SOPHOS
Cybersecurity evolved.

Les équipes de cybersécurité : en 2021 et au-delà

Résultats d'une enquête menée auprès de 5 400 responsables informatiques dans 30 pays

Un livre blanc Sophos. Juin 2021

Partout dans le monde, les équipes informatiques ont été en première ligne de la réponse à la pandémie. Les professionnels de l'informatique ont joué un rôle essentiel en aidant les organisations à maintenir leurs activités malgré les restrictions et les limitations imposées par le COVID-19. C'est en grande partie grâce aux équipes informatiques engagées et passionnées du monde entier que tant d'organisations ont pu rester opérationnelles pendant la pandémie. Elles ont aidé les établissements d'enseignement à dispenser des cours en ligne, permis aux commerçants d'évoluer vers le commerce en ligne et fait en sorte que les organismes publics puissent continuer à fournir des services essentiels, pour ne citer que quelques exemples.

Ce présent rapport, basé sur les commentaires de 5 400 responsables informatiques venant de 30 pays, met en lumière les réalités auxquelles les équipes informatiques ont dû faire face en 2020. Il révèle comment les expériences de cybersécurité vécues par les équipes ont changé au cours de l'année 2020 et l'impact que ces changements ont eu sur les membres de l'équipe. Il s'intéresse également à l'avenir des équipes informatiques, en révélant les attentes en matière de cybersécurité pour les cinq prochaines années et en aidant les organisations à constituer leur équipe informatique du futur, dès aujourd'hui.

Principales découvertes

Évolution des expériences des équipes IT en 2020

- **La charge de travail informatique ET de cybersécurité a augmenté :** 63 % ont constaté une augmentation de la charge de travail non liée à la sécurité, et 69 % une augmentation de la charge de travail liée à la cybersécurité.
- **Les cyberattaques sont devenues plus fréquentes :** 61 % signalent une augmentation du nombre de cyberattaques contre leur organisation.
- **Les équipes IT ont pu renforcer leurs capacités en matière de cybersécurité :** 70 % ont déclaré avoir renforcé leurs compétences et leur expertise en matière de cybersécurité au cours de cette période.
- **Les équipes se sont rapprochées face à l'adversité :** 52 % affirment que le moral de l'équipe a augmenté au cours de l'année. Les victimes de ransomwares étaient nettement plus susceptibles d'observer une augmentation du moral des équipes que celles qui n'avaient pas été touchées (60 % contre 47 %).

État des lieux actuel

- **Les équipes IT ont besoin d'aide pour faire face aux attaques complexes :** 54 % déclarent que les attaques sont désormais trop avancées pour que l'équipe IT puisse y faire face seule.
- **Les équipes IT se sentent bien équipées pour relever les défis à venir.** 82 % estiment disposer des outils et de l'expertise nécessaires pour investiguer pleinement les activités clairement suspectes.

Construire l'équipe IT du futur

- **Les équipes informatiques sont appelées à se développer**
  - 68 % prévoient une augmentation du personnel de cybersécurité interne d'ici 2023, et 76 % d'ici 2026.
  - 56 % s'attendent à ce que leur personnel informatique externalisé augmente d'ici 2023, et 64 % d'ici 2026.
- **L'IA est un outil clé dans les futures stratégies de sécurité**
  - 92 % s'attendent à ce que l'IA aide à faire face au nombre ou à la complexité croissants des menaces.

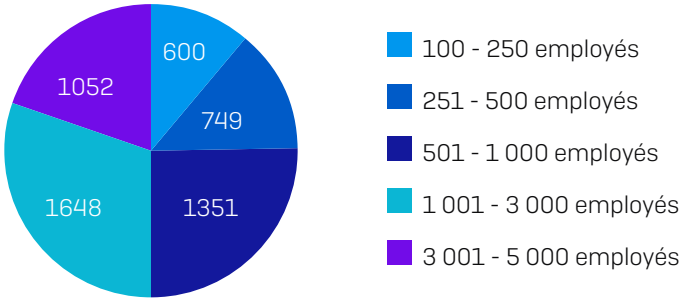
À propos de l'enquête

Sophos a chargé le cabinet d'étude indépendant Vanson Bourne d'interroger 5 400 décideurs informatiques dans 30 pays. Cette enquête s'est déroulée entre janvier et février 2021.

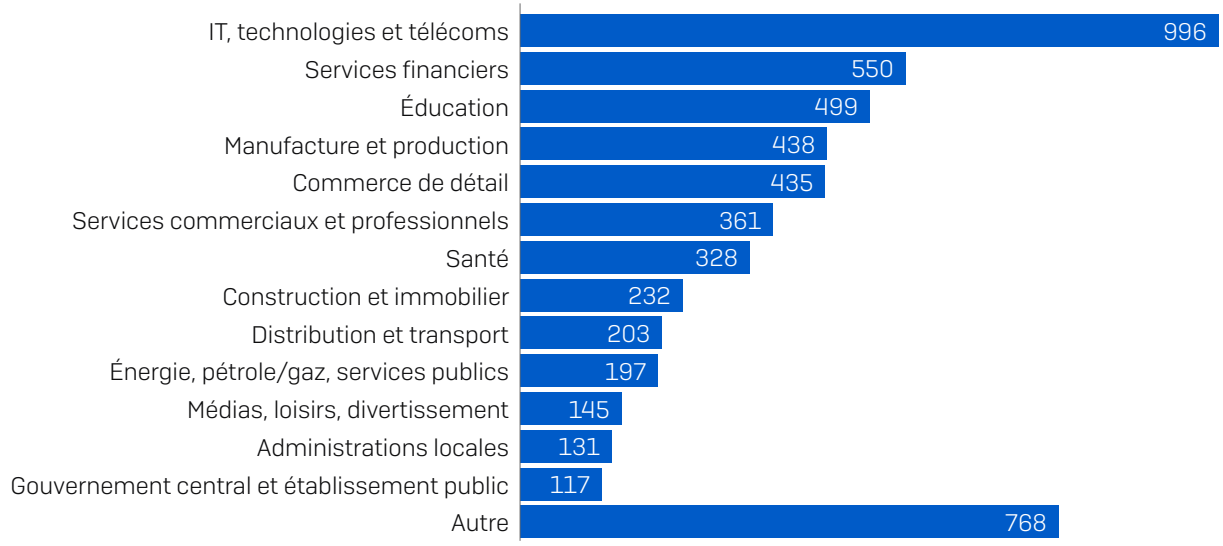
Pays	Nb de répondants	Pays	Nb de répondants	Pays	Nb de répondants
Australie	250	Inde	300	Arabie Saoudite	100
Autriche	100	Israël	100	Singapour	150
Belgique	100	Italie	200	Afrique du Sud	200
Brésil	200	Japon	300	Espagne	150
Canada	200	Malaisie	150	Suède	100
Chili	200	Mexique	200	Suisse	100
Colombie	200	Pays-Bas	150	Turquie	100
République tchèque	100	Nigeria	100	EAU	100
France	200	Philippines	150	Royaume-Uni	300
Allemagne	300	Pologne	100	États-Unis	500

