SOPHOS

L'état de la cybersécurité en 2023 : l'impact des cyberattaques sur les entreprises

Résultats d'une étude indépendante menée entre janvier et février 2023 auprès de 3 000 responsables informatiques et responsables de la cybersécurité répartis dans 14 pays.

Un livre blanc Sophos. Avril 2023

Méthodologie

Afin de mieux appréhender l'impact réel de la cybersécurité sur les entreprises en 2023, Sophos a commandé une enquête indépendante auprès de 3 000 DSI et DSSI dans 14 pays. Tous les répondants appartenaient à des organisations comptant entre 100 et 5 000 employés. L'enquête a été menée par le cabinet Vanson Bourne en janvier et février 2023.

3 000
répondants

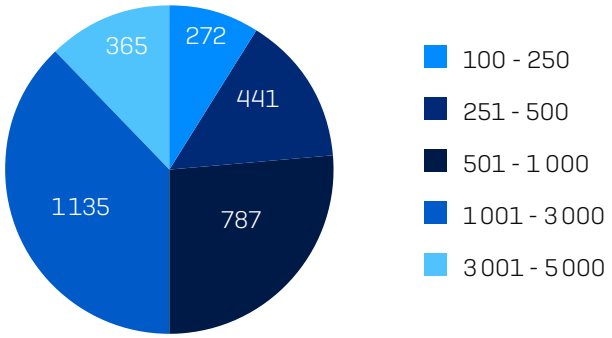
100 - 5 000
employés

14
pays

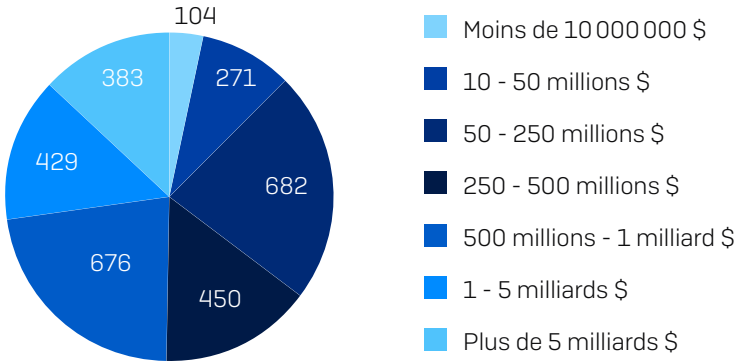
-10 M à +5 Mds $
revenus annuels

Janv.-févr. 23
période d'étude

Répondants selon la taille de l'entreprise (nombre d'employés)



Répondants selon la taille de l'entreprise (revenus annuels)



Répondants par pays

PAYS	NOMBRE DE RÉPONDANTS	PAYS	NOMBRE DE RÉPONDANTS
États-Unis	500	Royaume-Uni	200
Allemagne	300	Afrique du Sud	200
Inde	300	France	150
Japon	300	Espagne	150
Australie	200	Autriche	100
Brésil	200	Singapour	100
Italie	200	Suisse	100

Résumé

Situation : Les attaquants redoublent d'efforts, les défenseurs peinent à suivre le rythme

L'étude a montré que, dans les faits, il existe actuellement un système à deux vitesses, avec des attaquants et des défenseurs qui progressent à des rythmes différents. En recourant à l'automatisation, aux modèles de cybercriminalité « as-a-service », à l'usurpation d'identité et en s'adaptant, les attaquants accélèrent le rythme et peuvent désormais exécuter un large éventail d'attaques sophistiquées à grande échelle. Avec 94 % des entreprises ayant subi une cyberattaque sous une forme ou une autre en 2022, toutes les entreprises, quels que soient leur taille ou leurs revenus, doivent s'attendre à être ciblées en 2023.

Et les défenseurs, manquant d'expertise, croulant sous les alertes et passant trop de temps à répondre aux incidents, ne parviennent plus à suivre le rythme. Le travail de détection et de réponse aux menaces est difficile à opérationnaliser : 93 % des entreprises trouvent les opérations de sécurité essentielles difficiles à exécuter.

L'investigation des alertes de sécurité est un problème très répandu. En moyenne, moins de la moitié (48 %) des alertes sont analysées à la recherche de signes d'une activité malveillante, et la plupart des entreprises ont du mal à identifier (71 %) et à prioriser (71 %) les alertes/événements qui doivent être investiguées. Pour les alertes qui le nécessitent, le processus complet de détection, d'investigation et de réponse prend en moyenne 9 heures pour les entreprises de 100 à 3 000 employés, et 15 heures pour celles de 3 001 à 5 000 employés.

Sur le plan opérationnel, les défenseurs manquent de confiance dans leurs processus, estimant que les mauvaises configurations des outils de sécurité sont le principal risque de sécurité en 2023. Plus de la moitié (52 %) des professionnels de l'IT rapportent que les cybermenaces sont désormais trop avancées pour que leur entreprise puisse y faire face seule, ce chiffre atteignant 64 % chez les petites entreprises (100 à 250 employés).

Impact sur les entreprises : La situation a des répercussions sur les ressources financières, opérationnelles et humaines

Ce système à deux vitesses a un impact considérable sur l'ensemble de l'entreprise. Les conséquences financières directes d'un cyber incident sont colossales et déjà bien connues. Pour une petite ou moyenne entreprise par exemple, le coût moyen de remédiation suite à une attaque de ransomware s'élève à 1,4 million de dollars (env. 1,23 million d'euros).[1]. Et ces frais de nettoyage ne constituent qu'une partie du coût global.

La capacité d'exécution des projets du service informatique est réduite, avec 55 % des répondants déclarant que la gestion des cybermenaces met un frein à d'autres projets sur lesquels l'équipe informatique travaille. Le caractère urgent et imprévisible de la cybersécurité entrave également les efforts stratégiques de l'entreprise : 64 % souhaitent que l'équipe IT consacre plus de temps aux questions stratégiques et moins de temps à la gestion des menaces.

Le temps dédié à la détection, à l'investigation et à la remédiation des alertes de sécurité a également un impact financier considérable en matière de coût de ressources.

Sans compter que cette situation génère aussi beaucoup de stress pour les employés. En moyenne, 57 % des professionnels de l'informatique s'inquiètent du risque de cyberattaque sur leur entreprise, parfois au point de ne pas en dormir la nuit, et ce taux atteint 65 % dans les grandes entreprises (entre 3 001 et 5 000 employés). Compte tenu des coûts élevés de recrutement, de formation et de rétention du personnel dans ce secteur, ces répercussions entraînent des difficultés et des coûts supplémentaires pour l'entreprise.

1 L'état des ransomwares 2022, Sophos

Recommandation : accélérer la force d'inertie des défenseurs pour devancer les attaquants

Pour donner aux défenseurs les moyens de dépasser les attaquants dans cette course à la cybersécurité, il faut une approche simple mais globale. Premièrement, les entreprises doivent mettre en œuvre un processus de réponse aux incidents réactif et évolutif. Cela suppose de réduire la surface d'attaque et le volume d'alertes à investiguer d'une part, et d'optimiser le temps de réponse en faisant appel à des services spécialisés d'autre part.

Ensuite, elles doivent implémenter des défenses qui s'adaptent automatiquement à la situation, afin de ralentir les adversaires et de gagner du temps pour mieux répondre.

