Enterprise Strategy Group | Getting to the bigger truth.™

Ce que les équipes de sécurité attendent des fournisseurs MDR

Par Dave Gruber, Principal Analyst

SEPTEMBRE 2022

Objectifs de la recherche

L'utilisation de services managés de détection et de réponse ou Managed Detection and Response (MDR) est devenue une stratégie courante dans les programmes de sécurité modernes. Mais les départements IT ne doivent pas s'arrêter à ce nom : les offres des fournisseurs MDR dépassent de loin les services basiques de détection et de réponse. Elles aident les responsables de l'IT et de la sécurité à accélérer le développement des programmes et à améliorer la posture de sécurité. Alors que la pénurie de compétences dans le domaine de la cybersécurité semble partie pour durer, les services MDR peuvent apporter des ressources d'experts, disponibles immédiatement en ligne, ainsi que des processus et des outils de pointe et éprouvés, capables d'aider les équipes de sécurité à prendre le contrôle et à se préparer à la réussite future de leur programme de sécurité.

Pour comprendre ces tendances et évaluer globalement les offres de services MDR, ESG a interrogé personnellement 373 professionnels de la cybersécurité impliqués dans les technologies de cybersécurité, notamment les produits, les services et les processus.

LES OBJECTIFS DE CETTE ÉTUDE :

Déterminer comment, où et pourquoi les services MDR sont utilisés pour prendre en charge les programmes de sécurité.

Découvrir ce qui compte le plus pour les opérations IT, les responsables des lignes de produits et les utilisateurs finaux.

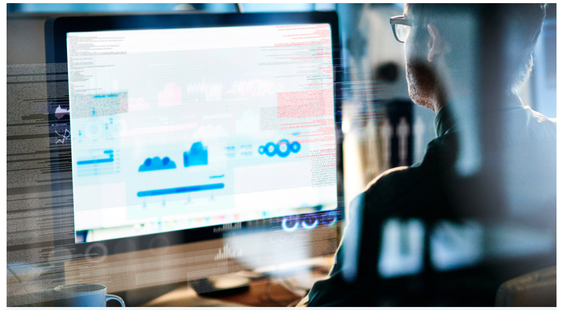
Isoler des cas d'utilisation MDR spécifiques et les profils organisationnels de ceux qui les utilisent.

Déterminer les grandes tendances du secteur qui ont un impact sur le choix d'un fournisseur MDR.

REVENIR AU CONTENU

PRINCIPALES **CONCLUSIONS**

CLIQUEZ POUR CONSULTER



Trois facteurs clés déclenchent l'engagement MDR initial

Les organisations sont poussées par des évaluations proactives, des lacunes opérationnelles et des actes de réponse aux incidents.

Différents cas d'utilisation sont pris en charge par les services MDR

Les experts, l'intelligence sur les menaces, la formation des compétences, la couverture et le développement des programmes favorisent notamment l'engagement continu.

Les services MDR engendrent des résultats positifs en matière de sécurité

Les organisations constatent des améliorations dans leur maturité, dans la baisse du nombre d'attaques réussies, dans leurs compétences en cybersécurité et dans leur confiance en la direction.

Les clients attendent une pile technologique ouverte, mais les services MDR doivent intégrer tous les mécanismes de sécurité déjà en place

Les fournisseurs doivent disposer d'une pile technologique complète si nécessaire, mais aussi s'intégrer à l'infrastructure existante pour réussir.

Les modèles d'engagement client des services MDR ont leur importance

Bien que les modèles varient, la confiance repose sur des communications régulières et centrées sur l'humain.

Les grandes tendances du secteur ont un impact sur la sélection d'un fournisseur MDR

Le mouvement XDR, la prise en charge MITRE ATT&CK et la modernisation du SOC pèsent de tout leur poids.

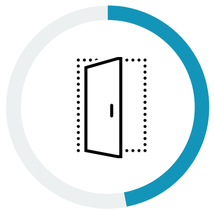
Trois facteurs clés favorisent l’engagement MDR initial

Les évaluations proactives sont les plus susceptibles de donner naissance à un engagement MDR initial

Qu'est-ce qui pousse les équipes de l'IT et de la sécurité à choisir un prestataire de services managés de détection et de réponse (MDR) ? La réponse évidente fait appel à l'interprétation la plus littérale des services MDR et concerne les compétences, la couverture et les processus capables de remédier aux lacunes en matière d'opérations de sécurité. Cependant, il s'avère que plus de la moitié (57 %) des organisations ont cité les évaluations de sécurité proactives comme un facteur déclencheur de leur engagement MDR initial. En effet, les engagements avec les fournisseurs MDR commencent souvent par des évaluations de sécurité, notamment celles des failles de sécurité, car elles peuvent révéler les faiblesses de la posture de sécurité au niveau des programmes, des outils, de la couverture et des compétences. Le troisième facteur important est une réponse aux crises/incidents qui révèle des lacunes dans le programme de sécurité. Les besoins opérationnels tels que la réponse aux incidents sont également des déclencheurs courants des engagements MDR.

Facteurs ayant déclenché des engagements initiaux avec les fournisseurs MDR.

57 %
Évaluations de sécurité



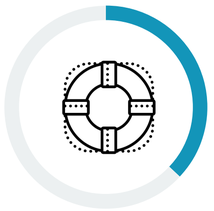
47 %
Évaluation et gestion des failles de sécurité