50 % des personnes interrogées dans chaque pays proviennent d'entreprises de 100 à 1 000 employés et 50 % d'entreprises de 1 001 à 5 000 employés. Les répondants provenaient de secteurs industriels variés.

Combien d'employés votre entreprise compte-t-elle dans le monde entier ? [5 400]



Quel est votre secteur d'activité ? [5 400]



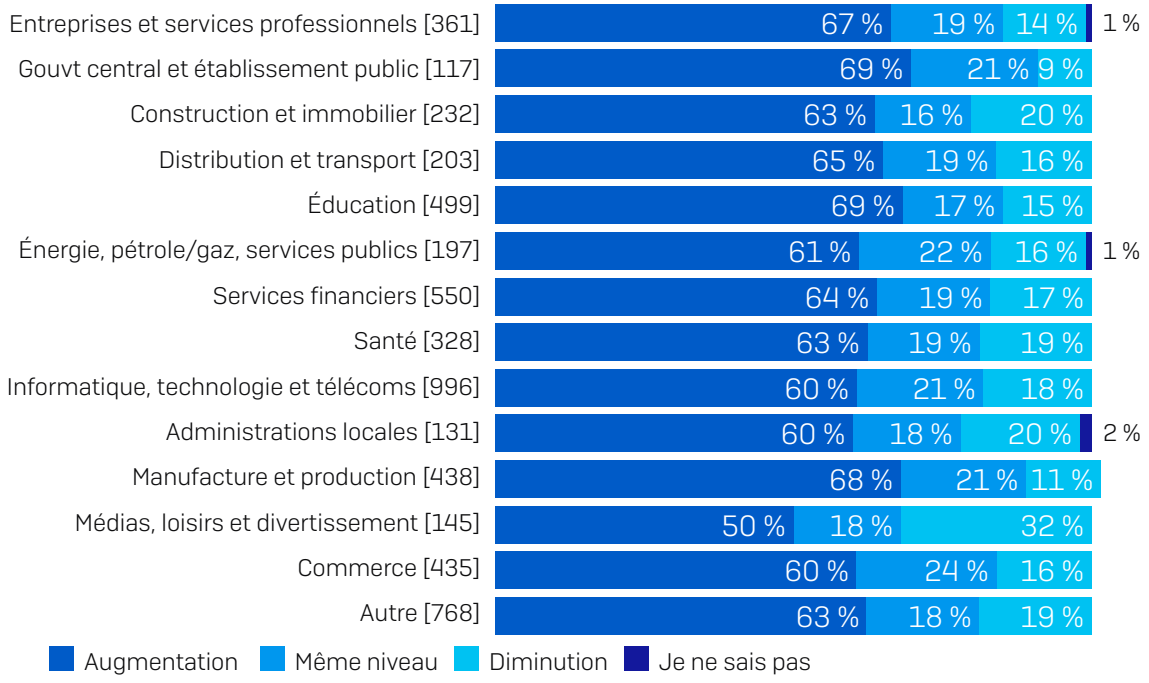
2020 : une année de changement

L'année 2020 n'a pas été une année comme les autres, et les équipes informatiques ont été en première ligne pour permettre aux organisations d'adapter leurs activités en réponse à la pandémie. Il n'est pas surprenant que cela ait eu un impact considérable sur la charge de travail.

La charge de travail IT non liée à la sécurité a augmenté…

2020 a apporté beaucoup de nouvelles tâches aux équipes informatiques : 63 % des responsables IT ont déclaré que leur charge de travail non liée à la sécurité a augmenté au cours de l'année 2020. Seuls 17 % ont eu, au contraire, une baisse de travail. Les répondants en Turquie (84 %), en Autriche (81 %) et aux États-Unis (75 %) étaient les plus susceptibles de signaler une augmentation de la charge de travail.

Évolution de la charge de travail informatique (non liée à la sécurité) au cours de l'année 2020



En 2020, notre charge de travail informatique (non liée à la sécurité) a diminué/augmenté/est restée stable [nombre dans le graphique], répartition par secteur

En examinant les données par secteur, nous constatons que les équipes informatiques du **gouvernement central et des établissements publics** et **de l'éducation** ont été les plus touchées. 69 % des répondants ont indiqué une augmentation au cours de l'année 2020, probablement en raison du rôle central joué par le gouvernement et les établissements d'enseignement dans la réponse à la pandémie. À l'inverse, **les médias, les loisirs et les divertissements** sont le secteur ayant signalé la plus forte baisse de la charge de travail (32 %), la pandémie ayant probablement contraint de nombreux établissements à limiter leurs services.

