SANS | Research Program

Enquête

# Enquête SANS 2024 sur la détection et la réponse

## Transformer les opérations de cybersécurité : IA, automatisation et intégration dans Détection et réponse

Écrit par Josh Lemon

Novembre 2024

RAPID7

# Résumé exécutif

C'est la première année que SANS mène son enquête sur la détection et la réponse, qui visait à recueillir des informations sur la manière dont les organisations du monde entier gèrent les menaces de cybersécurité. Notre objectif était d'interpréter les données brutes des répondants et d'offrir des informations et des conseils pour aider d'autres professionnels du domaine à améliorer leurs stratégies de détection et de réponse.

L'un des principaux objectifs était d'explorer comment les organisations détectent et réagissent aux cybermenaces. Alors que nous analysions l'état de la détection et de la réponse en 2024, il est devenu évident que ces capacités sont au cœur de la stratégie de cybersécurité d'une organisation, mais peuvent être laissées de côté lorsqu'il s'agit d'établir des budgets de cybersécurité.

En examinant les structures organisationnelles de détection et de réponse, nous avons constaté une répartition presque égale entre celles qui utilisent des équipes intégrées et celles qui emploient des équipes spécialisées distinctes. Cela suggère qu'il n'y a pas de consensus clair dans le secteur sur la meilleure approche, mettant en évidence diverses stratégies basées sur les besoins, les ressources et les priorités de l'organisation. Les données mettent également en lumière les défis spécifiques auxquels les organisations sont confrontées, comme les contraintes budgétaires.

Nos résultats mettent en évidence le paysage complexe de la détection et de la réponse en matière de cybersécurité moderne, où l'interaction entre l'expertise humaine et les outils automatisés est cruciale pour garder une longueur d'avance sur les menaces. L'enquête a révélé que :

- Une majorité significative d'organisations (64 %) intègrent des réponses automatisées mécanismes dans leurs opérations.
- Seuls 16 % des répondants déclarent avoir entièrement automatisé leurs processus de réponse.
- À 59 %, le besoin de personnel qualifié était le principal obstacle à la mise en œuvre.
- 47 % des répondants ont indiqué que les contraintes budgétaires étaient une préoccupation majeure.
- Environ deux tiers des répondants (67 %) ont indiqué qu'ils prévoyaient d'étendre leur utilisation de l'intelligence artificielle (IA) et de l'apprentissage automatique pour la détection et la réponse aux menaces.

À l'avenir, l'enquête indique une tendance à l'utilisation croissante de l'IA et de l'apprentissage automatique pour la détection et la réponse aux menaces. Cette focalisation sur les technologies avancées reflète une position proactive face à l'évolution du paysage des menaces, visant à automatiser la détection des menaces et à améliorer la précision des réponses. Cependant, à mesure que les organisations adoptent ces technologies, le besoin de personnel qualifié pour gérer et interpréter les informations générées par l'IA reste primordial. L'enquête 2024 fournit une vue détaillée de l'état actuel de la détection et de la réponse en matière de cybersécurité, offrant une référence précieuse aux organisations pour affiner et faire progresser leurs stratégies de défense.

Bien qu'il s'agisse de la première année d'enquête sur la détection et la réponse au SANS, nous avons eu le plaisir d'avoir près de 400 répondants. La figure 1 donne un aperçu des caractéristiques démographiques des répondants.

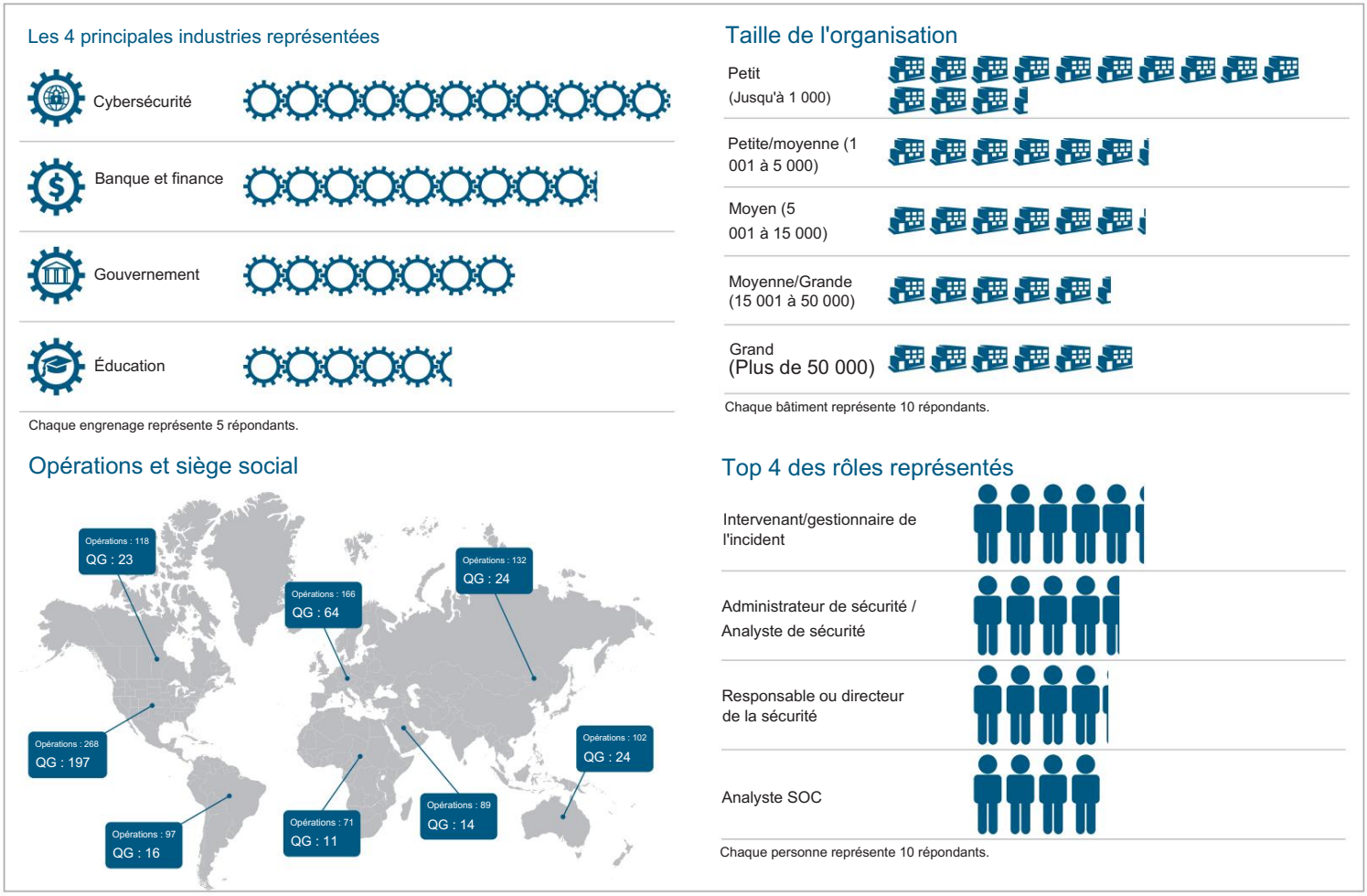


Figure 1. Enquête démographique

## Détection des menaces : jouez-vous avec le bon deck ?

La plupart des répondants (87 %) ont déclaré utiliser des outils automatisés ou assistés pour détecter les menaces. Cela peut donner aux organisations un avantage significatif au début de la Cyber Kill Chain1 dans l'espoir de réduire les dommages ou la destruction causés par les acteurs malveillants. Cependant, un nombre important de répondants (66 %) utilisent encore la surveillance manuelle (voir la figure 2). Cela est quelque peu inquiétant, compte tenu de la vitesse à laquelle les acteurs malveillants se déplacent ainsi que du temps nécessaire aux organisations pour détecter une menace à l'intérieur du réseau. Cela pourrait signifier que certaines organisations effectuent davantage de surveillance manuelle et ont du mal à faire face au paysage actuel des menaces. Une autre proportion non négligeable de répondants (39 %) ont indiqué qu'ils utilisent des technologies basées sur l'IA et l'apprentissage automatique (ML) pour détecter les menaces.