46 %
Services d'intelligence sur les menaces

39 %
Réponse aux incidents/ atténuation

39 %
Détection des incidents

39 %
Mesures correctives/ récupération après incident



37 %
Engagement en réponse à une violation ou un incident majeur

36 %
Réponse à une violation/crise qui a révélé des lacunes dans notre programme

34 %
Procédure d'enquête sur les incidents

33 %
Tri et hiérarchisation des alertes quotidiennes

30 %
Chasse aux menaces

25 %
Red Team, simulation de violation et d'attaque

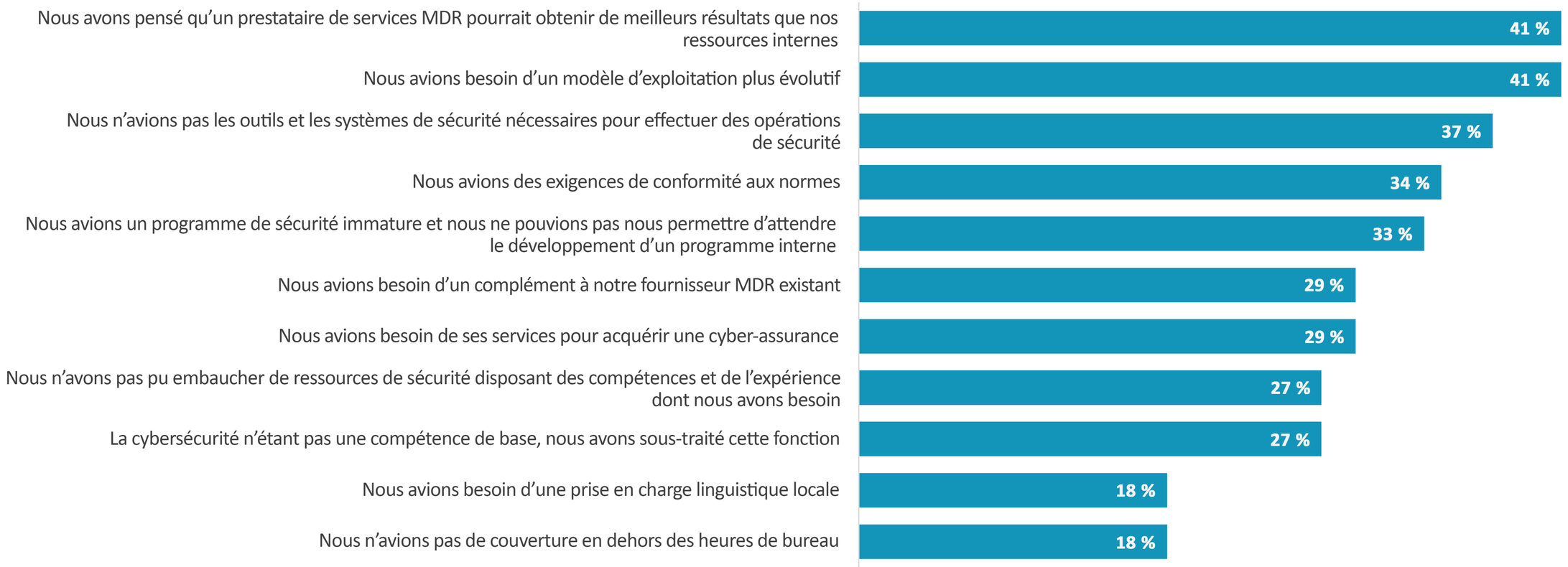
REVENIR AU CONTENU

Facteurs ayant déclenché l'engagement auprès des prestataires de services MDR actuels

Alors que les équipes de sécurité peinent à mettre à l'échelle les programmes de sécurité pour répondre à la fois à la croissance et à la complexité de la surface d'attaque et du paysage des menaces, bon nombre d'entre elles font appel à des fournisseurs MDR pour accélérer et faire évoluer leurs modèles d'exploitation. Les organisations considèrent les services MDR comme un moyen pour accélérer le développement des programmes et combler les lacunes. Plus de quatre sur dix pensent que les prestataires de services MDR peuvent tout simplement obtenir de meilleurs résultats que leurs ressources internes. Un tiers d'entre elles pointent du doigt des programmes de sécurité immatures qui ne disposent pas des outils et des systèmes nécessaires. Parmi les autres facteurs importants, on retrouve la liste exponentielle des contrôles et processus de sécurité requis pour acquérir une assurance de cybersécurité, ainsi que les exigences de conformité aux normes.

En ce qui concerne les lacunes en matière de compétences et de couverture, certaines organisations signalent des lacunes, mais celles-ci figurent en bas de la liste par rapport à l'ensemble des objectifs de développement et de croissance des programmes.

Facteurs ayant déclenché l'engagement des organisations auprès de leurs fournisseurs MDR actuesl.



REVENIR AU CONTENU

Différents cas d’utilisation **sont pris en charge par les services MDR**

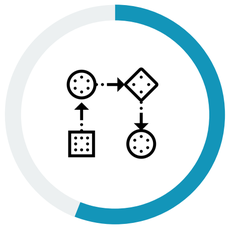
« Près de la moitié des organisations choisissent un fournisseur MDR **pour sous-traiter entièrement les opérations de sécurité. »**

Principaux cas d'utilisation : Accès aux ressources d'experts et au développement du programme de sécurité

Les fournisseurs MDR offrent un éventail de services pour répondre à différents cas d'utilisation. Tout en accélérant le développement du programme de sécurité et en accédant à des ressources de sécurité expertes, près de la moitié des organisations tirent parti d'un fournisseur MDR pour sous-traiter entièrement les opérations de sécurité. L'autre moitié utilise les services MDR pour compléter son programme interne, combler les lacunes en matière de couverture, accéder à une intelligence supplémentaire sur les menaces et ajouter des fonctionnalités de chasse aux menaces. Il est également important de noter que près de la moitié des organisations sous-traitent entièrement leurs opérations de sécurité ou aspirent à le faire.

Cas d'utilisation MDR au sein des programmes de sécurité des organisations.