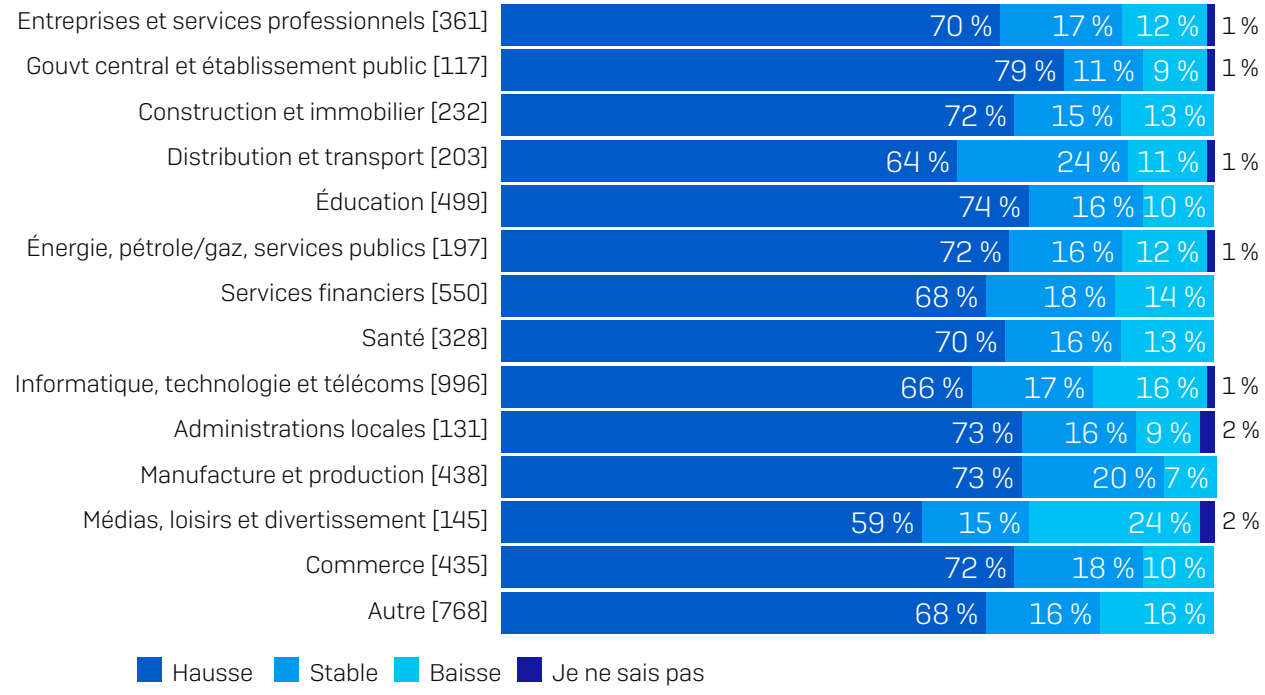
... et la charge de travail de cybersécurité a augmenté encore davantage

Évolution de la charge de travail de cybersécurité en 2020

Au cours de 2020, notre charge de travail en matière de cybersécurité a diminué/augmenté/est restée stable [5 400], en omettant « Je ne sais pas »

69 % des répondants ont signalé une augmentation de leur charge de travail de cybersécurité par rapport à l'année précédente, 13 % une diminution et 17 % une activité stable. La Turquie (82 %) a de nouveau enregistré le plus haut niveau d'augmentation, suivie par la Suède (80 %) et Israël et le Brésil (78 % chacun). À l'autre extrémité du spectre, les répondants des Émirats arabes unis étaient plus nombreux à signaler une diminution de la charge de travail de cybersécurité (26 %), suivis de la Suisse (22 %) et du Nigeria et des Philippines (19 % chacun).

Évolution de la charge de travail de cybersécurité en 2020



Au cours de 2020, notre charge de travail en matière de cybersécurité a diminué/augmenté/est restée stable [nombre dans le graphique], répartition par secteur

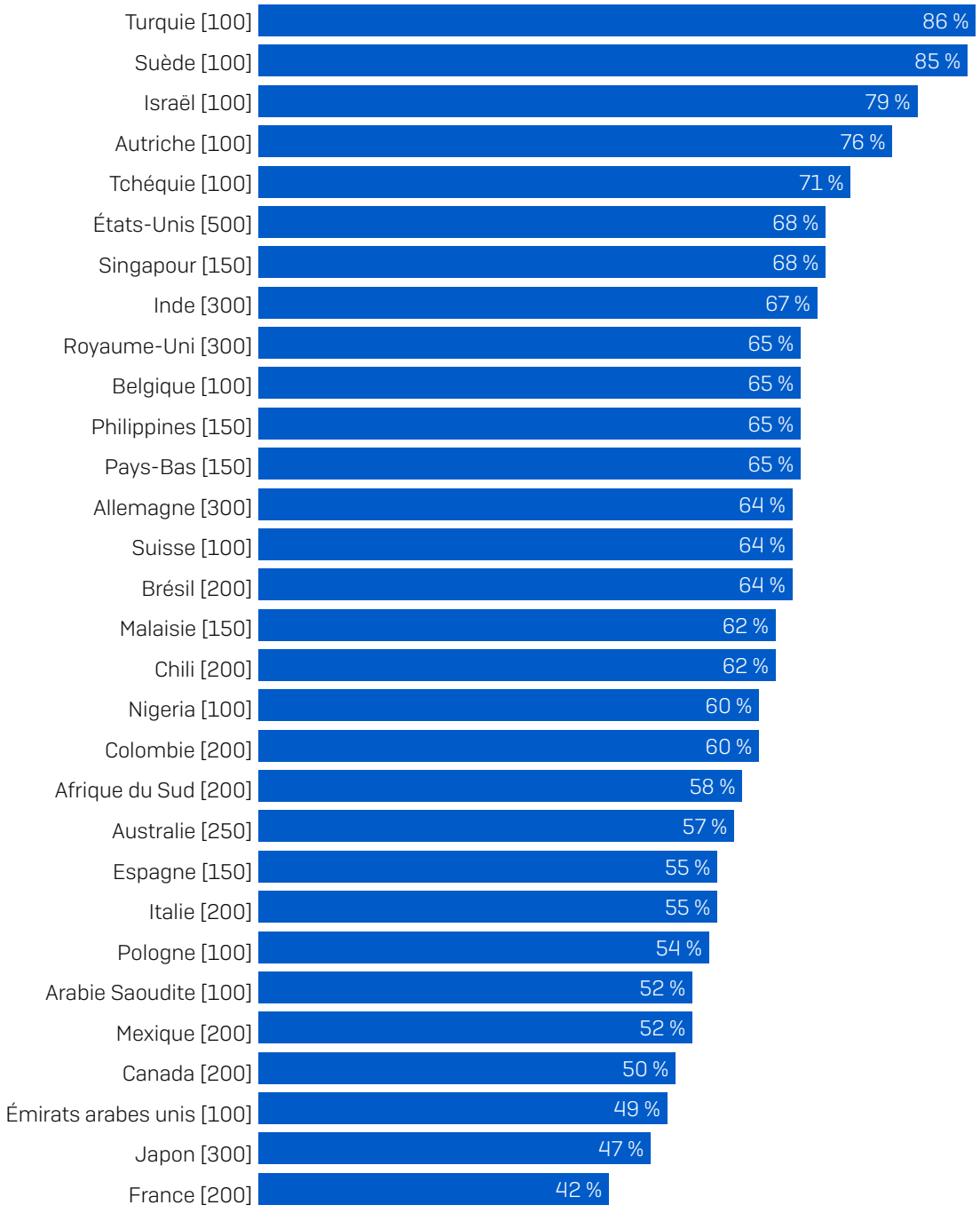
Faisant écho à la tendance observée précédemment, les responsables informatiques du **gouvernement central et des établissements publics** (79 %) et **de l'éducation** (74 %) étaient plus nombreux à signaler une augmentation de la charge de travail de cybersécurité par rapport à l'année précédente, tandis que ceux des **médias, des loisirs et du divertissement** étaient plus nombreux à signaler une baisse (24 %). Encore une fois, il est probable que cela soit dû au fait que ces secteurs sont parmi les plus touchés par la pandémie, mais de façon très différente.