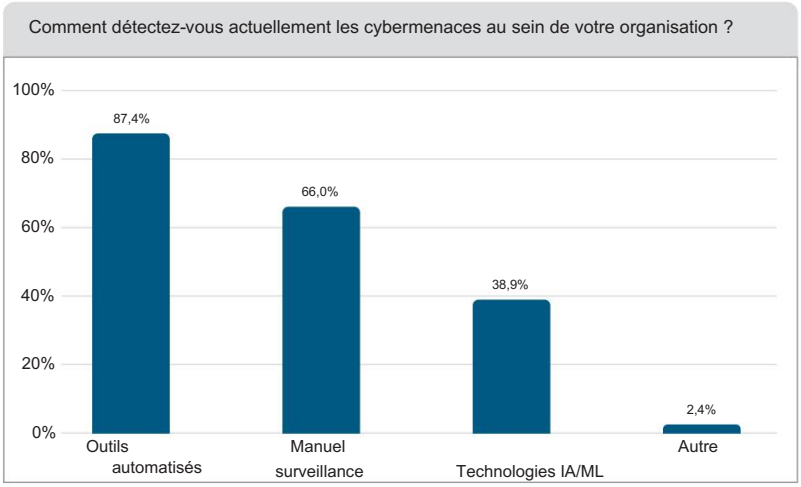


Figure 2. Méthodes de détection des menaces

Il est essentiel de comprendre comment les organisations effectuent les détections ainsi que les types d'outils qu'elles utilisent et leur utilité. Nous avons demandé aux répondants quelle était l'efficacité des différents outils de détection des menaces, sans aucune limite quant au nombre d'outils qu'ils pouvaient sélectionner. Nous avons découvert que les organisations exploitent une gamme de technologies pour améliorer leurs capacités de détection. À 42 %, les outils de détection et de réponse aux points d'extrémité (X/EDR) sont perçus comme les plus efficaces, ce qui indique une dépendance croissante aux solutions X/EDR. Cela est probablement dû à leur capacité à fournir une visibilité complète sur les points d'extrémité, à la fois dans les limites d'un réseau d'entreprise et en dehors de celui-ci, et à leur capacité à réagir rapidement aux menaces émergentes. Nous avons également constaté que le secteur s'oriente considérablement vers la détection sur les points d'extrémité, ce qui correspond étroitement au résultat de ce type d'outils.

En deuxième position (30 %), l'implication d'une équipe dédiée à la recherche de menaces a été jugée « extrêmement efficace ». Cela suggère que, bien que les outils automatisés soient essentiels, un chasseur humain reste une condition essentielle pour une détection réussie des menaces. La capacité des chasseurs de menaces à non seulement appliquer une compréhension contextuelle des preuves ou des indicateurs, mais aussi à penser de manière créative, pourrait expliquer pourquoi cette approche reste très appréciée, au même titre que les solutions technologiques.

1 « La chaîne de destruction cybernétique », www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

En ce qui concerne l'efficacité des outils, la répartition est homogène entre tous les types d'outils (voir Figure 3). Avec 67 %, la détection et la réponse réseau (NDR) arrivent en tête des listes des répondants, ce qui indique un besoin important de surveillance et de détection des menaces au niveau de la couche réseau. La NDR constitue également une solution de secours précieuse, en particulier dans les environnements qui ne disposent pas d'outils EDR déployés sur les points de terminaison, notamment les systèmes liés aux ICS ou les systèmes hérités qui ne relèvent pas des accords de support des fournisseurs, ce qui constitue un tout autre risque.

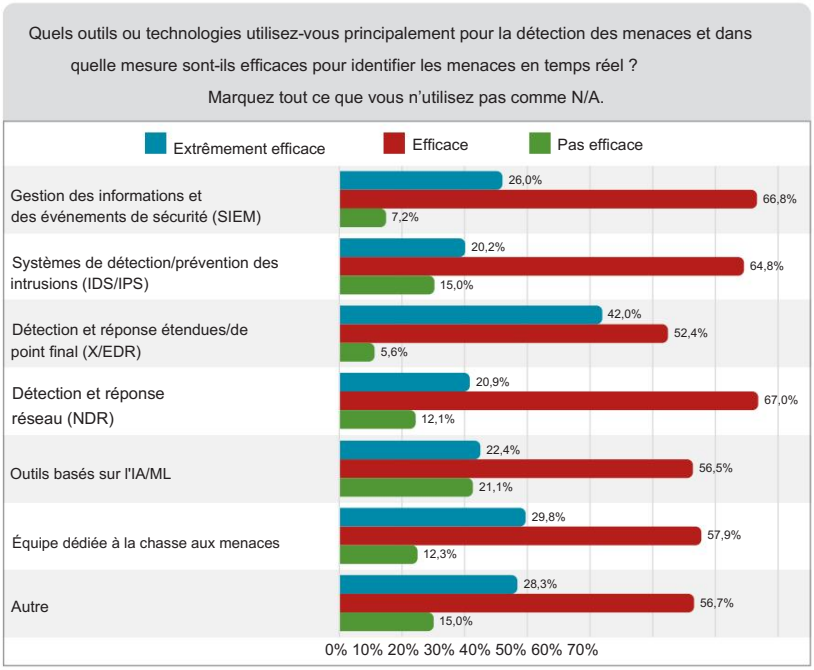


Figure 3. Utilisation et efficacité des outils

## Détection par la Machine Vivante

En revanche, les répondants ont des avis mitigés sur l'utilité des outils basés sur l'IA/ML pour effectuer la détection. Seuls 22 % des répondants ont jugé ces outils extrêmement efficaces ; 57 % les ont jugés efficaces, tandis que 21 % les ont jugés inefficaces. Dans l'ensemble, les outils basés sur l'IA/ML se classent à peu près au milieu de la liste des outils extrêmement efficaces et sont classés parmi les moins efficaces pour détecter les menaces. Cela ne signifie pas nécessairement que les outils basés sur l'IA et le ML ne doivent pas être utilisés pour la détection des menaces. Cela signifie simplement que les outils de cette catégorie doivent devenir plus efficaces pour attraper les acteurs de la menace.

Nous avons également demandé aux entreprises si elles utilisaient actuellement des algorithmes d'apprentissage automatique pour la détection des menaces. Nous avons constaté qu'un peu plus de 51 % d'entre elles le faisaient (voir la figure 4). Cela pourrait refléter une tendance croissante à adopter rapidement des technologies de cette catégorie, même si le secteur semble encore quelque peu indécis. Il convient de noter que 22 % des répondants ne savaient pas si leur entreprise utilisait des algorithmes d'apprentissage automatique pour la détection des menaces.

Parmi les organisations qui utilisent l'apprentissage automatique pour détecter les menaces, seulement un quart l'utilisent de manière intensive. La majorité (51 %) l'utilisent de manière modérée, tandis que 22 % supplémentaires l'utilisent de manière assez minimale, ce qui indique peut-être que les expérimentations et les réglages sont toujours en cours.