56 %
Accès à des ressources de sécurité expertes

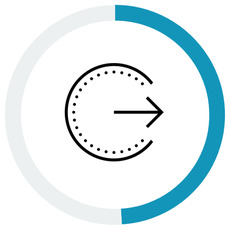


56 %
Développement du programme de sécurité

54 %
Complète le programme des opérations de sécurité internes

50 %
Couverture

50 %
Intelligence sur les menaces



49 %
Sous-traitance complète de nos opérations de sécurité

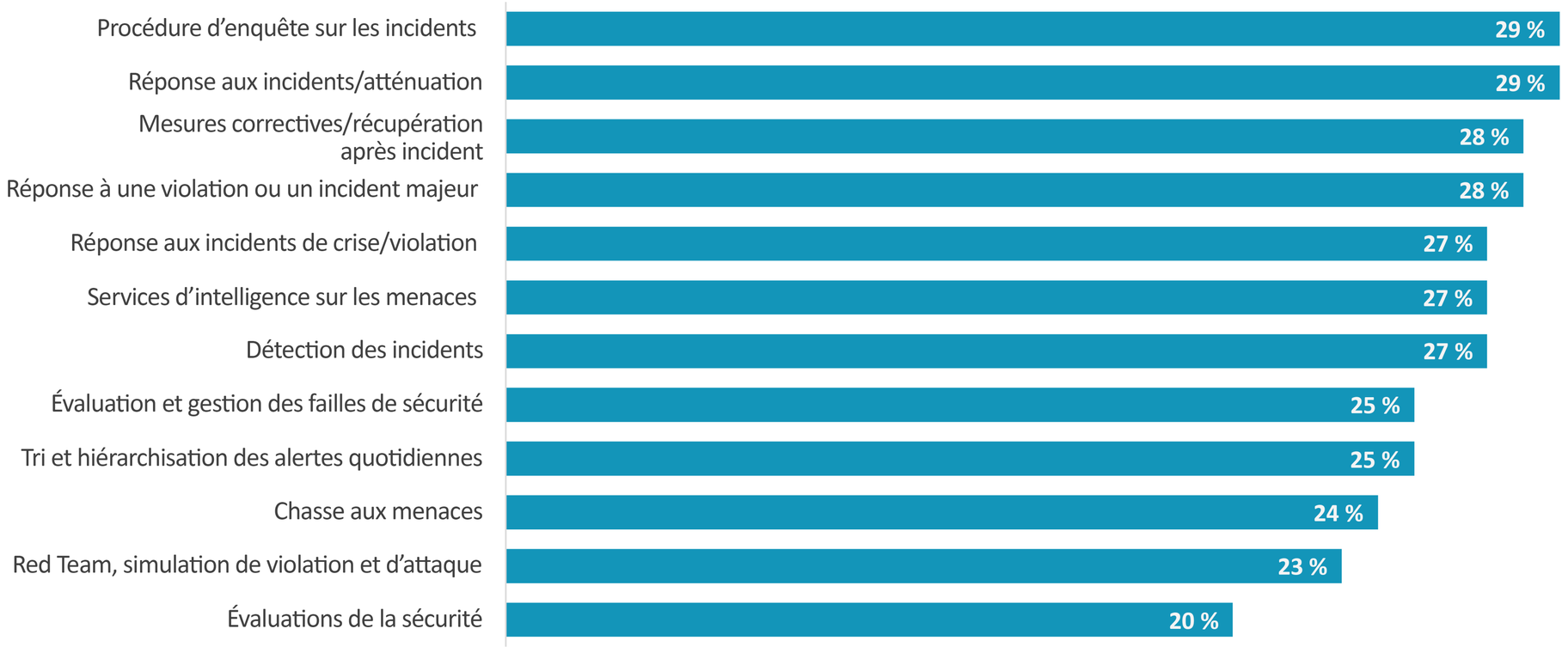
49 %
Recherche proactive des menaces

REVENIR AU CONTENU

Les engagements MDR évoluent généralement au fil du temps

Les engagements MDR évoluent généralement au fil du temps, avec l'ajout de nouveaux services pour renforcer la procédure d'enquête sur les incidents, l'atténuation des incidents et la réponse à tous les éléments, qu'il s'agisse d'un événement majeur de crise/faille ou d'activités quotidiennes de réponse. Les fournisseurs MDR modernes étendent les fonctionnalités au-delà des fonctions SecOps standard, que l'on trouve traditionnellement dans le domaine de la réactivité, en proposant des services proactifs d'intelligence sur les menaces, de chasse aux menaces, de simulation d'attaque, d'évaluation de la sécurité et de gestion des failles de sécurité. Au regard de cette vaste gamme de services, les fournisseurs MDR offrent bien plus que la détection et la réponse basiques et deviennent des partenaires à part entière qui aident les organisations de toutes tailles à faire évoluer leurs programmes de sécurité.

Activités de sécurité ajoutées depuis l'engagement initial avec les fournisseurs MDR.



« Les fournisseurs MDR offrent **bien plus que la détection et la réponse basiques. »**

REVENIR AU CONTENU

Au-delà de la détection et de la réponse : les fournisseurs MDR sont des partenaires opérationnels et stratégiques à long terme

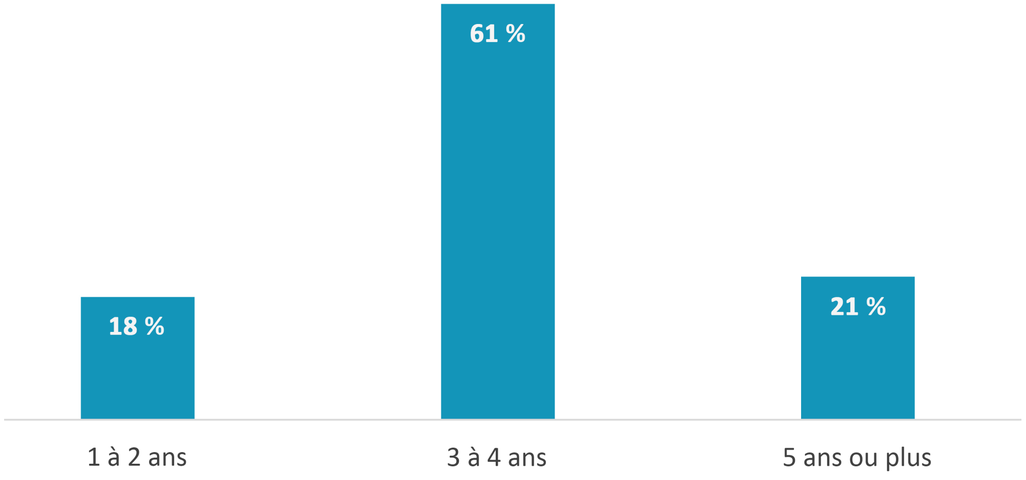
Avec la persistance des engagements MDR et le renforcement des relations, les fournisseurs MDR joueront un rôle plus stratégique. Cela est clairement démontré par le fait que plus des trois quarts (77 %) des organisations décrivent leur fournisseur MDR comme un partenaire opérationnel et stratégique, capable de s'aligner sur leur programme de sécurité. Ces relations sont durables : 82 % des organisations décrivent un engagement auprès de leur fournisseur MDR depuis au moins trois ans. La majorité d'entre elles utilisent plusieurs fournisseurs MDR et 34 % s'associent avec au moins trois prestataires de services MDR pour prendre en charge les cas d'utilisation et les ressources qui composent leur surface d'attaque.

Comment les organisations voient-elles leurs fournisseurs MDR actuels ?

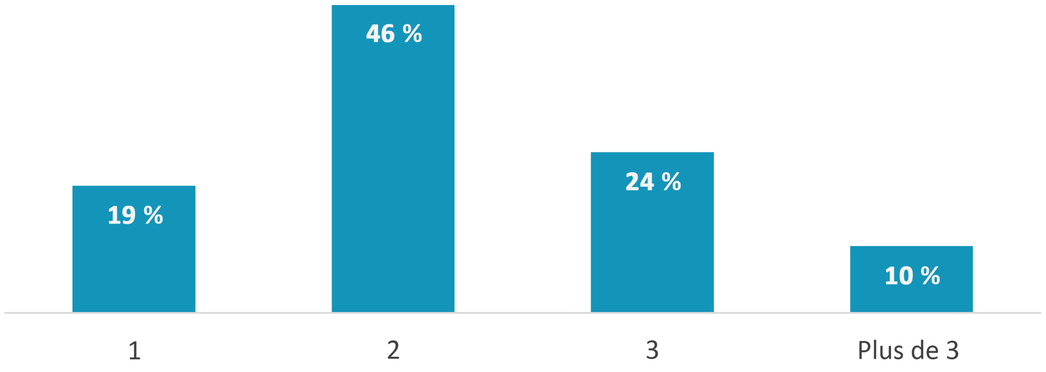
77 %

Comme un partenaire opérationnel et stratégique **qui a amélioré notre programme de sécurité global**

Depuis combien de temps les organisations travaillent-elles avec leur fournisseur MDR ?



Avec combien de prestataires de services MDR les organisations travaillent-elles ?



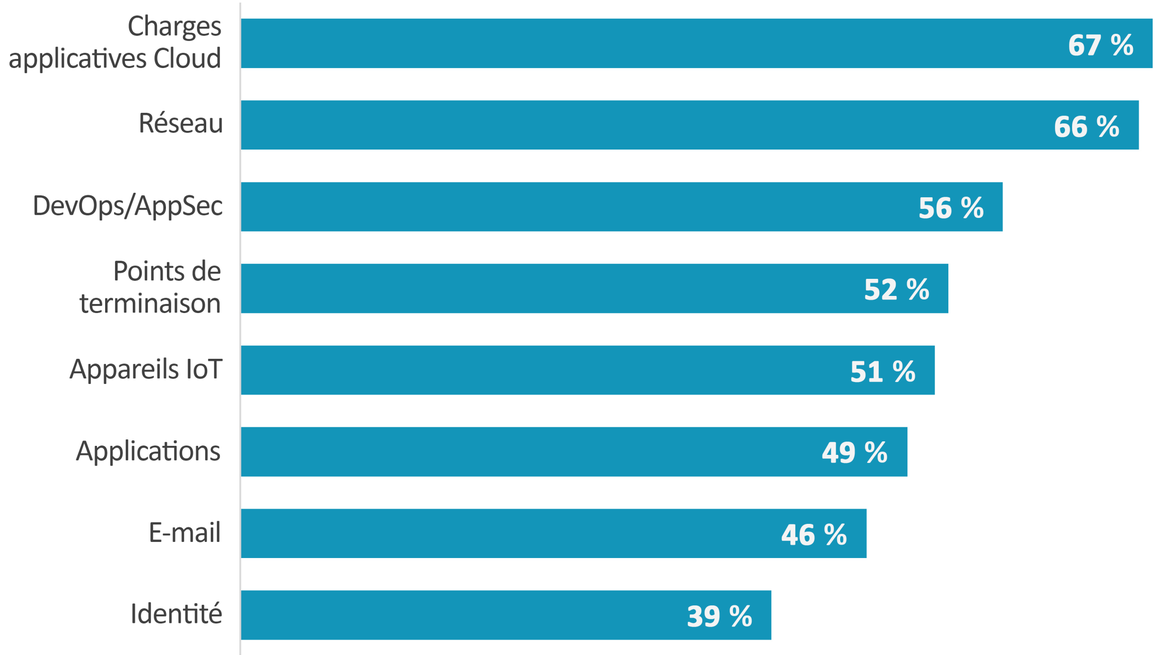
REVENIR AU CONTENU

« Peu d'organisations font appel aux prestataires MDR **pour couvrir toute leur surface d'attaque. »**