Le nombre de cyberattaques a augmenté

L'augmentation de la charge de travail de cybersécurité en 2020 a été due en partie à une augmentation du nombre de cyberattaques : plus de 6 personnes interrogées sur 10 (61 %) ont signalé une augmentation du nombre d'attaques contre leur organisation l'année dernière. Seuls 19 % ont signalé une baisse.

Cette hausse a été observée dans tous les secteurs, et la variance entre ceux qui ont connu la plus grande quantité d'attaques (**gouvernement central et établissements publics**) et la plus petite quantité (**IT, technologies et télécoms** et **médias, loisirs et divertissement**) n'est que de 16 % (74 % contre 58 %).

Pourcentage des organisations interrogées ayant connu une augmentation des cyberattaques au cours de 2020



Au cours de 2020, le nombre de cyberattaques a augmenté [nombre dans le graphique] en omettant certaines options de réponse, répartition par pays

Cependant, lorsque nous examinons les données par pays, nous constatons une variation beaucoup plus importante dans les expériences vécues. Par exemple, deux fois plus de répondants en Turquie ont signalé une augmentation du nombre d'attaques par rapport à ceux de la France (86 % contre 42 %). Un très grand nombre de répondants en Suède (85 %), en Israël (79 %) et Autriche (76 %) ont également signalé une augmentation du nombre de cyberattaques contre leur organisation au cours de l'année 2020. À l'inverse, en France, au Japon et aux Émirats arabes unis, moins de la moitié ont signalé une augmentation des attaques.

Les attaques sont de plus en plus difficiles à bloquer

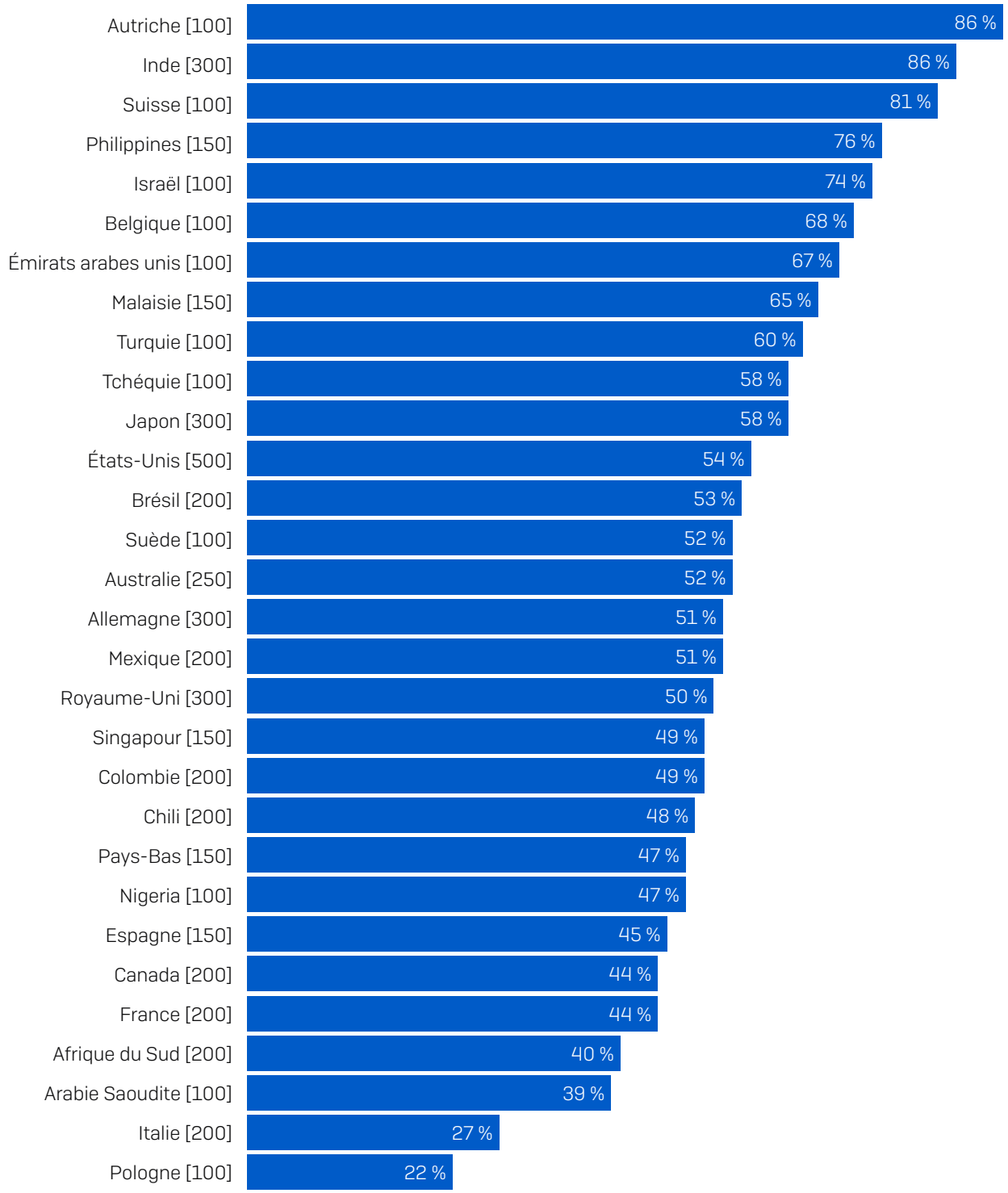
Les cyberattaques avancées sont complexes et multi-étapes, avec des adversaires qui utilisent une myriade de tactiques, techniques et procédures (TTP) tout au long de l'attaque. La gestion de ces attaques est un défi. Pour plus de la moitié des répondants (54 %), les attaques sont désormais trop avancées pour que leur équipe IT puisse les gérer seule.