Enfin, elles doivent mettre en place un cycle vertueux qui allie la technologie et l'expertise humaine à des défenses renforcées, pour intensifier la rapidité d'action, l'efficacité et l'impact. Toutes ces actions combinées vont accélérer la force d'inertie des défenseurs et leur permettre de prendre une longueur d'avance.

La réussite de cette approche, néanmoins, ne peut se faire sans le recours à des spécialistes externes. La bonne nouvelle est que les entreprises ont déjà adopté une approche hybride pour assurer leur cybersécurité : 94 % font appel à des experts externes dans une certaine mesure pour les aider dans leurs opérations. Et face à des attaquants qui redoublent sans cesse d'efforts, pouvoir compter sur une équipe d'experts dédiée est devenu indispensable.

Principales découvertes

94 % des entreprises ont subi une cyberattaque sous une forme ou une autre en 2022

L'exfiltration de données est la principale préoccupation en matière de sécurité pour 2023

93 % trouvent difficile l'exécution de tâches essentielles en matière d'opérations de sécurité

48 % des alertes de sécurité sont investiguées

15 heures est la durée moyenne nécessaire pour détecter, investiguer et répondre à une alerte dans les entreprises de 3 001 à 5 000 employés

La mauvaise configuration des outils de sécurité est perçue comme le principal risque de sécurité en 2023

52 % des répondants estiment que les cybermenaces sont désormais trop avancées pour que leur entreprise puisse y faire face seule

55 % déclarent que la gestion des cybermenaces a une incidence négative sur les autres projets informatiques de l'équipe IT

64 % aimeraient que l'équipe IT consacre plus de temps aux questions stratégiques et moins de temps à la gestion des menaces

57 % des professionnels de l'informatique perdent le sommeil à l'idée que leur entreprise puisse être victime d'une cyberattaque

Les cybermenaces en 2023 : la réalité sur le terrain

Principales préoccupations pour 2023

99 % des professionnels de l'IT sont préoccupés par les cybermenaces qui affecteront leur entreprise en 2023. L'exfiltration de données (vol par un attaquant externe) arrive en tête de la liste des menaces que les professionnels de l'IT craignent le plus, suivie de près par le phishing (spearphishing compris). Les ransomwares viennent compléter ce podium.

Il est important de rappeler que ces trois menaces travaillent souvent de pair : un email de phishing sera à l'origine de l'attaque, qui aboutira à une exfiltration de données, puis se conclura par un ransomware.

CYBERMENACE	POURCENTAGE DE RÉPONDANTS DÉCLARANT QU'IL S'AGIT D'UNE PRÉOCCUPATION MAJEURE
Exfiltration de données (vol par un attaquant externe)	41 %
Phishing (y compris spearphishing)	40 %
Ransomware	35 %
Cyber extorsion	33 %
Attaques par déni de service (DDoS)	32 %
Compromission de la messagerie professionnelle (BEC)	31 %
Adversaires actifs (attaquants pilotant manuellement une attaque)	30 %
Malwares mobiles	30 %
Cryptomineurs	22 %
Wipers	16 %
Autres	0 %
Je ne crains pas que des cybermenaces affectent mon entreprise en 2023	1 %
Ne sait pas	0 %

Dans la perspective de 2023, quelles sont les cybermenaces dont vous craignez le plus qu'elles affectent votre entreprise ? (n=3 000)

Les attaquants exécutent désormais une myriade d'attaques à grande échelle

Les préoccupations des professionnels de l'IT sont légitimes et correspondent bien à la réalité des faits sur le terrain : 94 % des entreprises ont subi au moins une cyberattaque en 2022. Si le ransomware est l'attaque la plus signalée, les attaquants exécutent un large éventail d'attaques à grande échelle. L'ampleur et la diversité de ces attaques constituent un défi considérable et grandissant pour les défenseurs.

Ces chiffres s'expliquent par la professionnalisation croissante de l'économie cybercriminelle, et notamment le recours au modèle « as-a-service » et ses déclinaisons : l'« access-as-a-service », le « phishing-as-a-service » ou encore le « scamming-as-a-service ». Cette évolution de la cybercriminalité a baissé toutes sortes de barrières, facilitant l'entrée d'aspirants cybercriminels. [Pour plus d'informations, consultez le Rapport Sophos 2023 sur les menaces.]

Principales cyberattaques autres que des ransomwares et pourcentage des entreprises les ayant signalées

27 %	**27 %**	**26 %**
Emails malveillants	Phishing (y compris spearphishing)	Exfiltration de données (par l'attaquant)
24 %	**24 %**	**21 %**
Cyber extorsion	Business Email Compromise (BEC)	Malwares mobiles
18 %	**24 %**	**14 %**
Cryptomineurs	Déni de service (DDoS)	Wipers

Les attaques d'adversaires actifs sont désormais monnaie courante

23 %
des entreprises ont subi une attaque impliquant un adversaire actif en 2022

30 %
affirment que les adversaires actifs sont une préoccupation majeure pour 2023

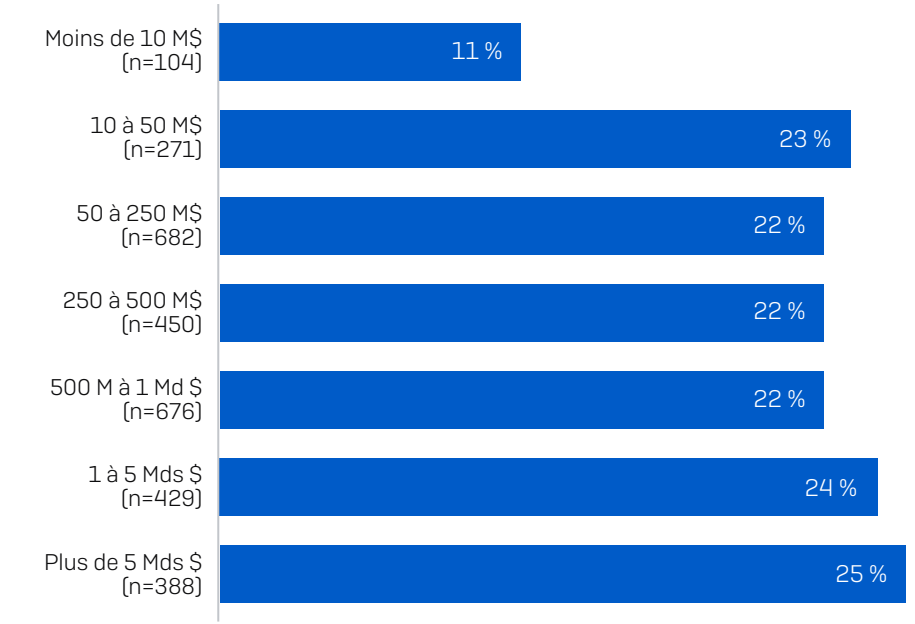
Les adversaires actifs sont des attaquants qui adaptent leurs techniques, tactiques et procédures sur le vif, agissant en temps réel sur leur clavier en réponse aux actions des défenseurs et de leurs outils de sécurité, mais aussi pour échapper à la détection. Ces attaques, qui se traduisent souvent par des incidents dévastateurs comme des ransomwares ou des violations de données, sont parmi les plus difficiles à bloquer.