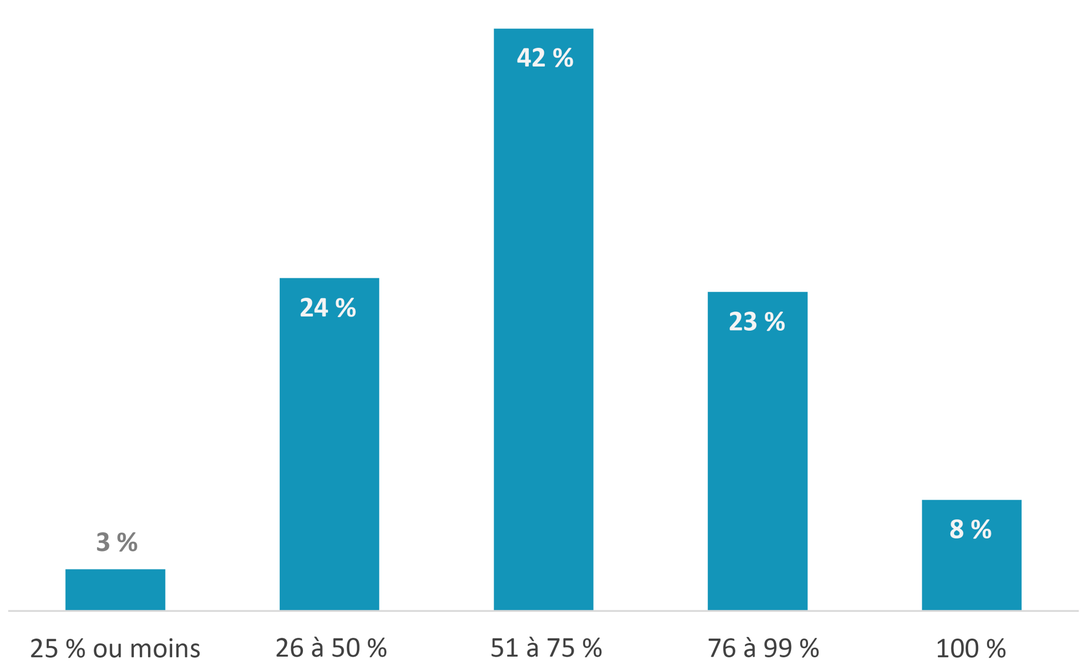
Les fournisseurs MDR doivent surveiller tous les types d'actifs, mais rarement l'intégralité du parc

En ce qui concerne la couverture de la surface d'attaque, les organisations demandent généralement aux prestataires MDR de prendre en charge les opérations de sécurité pour tous les types de ressources IT. Pourtant, peu d'entre elles font appel aux fournisseurs MDR pour couvrir toute leur surface d'attaque. Plus précisément, plus des deux tiers déclarent que leur fournisseur MDR ne couvre pas plus de 75 % de leur parc, tandis que seulement 8 % indiquent que leur fournisseur MDR en couvre la totalité.

Champ d'application de la couverture des fournisseurs MDR actuels des organisations.



Pourcentage de surface d'attaque dont les fournisseurs MDR ont la responsabilité.



REVENIR AU CONTENU


Les services MDR
génèrent des
**résultats positifs en
matière de sécurité**

Les fournisseurs MDR contribuent à améliorer la maturité du programme de sécurité et des ressources sur site

En ce qui concerne les résultats concrets, les fournisseurs MDR aident les organisations à limiter le nombre d'attaques réussies, à accélérer le développement global du programme de sécurité et à ouvrir des opportunités d'investissement dans des initiatives de sécurité plus stratégiques. Plus précisément, la moitié des organisations affirment que leur fournisseur MDR contribue à améliorer les compétences de sécurité de leurs ressources internes, et 45 % d'entre elles ont pu investir dans des initiatives de sécurité plus stratégiques. Plus de quatre organisations sur dix signalent un nombre nettement inférieur d'attaques réussies et/ou une amélioration générale de leur programme de sécurité. Du point de vue de la direction opérationnelle, 42 % des organisations affirment que la confiance des dirigeants et/ou du conseil d'administration a augmenté, tandis que 38 % déclarent être en mesure de répondre aux objectifs de conformité ou aux exigences de cyber-assurance. Pour appuyer ces bons résultats opérationnels, le nombre d'organisations ayant qualifié la maturité de leurs programmes de sécurité comme « très élevée » s'est considérablement accru après leur engagement auprès d'un fournisseur MDR.

Résultats obtenus suite à la collaboration avec un fournisseur MDR

50 %
Amélioration des compétences du personnel de sécurité acquises auprès du fournisseur MDR

45 %
Investissement dans des initiatives de sécurité plus stratégiques

42 %
Réduction significative du nombre d'attaques réussies

42 %
Amélioration significative du programme de sécurité

42 %
Augmentation de la confiance des dirigeants et/ou du conseil d'administration

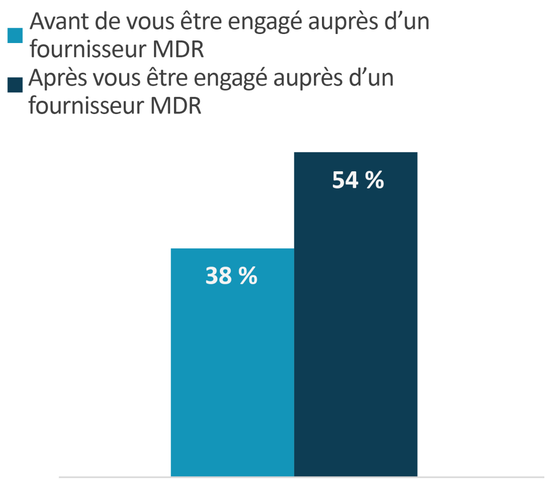
38 %
Respect des exigences de conformité/cyber-assurance

38 %
Baisse des coûts d'exploitation liés à la sécurité

35 %
Moins de stress pour l'équipe de sécurité interne

32 %
Réduction des frais de cyber-assurance

Maturité du programme MDR.



Très mature (c'est-à-dire processus formels et opérationnalisés, experts parmi le personnel, couverture complète et visibilité de la surface d'attaque, profils de risque, programme formel et testé de réponse aux incidents, collaboration IT, outils et analytique de sécurité hautement efficaces, etc.)