estiment que les attaques sont désormais trop avancées pour que l'équipe IT de leur organisation puisse y faire face seule

Ce défi est le plus critique dans le secteur des **services commerciaux et professionnels**, où 63 % des personnes interrogées pensent qu'elles ne sont plus capables de faire face seules aux cyberattaques, suivies de près par le **gouvernement central et les établissements publics** (62 %) et la **santé** (60 %). À l'inverse, **la construction et l'immobilier** et **les administrations locales** étaient les moins susceptibles (47 %) d'être d'accord avec cet énoncé. Dans le cas du gouvernement local, c'est une conclusion surprenante, puisque, comme nous l'avons rapporté dans le rapport L'état des ransomwares en 2021, ce secteur est le plus susceptible d'avoir ses données chiffrées dans une attaque par ransomware.

Parmi les pays étudiés, nous constatons une variation considérable des niveaux de confiance des équipes dans la gestion des attaques complexes.

Répondants qui estiment que les attaques sont désormais trop avancées pour que l'équipe It puisse y faire face seule



Les répondants qui s'accordent à dire que les cyberattaques sont désormais trop avancées pour que l'équipe informatique de leur organisation puisse y faire face seule [nombre dans le graphique] en omettant certaines options de réponse, répartition par pays

Les personnes basées en Autriche et en Inde sont les moins confiantes dans la gestion des attaques : 86 % déclarent qu'elles sont maintenant trop complexes pour leur équipe IT, suivies par la Suisse (81 %), les Philippines (76 %) et Israël (74 %).

Reconnaitre la complexité des attaques et identifier le moment où une expertise externe est nécessaire constituent une étape clé dans la défense contre les cyberattaques avancées actuelles. Les équipes des SophosLabs et Sophos Managed Threat Response ont constaté une augmentation constante du nombre d'attaques combinant automatisation et piratage en direct dans le but de contourner les défenses des organisations. Pour bloquer ces attaques sophistiquées, il est nécessaire que des experts qualifiés soient présents et que les organisations sachent reconnaitre le moment où ces compétences doivent être externalisées.

À l'autre bout du spectre, la Pologne signale le moins de difficultés à gérer les cyberattaques en interne, avec seulement 22 % des répondants affirmant que les attaques sont trop avancées pour leur équipe IT, suivie de près par l'Italie (27 %). Cette confiance face au nombre croissant d'attaques peut s'expliquer par un investissement dans le recrutement et le développement des compétences du personnel qui sont alors capables de garder une longueur d'avance sur les adversaires. Toutefois, cela peut aussi refléter une confiance malavisée face aux attaques avancées d'aujourd'hui. Alors que les adversaires évoluent constamment dans leurs approches, il est important d'être réaliste quant au niveau d'expertise nécessaire pour les bloquer.

Les temps de réponse sont en baisse

Compte tenu de l'augmentation généralisée de la charge de travail au cours de l'année 2020 et des difficultés liées à l'adaptation à la pandémie, il n'est peut-être pas surprenant qu'une grande majorité des répondants (61 %) aient signalé une augmentation du temps de réponse aux tickets informatiques au cours de cette période. 20 % ont déclaré que le temps de réponse a diminué au cours de cette période, et il est resté le même pour 19 %.

Évolution du temps de réponse aux tickets informatiques en 2020

Au cours de 2020, notre temps de réponse aux tickets informatiques a diminué/augmenté/est restée stable [5 400], en omettant « Je ne sais pas »

Le secteur de l'**éducation** est celui où l'augmentation du temps de réponse est la plus fréquente : 65 % des répondants ont signalé une hausse. La nécessité pour les établissements scolaires de la plupart des pays de se tourner vers l'enseignement en ligne en 2020 a créé un travail considérable pour les équipes IT, ce qui a probablement eu un impact sur leur capacité à répondre rapidement aux tickets.

Les médias, les loisirs et le divertissement ont signalé la plus forte diminution du temps de réponse : près d'un tiers (32 %) indiquant qu'ils étaient en mesure de répondre plus rapidement aux tickets. Encore une fois, la pandémie a joué un rôle majeur dans ce changement avec une réduction de la production organisationnelle, libérant du temps pour les équipes IT qui ont pu accélérer les réponses.

