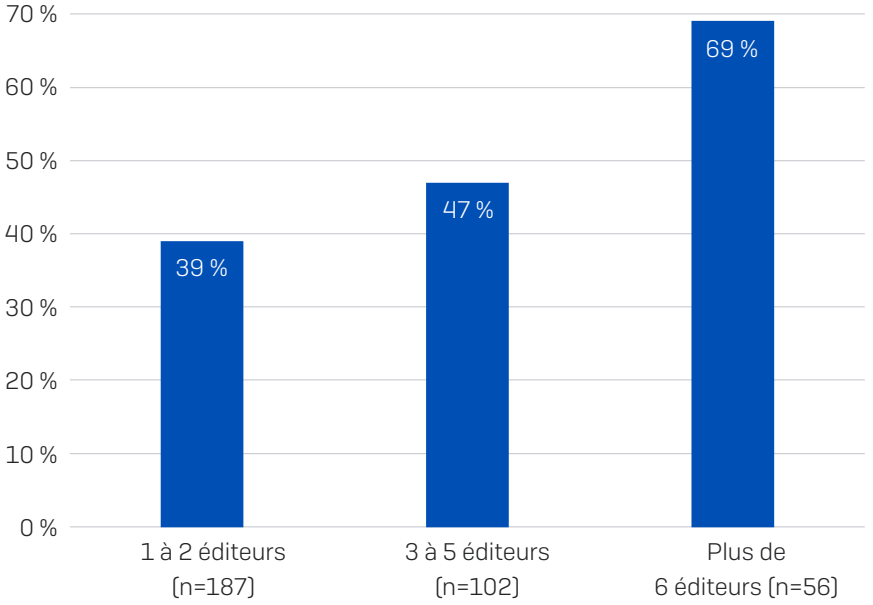
Les MSP qui utilisent actuellement plusieurs plateformes estiment qu'ils réduiraient de 48 % (en moyenne) leur temps de gestion quotidienne s'ils pouvaient gérer tous leurs outils de cybersécurité à partir d'une plateforme unique.

Estimation du gain de temps pour la gestion quotidienne grâce à la centralisation sur une plateforme unique de cybersécurité



La réduction potentielle du temps de gestion augmente avec le nombre d'éditeurs de cybersécurité utilisés. Les MSP qui travaillent avec six éditeurs de solutions de cybersécurité ou plus estiment qu'ils réduiraient leur temps de gestion quotidienne de plus de deux tiers (69 %) s'ils avaient la possibilité de gérer tous leurs outils de cybersécurité à partir d'une plateforme unique. Une réduction des frais généraux de gestion de cette ampleur aurait un impact considérable du point de vue de la rentabilité, tout en libérant les membres de l'équipe qui pourraient se concentrer sur des activités génératrices de revenus.

Estimation du gain de temps lié à la gestion quotidienne grâce à la centralisation sur une plateforme unique de cybersécurité — répartition par nombre d'éditeurs utilisés



Veuillez estimer le gain de temps que votre organisation pourrait réaliser au quotidien, si elle était en mesure de gérer tous ses outils de cybersécurité sur une seule et même plateforme, le cas échéant ? Chiffres de base dans le graphique.

Recommandation : Les MSP qui utilisent plusieurs plateformes de cybersécurité devraient envisager des options de consolidation et les économies en matière de coût total de possession (TCO) qu'ils pourraient réaliser en gérant tous leurs outils de cybersécurité à partir d'une plateforme unique.

Services MDR

Adoption des services MDR

La demande pour des services MDR (Managed Detection and Response) est en forte augmentation, en raison de la complexité croissante des cybermenaces et des outils et technologies qui permettent de les contrer. Selon une étude récente de Gartner, la valeur totale du marché s'élève à 7,5 milliards de dollars, avec un taux de croissance annuel composé (TCAC) de 25,8 %.