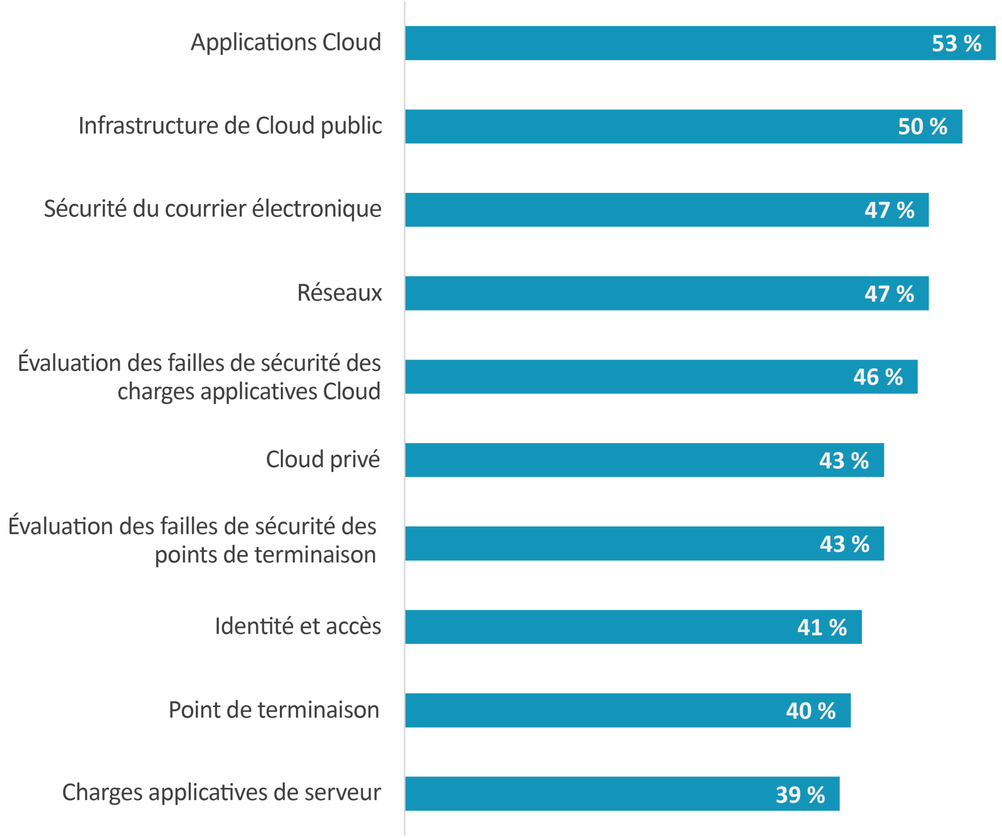
REVENIR AU CONTENU


Les clients attendent une pile technologique ouverte, mais
les services MDR doivent intégrer tous les mécanismes de sécurité déjà en place

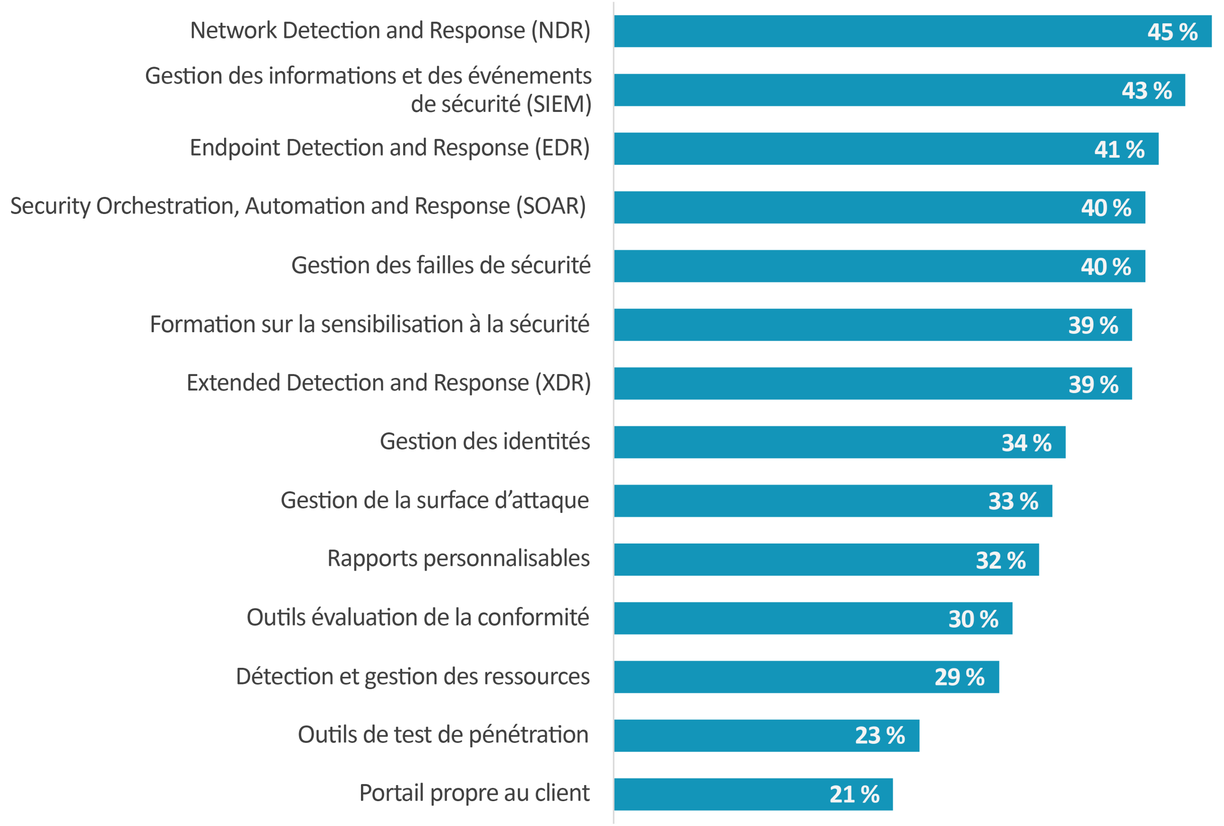
Les opérations Cloud et de sécurité sont des critères technologiques clés pour la sélection de services MDR

Les clients MDR attendent de leur fournisseur une couverture de sécurité complète sur tous les vecteurs d'attaque. Mais en plus, les utilisateurs MDR souhaitent que leur fournisseur s'intègre aux mécanismes de sécurité déjà en place, qu'il s'agisse d'un ensemble complet de contrôles de sécurité, notamment pour les points de terminaison, le réseau, le Cloud et les e-mails, ou d'une pile complète d'outils d'opérations de sécurité, notamment SIEM, SOAR, EDR, NDR, XDR, la gestion de surface d'attaque, la découverte des ressources et la gestion des vulnérabilités.

Technologies de détection/d'agent que les organisations attendent d'un fournisseur MDR.



Technologies d'opérations de sécurité que les organisations attendent d'un fournisseur MDR.