23 % des répondants ont rapporté que leur entreprise avait subi une attaque impliquant un adversaire actif en 2022. Le taux d'attaque était identique quelle que soit la taille de l'entreprise, ne variant que de deux points de pourcentage entre les différents segments de taille d'entreprises.

Fait intéressant, le taux d'attaques par adversaires actifs est de seulement 11 % pour les entreprises dotées de revenus inférieurs à 10 millions de dollars, ce qui laisse supposer que les attaquants se concentrent délibérément sur des cibles plus lucratives. Être capable de détecter un adversaire actif demande un très haut niveau de compétences, c'est pourquoi il est probable que le taux d'incidents soit en réalité plus élevé.

Témoignant du potentiel dévastateur de ces attaques, 30 % des personnes interrogées ont déclaré que les adversaires actifs constituaient l'une de leurs principales préoccupations en matière de cybermenaces pour 2023.

Attaque par adversaires actifs selon le revenu

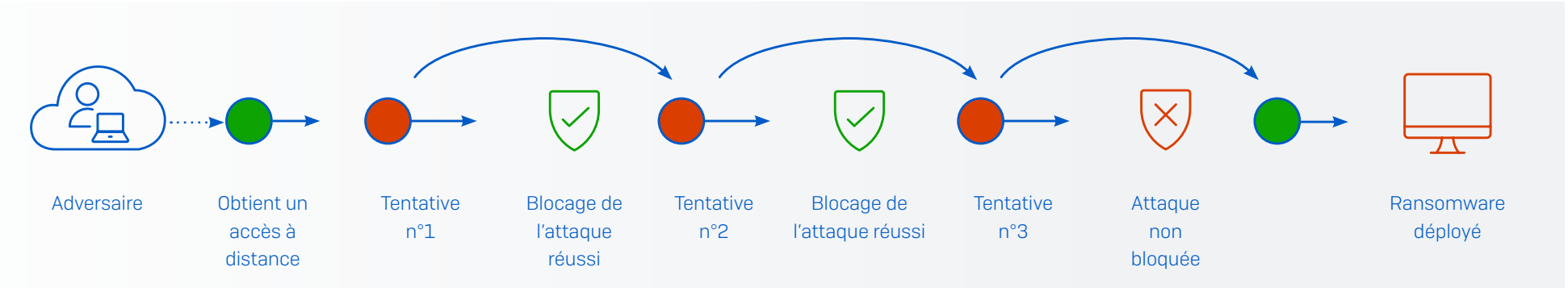


Avez-vous été victime d'une ou plusieurs cyberattaques au cours des douze derniers mois? Oui - Adversaires actifs (attaquants pilotant manuellement une attaque)

Comprendre les adversaires actifs

Pour mieux appréhender le défi auquel sont confrontés les défenseurs, il est essentiel de comprendre qu'il ne suffit pas de bloquer les adversaires actifs pour les neutraliser. Ces acteurs malveillants, persistants et chevronnés, déploient de multiples techniques, tactiques et procédures (TTP) pour atteindre leurs objectifs, notamment :

- Exploiter les failles de sécurité pour pénétrer le réseau de l'entreprise et se déplacer latéralement une fois à l'intérieur, à l'aide d'identifiants volés, de vulnérabilités non corrigées et d'erreurs de configuration des outils de sécurité ;
- Abuser les outils IT légitimes (utilisés par les défenseurs) afin d'éviter de déclencher des détections ;
- Modifier leurs attaques en temps réel en réponse aux contrôles de sécurité, en continuant d'utiliser de nouvelles techniques jusqu'à ce qu'ils trouvent le moyen d'atteindre leurs objectifs.



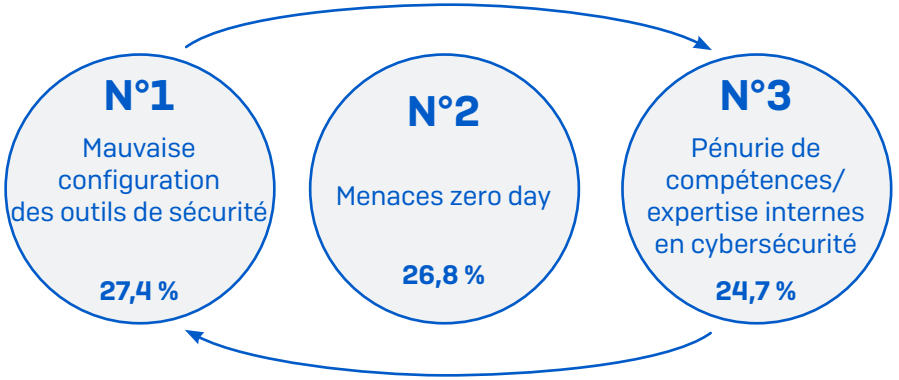
La cybersécurité en 2023 : l'état des défenseurs

Principales préoccupations en matière de cyber risques

Une mauvaise configuration des paramètres de sécurité (par ex. sur un poste de travail ou un pare-feu) est le risque de sécurité perçu le plus largement cité, avec 27,4 % des répondants l'incluant dans leur top 3 des cyber risques. Ce classement illustre les défis auxquels sont confrontées les équipes informatiques pour s'assurer que les contrôles de sécurité restent bien configurés et déployés à tout moment, ainsi que la rapidité avec laquelle les attaquants sont prêts à exploiter n'importe quelle faille dans les défenses d'une entreprise.

Les attaques de type zero day, c'est-à-dire qui exploitent une vulnérabilité ou une faille logicielle inconnue jusqu'alors, figurent également parmi les trois principaux risques de sécurité, arrivant en deuxième position (26,8 %). En troisième position, on trouve la pénurie de compétences/expertise internes en cybersécurité, citée par 25 % des personnes interrogées.

En fait, il existe un lien direct entre pénurie de compétences et mauvaise configuration des outils de sécurité ; si vous manquez de temps, de connaissances et d'expérience pour bien configurer vos contrôles, vous créerez immanquablement des failles dans vos défenses.



RISQUE DE CYBERSÉCURITÉ	POURCENTAGE DE CLASSEMENT DANS LE TOP 3 DES PRÉOCCUPATIONS
Mauvaise configuration des contrôles de sécurité (par ex. poste ou pare-feu)	27 %
Menaces zero day (une menace qui exploite une technique d'attaque inédite).	27 %
Pénurie de compétences et d'expertise internes en cybersécurité	25 %
Vol de données et d'identifiants d'accès	24 %
Appareils non protégés (y compris les appareils inconnus)	24 %
Manque d'outils de sécurité	23 %
Vulnérabilités non corrigées	22 %
Accès activé pour les utilisateurs distants	20 %
Réseau Wi-Fi non sécurisé	20 %
Utilisateurs internes (accidentel)	18 %
Partenaires/Supply Chain	18 %
Outils d'accès à distance	18 %
Utilisateurs internes (intentionnel)	17 %
Appareils connectés (IoT)	17 %
Autres	0 %
Aucun de ces éléments ne représente un risque pour la cybersécurité de mon entreprise	0 %
Ne sait pas	0 %

Quels sont, selon vous, les trois principaux risques de cybersécurité pour votre entreprise ? Combinaison de réponses classées en première, deuxième et troisième position (n=3 000)

Différentes approches en matière d'investigation des alertes

Les entreprises vérifient **48 % de leurs alertes de sécurité** pour déterminer s'il s'agit d'une activité malveillante.