Avec un tel niveau de demande et de croissance, il n'est guère surprenant que la majorité (81 %) des MSP fournisse déjà un certain niveau de services MDR, et que la plupart des autres prévoient de le faire à court ou à moyen terme. Cependant, cette enquête a révélé des disparités considérables quant à la maturité de l'adoption des services MDR dans les quatre pays visés par l'enquête.

Les MSP aux États-Unis sont les plus nombreux à proposer un service MDR (94 %), contre 70 % en Allemagne, 62 % au Royaume-Uni et 58 % en Australie. Globalement, parmi les MSP qui ne proposent pas actuellement de services MDR, presque tous prévoient de le faire dans les années à venir, avec près d'un tiers (32 %) des MSP britanniques qui prévoient de les ajouter à leur portefeuille en 2024.

				
Offre actuellement des services MDR	**94 %**	**62 %**	**70 %**	**58 %**
Envisage d'ajouter des services MDR en 2024	5 %	32 %	20 %	18 %
Envisage d'ajouter des services MDR en 2025 ou après	2 %	6 %	10 %	22 %

Votre organisation fournit-elle actuellement un service MDR (Managed Detection and Response) à ses clients ? n=350 (États-Unis 200, Royaume-Uni 50, Allemagne 50, Australie 50), certaines options de réponse ne sont pas prises en compte.

Prestation de services MDR

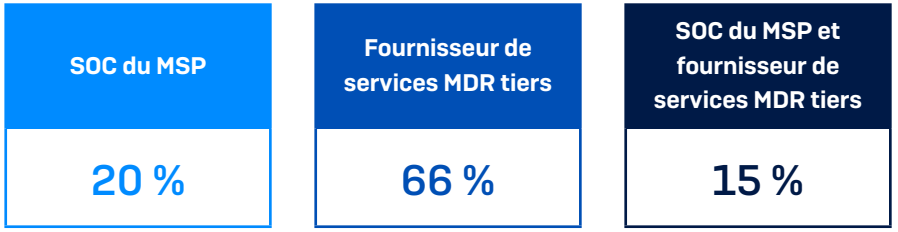
Il existe trois modèles principaux de prestation de services MDR par les MSP : par l'intermédiaire de leur propre centre d'opérations de sécurité (SOC), par l'intermédiaire d'un fournisseur tiers, et conjointement par le SOC du MSP et le fournisseur tiers.

L'enquête révèle que 66 % font appel à un fournisseur tiers pour la fourniture de leur service MDR, 20 % à leur propre SOC et 15 % à un fournisseur tiers combiné à leur propre SOC. Dans l'ensemble, près de 80 % des MSP travaillent avec un prestataire tiers pour fournir leur service MDR.

34 % (en arrondissant) des MSP disposent d'un SOC interne qui fournit des services MDR — soit de manière autonome, soit en collaboration avec un fournisseur tiers. La fourniture en interne est remarquablement cohérente, quelle que soit la taille de l'organisation, avec seulement quatre points de pourcentage de différence entre la propension la plus élevée à disposer d'un SOC en interne

(37 % — 26 à 50 employés) et la plus faible (33 % — toutes les autres catégories).

Méthode de fourniture des services MDR



Votre organisation fournit-elle actuellement un service MDR (Managed Detection and Response) à ses clients ? n=282 qui fournissent un service MDR. Exclue certaines options de réponse.

Capacités attendues d'un fournisseur de services MDR

Comme nous l'avons vu, quatre MSP sur cinq font appel à des fournisseurs tiers pour assurer leur service MDR. Compte tenu de la demande importante et croissante en matière de services MDR, il est essentiel que les MSP sélectionnent le bon partenaire pour eux et pour leurs clients.

Les fournisseurs de services MDR agissent comme une extension du MSP, de sorte que leur envergure et leur compétence influent directement sur le MSP. Qui plus est, les capacités du fournisseur de services MDR ont une incidence sur la gamme de services que le MSP peut fournir à ses clients et sur le niveau de travail et de contribution que celui-ci doit fournir.