L'impact de l'année 2020 sur les équipes informatiques

Mais il n'y a pas que de mauvaises nouvelles. En ce qui concerne l'état des équipes informatiques, il y a de quoi être encouragé. 70 % des DSI ont déclaré que la capacité de leur équipe à développer davantage leurs compétences et leur expertise en matière de cybersécurité s'était accrue au cours de l'année 2020, avec seulement 12 % d'entre eux déclarant qu'elle avait diminué.

Changements dans la capacité à développer davantage de compétences et d'expertise en cybersécurité en 2020

Au cours de 2020, la capacité à développer davantage nos compétences et notre expertise en matière de cybersécurité a diminué/augmenté/est restée stable [5 400], en omettant « Je ne sais pas ».
En raison des arrondis, la somme des résultats n'est pas égale à 100 %.

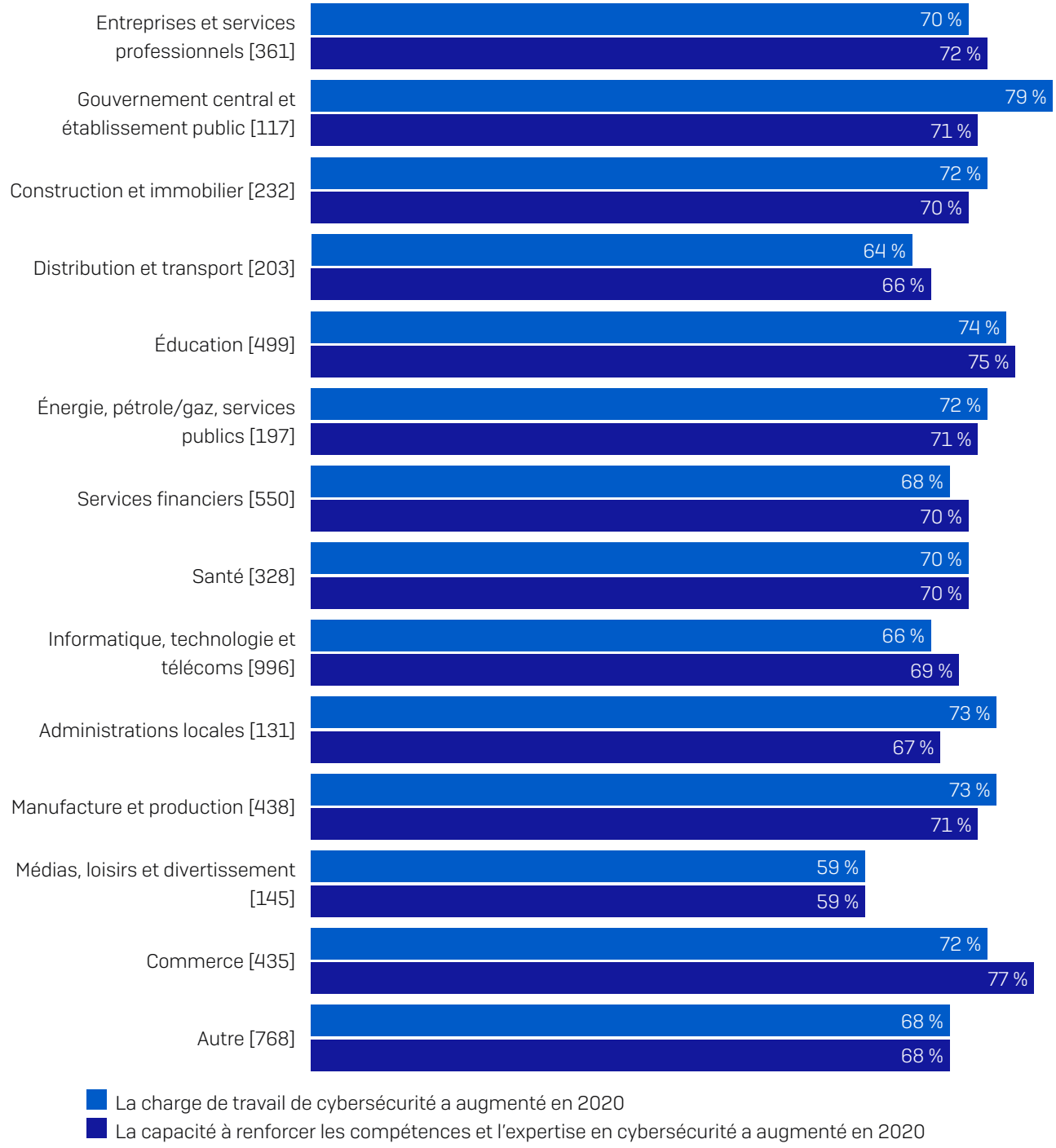
Il est intéressant de noter que plusieurs secteurs ayant été particulièrement touchés par la pandémie ont signalé des expériences contrastées :

- **Les commerces** sont le secteur où les équipes ont le plus accru leurs compétences et leur expertise en matière de cybersécurité (77 %). Il est probable que le passage à la vente en ligne pendant les périodes de confinement ait posé de nouveaux défis et offert de nouvelles opportunités de croissance aux équipes IT de ce secteur.
- **L'éducation** est le deuxième secteur où les équipes ont le plus développé leurs compétences et expertise en matière de cybersécurité (75 %). Ce secteur a lui aussi connu une transformation majeure au cours de l'année 2020, et alors que l'évolution vers la formation en ligne a sans aucun doute représenté un énorme défi pour les équipes IT, elle a également créé une énorme opportunité d'apprentissage.
- **Les médias, les loisirs et les divertissements** ont enregistré la plus faible augmentation (59 %). Ce secteur constatant également la plus forte baisse des charges de travail non liées à la sécurité et à la cybersécurité, il est probable que la réduction de l'activité ait limité les opportunités de développement.