L'un des défis pour les défenseurs consiste à identifier quelles alertes investiguer et comment utiliser au mieux leurs ressources limitées.

En moyenne, un peu moins de la moitié (48 %) de toutes les alertes de sécurité font l'objet d'une investigation pour identifier les signes d'une activité malveillante. Ce pourcentage atteint 54 % dans les plus grandes entreprises (3 001 et 5 000 employés). Toutefois, les approches diffèrent grandement : 16 % des entreprises vérifient plus des trois quarts de leurs alertes (y compris 5 % qui déclarent investiguer toutes les alertes), tandis que 18 % en analysent un quart ou moins.

Si l'on regarde le domaine d'activité, le secteur public est celui qui vérifie le moins d'alertes (avec un pourcentage de seulement 39 %) (n=89), tandis que le secteur de l'énergie, du pétrole/gaz et des services d'utilité publique affiche le pourcentage le plus élevé (vérifiant 55 % des alertes) (n=69).

Coût du travail de détection, d'investigation et de réponse

Le temps moyen pour détecter, investiguer et répondre à une alerte est de 9 heures pour les entreprises de 100 à 3 000 employés, et de 15 heures pour celles de 3 001 à 5 000 employés. Cette différence s'explique probablement par la complexité accrue des environnements opérationnels des grandes entreprises.

L'enquête a révélé des variations considérables selon le domaine d'activité. Les entreprises du secteur manufacturier (15 heures) et du secteur de l'énergie, du pétrole/gaz et des services d'utilité publique (18 heures) mettent plus du double de temps que celui du secteur de l'informatique, technologie et télécoms (6,75 heures).

Il est important de noter que la majorité des alertes n'atteindront pas le stade de la réponse. La plupart des attaques seront bloquées de manière proactive par les outils de sécurité, et seulement un sous-ensemble d'alertes sera trié et soumis à investigation. De même, les actions de réponses varieront considérablement en fonction de la nature de l'événement nécessitant une remédiation, allant de la suppression d'un email de phishing dans la boite de réception d'un utilisateur à la reconstitution intégrale d'un parc de serveurs.

Durée moyenne pour détecter, investiguer et répondre à une alerte

ACTIVITÉ	100 - 3 000 EMPLOYÉS (n=2 460)	3 001 - 5 000 EMPLOYÉS (n=350)	INFORMATIQUE, TECHNOLOGIE ET TÉLÉCOMS (n=98)	MANUFACTURE ET PRODUCTION (n=331)	ÉNERGIE, PÉTROLE/ GAZ, SERVICES D'UTILITÉ PUBLIQUE (n=66)
Détection	3 heures	3 heures	1,5 heure	3 heures	6 heures
Investigation	3 heures	6 heures	2,25 heures	6 heures	6 heures
Response	3 heures	6 heures	3 heures	6 heures	6 heures
Total	**9 heures**	**15 heures**	**6,75 heures**	**15 heures**	**18 heures**

Combien de temps faut-il à votre entreprise pour détecter, investiguer et, le cas échéant, remédier à un incident potentiel ? (n=2 812 répondants qui investiguent les alertes en interne)

Les entreprises manquent de compétences essentielles en matière d'opérations de sécurité

Nous l'avons déjà mentionné, pour les professionnels de l'IT, la pénurie de compétences/expertise en interne constitue l'un des principaux risques en matière de sécurité pour 2023. Selon notre enquête, la majorité des entreprises rencontrent des difficultés pour exécuter les tâches essentielles des opérations de sécurité quotidiennes, avec 93 % d'entre elles qualifiant au moins l'une des activités suivantes de « difficile » :

- Séparer le signal du bruit (tâche difficile pour 71 %)
- Prioriser les signaux/alertes à investiguer (tâche difficile pour 71 %)
- Obtenir suffisamment d'informations pour déterminer si un signal est malveillant ou bénin (tâche difficile pour 71 %)
- Remédier aux alertes ou incidents malveillants dans un délai imparti (tâche difficile pour 71 %)
- Identifier la cause première de l'incident (tâche difficile pour 75 %)
- Tenir un registre précis des investigations (tâche difficile pour 68 %)

Identifier la cause première de l'incident est le problème le plus répandu, avec 75 % des répondants qualifiant cette tâche de véritable défi.

Les entreprises aux revenus annuels les plus faibles (moins de 10 millions de dollars) sont les plus susceptibles de trouver les tâches liées aux opérations de sécurité difficiles, suivies par celles dont les revenus sont les plus élevés (5 milliards de dollars et plus). Les deux extrémités du spectre seront confrontées à des obstacles différents, la complexité en termes d'organisation et de systèmes jouant probablement un rôle plus important dans les grandes entreprises.

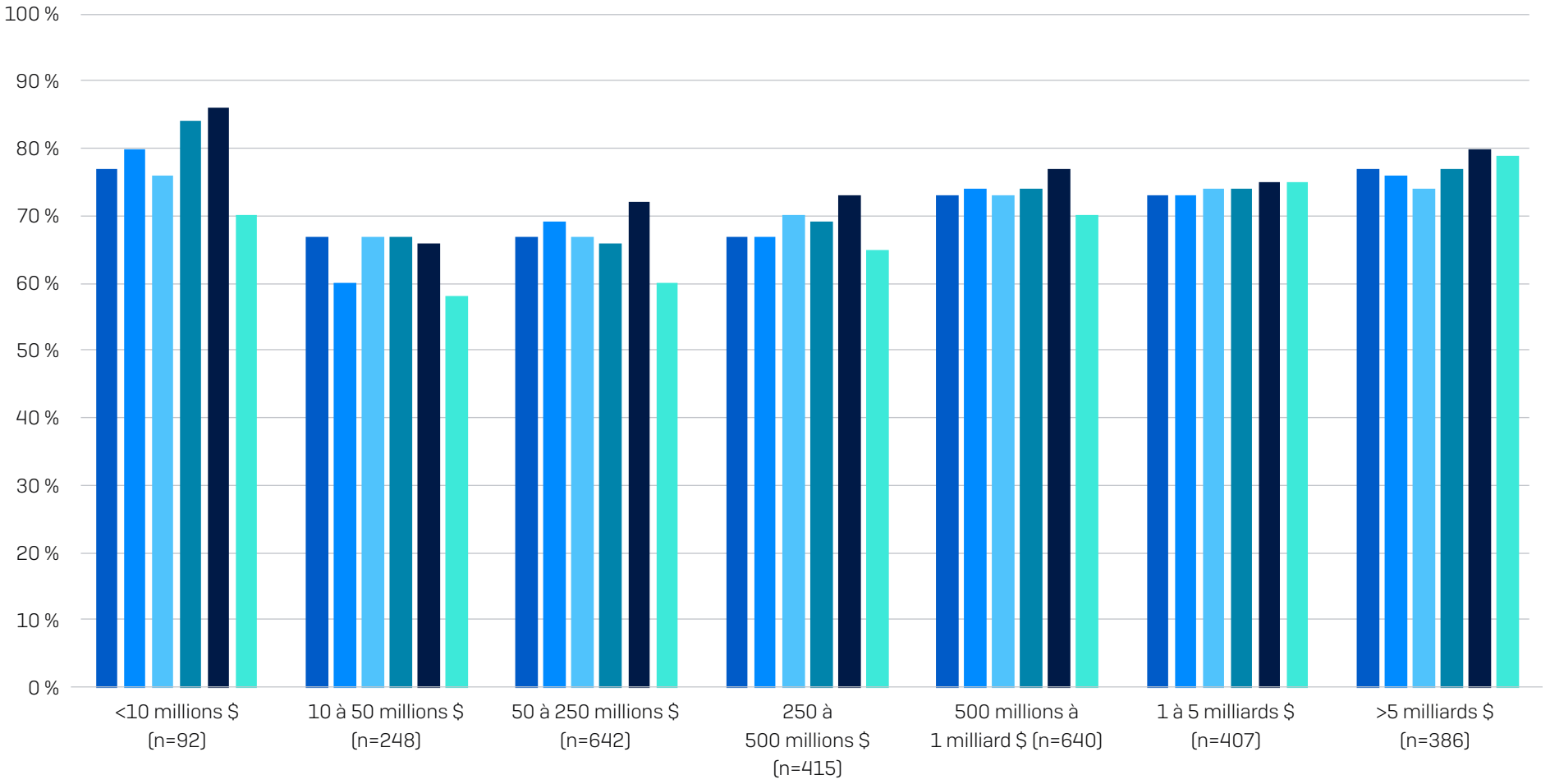
Cette pénurie de compétences crée un effet domino : l'investigation des alertes prend plus de temps, ce qui, en retour, réduit les moyens de l'équipe IT et accroît l'exposition aux risques.