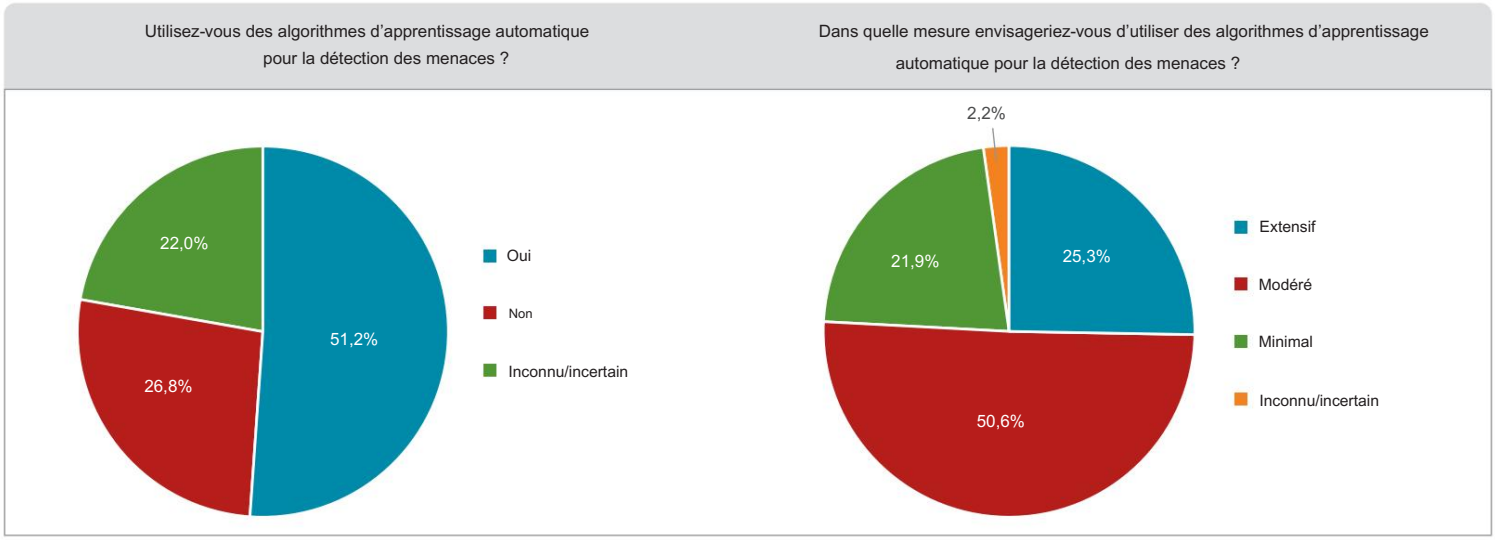


Figure 4. Utilisation de l'apprentissage automatique

## Détection dans les nuages

L'un des résultats les plus intéressants concerne les capacités et l'efficacité des répondants à détecter les menaces basées sur le cloud. Cela inclut l'infrastructure en tant que service (IaaS), le logiciel en tant que service (SaaS) et les fonctions en tant que service (FaaS). Toutes ces technologies basées sur le cloud font partie de la surface d'attaque d'une organisation et doivent être surveillées pour détecter les acteurs malveillants. Très peu d'organisations estiment qu'elles sont extrêmement efficaces dans l'utilisation d'outils natifs du cloud (21 %), d'outils tiers (17 %) ou d'outils développés en interne (19 %) pour effectuer la détection des menaces. La plupart des répondants estiment toutefois qu'ils sont efficaces dans l'utilisation de tous ces outils, les outils natifs du cloud (67 %) recevant la note d'efficacité la plus élevée.

## Créer des détections et les partager

Il est important de comprendre comment les organisations se procurent leurs règles de détection pour avoir une meilleure idée de la manière dont le secteur détecte les acteurs. La plupart des répondants utilisent les plateformes de renseignement sur les menaces du secteur (65 %) comme principale source, suivies des équipes internes qui développent des règles pour eux (62 %). Ils préfèrent également faire appel à des fournisseurs de sécurité (59 %) et à des agences gouvernementales ou réglementaires (57 %), les communautés open source (46 %) étant la source de règles de détection la moins utilisée. Le fait que les communautés open source aient une priorité aussi faible est quelque peu surprenant, étant donné qu'une grande partie de la technologie utilisée pour élaborer et partager des règles provient de la communauté open source. Mais il n'est pas surprenant non plus que les organisations soient plus disposées à faire confiance aux plateformes de renseignement sur les menaces du secteur qui ont des règles préparées et prêtes à l'emploi.

Il était également important de comprendre quel format les organisations préfèrent pour leurs règles de détection des menaces. Par ordre de priorité, les formats lisibles par machine tels que YARA2 et STIX3 sont les plus préférés, suivis des règles déjà intégrées aux outils de sécurité ; les détections lisibles par l'homme et les notifications par e-mail sont les formats les moins souhaitables pour recevoir les règles de détection. Le plus grand défi auquel les organisations sont confrontées lors de la réception des règles de détection est la qualité et la fiabilité des règles : 73 % des répondants considèrent cela comme un défi. Viennent ensuite les problèmes de compatibilité avec les outils existants (55 %), le volume considérable d'informations (54 %) et le manque de contexte ou de pertinence pour la détection (50 %).

En tant qu'enfants, on nous apprend que « partager, c'est prendre soin des autres ». Dans quelle mesure cela s'applique-t-il au partage de règles de détection utiles avec d'autres entités ? Seuls 39 % des répondants partagent des règles de détection ou des indicateurs de compromission avec d'autres entités. Ceux qui partagent préfèrent largement partager quotidiennement avec des équipes internes (35 %), avec des plateformes de renseignement sur les menaces spécifiques à leur secteur (27 %) ou avec des organismes gouvernementaux ou de réglementation (19 %). Très peu d'organisations partagent leurs renseignements sur la détection des menaces avec la communauté open source. La principale motivation des organisations à partager leurs renseignements sur la détection des menaces est le partage réciproque d'informations (68 % des répondants) : partager des informations afin que des informations similaires leur soient partagées en retour. Soixante-cinq pour cent des répondants souhaitent améliorer la posture de sécurité globale de leur organisation, et 58 % le font dans le cadre de contributions communautaires, ce qui est louable étant donné que c'est ainsi que naissent une grande partie des renseignements sur les menaces destinés à la communauté plus large de la cybersécurité.

2 « YARA », https://virustotal.github.io/yara/

3 « Introduction à STIX », https://oasis-open.github.io/cti-documentation/stix/intro

# L'automatisation en action : l'avenir de la réponse aux incidents

Cette section examine en détail la manière dont les organisations réagissent aux menaces détectées. La plupart des répondants (68 %) déclarent qu'ils effectuent une réponse semi-automatique ; cependant, une grande proportion d'entre eux utilisent des techniques de réponse manuelle (23 %). (Voir la figure 5.) Les petites organisations ne sont pas les seules à réagir manuellement ; cela varie des organisations de moins de 100 employés jusqu'aux grandes organisations multinationales.

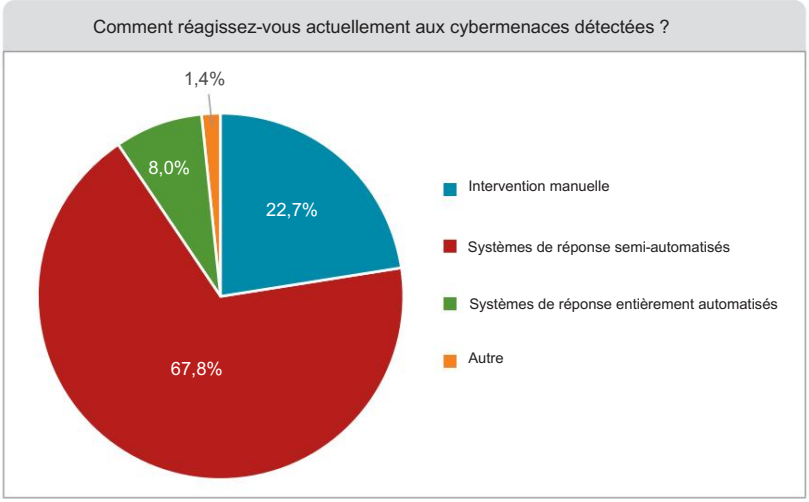


Figure 5. Méthodes de réponse aux menaces

FrançaisLors de l'examen des outils et technologies utilisés par les organisations pour répondre aux menaces, la détection et la réponse aux points d'extrémité (EDR) apparaissent comme le choix prédominant, avec 82 % des répondants qui y font confiance (voir Figure 6). Cela correspond étroitement aux tendances observées dans la détection des menaces, où la visibilité des points d'extrémité et les capacités de réponse rapide sont cruciales. La capacité de l'EDR à observer, détecter et répondre aux menaces au niveau des points d'extrémité en fait un outil essentiel pour de nombreuses organisations, en particulier étant donné que les acteurs de la menace démarrent généralement leurs attaques aux points d'extrémité ou les utilisent comme « tête de pont »4 lorsqu'ils mènent une attaque au sein d'une organisation. Il n'est pas surprenant que l'EDR soit une technologie si largement utilisée, étant donné qu'elle couvre les organisations non seulement pour la détection mais aussi pour la réponse, tout en étant un moyen efficace de consolider les coûts d'outillage.

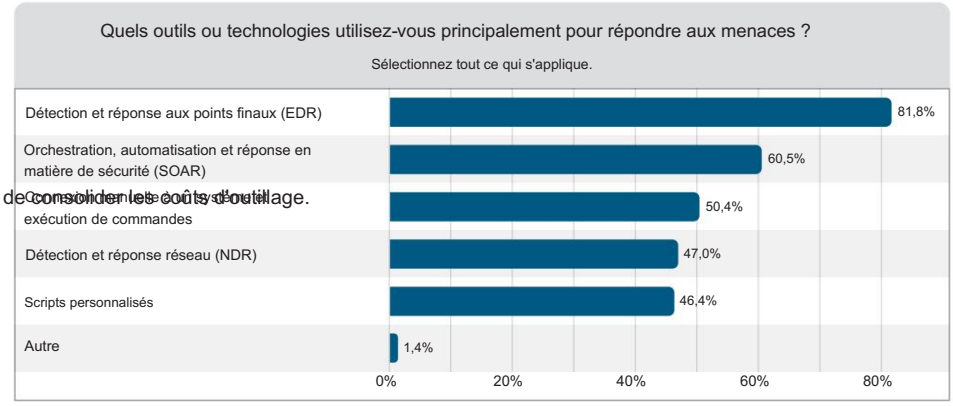


Figure 6. Outils de réponse aux menaces

L'enquête révèle également une dépendance notable aux plateformes d'orchestration, d'automatisation et de réponse en matière de sécurité (SOAR) : 61 % des répondants intègrent ces outils dans leurs stratégies de réponse aux menaces. La capacité de SOAR à automatiser les tâches de routine et à intégrer divers outils de sécurité permet aux organisations de rationaliser leurs processus de réponse afin de réduire le temps nécessaire pour traiter les incidents. Il est intéressant de noter que malgré les progrès en matière d'automatisation et d'outils (commerciaux et open source) disponibles pour les terminaux, 50 % des répondants se connectent encore manuellement aux systèmes et exécutent des commandes, ce qui indique que la réponse pratique et dirigée par l'homme reste une composante importante des activités de réponse aux menaces. L'utilisation de scripts personnalisés est étroitement liée à l'exécution de tâches manuelles, il n'est donc pas surprenant que 46 % des répondants les utilisent également. L'enquête montre également que même si une large sélection d'outils prêts à l'emploi est disponible aujourd'hui, il existe encore des écarts entre ce dont les intervenants ont besoin et ce qui est disponible.