L'augmentation de la charge de travail entraîne une amélioration des compétences et de l'expertise

Dans l'ensemble, les données ont révélé une corrélation nette entre la hausse de la charge de travail de cybersécurité et le développement de l'expertise et des compétences en cybersécurité, et ce dans tous les secteurs.

Augmentation de la charge de travail de cybersécurité et de la capacité à développer des compétences et de l'expertise en cybersécurité



Au cours de 2020, notre charge de travail en matière de cybersécurité a augmenté / Au cours de l'année 2020, notre capacité à renforcer les compétences et l'expertise en cybersécurité a augmenté [nombre dans le graphique], répartition par secteur.

Parmi les répondants ayant connu une hausse de la charge de travail de cybersécurité en 2020, 84 % ont également signalé une hausse de leur capacité à développer leurs compétences et leur expertise en cybersécurité. De même, plus de 8 personnes sur 10 (82 %) ayant signalé une augmentation des cyberattaques contre leur organisation ont également signalé une hausse de leur capacité à développer leurs compétences et expertise en cybersécurité. Cela est logique : si l'augmentation de la charge de travail et les cyberattaques ajoutent de la pression, elles offrent également des opportunités de développement de nouvelles compétences.

Le moral de l'équipe s'est amélioré

Plus de la moitié des responsables informatiques interrogés (52 %) ont déclaré que le moral des équipes avait augmenté au cours de l'année 2020. 26 % ont déclaré qu'il avait diminué et 22 % qu'il était resté le même.

Évolution du moral des équipes en 2020

Au cours de 2020, le moral de l'équipe a diminué/augmenté/est resté stable [5 400], en omettant « Je ne sais pas »

Sur le plan géographique, le moral a été le plus boosté en Turquie (75 %), en Autriche (71 %), en Inde et en Afrique du Sud (69 % chacun). À l'autre extrémité de l'échelle, les équipes IT d'Israël (26 %), de France (31 %), d'Italie (33 %) et de Pologne (36 %) sont celles dont le moral de l'équipe a été le moins boosté.

Vous avez peut-être remarqué que plusieurs pays listés ici ont également été mentionnés dans les sections précédentes. La Turquie et l'Autriche, qui ont le plus grand nombre de répondants ayant vu une augmentation du moral de l'équipe, figuraient parmi les quatre premiers pays à avoir signalé une augmentation du nombre de cyberattaques. De même, la France a le deuxième plus faible nombre de répondants ayant signalé une hausse du moral de l'équipe et aussi le plus faible nombre de cyberattaques de tous les pays étudiés. La corrélation entre quantité de cyberattaques et hausse du moral des équipes est l'une des conclusions les plus frappantes de l'enquête.

Pour appuyer davantage ce point, 60 % des personnes interrogées dont l'organisation a été touchée par une attaque de ransomware en 2020 ont signalé une amélioration du moral de l'équipe, contre 47 % pour celles qui n'ont pas été touchées.

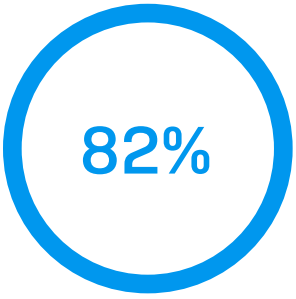
Évolution du moral des équipes en 2020

Au cours de 2020, le moral de notre équipe a diminué/augmenté/est resté stable [5 400] en omettant certaines options de réponse, répartition par les répondants dont l'organisation a été touchée par un ransomware en 2020.

Il y a un certain nombre de facteurs probables derrière cette corrélation. L'adversité — en l'occurrence les cyberattaques — est souvent l'occasion pour le personnel de s'entraider et de faire front vers un objectif commun, ce qui stimule le moral de l'équipe. En outre, pouvoir soutenir son organisation face à l'augmentation des attaques apporte un sentiment de satisfaction. La plus forte hausse du moral a été signalée par deux secteurs qui ont été fortement touchés par la pandémie : **l'éducation** ayant connu la plus forte augmentation (58 %), suivie de près par la **santé** (57 %).

Dans le même temps, le rôle central joué par les équipes informatiques pour assurer la continuité des activités face à la pandémie peut avoir entraîné une plus grande sensibilisation et une meilleure reconnaissance de leur contribution, ce qui contribue également à remonter le moral de l'équipe. Si le travail des équipes informatiques n'a pas encore été dûment reconnu, le moment est venu de le faire.

Les équipes IT se sentent bien équipées pour relever les défis à venir



déclarent disposer des outils et de l'expertise nécessaires pour investiguer pleinement les activités suspectes

Répondants estimant disposer des outils et de l'expertise nécessaires pour mener une investigation approfondie s'ils détectent des activités suspectes dans leur organisation [5400] omettant certaines options de réponse.

Face à l'augmentation de la charge de travail et du nombre de cyberattaques en 2020, il est encourageant de constater que 82 % des responsables informatiques affirment disposer des outils et de l'expertise nécessaires pour investiguer les activités suspectes si elles sont détectées dans leur organisation. Les opportunités offertes pour développer les compétences et l'expertise au cours de 2020 permettent aux équipes de bien répondre aux défis à venir. Il est essentiel de poursuivre cet investissement dans des outils et des formations si l'on veut que les équipes informatiques soient en mesure de suivre l'évolution constante des cyberattaques.

Cependant, lorsque nous examinons les réponses à cette question par secteur, il y a deux aberrations claires : **le gouvernement central et les établissements publics** (67 %) et **le gouvernement local** (64 %). Partout dans le monde, le secteur public a été fortement touché par la pandémie. Il a dû assurer la continuité de services essentiels pendant une période prolongée de bouleversements, tout en fournissant un soutien supplémentaire aux citoyens et aux organisations. Par ailleurs, pour de nombreux pays, le financement du secteur public est un défi permanent, ce qui peut limiter les ressources disponibles. Les auteurs de ransomware se concentrent particulièrement sur les organisations gouvernementales, il est donc essentiel que ces dernières disposent des ressources et des compétences nécessaires pour analyser efficacement les activités suspectes.