Parmi les capacités indispensables, un *service 24/7 de réponse aux incidents* arrive en tête, puisque 36 % des personnes interrogées le considèrent comme « essentiel », ce chiffre atteignant 49 % au sein des MSP comptant de 1 à 5 employés. Sachant que 91 % des attaques de ransomware commencent en dehors des heures de travail normales[1], il est essentiel de disposer d'une couverture 24 h/24 pour défendre efficacement une organisation. Travailler avec un fournisseur de services MDR qui offre une couverture complète 24 h/24 et 7 j/7 rassure les MSP sur le fait que leurs clients sont toujours protégés, sans avoir à mettre en place un tel niveau d'expertise en interne.

En deuxième position, on trouve la *capacité à détecter le piratage de compte dans Microsoft 365 ou Google Workspace*, puisqu'un tiers (33 %) des MSP déclarent qu'il s'agit d'une exigence « essentielle » et que 43 % la jugent « très importante ».

La *possibilité de bénéficier d'outils de sécurité supplémentaires — en particulier des pare-feux/une sécurité réseau et une protection endpoint — auprès du fournisseur de services MDR* est également très prisée, les trois quarts des personnes interrogées la jugeant « essentielle ou très importante ». Le fait de pouvoir travailler avec un seul fournisseur pour les outils de cybersécurité et les services MDR réduit les frais administratifs tout en rationalisant les opérations.

Dans le même temps, l'étude montre clairement que les MSP ont besoin de flexibilité et ne veulent pas être limités dans les outils qu'ils peuvent utiliser ni obligés de se procurer des outils de cybersécurité auprès de leur fournisseur de MDR. Pour 71 % des personnes interrogées, il est « essentiel ou très important » que le fournisseur puisse *utiliser les données télémétriques de leurs outils de sécurité existants pour détecter les menaces et y répondre.*

Un service de réponse aux incidents 24/7/365 est la principale capacité attendue d'un fournisseur de services MDR.

CAPACITÉ	« ESSENTIEL »	« ESSENTIEL » OU « TRÈS IMPORTANT »
Service **de réponse aux incidents 24/7**	36 %	74 %
Capacité à détecter le piratage de compte dans **Microsoft 365 ou Google Workspace.**	33 %	77 %
Possibilité de disposer d'une **sécurité pare-feu/réseau** auprès du fournisseur de services MDR	31 %	74 %
Possibilité de disposer d'une **protection endpoint** auprès du fournisseur de services MDR	28 %	75 %
Console unique pour les services MDR et les autres solutions de sécurité	28 %	74 %
Clause de **garantie contre les** violations	26 %	70 %
Capacité à utiliser les données télémétriques provenant **des outils de sécurité existants** pour détecter les menaces et y répondre	25 %	71 %

Si votre organisation doit choisir un fournisseur de services MDR, dans quelle mesure est-il important que ce fournisseur offre les capacités suivantes ? n=350 (États-Unis 200, Royaume-Uni 50, Allemagne 50, Australie 50), certaines options de réponse ne sont pas prises en compte.