4 Une tête de pont est un lieu de transit à partir duquel un acteur malveillant peut opérer au sein d'une organisation. Elle est également souvent utilisée pour stocker les informations collectées auprès d'une victime avant l'exfiltration ou comme lieu de transit pour accéder à plusieurs systèmes.

Le fait que 47 % des répondants utilisent le NDR est un résultat positif, car il s'agit d'un moyen très efficace de répondre à une menace sans que les acteurs de la menace puissent la détecter, contrairement à un acteur de la menace qui peut voir les actions des intervenants sur les points de terminaison lorsqu'ils utilisent des outils EDR. La seule différence significative entre les outils de type NDR et les outils de type EDR est que les outils NDR nécessitent plus de prévoyance et de planification pour mettre en place des prises réseau et accéder à l'infrastructure réseau ; en revanche, les outils EDR peuvent être déployés alors qu'un incident est encore en cours.

## Le Fast and the Furious pour la réponse

L'analyse de la rapidité avec laquelle les organisations peuvent réagir aux menaces confirmées fournit des informations précieuses sur la maturité et l'efficacité de leurs capacités de réponse aux menaces. Une part importante des organisations (41 %) affirme pouvoir réagir aux menaces confirmées en quelques minutes, ce qui est impressionnant (voir la figure 7). Cette tendance prometteuse suggère que de nombreuses organisations ont mis en place des systèmes bien intégrés et réactifs, utilisant probablement des outils tels que les plateformes SOAR et les solutions X/EDR pour faciliter la détection rapide et la réponse immédiate. De plus, 8 % des organisations déclarent être capables de réagir en quelques secondes ! Une fois qu'une détection de menace a été déclenchée, la capacité à agir et à réagir rapidement est une capacité essentielle pour les organisations d'aujourd'hui. D'après les statistiques de l'équipe Google Cloud Security5, le défi consiste souvent à détecter les acteurs de la menace suffisamment tôt. Selon leurs statistiques, un acteur de la menace dispose d'au moins 10 jours pour réagir. Par conséquent, être capable de réagir rapidement est un moyen de rattraper lentement le retard. acteurs de la menace présents dans un environnement depuis un certain temps.

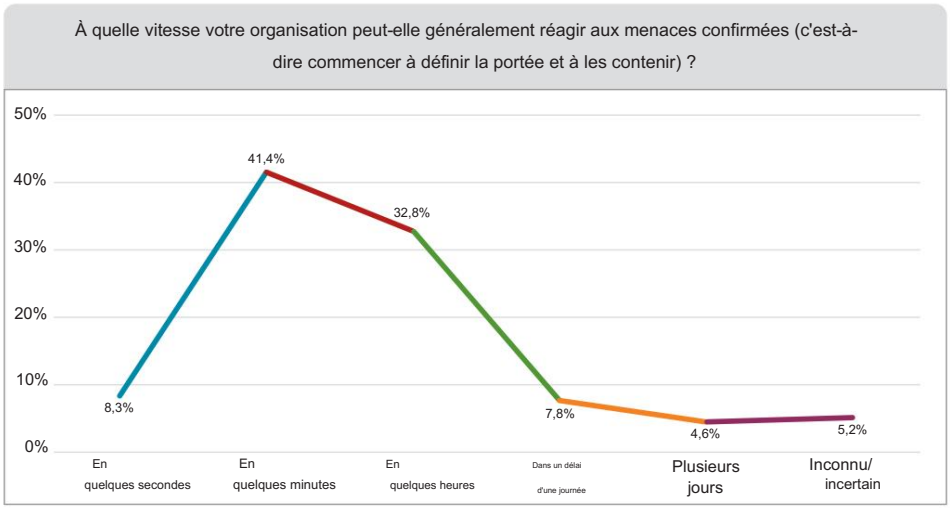


Figure 7. Vitesse de réponse aux menaces

Il est toutefois important de noter que 33 % des répondants indiquent que leur organisation réagit généralement en quelques heures, et que 12 % prennent entre un et plusieurs jours, ce qui peut impliquer des niveaux de préparation ou d'allocation de ressources variables selon les organisations. Ces délais de réponse, bien que toujours proactifs, suggèrent qu'il peut y avoir des défis tels que des processus internes plus lents, une automatisation limitée ou des contraintes de ressources qui peuvent retarder l'action immédiate. Bien qu'il soit rassurant de constater que 83 % des répondants peuvent répondre à une menace en quelques secondes ou quelques heures, il semble qu'une partie des organisations aient encore du mal à passer de cette étape de réponse initiale à la compréhension du degré d'intégration d'un acteur, jusqu'à la compréhension de la manière dont elles pourraient s'y prendre pour expulser un acteur de menace de leur environnement.

5 « Rapport spécial M-Trends 2024 », https://cloud.google.com/security/resources/m-trends

L'adoption de mécanismes de réponse automatisés est de plus en plus répandue parmi les organisations, avec 64 % des répondants indiquant avoir partiellement intégré ces systèmes dans leurs opérations de cybersécurité. Cela suggère une reconnaissance croissante des avantages que l'automatisation peut apporter, tels que des temps de réponse plus rapides et une gestion plus efficace des menaces. Cependant, seulement 16 % ont entièrement mis en œuvre des mécanismes de réponse automatisés, ce qui indique qu'il y a encore beaucoup de progrès à faire dans ce domaine. Parmi les répondants restants, 15 % n'ont adopté aucune automatisation et 5 % ne sont pas sûrs. Il peut s'agir d'organisations qui sont soit prudentes quant à la mise en œuvre de l'automatisation, soit confrontées à des obstacles tels que des contraintes budgétaires, une pénurie de compétences ou des inquiétudes concernant une dépendance excessive aux systèmes automatisés.

Les stratégies les plus couramment utilisées pour automatiser les flux de travail de détection à réponse sont des manuels prédéfinis : 74 % des répondants les utilisent pour normaliser et rationaliser les actions de réponse. Ce recours aux manuels souligne l'importance de mettre en place des processus clairs, structurés et reproductibles, qui peuvent contribuer à réduire les délais de réponse et à garantir la cohérence. En outre, cela peut aider les organisations lors du recrutement de nouveaux membres du personnel, en garantissant une structure pour la manière dont les nouveaux membres de l'équipe des opérations de sécurité réagissent lorsqu'un acteur de menace se trouve dans un environnement. Les scripts d'intégration et d'automatisation personnalisés sont également largement utilisés, cités par 64 % des répondants, ce qui reflète la nécessité de solutions sur mesure qui peuvent s'adapter aux besoins et aux environnements organisationnels spécifiques. Cela peut être dû à des environnements plus nuancés par nature ou simplement au fait que les outils existants, qu'ils soient commerciaux ou open source, ne fournissent tout simplement pas l'automatisation dont certaines organisations ont besoin. L'intégration avec les outils SOAR est également populaire, utilisée par 62 % des répondants. Il est intéressant de noter que les modèles d'apprentissage automatique ne sont utilisés que par 35 % des organisations, ce qui suggère que même si l'IA est un domaine en pleine croissance, elle est encore explorée et intégrée avec prudence. Ces résultats montrent que le personnel opérationnel souhaite une intégration plus étroite et moins de « clics sur un bouton » pour accomplir les tâches de réponse, ce qui est logique lorsqu'un acteur de la menace a au moins 10 jours d'avance, et correspond à certains des défis en matière de personnel que nous aborderons sous peu.