93 %
trouvent les opérations de sécurité difficiles

75 %
ont du mal à identifier la cause racine de l'incident

71 %
ont du mal à identifier les alertes à investiguer

Entreprises qui trouvent les tâches liées aux opérations de sécurité « difficiles », par revenus



Répondants dont l'entreprise trouve les tâches liées aux opérations de sécurité « très difficiles » ou « assez difficiles » lorsqu'elle analyse les alertes suspectes (n=2 812 répondants qui analysent les alertes de sécurité en interne)

- Identifier le signal du bruit, c'est-à-dire comprendre quels signaux/alertes doivent être examinés
- Prioriser les signaux/alertes à investiguer
- Obtenir suffisamment d'informations pour déterminer si un signal est malveillant ou bénin
- Identifier la cause racine de l'incident, c'est-à-dire la manière dont l'attaquant s'est introduit dans l'entreprise
- Remédier aux alertes ou incidents malveillants en temps utile
- Conserver des registres précis de l'investigation

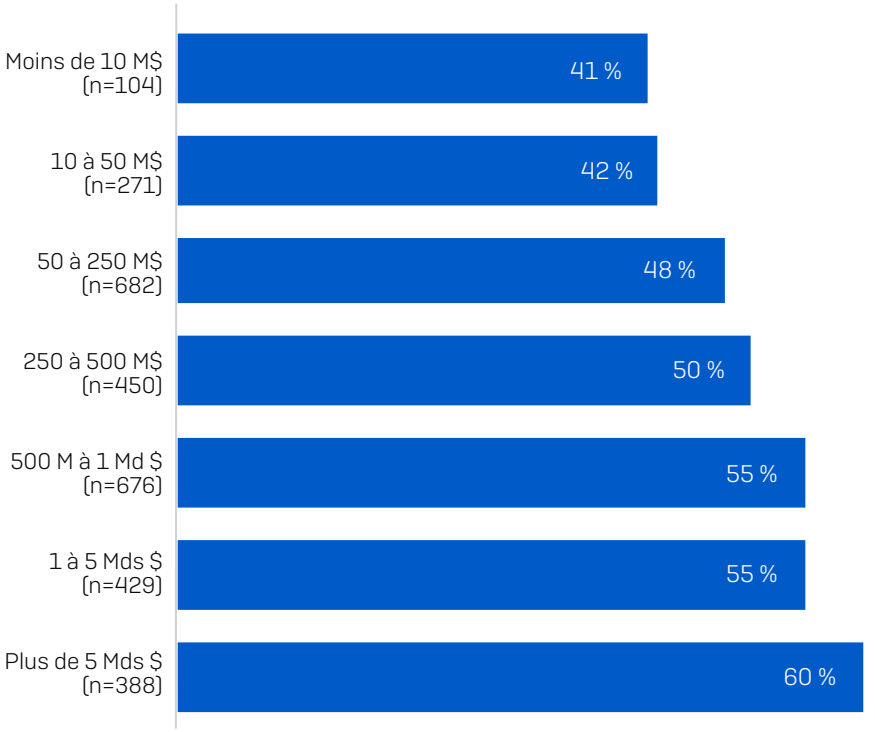
Les attaquants ont gagné du terrain sur les défenseurs

52 %
des répondants estiment que les cybermenaces sont désormais trop avancées pour que leur entreprise puisse y faire face seule

Plus de la moitié (52 %) des professionnels de l'IT rapportent que les cybermenaces sont désormais trop avancées pour que leur entreprise puisse y faire face seule, ce chiffre atteignant 64 % chez les petites entreprises (100 à 250 employés).

Plus le chiffre d'affaires augmente, plus l'équipe IT en interne semble avoir du mal à suivre le rythme. Ce constat s'explique probablement par un environnement interne plus complexe dans les entreprises aux revenus élevés et une plus grande propension à faire appel à des services de sécurité spécialisés. Cela peut également refléter une meilleure compréhension de l'environnement et des défis à relever pour se défendre contre les menaces avancées.

Les cybermenaces sont désormais trop avancées pour que mon entreprise puisse y faire face seule



Dans quelle mesure êtes-vous d'accord ou pas avec l'énoncé suivant : les cybermenaces sont trop avancées pour que notre entreprise puisse y faire face seule ? Tout à fait d'accord, plutôt d'accord (chiffres de base dans le graphique)

L'impact sur les entreprises

Répercussions sur le service IT

64 %
souhaitent que l'équipe IT consacre plus de temps aux questions stratégiques et moins de temps à la gestion des menaces