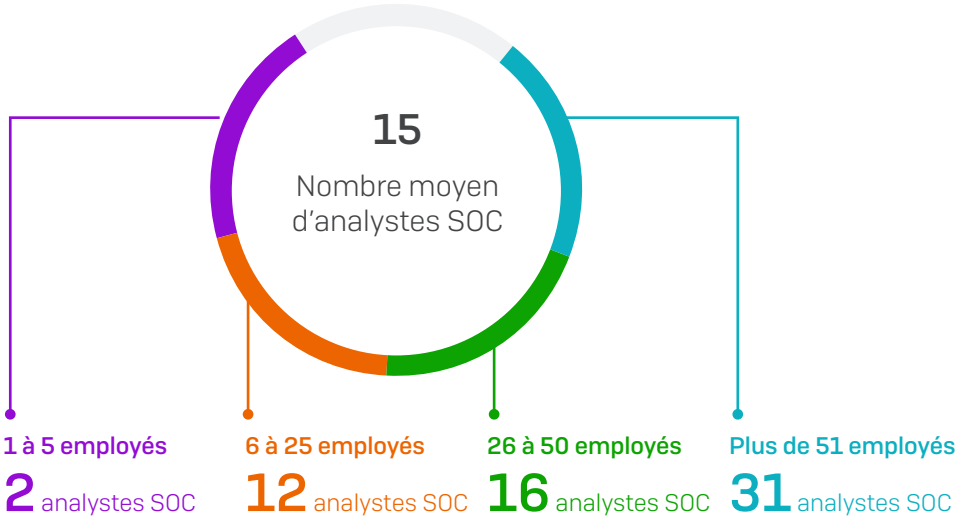
Analystes SOC internes

34 % des MSP fournissant un service MDR disposent d'un SOC interne, ce qui nécessite la présence d'analystes spécialisés en interne. L'étude révèle qu'un SOC classique de MSP compte en moyenne 15 analystes. Toutefois, ce chiffre recouvre des écarts considérables en fonction de la taille de l'organisation.

Les MSP comptant de 1 à 5 employés font appel, en moyenne, à deux analystes pour surveiller les environnements de leurs clients, détecter les menaces et y répondre. Le nombre d'analystes augmente régulièrement avec la taille de l'organisation, les plus grands MSP déclarant en moyenne 31 analystes SOC. Il est à noter que le nombre de répondants dans chaque segment individuel étant assez faible, ces résultats sont donnés à titre indicatif et ne sauraient être considérés comme statistiquement significatifs.

Comme les adversaires planifient délibérément leurs attaques au cours de la nuit, des week-ends et des jours fériés, une couverture 24/7 est essentielle pour un service MDR efficace. Pour les MSP de plus petite taille disposant de moins d'analystes SOC, la fourniture en interne uniquement est susceptible d'exercer une pression énorme sur leurs ressources limitées.

Recommandation : Les MSP qui n'offrent pas encore de services MDR devraient envisager de les ajouter à leur portefeuille le plus tôt possible pour ne pas perde de clients. Lors de la sélection d'un fournisseur MDR tiers, veillez à identifier les fonctionnalités les plus importantes pour vous et à évaluer les capacités des fournisseurs à les fournir.



Concernant le centre d'opération de sécurité (SOC) de votre entreprise, combien d'analystes surveillent les événements suspects dans les environnements de vos clients et y répondent ?

Défis et cyber-risques

Les principaux défis auxquels sont confrontés les MSP aujourd'hui

L'univers des MSP est en constante évolution. Les menaces ne cessent d'évoluer, entraînant des mutations et des avancées dans les contrôles de cybersécurité et les besoins des clients.

L'enquête révèle que ***rester informé des dernières actualités et informations sur les solutions de cybersécurité/technologies*** est le plus grand défi auquel sont confrontés les MSP aujourd'hui, qu'il s'agisse de leur plus grand défi ou d'un de leurs trois plus grands défis.

Compte tenu de la rapidité de l'innovation dans ce domaine, il n'est pas surprenant que de nombreux MSP soient à la traîne. Les menaces évoluent, de même que les cyber contrôles qui les neutralisent. Les technologies existantes acquièrent de nouvelles capacités, tandis que de tout nouveaux produits sont régulièrement mis sur le marché. Il est difficile autant que fastidieux de se tenir au fait de toutes ces évolutions.