## Où réagir en premier

Il est essentiel de réagir rapidement aux menaces, mais il est tout aussi important de hiérarchiser les menaces qui nécessitent une attention immédiate. Nous avons demandé aux répondants d'identifier les types de menaces qu'ils considèrent comme les plus graves. En comprenant comment les organisations classent la gravité des différentes menaces, nous pouvons obtenir des informations sur la manière dont elles hiérarchisent leurs efforts de réponse, en veillant à ce que les menaces les plus critiques soient traitées en premier.

Lorsque plusieurs menaces sont détectées, une moyenne pondérée des répondants (41 %) s'accorde à dire que la priorité de la réponse en fonction de la gravité de la menace est le facteur le plus important pour éviter de causer des dommages importants à une organisation. L'impact potentiel sur l'activité est le deuxième facteur clé, 29 % des répondants indiquant qu'ils se concentrent sur la protection des opérations et la minimisation des perturbations. Le type d'actif affecté est considéré comme la troisième priorité la plus élevée et est probablement lié aux actifs essentiels au fonctionnement de l'organisation, tels que les données clients, la propriété intellectuelle ou les ressources critiques pour l'entreprise. Le facteur le plus souvent cité par les répondants (71 %) est que la disponibilité des ressources est la priorité la plus basse parmi les options proposées.

# Dream Team en matière de cybersécurité : intégrer ou séparer ?

La structure des fonctions de détection et de réponse des organisations affecte non seulement la dynamique de ces fonctions, mais peut également avoir des effets secondaires positifs et négatifs sur les opérations de cybersécurité. Lorsqu'on leur a demandé si ces fonctions étaient intégrées au sein d'une seule équipe ou gérées par des équipes distinctes, les résultats de l'enquête ont révélé une répartition presque égale : 48 % des répondants ont indiqué qu'ils géraient ces fonctions au sein d'équipes distinctes, tandis que 48 % ont déclaré fonctionner comme une équipe unique et intégrée. (Les 4 % restants des répondants n'étaient pas sûrs de leur structure organisationnelle.) Cette division presque égale6, bien qu'inattendue, suggère qu'il n'existe pas de consensus clair au sein du secteur sur la meilleure approche à adopter pour organiser les activités de détection et de réponse. Elle peut également refléter des besoins organisationnels, une disponibilité des ressources et des priorités stratégiques différents. Ces informations aideront à clarifier les différentes approches adoptées par les organisations pour équilibrer l'expertise spécialisée et les opérations intégrées dans leurs efforts de défense en matière de cybersécurité.

En ce qui concerne la structuration des équipes de détection et de réponse, les organisations semblent être guidées principalement par le besoin de compétences spécialisées, comme l'ont souligné 68 % des répondants. Cet accent mis sur la spécialisation pourrait refléter la complexité croissante des opérations cybernétiques, où le fait de disposer d'experts concentrés sur des aspects spécifiques de la sécurité peut conduire à une détection et une réponse plus efficaces. L'efficacité des opérations est également un facteur important, cité par 56 % des répondants, ce qui indique que de nombreuses organisations pensent qu'une bonne structure d'équipe peut rationaliser les processus et réduire les délais de réponse. En outre, 40 % des répondants ont indiqué que les politiques organisationnelles influencent la structure de leurs équipes, ce qui suggère que les réglementations et directives internes jouent souvent un rôle dans la manière dont ces fonctions critiques sont organisées. Il est quelque peu décevant de constater qu'un pourcentage aussi élevé de répondants se laissent dicter par les politiques organisationnelles la meilleure façon de détecter et de répondre aux cybermenaces, au lieu de s'appuyer sur l'expérience et les compétences de leur personnel chargé des opérations de sécurité.

En examinant l'impact de ces structures sur la posture de sécurité globale, 48 % des répondants ont exprimé une opinion positive (29 %) ou très positive (19 %) de leur configuration actuelle. Cela indique que de nombreuses organisations sont convaincues que l'approche choisie, qu'elle soit intégrée ou séparée, améliore efficacement leurs capacités de sécurité. Une part importante des répondants (33 %) avait une opinion neutre, suggérant que même si leur structure actuelle fonctionne, ils pourraient être ouverts à des améliorations ou des ajustements. Il est intéressant de noter que seul un petit pourcentage (14 %) avait une opinion négative ou très négative sur la structure des équipes de leur organisation. Il sera intéressant de voir comment cela évolue au cours des prochaines enquêtes pour comprendre si les organisations trouvent une manière plus prédominante de structurer leurs équipes de détection et de réponse.

6 Les chiffres semblent égaux en raison de l'arrondissement. Les chiffres réels montrent une variation de 0,3 % en faveur des équipes séparées ; toutefois, aux fins du présent rapport, ce petit pourcentage est négligeable.

Les entreprises envisagent différentes stratégies pour structurer leurs équipes de détection et de réponse afin d'améliorer leur efficacité. L'approche la plus populaire, choisie par près de 50 % des répondants, est une structure hybride. Cela suggère que de nombreuses entreprises voient l'intérêt de combiner des éléments d'intégration et de spécialisation, dans le but de tirer parti des avantages de chaque approche. Un tel modèle hybride peut offrir la flexibilité nécessaire pour s'adapter à différents types de menaces tout en permettant une expertise ciblée là où elle est nécessaire. Parallèlement, 44 % des répondants prévoient de maintenir des équipes distinctes spécialisées, ce qui indique qu'ils continuent de croire en l'importance de domaines de connaissances approfondis et ciblés pour la détection et la réponse.

Il est intéressant de noter que 32 % des organisations souhaitent évoluer vers une équipe unique intégrée, ce qui peut refléter un désir d'opérations plus cohérentes ou une volonté de regrouper davantage les effectifs. Le faible pourcentage (3 %) choisissant d'autres approches suggère que les organisations pourraient envisager d'autres structures non prises en compte dans l'enquête, bien qu'aucune n'ait été exprimée dans les sections de texte libre de l'enquête. Étant donné que les répondants ont actuellement une répartition presque égale entre une équipe unique et des équipes distinctes, il semble qu'il pourrait y avoir à l'avenir une évolution vers des équipes plus hybrides ou distinctes.

## Lutter contre les menaces du cloud depuis le bas

La détection et la réponse dans le cloud présentent des défis et des opportunités uniques par rapport à la détection et à la réponse traditionnelles aux points d'extrémité, principalement en raison de la nature dynamique et de l'échelle des environnements cloud. Les organisations sont confrontées à des défis importants, 56 % d'entre elles citant une expertise limitée en matière de sécurité cloud comme un obstacle majeur. Cela souligne le besoin crucial de connaissances spécialisées pour gérer efficacement les menaces cloud. La complexité de la gestion des configurations multicloud et de l'intégration avec les outils de sécurité existants constitue également un défi majeur, affectant respectivement 51 % et 49 % des répondants, soulignant les difficultés techniques et opérationnelles inhérentes à la sécurité cloud.

En matière de détection des menaces, les outils de sécurité natifs du cloud sont considérés comme les plus efficaces, 21 % des personnes interrogées les jugeant extrêmement efficaces et 67 % comme efficaces. Cela suggère que l'utilisation d'outils de sécurité conçus spécifiquement pour les environnements cloud présente des avantages pour ceux qui les utilisent. Cependant, 13 % des personnes interrogées estiment toujours que les outils cloud natifs ne sont pas efficaces, ce qui indique qu'il y a une marge de progression. Les outils tiers et développés en interne affichent également une efficacité modérée, mais 19 % et 21 % respectivement estiment que ces outils doivent être améliorés. Cela peut simplement être dû à la rapidité avec laquelle l'environnement cloud évolue, ce qui rend ces outils difficiles à maintenir au fil du temps. Bien que 59 % des personnes interrogées trouvent la surveillance manuelle efficace, seulement 15 % la considèrent comme extrêmement efficace et 26 % la trouvent inefficace. Cela reflète probablement les limites que les processus manuels peuvent présenter dans les environnements cloud à grande échelle.

Pour relever ces défis, 71 % des organisations prévoient d'améliorer la formation des équipes de sécurité sur les menaces spécifiques au cloud, reconnaissant clairement la nécessité de développer une expertise interne. En outre, 53 % envisagent d'adopter des outils de sécurité cloud natifs plus avancés et 52 % visent à intégrer l'IA/ML pour la détection et la réponse aux menaces ; cependant, compte tenu des résultats fournis par les organisations dans les réponses précédentes à l'IA/ML, cela peut s'avérer insignifiant.
L'accent mis sur la formation, l'adoption de la technologie et la collaboration accrue avec les fournisseurs de services cloud (40 %) suggère que les organisations voient un besoin évident de faire évoluer leurs stratégies de détection et de réponse au cloud.