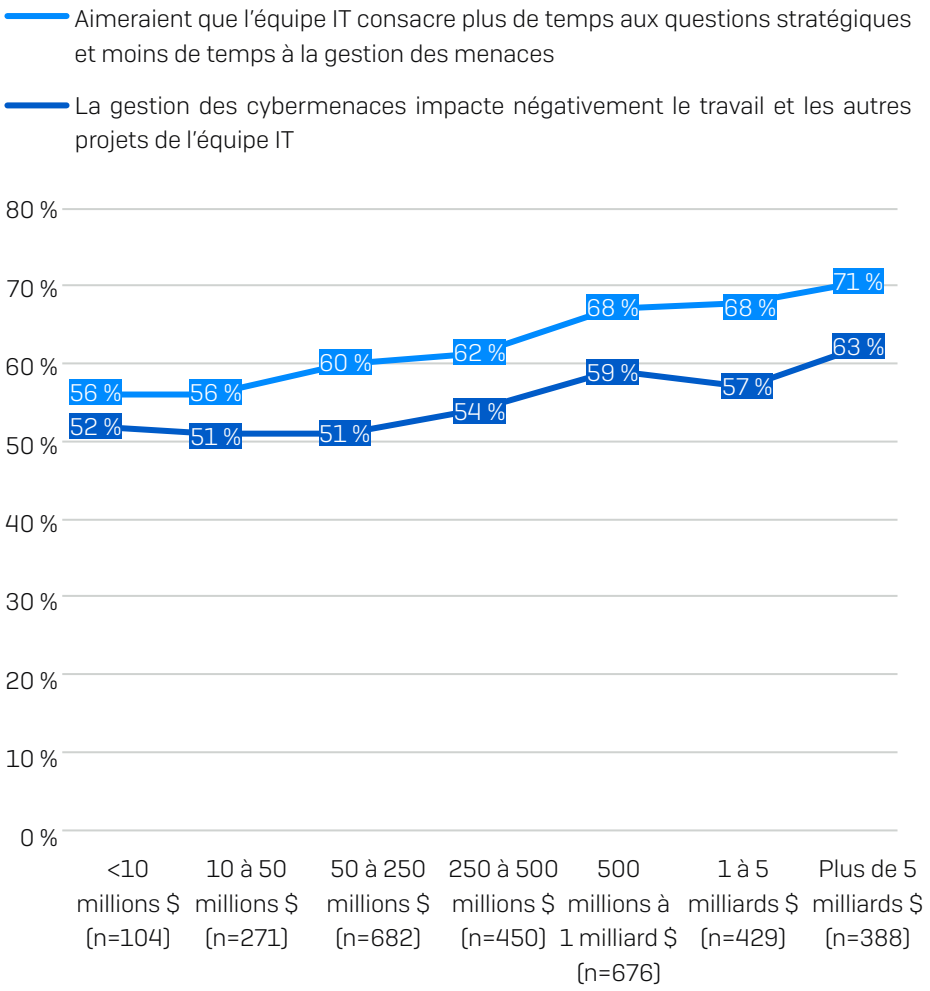
55 %
déclarent que la gestion des cybermenaces a une incidence négative sur les autres projets informatiques de l'équipe IT

Pour 60 % des entreprises, la cybersécurité et le service informatique dans son ensemble sont étroitement liés : 52 % ont une équipe de cybersécurité au sein de leur équipe IT, tandis que 8 % ont une équipe IT qui gère aussi la cybersécurité. Les 40 % restants ont des équipes distinctes de cybersécurité et d'informatique. Le temps et les efforts requis pour assurer la cybersécurité ont des répercussions considérables sur l'organisation du service informatique.

Plus de la moitié (55 %) des répondants rapporte que le traitement des cybermenaces a une incidence négative sur le travail et les autres projets de l'équipe informatique, cet impact étant le plus fort dans les entreprises aux revenus les plus élevés.

Le caractère urgent et imprévisible de la cybersécurité entrave également les efforts stratégiques de l'entreprise : En moyenne, 64 % souhaitent que l'équipe IT consacre plus de temps aux questions stratégiques et moins de temps à la gestion des menaces. Encore une fois, plus le chiffre d'affaires augmente, plus l'impact se fait ressentir sur les capacités du service IT à bien faire son travail.

La cybersécurité a un impact négatif sur l'exécution des projets informatiques



Dans quelle mesure êtes-vous d'accord ou pas avec l'énoncé suivant : La gestion des incidents de cybersécurité a eu une incidence négative sur le travail et les autres projets de l'équipe informatique. J'aimerais que l'équipe IT consacre plus de temps aux questions stratégiques et moins de temps à la gestion des menaces (chiffres de base dans le graphique).

Impact financier

L'environnement difficile de la cybersécurité a de multiples incidences financières sur l'entreprise. En cas de cyber incident majeur, la facture peut être faramineuse. Comme l'indique le Rapport Sophos sur l'état des ransomwares en 2022, la facture globale de remédiation d'une attaque de ransomware s'élève en moyenne à 1,4 million de dollars (env. 1,23 million d'euros).

Mais les répercussions financières des cyberattaques ne se limitent pas aux coûts de nettoyage. Avec un salaire moyen autour de 50 000 €/an [2]pour un spécialiste de la cybersécurité en France, le coût en termes de ressources horaires pour chaque alerte de sécurité investiguée est très élevé. Et même si les salaires varient selon les pays, l'impact financier d'un long processus d'investigation des incidents reste considérable.

2 Basé sur le salaire moyen d'un expert en sécurité informatique en avril 2023, https://fr.indeed.com/career/sp%C3%A9cialiste-en-s%C3%A9curit%C3%A9-informatique/salaries

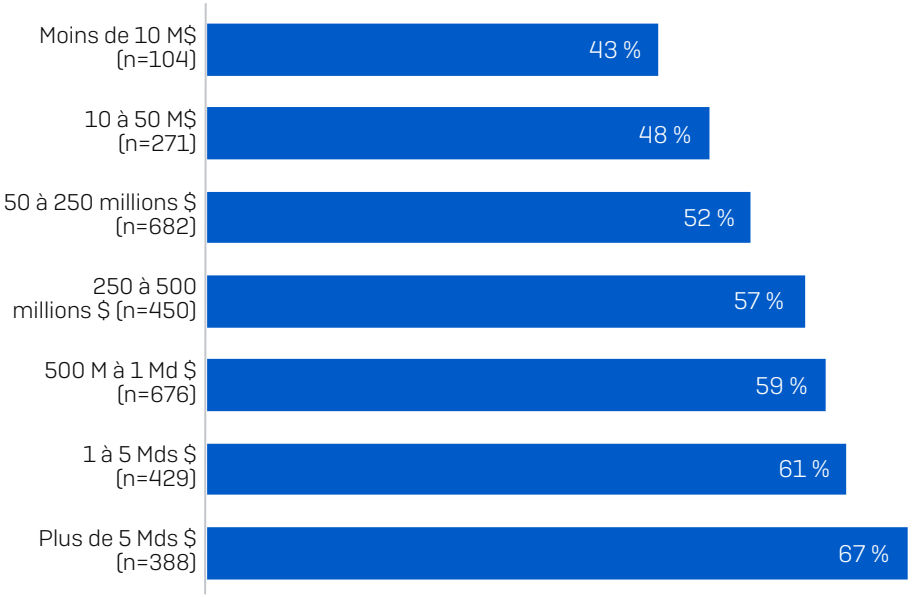
Impact sur l'équipe

57 % des répondants déclarent perdre parfois le sommeil à l'idée que leur entreprise puisse être victime d'une cyberattaque. Compte tenu des coûts élevés de recrutement et de rétention du personnel dans ce secteur, cette situation est une vraie source de préoccupation tant sur le plan du bien-être des employés que sur le plan financier. Cela témoigne également du manque de confiance des défenseurs dans leurs outils de sécurité.

Le burn-out est un problème majeur du monde de la cybersécurité. Trop d'alertes à gérer et trop de travail à accomplir, génère un stress considérable pour les employés. Les équipes surchargées sont plus susceptibles de rater des signaux d'alerte importants, ce qui rajoute encore plus de pression. Face à cette tension, les gens finissent par craquer.

La propension des responsables IT à s'inquiéter des risques de cybersécurité et à en perdre le sommeil grandit à mesure que les revenus de l'entreprise augmentent, allant de 43 % dans les entreprises de 10 millions de dollars de revenus à 67 % pour celles aux revenus supérieurs ou égaux à 5 milliards de dollars.

Pourcentage de répondants affirmant que la crainte d'une cyberattaque les empêche de dormir



Dans quelle mesure êtes-vous d'accord ou pas avec l'énoncé suivant : La crainte que mon organisation soit touchée par une cyberattaque m'empêche parfois de dormir (chiffres de base dans le graphique).