Le deuxième plus grand défi auquel sont confrontés les MSP aujourd'hui est la pénurie de ressources d'analystes en cybersécurité :

- ***Offrir une couverture en dehors des heures de travail (y compris les soirs et les week-ends)*** est le deuxième défi le plus important pour les MSP
- ***Le recrutement de nouveaux analystes en cybersécurité pour faire face à la croissance de leur activité*** est le deuxième des trois principaux défis rencontrés

Les analystes spécialisés en cybersécurité sont rares et leurs salaires sont élevés. Pour compliquer les choses, une couverture complète 24 h/24 et 7 j/7 requiert au minimum 5 à 6 analystes, ce qui n'est pas une mince affaire pour de nombreux MSP.

Le plus grand défi

N°1	Rester informé des dernières actualités et informations sur les solutions de cybersécurité/technologies
N°2	Garantir une couverture en dehors des heures de travail (y compris les soirs, week-ends et jours fériés)
N°3	Gagner de nouveaux clients

Les trois principaux défis

N°1	Rester informé des dernières actualités et informations sur les solutions de cybersécurité/technologies
N°2	Embaucher des analystes en cybersécurité pour accompagner la croissance de la clientèle
N°3	Rester au fait des dernières cybermenaces

Quels sont les plus grands défis auxquels votre organisation est confrontée au quotidien ? Veuillez classer par ordre d'importance les trois premiers. n=350

Cyber-risques

L'enquête a exploré ce que les MSP perçoivent comme les plus grands risques cyber pour leur propre organisation et pour celle de leurs clients. Les résultats révèlent à la fois des points communs et des différences.

Deux facteurs figurent en tête de liste, tant pour les MSP que pour leurs clients :

- Vol de données et d'identifiants d'accès
- Pénurie de compétences et d'expertise internes en cybersécurité

Les adversaires n'entrent pas par effraction dans les organisations — ils s'y connectent. À l'aide de données d'accès et d'identifiants volés, souvent achetés sur le Dark Web auprès d'un courtier d'accès initial (IAB), ils se font passer pour des employés légitimes avant de s'introduire dans le réseau ciblé. Comme le montre le rapport L'état des Ransomwares 2024 de Sophos, 29 % des attaques de ransomware l'an dernier ont débuté par une compromission d'identifiants, ce qui montre l'ampleur du défi à relever.

MSP

	Le plus grand risque	Trois principaux risques
N°1	Pénurie de compétences et d'expertise internes en cybersécurité	Vol de données et d'identifiants d'accès
N°1	Réseau Wi-Fi non sécurisé	Mauvaise configuration des outils de sécurité
N°3	Manque d'outils de sécurité	Réseau Wi-Fi non sécurisé

Clients MSP

	Le plus grand risque	Trois principaux risques
N°1	Pénurie de compétences et d'expertise internes en cybersécurité	Vol de données et d'identifiants d'accès
N°2	Vulnérabilités non corrigées	Manque d'outils de sécurité
N°3	Outils d'accès à distance	Vulnérabilités non corrigées

Selon vous, quels sont les risques les plus importants en matière de cybersécurité pour votre organisation/les clients de votre organisation ? n=350

Malgré les progrès constants des technologies de cybersécurité et de l'intelligence artificielle, l'aspect humain reste central pour l'efficacité de la cybersécurité. La configuration, le déploiement, la gestion, la réponse et la mise à jour des solutions technologiques doivent être confiés à des professionnels qualifiés. Par ailleurs, la technologie à elle seule ne peut pas bloquer automatiquement toutes les cybermenaces. La pénurie de professionnels qualifiés est bien connue, et les organisations se tournent de plus en plus vers les MSP pour combler leurs lacunes, ce qui ne fait qu'exacerber le problème.

Si les principaux risques perçus sont communs aux MSP et à leurs clients, des différences de classement apparaissent au fur et à mesure que l'on descend dans le classement.

Les réseaux sans fil non sécurisés constituent l'un des principaux cyber-risques perçus par les MSP (n° 1 du classement commun des « Plus grand risque », n° 3 des « Trois principaux risques »). L'utilisation de réseaux non sécurisés peut entraîner plusieurs dangers, notamment l'interception de données et leur utilisation en vue d'extraire des identifiants de connexion et de mot de passe permettant à des adversaires d'accéder à des comptes personnels et professionnels.