## Investir dans les talents pour assurer le succès des opérations de détection et de réponse

Lorsqu'il est question de la création et de l'utilisation efficace d'outils d'automatisation pour la détection et la réponse, l'importance d'un personnel qualifié ne peut être surestimée. Les organisations s'appuyant de plus en plus sur des systèmes automatisés pour gérer le volume et la complexité croissants des cybermenaces, il devient essentiel de disposer d'une équipe dotée des compétences nécessaires. Les données de l'enquête montrent qu'il ne suffit pas de lancer un « nouvel outil génial » et de s'attendre à ce qu'il détecte « tous les problèmes ». Près de 77 % des organisations comblent les lacunes en matière de compétences grâce à des programmes de formation, ce qui indique clairement que les organisations et leur personnel reconnaissent que la défense de leur environnement nécessite des connaissances spécialisées provenant d'autres personnes extérieures à leur organisation. Cet engagement en matière de formation s'aligne sur les projets de 71 % des répondants visant à améliorer la formation aux menaces spécifiques au cloud, soulignant encore davantage la nécessité de connaissances spécialisées pour gérer les défis uniques posés par les environnements cloud.

L'embauche de personnel qualifié est une autre stratégie essentielle, 61 % des répondants ayant fait appel à une expertise externe pour renforcer leurs équipes de détection et d'intervention. Cette approche complète les efforts de formation interne, en offrant un accès immédiat à des compétences avancées qui peuvent accélérer les capacités de détection et d'intervention, du moins à court terme. Cependant, cette approche pourrait ne pas être durable dans le temps pour développer les compétences en interne. Ce type de stratégie pourrait réduire le nombre de nouveaux diplômés ou de personnel junior entrant dans le domaine de la cyberdéfense au sein de notre secteur. Bien qu'il puisse s'agir davantage d'un plan stratégique pour l'état actuel de l'économie, il s'agira d'une tendance intéressante à observer au fil du temps.

L'externalisation, utilisée par 40 % des organisations, peut offrir une solution flexible pour accéder à des compétences et des connaissances spécialisées sans l'investissement à long terme lié à l'embauche de personnel à temps plein. Cette approche peut être particulièrement utile pour les petites entreprises ou celles qui ont des contraintes budgétaires, car elle leur permet de bénéficier des connaissances et des compétences d'experts en fonction des besoins. Un peu plus de 30 % d'entre elles ont recours à des rotations internes, ce qui suggère que certaines organisations étudient également des moyens de diversifier leurs talents existants, en veillant à ce que les membres de l'équipe acquièrent de l'expérience dans différents domaines de la cybersécurité.

Les entreprises semblent adopter une approche multidimensionnelle pour améliorer la détection et la réponse aux menaces au sein de l'infrastructure cloud. Au-delà de la formation, 53 % des répondants prévoient d'adopter des outils de sécurité cloud natifs plus avancés, et 53 % supplémentaires cherchent à intégrer l'IA et le ML pour améliorer la détection et la réponse aux menaces. Bien que cruciales, ces améliorations technologiques nécessitent du personnel capable de gérer et d'optimiser ces outils pour s'assurer qu'ils délivrent tout leur potentiel et détectent et activent avec précision les fonctions de réponse aux menaces. Les données montrent que les entreprises reconnaissent ce besoin, comme en témoigne le pourcentage élevé d'entreprises qui se concentrent sur la formation et l'embauche de personnel qualifié. Les résultats de l'enquête sur la formation et l'éducation soulignent clairement la nécessité de disposer d'un personnel formé pour créer et maintenir des outils d'automatisation et améliorer les capacités de protection des environnements cloud. N'oubliez pas que l'outil d'IA ou de machine learning coûteux qui vous est vendu nécessite un opérateur expérimenté pour interpréter ce qu'il fait et s'assurer qu'il défend correctement votre organisation.

## Payer maintenant ou payer plus tard : le coût de la cybersécurité

De nombreuses organisations sont soumises à des contraintes budgétaires en matière de détection et de réponse aux menaces. Une part importante des répondants (42 %) décrit leur allocation budgétaire comme adéquate mais limitée, et 22 % la trouvent carrément insuffisante (voir Figure 8). Cela suggère que même si les organisations sont conscientes de l'importance d'investir dans la détection et la réponse aux menaces, elles sont souvent obligées de se contenter de ressources limitées. Seuls 26 % des répondants considèrent que leur budget est suffisant, et seulement 5 % le considèrent comme plus que suffisant, ce qui met en évidence un sentiment général de tension financière dans ce domaine critique de la cybersécurité. Ces limitations pourraient avoir un impact sur l'efficacité de la détection et de la réponse aux menaces, car les ressources financières sont cruciales pour acquérir et maintenir des outils et des formations de pointe, et pour conserver un personnel qualifié.

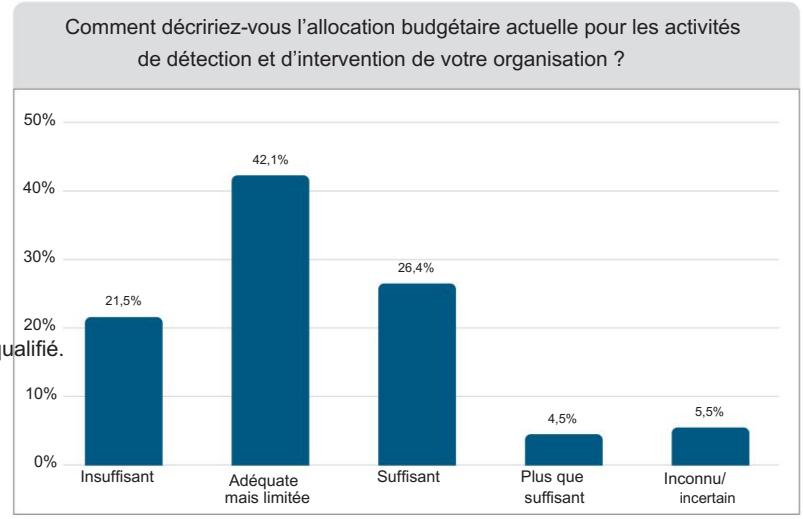


Figure 8. Adéquation du budget de détection et d'intervention

En ce qui concerne l'avenir, un certain optimisme, quoique prudent, semble régner en ce qui concerne les augmentations budgétaires des services de détection et d'intervention. Environ 42 % des répondants prévoient une augmentation modérée du budget, ce qui indique que certaines organisations commencent à reconnaître la nécessité d'investissements plus importants pour améliorer leur posture de cybersécurité. Cependant, cet optimisme est tempéré par le fait que seulement 7 % prévoient une augmentation significative, tandis que 25 % ne prévoient aucun changement. En outre, 9 % prévoient une diminution modérée du budget et 2 % une diminution significative. Ces résultats suggèrent que même si l'on est conscient de la nécessité d'accroître les investissements, les contraintes financières et les priorités concurrentes limitent la mesure dans laquelle les budgets peuvent être augmentés.

Les scénarios budgétaires actuels et prévus présentent des défis pour les organisations qui cherchent à améliorer leurs capacités de détection et de réponse. Le fait qu'un nombre important d'organisations travaillent avec des budgets insuffisants ou limités pourrait entraver leur capacité à adopter de nouvelles technologies, à embaucher du personnel qualifié supplémentaire et à investir dans les programmes de formation nécessaires. Alors que le paysage des menaces continue d'évoluer et de devenir plus sophistiqué, ces limitations budgétaires pourraient rendre de plus en plus difficile pour les organisations de suivre le rythme des menaces émergentes. Il est ironique que de nombreux pays représentés dans l'enquête de cette année imposent des amendes importantes pour les violations de données. Étant donné que les équipes de détection et de réponse au sein d'une organisation sont directement liées à la prévention d'une violation de données, il se peut qu'une organisation paie pour investir dans son équipe de détection et de réponse ou paie une amende pour violation de données si elle ne le fait pas. Dans les deux cas, le financement de cette équipe est très coûteux. devrait venir de quelque part.