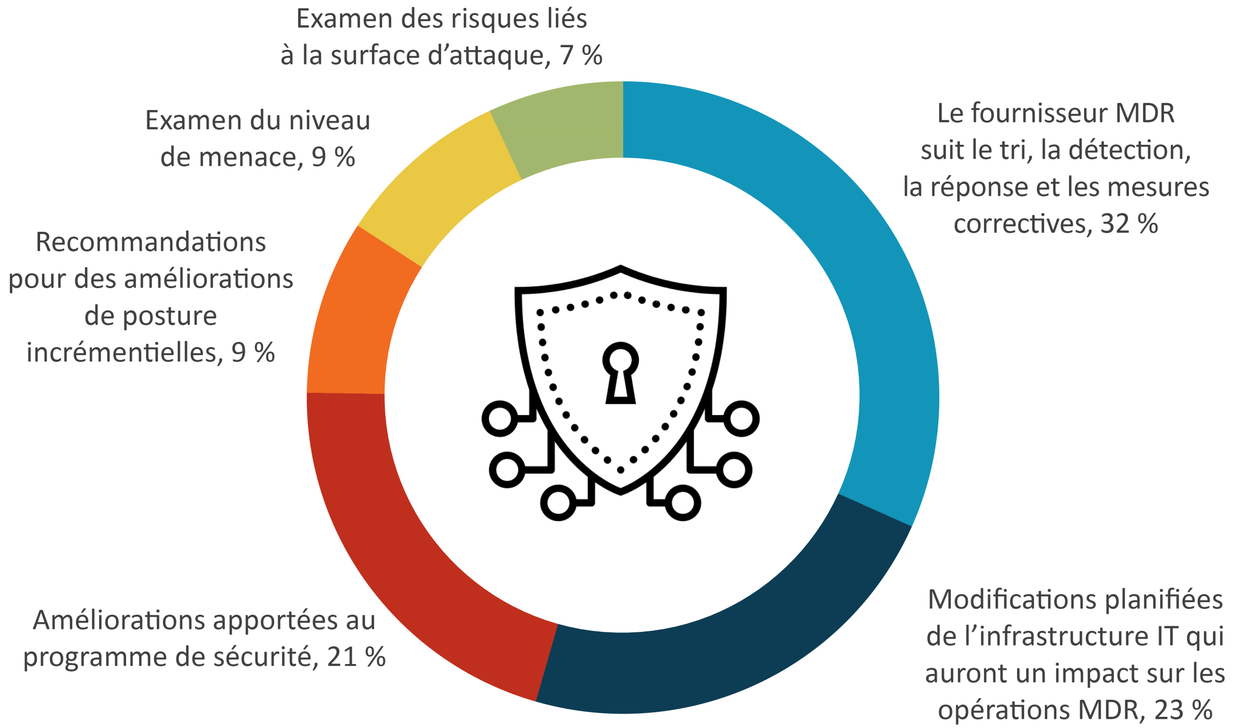
REVENIR AU CONTENU

Les modèles d’engagement client des services MDR **ont leur importance**

Examen opérationnel des services MDR : éléments les plus importants

Les responsables de la sécurité soulignent que les modèles d'engagement des services MDR ont une grande importance. Ils demandent aux fournisseurs MDR non seulement de suivre leur détection, leur réponse et leurs mesures correctives en matière de tri, mais également de rester informés des modifications planifiées de l'infrastructure IT, des améliorations continues du programme de sécurité, de l'examen des risques de surface d'attaque et de l'examen du niveau de menace, tout en recommandant des actions pour améliorer la posture de sécurité. Ces attentes sont élevées, mais démontrent néanmoins pourquoi la plupart des organisations considèrent leur fournisseur MDR comme un partenaire stratégique.

Aspect le plus important des révisions opérationnelles d'un fournisseur MDR.



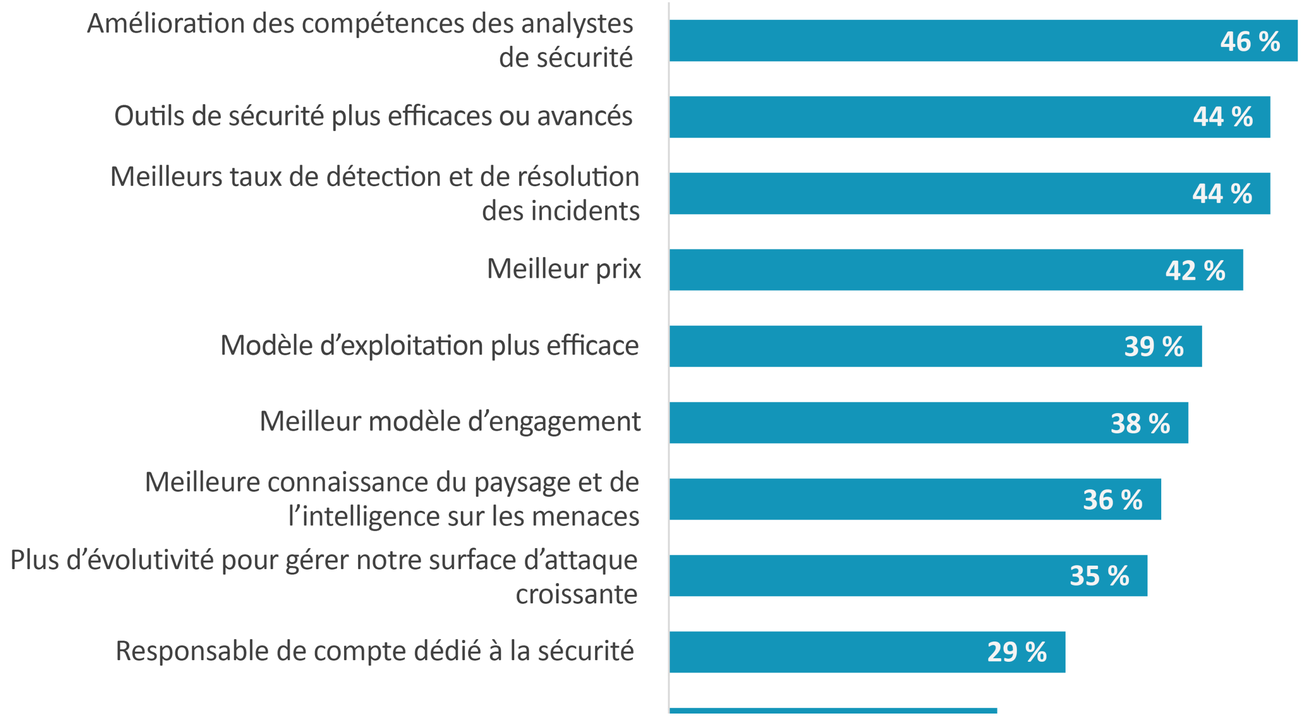
« Les responsables de la sécurité soulignent que les **modèles d'engagement MDR ont une grande importance.** »

REVENIR AU CONTENU

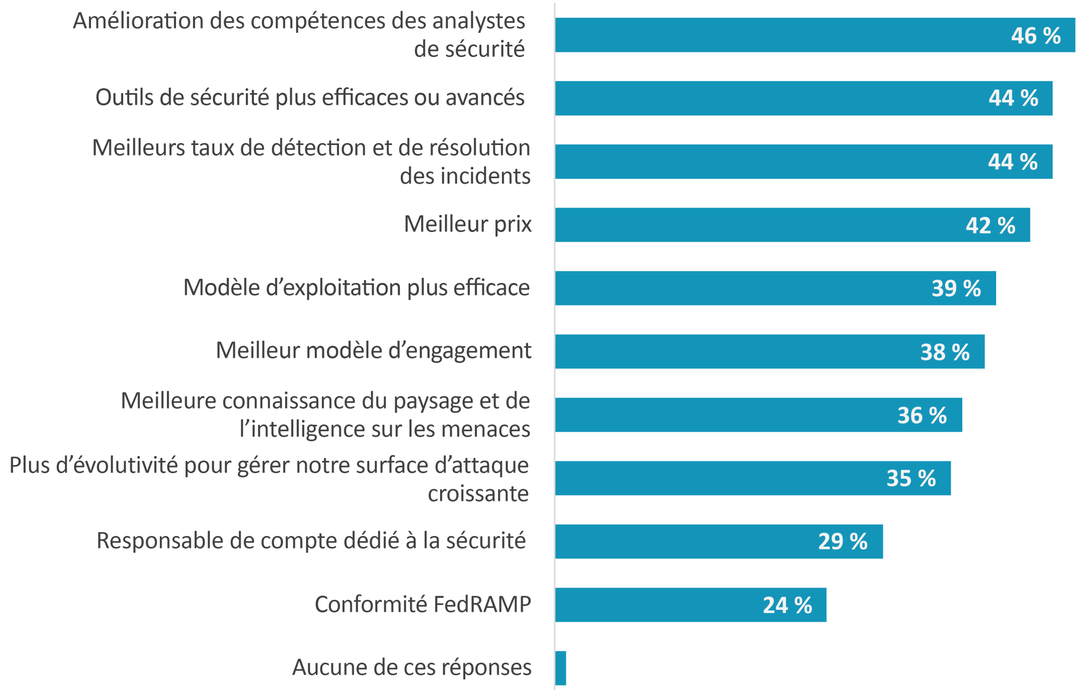
Les compétences et les outils avancés ont la possibilité de stimuler le changement de fournisseur MDR