Recommandations

Remédier à cette situation requiert une approche simple en trois temps : mettre en place un processus de réponse aux incidents plus modulable qui accélère le temps d'action ; exploiter des défenses adaptatives pour ralentir les attaquants ; et créer un cercle vertueux qui améliore la protection et réduit les coûts.

L'analogie avec une « levée de boucliers » s'applique bien ici. Pour pouvoir stopper les attaques avancées et persistantes, les entreprises doivent optimiser l'efficacité de leurs défenses (« boucliers »), notamment les technologies sensibles au contexte qui peuvent élever le niveau de protection en fonction de la situation. Et surtout, elles devront mettre à profit ce temps que leurs défenses leur permettent de gagner pour recourir à l'expertise humaine et s'attaquer à la cause racine.

Des boucliers solides sont essentiels

La qualité de vos technologies de cybersécurité est primordiale. De bons outils doivent :

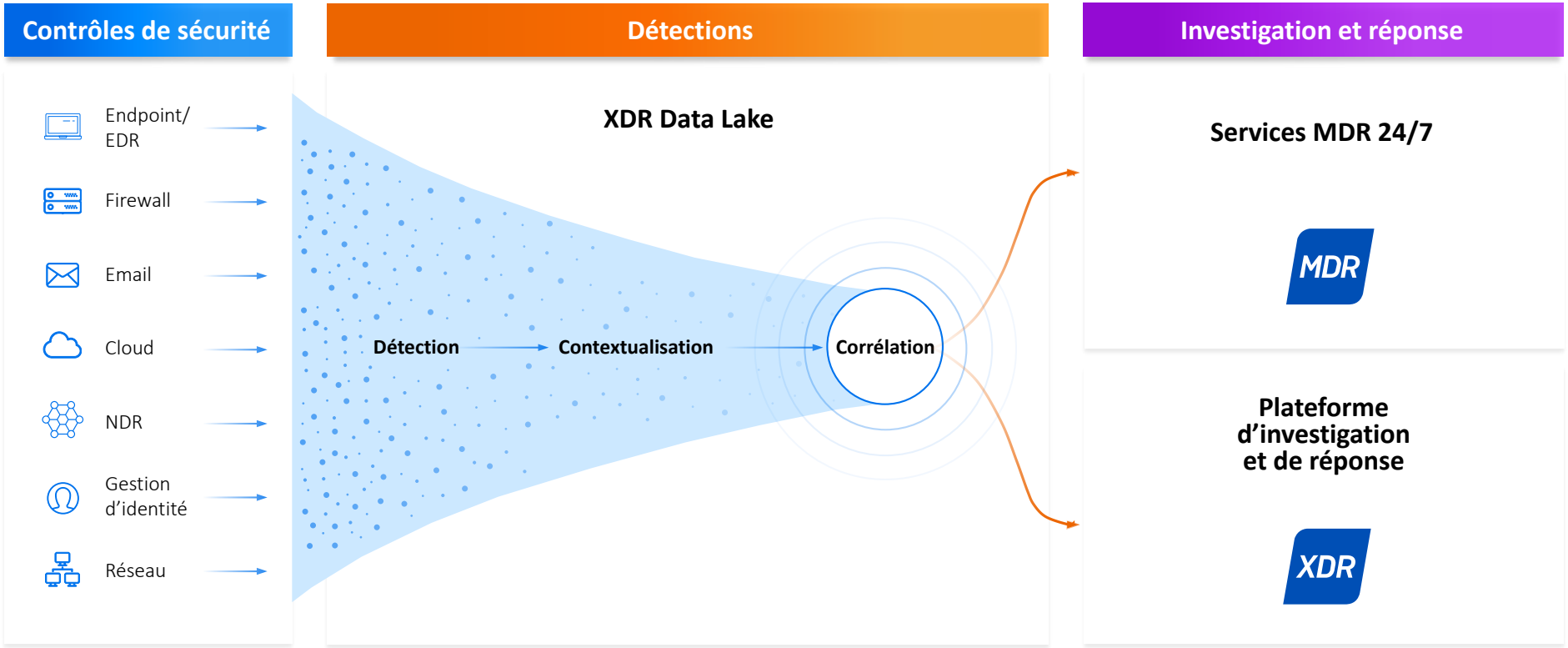
- **Optimiser la prévention**, en détectant et en bloquant automatiquement le plus grand nombre de menaces possible aux prémices de la chaîne d'attaque. Ce faisant, vous réduisez les risques pour votre entreprise tout en allégeant la tâche de vos défenseurs qui se retrouvent avec moins d'incidents à gérer.
- **Réduire l'exposition**, en faisant en sorte que vos investissements de sécurité soient déployés correctement et de manière optimale, et en évitant les erreurs de configuration.
- **Interrompre les attaquants**. Les technologies capables de détecter et d'interrompre automatiquement les activités adverses frustrent les attaquants tout en donnant aux défenseurs le temps de neutraliser l'incident.

S'attaquer à la cause racine grâce à l'expertise humaine et la technologie

Les boucliers permettent aux défenseurs de gagner un temps précieux qui leur permet d'investiguer et de répondre aux attaques. Cependant, ils ne garantissent pas une prévention à 100 %, c'est pourquoi identifier la cause racine et y remédier à temps et de manière parfaitement éclairée est essentiel.

Comme le montre l'enquête, les attaquants ne suivent pas une seule route. Pouvoir exploiter la télémétrie de tout l'environnement, en utilisant les contrôles de sécurité déjà mis en place par l'entreprise, permet aux défenseurs d'identifier les menaces et d'y répondre plus rapidement, tout en augmentant le retour sur les investissements existants.

Bien souvent, trouver une activité malveillante parmi les alertes bénignes s'apparente à rechercher une aiguille dans une botte de foin. C'est pourquoi le fait de gérer les signaux à partir d'une plateforme XDR (Extended Detection and Response), qui ajoute des informations contextuelles et corrèle les alertes connexes, permet aux défenseurs internes de se focaliser plus rapidement sur les tâches importantes. Ce travail de détection, d'investigation et de réponse peut être réalisé soit par l'équipe interne depuis une plateforme XDR, soit en externe, en faisant appel à un service spécialisé MDR (Managed Detection and Response).



Accélérer la force d'inertie du défenseur

Lorsqu'un volant d'inertie commence à tourner à grande vitesse, il ne s'arrête plus. Plus il y a de force dans un volant d'inertie, plus il tourne vite. Cette même force d'inertie peut être obtenue en cybersécurité en associant technologie et expertise humaine. Des contrôles de sécurité complets réduisent le volume d'alertes que les défenseurs doivent traiter, ce qui leur permet d'être plus actifs sur la neutralisation des attaques et l'amélioration de leur posture de sécurité. En retour, l'efficacité des contrôles de sécurité s'en trouve renforcée, créant ainsi un cercle vertueux.

La majorité des entreprises prévoient d'adopter les contrôles et les services de sécurité nécessaires

L'enquête montre que la plupart des entreprises prévoient d'ajouter des solutions de détection et de réponse aux menaces à leur dispositif de sécurité dans les douze prochains mois. Plus des trois quarts d'entre elles (78 %) prévoient d'ajouter des outils EDR (Endpoint Detection and Response) ou XDR (Extended Detection and Response) dans les douze prochains mois.