## Les indicateurs qui comptent dans la réponse aux menaces

Il est essentiel de mesurer les performances des équipes de détection et de réponse pour démontrer la valeur et l'efficacité des efforts de cybersécurité aux dirigeants et à l'ensemble de l'organisation. La plupart des organisations utilisent des indicateurs clés de performance (ICP) qui se concentrent sur la rapidité et l'efficacité de leur réponse, 67 % d'entre elles surveillant le temps moyen de réponse (MTTR) et 52 % surveillant le temps moyen de détection (MTTD). Ces mesures sont cruciales car elles mettent en évidence la rapidité avec laquelle une équipe peut réagir et identifier les menaces, ce qui est essentiel pour minimiser les dommages potentiels. Parmi les autres ICP courants figurent le nombre d'incidents détectés (64 %) et résolus (58 %), bien que ces chiffres puissent parfois être trompeurs. À mesure que les capacités de détection et l'automatisation s'améliorent, le volume d'incidents peut augmenter, ce qui n'est pas nécessairement corrélé à un niveau de menace accru, mais plutôt à une capacité améliorée à découvrir et à résoudre les problèmes potentiels.

Malgré l'importance de ces indicateurs, l'efficacité des pratiques de mesure actuelles est mitigée. Seulement 26 % des répondants estiment que leurs indicateurs sont très ou extrêmement efficaces pour comprendre clairement les performances de leur équipe ; une plus grande partie (39 %) les trouve seulement modérément efficaces. Cela suggère que même si les indicateurs sont suivis, ils ne fournissent pas toujours les informations complètes nécessaires pour évaluer pleinement les performances des membres de l'équipe de détection ou d'intervention. Un défi notable souligné par 51 % des répondants est la difficulté de collecte des données, aggravée par un manque de personnel qualifié (49 %) et d'indicateurs standardisés (45 %). Bien que les indicateurs soient au cœur des préoccupations des équipes de détection et d'intervention, ils peuvent être négligés en raison de problèmes liés à la capacité à mieux automatiser et à suivre les indicateurs au lieu de détourner l'attention du travail opérationnel de défense d'un réseau.

L'analyse comparative des normes du secteur peut fournir un contexte précieux pour ces mesures, mais seulement 23 % des organisations le font régulièrement, contre 31 % de manière occasionnelle. Cela indique un domaine d'amélioration potentiel, car une analyse comparative régulière pourrait aider les organisations à comprendre leurs performances par rapport à leurs pairs du secteur. Des défis tels que l'insuffisance des outils d'analyse (42 %) et le volume élevé d'incidents (31 %) soulignent également la nécessité de meilleures ressources. Le défi consiste souvent à prendre ces données et à communiquer ce défi à la direction.

Il est essentiel pour les entreprises de comprendre et de mesurer la couverture de détection afin de maintenir une posture de sécurité robuste. Selon l'enquête, une majorité significative d'entreprises (64 %) évaluent ou mesurent activement leur couverture et leurs capacités de détection, démontrant ainsi un engagement clair à comprendre et à améliorer l'efficacité de leur sécurité. Cependant, 23 % n'évaluent ni ne mesurent leur couverture de détection, ce qui pourrait les rendre vulnérables aux failles de leurs défenses de détection qui passent inaperçues.

Une évaluation régulière est essentielle. Cela ne nécessite pas nécessairement d'adhérer à une norme sectorielle spécifique, mais plutôt d'appliquer une méthodologie cohérente qui identifie les lacunes et surveille les améliorations au fil du temps. Sans cela, les organisations risquent d'avoir des angles morts dans leurs défenses, que les acteurs malveillants exploiteront.

Les entreprises qui mesurent leur couverture de détection utilisent souvent des cadres et des informations établis. La matrice MITRE ATT&CK, un outil populaire utilisé par 74 % des répondants, aide les organisations à suivre les tactiques et techniques utilisées par les adversaires et à évaluer ainsi leur capacité à détecter ces comportements. En outre, 72 % des organisations s'appuient sur des rapports de renseignements sur les menaces, qui leur donnent un aperçu des menaces actuelles et émergentes. Les opérations de l'équipe rouge sont utilisées par 62 % des répondants, ce qui indique une approche proactive pour tester et valider leurs capacités de détection. Bien que ces méthodes soient efficaces, s'appuyer uniquement sur des outils de fournisseurs (35 %) ou des fournisseurs tiers (36 %) peut limiter la capacité d'une organisation à comprendre et à contrôler pleinement ses capacités de détection.

La fréquence à laquelle les organisations examinent les indicateurs de performance de leurs équipes de détection et de réponse varie considérablement. Près d'un tiers des répondants (29 %) effectuent des examens mensuels, ce qui suggère que de nombreuses organisations doivent peut-être surveiller leurs performances de plus près. Près de 9 % le font quotidiennement, ce qui est compréhensible si une organisation dispose des données et de la capacité de s'adapter aux problèmes. Environ 22 % des organisations effectuent des examens hebdomadaires, offrant une approche plus équilibrée de l'évaluation régulière des performances. Il est intéressant de noter que 14 % examinent les indicateurs tous les trimestres et 8 % tous les ans, ce qui est vraiment trop éloigné et limite probablement leur capacité à identifier et à s'adapter aux problèmes. Les acteurs de la menace n'attendent pas trois mois à un an pour ajuster leur technique, et les organisations ne devraient pas non plus le faire lorsqu'il s'agit d'évaluer leurs capacités.

En termes d'amélioration de la mesure des performances de détection et de réponse, aucune amélioration n'est clairement constatée, ce qui indique que les organisations ont pris conscience de la nécessité d'adopter des approches différentes pour résoudre divers problèmes. Les améliorations les plus fréquemment citées incluent les capacités de surveillance en temps réel (54 %) et les outils d'analyse et de reporting avancés (52 %), ce qui souligne le besoin de données plus immédiates et plus pertinentes sur les performances de sécurité. Une meilleure intégration avec d'autres outils de sécurité (50 %) et des formations et évaluations régulières des compétences (49 %) sont également considérées comme essentielles, ce qui indique que les organisations comprennent l'importance de disposer des bons outils et de s'assurer que leurs équipes peuvent les utiliser efficacement. Près de 48 % des répondants souhaitent des indicateurs plus complets, ce qui suggère que de nombreuses organisations estiment que leurs indicateurs actuels ne donnent pas une image complète de leurs capacités de détection et de réponse.

## Des faux positifs aux vrais problèmes

Les faux positifs constituent un défi majeur pour de nombreuses organisations qui tentent de détecter les cybermenaces : 64 % des répondants les ont identifiés comme un problème majeur (voir la figure 9). Environ 42 % des répondants ont rencontré fréquemment des faux positifs (représentant 41 à 80 % des cas), ce qui indique qu'il existe un important domaine d'amélioration dans les outils et les processus de détection. Lorsque les systèmes de détection génèrent un nombre élevé de faux positifs, cela peut entraîner une lassitude des alertes, où les équipes de sécurité deviennent insensibles aux alertes et risquent de négliger les véritables menaces. De plus, la gestion des faux positifs consomme un temps et des ressources précieux qui pourraient autrement être consacrés

64 % des répondants ont identifié les faux positifs comme un problème majeur.

Les entreprises doivent enquêter sur les menaces réelles et y répondre. Ce problème est exacerbé par le volume de données que les organisations doivent traiter, un défi souligné par 63 % des répondants. Cela augmente la probabilité de faux positifs et met encore plus à rude épreuve les opérations de sécurité.

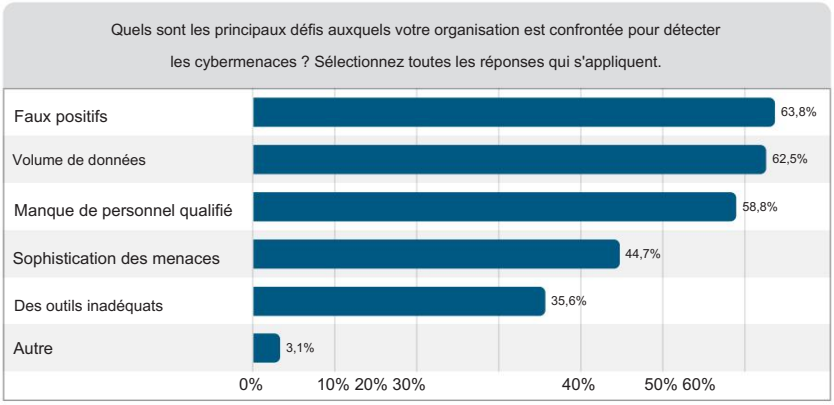


Figure 9. Défis liés à la détection des cybermenaces

La sophistication des menaces, citée par 45 % des répondants, et le manque de personnel qualifié, relevé par 59 %, ajoutent à la complexité du paysage de détection des menaces. Les attaques sophistiquées peuvent contourner les méthodes de détection traditionnelles, ce qui rend difficile pour les équipes de faire la différence entre les menaces légitimes et les anomalies bénignes. Cela explique probablement pourquoi la chasse manuelle aux menaces est le deuxième processus le plus utile pour détecter les menaces. En outre, le manque de personnel qualifié aggrave le problème, car les professionnels de la sécurité expérimentés sont plus capables d'affiner les systèmes de détection pour minimiser les faux positifs et identifier avec précision les menaces réelles. Avec seulement 10 % des répondants indiquant qu'ils rencontrent rarement des faux positifs, il est clair que les outils et techniques de détection ont encore un long chemin à parcourir pour détecter avec précision une menace réelle.