Quelles sont les considérations importantes pour les organisations lorsqu'elles évaluent et sélectionnent un fournisseur MDR ? Près de la moitié (49 %) des organisations déclarent qu'il doit travailler avec leur écosystème existant de technologies et d'outils de sécurité, tandis que 46 % souhaitent des fonctionnalités avancées de détection et de réponse. 43 % d'entre elles souhaitent que leur fournisseur MDR dispose de ressources de sécurité spécialisées, ce qui est également le facteur le plus souvent cité qui inciterait les organisations à changer leur fournisseur actuel. Les autres raisons incluent des outils de sécurité plus avancés et des taux de détection et de résolution améliorés, bien que le prix et les modèles d'exploitation soient également importants.

Critères de sélection importants pour les fournisseurs MDR.



Facteurs qui inciteraient les organisations à modifier les fournisseurs MDR.



REVENIR AU CONTENU


Les grandes
tendances du secteur
ont un impact
sur le choix d’un
fournisseur MDR

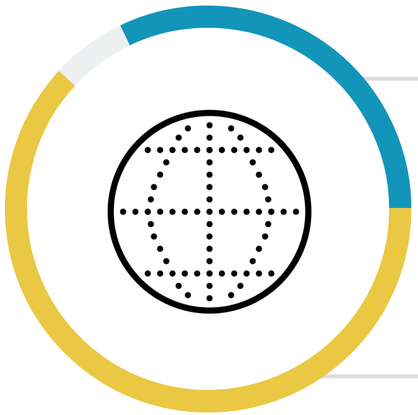
Plus de neuf organisations sur dix

identifient la prise en charge MITRE ATT&CK comme critique ou très importante.

La prise en charge MITRE et XDR est essentielle pour la plupart des choix de fournisseurs MDR

Le choix d'un fournisseur MDR va souvent bien au-delà d'une check-list de fonctionnalités et d'éléments de couverture. Les grandes tendances du secteur ont encore plus d'impact dans le choix d'un fournisseur MDR : plus de neuf organisations sur dix identifient la prise en charge MITRE ATT&CK comme critique (32 %) ou très importante (62 %). En outre, près des trois quarts (73 %) signalent que la technologie de sécurité XDR (Extended Detection and Response) a été prise en compte lors du processus de sélection des services MDR. Le SASE (Secure Service Access Edge) et l'ASM (Attack Surface Management) sont également considérés comme des éléments importants par les deux tiers des participants.

Importance de la prise en charge du cadre MITRE ATT&CK par le fournisseur.



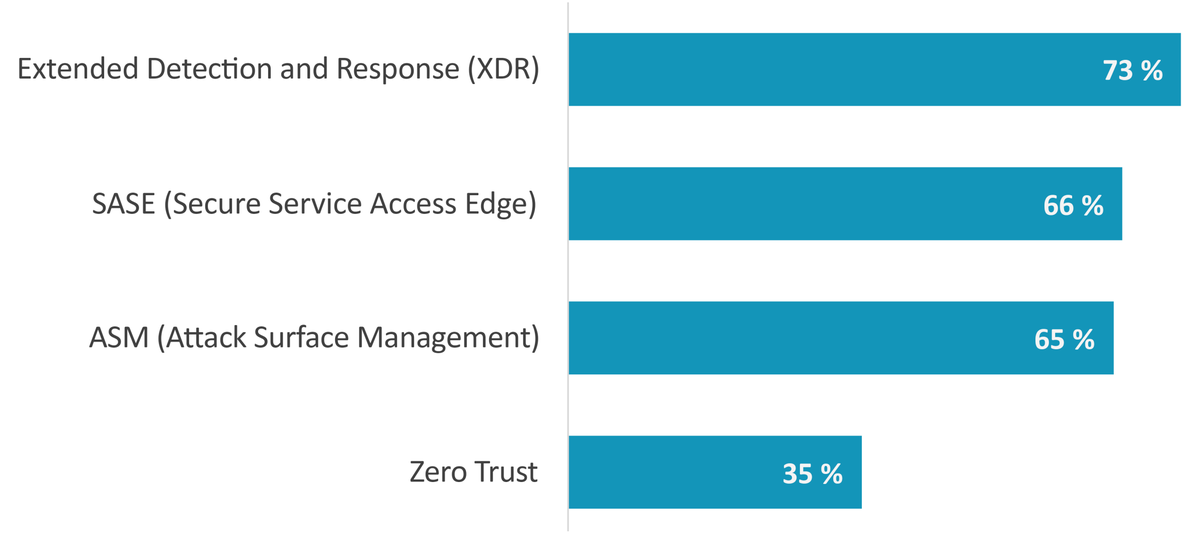
32 %

Critique : Nous n'envisagerions pas de collaborer avec un fournisseur MDR qui ne prend pas en charge le cadre MITRE ATT&CK

62 %

Très important : Nous préférons travailler avec un fournisseur MDR qui prend en charge le cadre MITRE ATT&CK, mais nous en étudierons d'autres

Les grandes tendances de sécurité prises en compte dans le choix de services MDR.