Le travail d'investigation et de réponse aux cybermenaces avancées requiert une expertise de pointe, avec un minimum de 5 ou 6 personnes pour assurer une couverture 24/7. La pénurie de compétences en interne étant citée comme l'un des trois principaux cyber risques pour 2023, bon nombre d'entreprises envisagent de faire appel à des experts externes pour les aider : 44 % d'entre elles déclarent vouloir commencer à travailler avec un fournisseur de services MDR (Managed Detection and Response) dans les 12 prochains mois.

Pourcentage d'entreprises qui prévoient d'adopter une solution de détection et de réponse dans les 12 prochains mois

78 %	**44 %**
EDR/XDR	MDR

Sophos peut vous aider

Sophos fournit des technologies et des services qui permettent aux entreprises d'accélérer la force d'inertie de leurs défenses et de prendre de l'avance sur les attaquants. Aujourd'hui, nous protégeons plus de 550 000 entreprises contre les menaces les plus avancées, et Sophos MDR est le service MDR le plus fiable sur le marché.

Commencer par les boucliers les plus solides

Nos solutions Endpoint/EDR, pare-feu, messagerie, réseau et Cloud ralentissent les attaquants et donnent aux défenseurs le temps et les informations dont ils ont besoin pour répondre :

- **Optimisation de la prévention :** Sophos bloque automatiquement 99,98 % des menaces en amont, ce qui minimise les risques et permet aux défenseurs de gérer moins d'incidents nécessitant une intervention humaine.
- **Réduction de l'exposition :** Sophos déploie automatiquement les paramètres de protection optimaux dès le premier jour, éliminant les failles de sécurité. Notre fonction « Vérifier l'état du compte » signale les logiciels manquants et les problèmes de configuration qui peuvent entraîner des infections autrement évitables.
- **Interruption des attaquants.** La protection Active Adversary adaptative déclenche immédiatement des défenses renforcées dès qu'une intrusion est détectée au niveau du poste de travail, ce qui décourage les attaquants et donne aux défenseurs plus de temps pour répondre à l'incident.

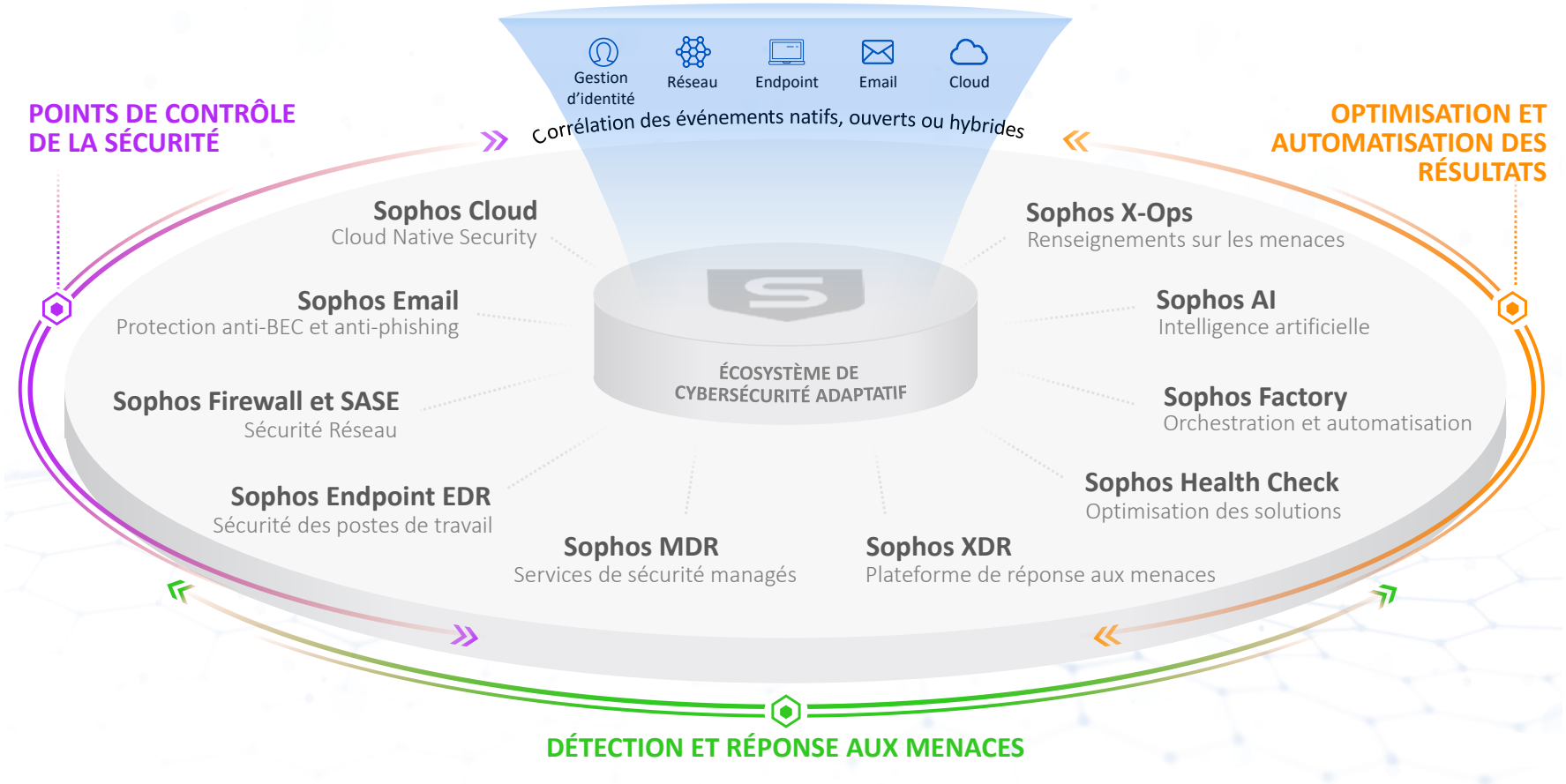
Optimiser la détection, l'investigation et la réponse

Plus les choses sont visibles pour les défenseurs, plus ils peuvent agir rapidement. Chez Sophos, nous exploitons les détections venant de l'ensemble de l'environnement de sécurité : nous intégrons la télémétrie des contrôles Sophos mais aussi d'autres fournisseurs afin d'accélérer la détection et la réponse, et de renforcer le retour sur les investissements en place.

Le service Sophos MDR mobilise plus de 500 experts qui chassent les menaces, investiguent et répondent aux adversaires actifs et autres attaques à votre place, 24/7/365. Avec un temps de réponse moyen aux menaces de seulement 38 minutes, Sophos MDR est considérablement plus rapide que l'équipe interne de sécurité la plus rapide. Les entreprises ont également la possibilité d'utiliser la plateforme Sophos XDR qui comprend toutes les fonctionnalités EDR pour investiguer et répondre aux attaques en interne ou de travailler en collaboration avec l'équipe Sophos MDR.

Peu importe où vous en êtes aujourd'hui et où vous voulez aller demain, Sophos peut vous aider à accélérer la force d'inertie de vos défenses et à prendre de l'avance sur les attaquants actuels les plus avancés. Pour plus d'informations, visitez www.sophos.fr ou discutez avec un de nos conseillers en sécurité.

Avec Sophos, obtenez des résultats optimaux en matière de cybersécurité



2023-03-29 (WP-NP)

SOPHOS