Pour relever ces défis, les entreprises doivent investir dans une meilleure formation de leur personnel et examiner de plus près les technologies et les outils dont elles disposent et qui génèrent des faux positifs. Une solution possible consiste à collecter des mesures sur les faux positifs générés par les outils commerciaux et à inciter ces fournisseurs à réduire les frais généraux que cela entraîne pour l'équipe de détection et de réponse.

En termes d'autres défis et obstacles, les contraintes budgétaires constituent l'obstacle le plus important auquel les organisations sont confrontées pour maintenir une capacité de détection et de réponse efficace, 47 % des répondants la classant comme leur principale préoccupation. Ce résultat met en évidence les pressions financières auxquelles de nombreuses organisations sont soumises, ce qui peut limiter leur capacité à investir dans des outils, des technologies et du personnel qualifié de pointe nécessaires pour améliorer leur posture de cybersécurité. L'acquisition et la rétention des talents sont considérées comme le deuxième obstacle (pondéré) le plus important, souligné par 21 % comme une préoccupation majeure, soulignant encore la difficulté de recruter et de conserver les professionnels qualifiés nécessaires pour gérer des opérations sophistiquées de détection et de réponse. Les limitations technologiques constituent le troisième obstacle (pondéré), 36 % des répondants la classant comme un problème important, reflétant les défis liés à l'évolution rapide des menaces et la nécessité de mises à jour et d'améliorations constantes des technologies de détection. La conformité réglementaire est classée au quatrième rang (pondéré), 13 % des répondants la considérant comme une préoccupation majeure. Bien que la conformité réglementaire soit la plus faible par rapport aux autres options, elle montre néanmoins le défi permanent auquel les organisations sont confrontées pour répondre aux diverses exigences légales et réglementaires, qui peuvent parfois détourner des ressources d'autres activités de sécurité critiques. Ces défis illustrent l'équilibre complexe que les organisations doivent réaliser lorsqu'elles tentent de défendre leur environnement, tout en répondant aux besoins de l'entreprise ou aux réglementations en même temps.

## L'avenir de la réponse aux menaces est automatisé

Les données de l'enquête indiquent une forte tendance à l'utilisation accrue de l'IA et de l'apprentissage automatique dans la détection et la réponse aux menaces, 67 % des répondants prévoyant d'étendre leur utilisation de ces technologies. Cela reflète une reconnaissance croissante du potentiel de l'IA pour améliorer les efforts de cybersécurité en automatisant et en améliorant la précision de la détection et de la réponse aux menaces. Seules 8 % des organisations ne prévoient pas d'accroître leur utilisation de l'IA et de l'apprentissage automatique, ce qui pourrait être dû à des contraintes budgétaires ou à des investissements existants dans d'autres technologies. Compte tenu des défis auxquels les répondants sont confrontés avec l'utilisation des technologies d'IA et d'apprentissage automatique, il peut être logique que 8 % d'entre eux souhaitent attendre et voir comment l'IA et l'apprentissage automatique se comportent dans le secteur. Les 25 % restants qui sont incertains ou indécis peuvent refléter une approche attentiste, car ces organisations évaluent l'efficacité de l'IA dans des scénarios réels avant d'engager des ressources supplémentaires.

Parmi ceux qui prévoient d'accroître l'utilisation de l'IA, la majorité (58 %) a l'intention de le faire de manière modérée, tandis que 29 % prévoient une adoption massive. Ce plan d'adoption modérée à massive indique que les organisations cherchent à trouver un équilibre entre l'exploitation des technologies avancées et le maintien du contrôle de leurs opérations de cybersécurité. Le grand intérêt pour les avancées telles que l'analyse comportementale (83 %) et la chasse automatisée aux menaces (64 %) souligne la volonté d'évoluer vers des méthodes de détection plus proactives et plus sophistiquées. L'analyse prédictive (60 %) et les moteurs de corrélation avancés (56 %) sont également à l'ordre du jour, ce qui suggère que les organisations cherchent à anticiper et à corréler les menaces plus efficacement, plutôt que de simplement y réagir. Nous garderons un œil sur ces technologies au fur et à mesure que cette enquête progressera au cours des prochaines années. Cependant, ces technologies ne sont pas une solution miracle pour détecter les menaces ; elles nécessitent un arrosage et une alimentation importants pour rester saines et utiles.

En termes d'automatisation des flux de travail de détection à réponse, les entreprises envisagent diverses stratégies. Les manuels améliorés (68 %) et l'intégration améliorée avec les outils SOAR (65 %) sont les principales priorités, reflétant le besoin de processus structurés et automatisés capables de rationaliser les réponses et de réduire le temps nécessaire pour atténuer les menaces. Près de 52 % des répondants prévoient de mettre en œuvre des scripts d'automatisation personnalisés, ce qui indique la nécessité de solutions plus manuelles, probablement pour des exigences très spécifiques ; 48 % prévoient des modèles d'apprentissage automatique avancés. Le projet d'achat de nouveaux outils avec des intégrations intégrées (38 %) montre en outre une tendance à la recherche de solutions complètes et prêtes à l'emploi qui peuvent simplifier les efforts de mise en œuvre et d'intégration, qui alimentent l'exigence initiale d'intégrations améliorées.

L'avenir de la détection et de la réponse semble encore un peu mitigé, avec une pointe de prudence pour de nombreux répondants. Il est clair que les répondants veulent jouer dans le monde de l'IA et du ML, même si les technologies doivent encore mûrir. Dans l'ensemble, les plus grandes avancées que les équipes de détection et de réponse réclament sont une plus grande automatisation avec les outils dont elles disposent ou qu'elles ont l'intention d'acheter. Être capable de réduire le nombre de tâches manuelles requises est une énorme victoire, il est donc logique que ce soit la force motrice pour l'avenir, du moins pour l'instant.

## Conclusion

Les résultats de la première année de l'enquête SANS Detection and Response dressent un tableau complet de la manière dont les organisations gèrent actuellement les complexités de la détection et de la réponse aux menaces. Les données soulignent systématiquement le rôle crucial de l'expertise humaine dans l'équilibre entre les technologies de pointe, comme en témoignent l'utilisation généralisée d'outils de détection et de réponse aux points d'extrémité (EDR), sur lesquels 82 % des répondants s'appuient, et l'adoption de systèmes de réponse semi-automatisés par 67 % des organisations. Malgré le rôle croissant de l'automatisation, il reste essentiel de disposer de personnel qualifié pour interpréter et agir sur ces technologies, comme le soulignent 59 % des organisations citant le manque de personnel qualifié comme un défi majeur. L'efficacité mitigée des outils basés sur l'IA et le ML souligne également la nécessité d'un développement et d'un réglage continus pour exploiter pleinement leur potentiel en matière de cybersécurité.

Les contraintes budgétaires et les limitations de ressources sont apparues comme des thèmes récurrents tout au long de l'enquête, près de la moitié des répondants citant le budget comme leur principal obstacle au maintien d'une capacité de détection et de réponse efficace. Ces défis financiers sont aggravés par la nécessité de se conformer aux exigences réglementaires et de suivre le rythme des avancées technologiques, qui sont essentielles mais nécessitent beaucoup de ressources. La nécessité de disposer de mesures plus complètes et d'une meilleure intégration des outils de sécurité souligne également l'évolution du paysage du secteur, où les organisations doivent continuellement adapter leurs stratégies pour faire face aux pressions internes et externes. Alors que les organisations se tournent vers l'avenir, elles reconnaissent clairement l'importance d'investir dans des capacités avancées de détection et de réponse, en mettant l'accent sur l'augmentation de l'utilisation de l'IA et du ML, l'amélioration de l'intégration avec les outils SOAR et l'amélioration des programmes de formation pour développer l'expertise interne. Il est clair que même si des technologies plus avancées se profilent à l'horizon et sont utilisées par les organisations, il existe un fort besoin de personnel qualifié derrière le clavier pour pouvoir suivre les acteurs de la menace au sein des réseaux des organisations.

## Parrainer

SANS souhaite remercier le sponsor de cet article :

RAPID7