Les erreurs de configuration des outils de sécurité constituent également un risque majeur pour les MSP. Les pare-feux, la protection Endpoint et tous les autres outils ne fonctionnent que s'ils sont correctement configurés.

Les vulnérabilités non corrigées sont l'un des principaux risques perçus par les clients MSP (n° 2 « Plus grand risque », n° 3 des « Trois principaux risques »). Étant donné que 32 % des attaques de ransomware l'année dernière ont commencé par l'exploitation d'une vulnérabilité non corrigée, les MSP ont tout intérêt à prendre conscience du danger majeur que cela représente pour leurs clients.

Recommandation : Pour minimiser les frais généraux des fournisseurs et de la gestion quotidienne face à ce large éventail de risques et de défis, les MSP ont tout intérêt à rechercher des partenaires en cybersécurité qui offrent une gamme complète de services et d'outils. La mise en place de solutions combinant une protection robuste et adaptative contre des menaces en constante évolution, sans nécessiter de configuration ni de déploiement complexe, leur facilitera grandement la tâche. En outre, les MSP devraient profiter des fournisseurs de services MDR pour développer et étendre leurs compétences et leur expertise internes en matière de cybersécurité, en privilégiant les partenaires qui soutiennent leur modèle d'entreprise et peuvent s'adapter à leurs besoins au fur et à mesure qu'ils évoluent et se développent.

Impact de la cyberassurance

Le recours à la cyberassurance pour transférer le risque cybernétique a augmenté de façon constante : selon une étude de Sophos, 90 % des entreprises de taille moyenne disposent désormais d'une couverture sous une forme ou une autre. 50 % ont une police d'assurance spécifique cyber, tandis que 40 % ont une couverture cyber dans le cadre d'une police d'assurance commerciale générale, telle qu'une police de responsabilité civile.

L'adoption massive de la cyberassurance entraîne un engagement important du channel, 99 % des MSP faisant état d'une augmentation du nombre de demandes d'assistance et de solutions pour répondre aux exigences de la cyberassurance.

Globalement, la demande la plus fréquente (47 %) émane de clients souhaitant mettre en place un service MDR pour améliorer leur assurabilité, suivie de près par les clients ayant besoin d'aide pour constituer leur dossier de demande d'assurance (45 %). Ces deux exigences offrent aux MSP des opportunités majeures de générer des revenus par le biais de la fourniture de services MDR et de la facturation de services professionnels.

BESOIN DU CLIENT	MONDIAL				
Disposer d'un **service MDR** pour améliorer l'assurabilité	**47 %**	49 %	38 %	56 %	36 %
Aide pour constituer le dossier de **demande d'assurance**	**45 %**	49 %	46 %	30 %	42 %
Disposer de capacités **EDR** pour améliorer l'assurabilité	**34 %**	31 %	32 %	28 %	52 %
Disposer de services et de technologies **non EDR/MDR** pour améliorer leur assurabilité	**33 %**	31 %	22 %	48 %	40 %

Votre organisation a-t-elle constaté une augmentation du besoin de soutien et de solutions pour répondre aux exigences de vos clients en matière de cybersécurité ? n=350 (États-Unis 200, Royaume-Uni 50, Allemagne 50, Australie 50).

Un tiers (34 %) des MSP signalent que leurs clients cherchent à ajouter une solution EDR (Endpoint Detection and Response) à leurs piles de sécurité pour améliorer leur assurabilité. Il est intéressant de noter qu'en dehors de l'Australie, la demande de services MDR émanant des assurances est considérablement plus importante que la demande de services EDR. Cela témoigne de la plus grande réduction des risques qu'un service MDR spécialisé, fonctionnant 24 h/24 et 7 j/7, peut apporter par rapport à une équipe interne mise à rude à épreuve.