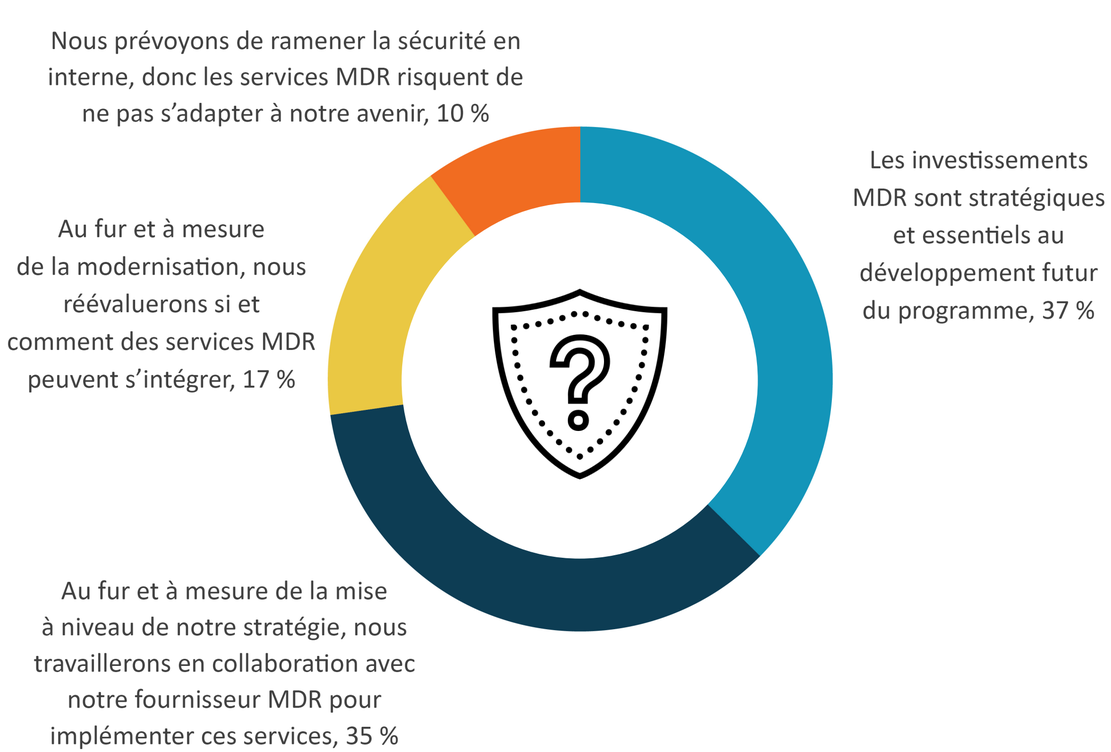
REVENIR AU CONTENU

L’utilisation de services MDR devient une stratégie de sécurité standard

L’utilisation de services MDR est devenue une composante essentielle de la stratégie du programme de sécurité, faisant passer les fournisseurs MDR au rang de partenaires stratégiques. Elles aident les équipes de l’IT et de la sécurité à accélérer le développement de programmes, à améliorer la posture de sécurité et à bénéficier d’avantages moins visibles, tels que la prise en charge des objectifs de conformité, l’acquisition d’une cyber-assurance et l’amélioration des compétences et des processus de sécurité internes. Par conséquent, la plupart des organisations considèrent les services MDR comme un élément à part entière de leur investissement dans le programme de sécurité : 37 % d’entre elles indiquent que les services MDR sont stratégiques et critiques, et 35 % prévoient de travailler avec leur fournisseur MDR au fur et à mesure de la mise à niveau et de l’implémentation de stratégies de sécurité futures.

ESG considère les services MDR comme une stratégie de sécurité standard importante et recommande aux organisations d’explorer davantage de cas d’utilisation qui peuvent accélérer le développement et la posture du programme de sécurité.

Positionnement des services MDR dans le contexte plus large de la modernisation du SOC.



« La plupart des organisations considèrent les services MDR comme un **élément à part entière de leur investissement dans le programme de sécurité.** »

REVENIR AU CONTENU

DELL Technologies

Dell Technologies (NYSE : DELL) aide les organisations et les particuliers à construire leur futur numérique et à transformer leur façon de travailler, de vivre et de jouer. La société fournit aux clients le portefeuille de technologies et de services le plus large et le plus innovant du secteur pour l'ère des données.

EN SAVOIR PLUS

À PROPOS D'ESG

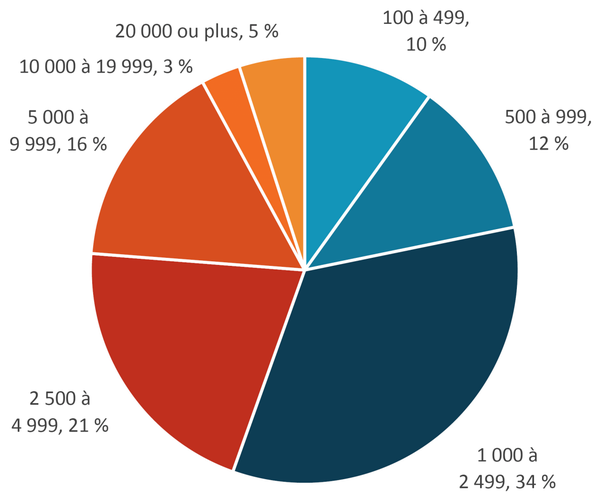
Enterprise Strategy Group est une entreprise intégrée d'analyse, de recherche et de stratégie technologiques qui fournit des données relatives aux marchés, des renseignements exploitables et des services de commercialisation à la grande communauté informatique.

Méthodologie de recherche et données démographiques

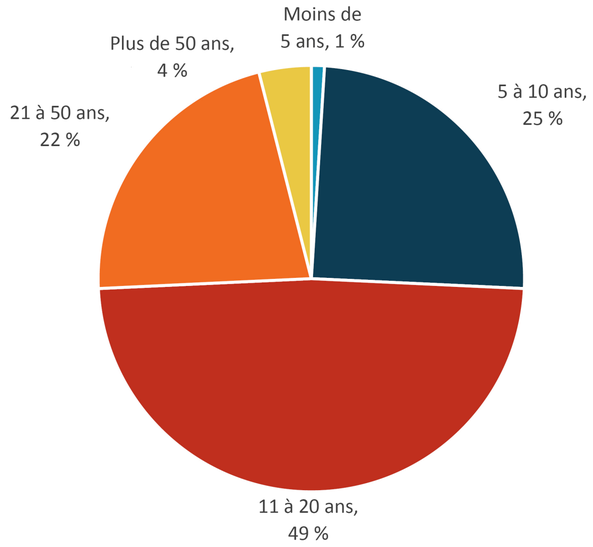
Pour collecter des données pour ce rapport, ESG a mené une enquête en ligne complète auprès de professionnels de la cybersécurité dans des organisations des secteurs privé et public en Amérique du Nord (États-Unis et Canada) entre le 3 août 2022 et le 14 août 2022. Pour être éligibles à cette enquête, les personnes interrogées devaient être des professionnels de la cybersécurité personnellement impliqués dans les technologies de cybersécurité, notamment les produits, les services et les processus. Toutes les personnes interrogées ont reçu une incentive pour répondre à l'enquête sous la forme de récompenses en espèces et/ou d'équivalents en espèces.

Après avoir éliminé les personnes interrogées non éligibles, supprimé les doublons et effectué le filtrage des réponses complètes qui restaient (sur la base de différents critères) pour l'intégrité des données, il est resté au final un échantillon total de 373 professionnels de la cybersécurité.

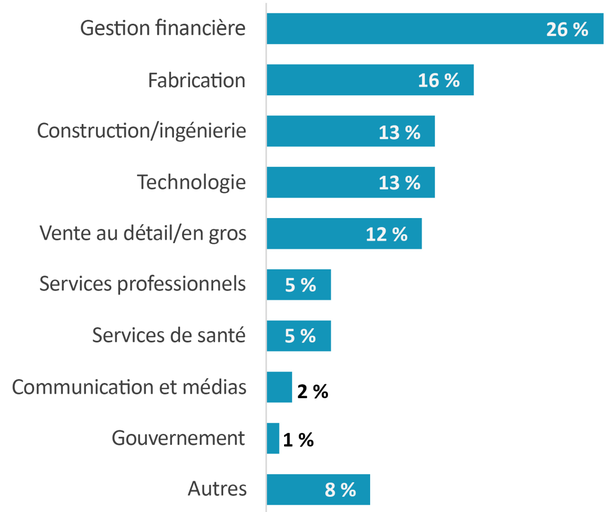
PERSONNES INTERROGÉES PAR NOMBRE DE COLLABORATEURS



PERSONNES INTERROGÉES PAR ÂGE DE LA SOCIÉTÉ



PERSONNES INTERROGÉES PAR SECTEUR D'ACTIVITÉ



REVENIR AU CONTENU

Enterprise Strategy Group est une entreprise intégrée d'analyse, de recherche et de stratégie technologiques qui fournit des données relatives aux marchés, des renseignements exploitables et des services de commercialisation à la grande communauté informatique.