Un tiers (33 %) des personnes interrogées ont déclaré avoir constaté une augmentation de la demande de services et de technologies non EDR/MDR de la part de clients soucieux d'améliorer leur assurabilité. Bien que l'étude n'ait pas approfondi ce point, il est probable que les exigences portent sur les outils d'authentification multifacteur (MFA), la protection des messageries et du réseau — autant d'éléments communément exigés/souhaités par les compagnies d'assurance.

Recommandation : La fourniture de services et de technologies qui améliorent l'assurabilité est une opportunité majeure pour les MSP, et les organisations ont tout intérêt à chercher à renforcer leur soutien dans ce domaine afin de maximiser leur potentiel de revenus.

Conclusion

Face aux cyberattaques inéluctables, les MSP ont de nombreuses possibilités de développer leurs activités et d'améliorer leur profitabilité. Qu'il s'agisse de réduire les frais généraux quotidiens en consolidant les plateformes de gestion, d'optimiser l'engagement avec des fournisseurs de services MDR tiers pour élargir leur offre de services ou de mettre en adéquation les activités avec les besoins en cyberassurance, les MSP sont en mesure de faire croître leurs activités tout en améliorant la protection de leurs clients contre les ransomwares et les violations de sécurité.

Le marché des MSP est un milieu concurrentiel. En exploitant ces informations pour progresser et se développer, les MSP peuvent tirer pleinement parti des possibilités qui s'offrent à eux.

Programme Sophos MSP

Sophos aide les MSP à développer leurs activités et à augmenter leur rentabilité. Des défenses innovantes et adaptatives et un système de cybersécurité MSP complet offrent une cyberconfiance qui favorise le succès.

- Avec un portefeuille complet de services et de produits de cybersécurité à votre disposition, vous serez en mesure de répondre aux besoins actuels et futurs de vos clients.
- Minimisez la charge de gestion quotidienne et libérez du temps facturable grâce à la plateforme de sécurité Sophos Central qui vous permet de gérer la sécurité de tous vos clients à partir d'une console unique.
- Bénéficiez de marges attrayantes, d'incentives lucratives et d'une facturation cumulée grâce au programme Sophos MSP.

1 Rapport Active Adversary pour les dirigeants, Sophos, 2023

Pour en savoir plus sur le programme Sophos MSP, visitez la page sophos.fr/MSP et pour découvrir Sophos MDR, visitez sophos.fr/MDR

Sophos MDR : Réponse aux incidents 24/7 de série

Sophos MDR est le service managé de détection et de réponse le plus apprécié sur le marché, plus d'entreprises faisant confiance à Sophos pour son service MDR qu'à tout autre fournisseur de cybersécurité. Avec un système de détection et d'intervention 24/7 fourni par défaut, les MSP et leurs clients ont la certitude que les experts Sophos sont là pour stopper les attaques à toute heure du jour ou de la nuit. Ses points forts incluent :

- Remédiation manuelle et proactive 24/7
- Réponse aux incidents complète
- Assistance téléphonique directe 24/7
- Interlocuteur dédié en cas d'incident
- Choix des modes de réponse
- Clause de garantie contre les violations
- Chasse aux menaces proactive
- Fonctionne avec la protection Endpoint de Sophos et non Sophos
- Détecte les tentatives de piratage de compte Microsoft 365 et Google Workspace
- Et bien plus encore.

Que vous recherchiez un service entièrement externalisé ou une extension flexible de votre SOC interne, Sophos MDR est la solution pour vous aider à développer votre activité.

« Sophos MDR a sauvé plusieurs clients de défaillances commerciales potentiellement catastrophiques. Nos marges ont augmenté de 100 % et notre chiffre d'affaires de 300 %. »

James Wagner, Président, The ITeam

2024-05-21 (WP-NP)

SOPHOS