L'équipe informatique du futur

Comme nous l'avons vu, l'année 2020 a été une période difficile pour beaucoup d'informaticiens. Cependant, les équipes IT ont admirablement relevé les défis de cette année et ont ainsi amélioré leurs compétences et leur moral. Ces expériences, ainsi que les changements dans le paysage informatique (tels que l'adoption croissante du travail flexible et de l'utilisation du Cloud) auront un impact direct sur les équipes de cybersécurité du futur.

Les équipes de cybersécurité sont appelées à se développer — rapidement

Face aux exigences croissantes des équipes informatiques, les répondants prévoient un développement considérable de la taille du personnel de cybersécurité, tant interne qu'externalisé, en particulier au cours des deux prochaines années :

- 68 % prévoient une augmentation du personnel interne au cours des deux prochaines années, et 76 % au cours des cinq prochaines années
- 56 % prévoient une augmentation du personnel informatique externalisé au cours des deux prochaines années, et 64 % au cours des cinq prochaines années
- Seulement 8 % s'attendent à ce que le nombre du personnel interne soit inférieur dans 5 ans.

Ressourcement en sécurité IT	Changement prévu	D'ici 2023	D'ici 2026
Personnel de sécurité IT interne	Augmentation	68 %	76 %
	Diminution	11 %	8 %
Personnel de sécurité IT externe	Augmentation	56 %	64 %
	Diminution	14 %	10 %

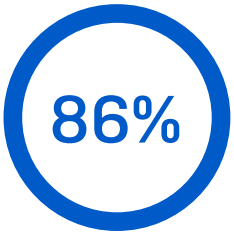
Selon vous, comment la taille de l'équipe de cybersécurité de votre organisation va-t-elle changer d'ici 2023 et 2026 ? [5 400] en excluant certaines options de réponse

Il est intéressant de noter que la croissance du personnel IT externalisé ne se fait pas au détriment des équipes internes. Près de la moitié (46 %) des personnes interrogées s'attendent à ce que le personnel de cybersécurité, tant interne qu'externalisé, augmente d'ici 2023, pour atteindre 55 % en 2026.

Dans l'ensemble, 77 % des répondants prévoient une croissance dans au moins un domaine de ressourcement (interne ou externe) au cours des deux prochaines années, passant à 85 % d'ici 2026.

L'intelligence artificielle est essentielle

S'attendent à ce que l'IA réponde au nombre croissant d'attaques



S'attendent à ce que l'IA réponde à la sophistication croissante des attaques

Les répondants s'accordent à dire qu'ils s'attendent à ce que les technologies de l'IA aident à gérer le nombre croissant d'attaques ou qu'ils s'attendent à ce que les technologies de l'IA aident à gérer la sophistication croissante des attaques [5 400] en omettant certaines options de réponse

Les professionnels de l'informatique se tournent presque universellement vers les technologies de l'IA pour les aider à lutter contre l'évolution des cybermenaces. 86 % s'attendent à ce que les technologies de l'IA aident à faire face au nombre croissant d'attaques, tandis que le même pourcentage s'attend à ces technologies aident à faire face à la sophistication croissante des attaques, 92 % ayant sélectionné au moins une des deux options.

Constituez dès maintenant l'équipe de cybersécurité du futur

Pour constituer l'équipe informatique du futur, il faut commencer dès maintenant. Ces retours des personnels informatiques au plus près du front permettront aux organisations de préparer la réussite de leur stratégie de cybersécurité d'ici 2023 et au-delà. Sur la base des enseignements tirés de ce rapport, Sophos propose cinq recommandations :

1. Implémentez des outils et des approches qui réduisent la charge de travail administrative de cybersécurité

L'augmentation de la charge de travail, liée ou non à la sécurité, au cours de l'année 2020 est indéniable. Les organisations doivent envisager d'implémenter des outils et des approches qui réduisent la charge de travail de cybersécurité, libérant du temps aux équipes qui pourront ainsi se consacrer à d'autres activités.

- **Automatiser.** Profitez de l'automatisation pour réduire la charge des tâches quotidiennes qui font perdre un temps et une énergie précieux aux professionnels de l'informatique et les détournent des projets stratégiques. Les machines sont toujours capables de réagir plus rapidement que les opérateurs, ce qui accélère le temps de réponse et réduit l'exposition.
- **Consolider.** Simplifiez l'administration quotidienne en gérant toutes vos solutions de cybersécurité dans une console unique et unifiée. Tout étant regroupé en un seul endroit, il n'est plus nécessaire de passer d'une console à l'autre pour gérer la sécurité et corréler les données entre les différents systèmes, ce qui permet aux équipes informatiques d'économiser un temps précieux. La consolidation de la sécurité informatique réduit également les frais généraux de gestion des fournisseurs.
- **Intégrer.** Choisissez des solutions qui s'intègrent et sont conçues pour fonctionner ensemble. Cela augmente l'automatisation des tâches tout en facilitant les investigations entre produits et en fournissant des informations plus approfondies sur votre posture de sécurité.

2. Investissez dans des outils et des formations qui permettent aux équipes IT d'utiliser leurs compétences acquises

Les équipes informatiques ont vu leurs compétences et leur expertise se développer considérablement en 2020. Les organisations ont tout intérêt à investir dans les outils et les formations qui leur permettent d'utiliser ces nouvelles compétences et de continuer à apprendre. Ces ressources permettront également de recruter de nouveaux talents dans l'équipe.

3. Combiner l'expertise de l'équipe IT interne et externalisée

Les cybermenaces sont déjà trop complexes pour que plus de la moitié des responsables informatiques puissent y faire face seuls — et elles ne feront que s'aggraver. En combinant l'expertise interne et externe de vos équipes de sécurité, vous pouvez obtenir le meilleur des deux mondes : des experts ayant une connaissance approfondie des menaces et de votre organisation. Cette structure combinée permet également de s'adapter et de répondre plus facilement aux changements, en faisant appel aux meilleures personnes pour chaque situation. Les organisations doivent rechercher des partenaires sécurité capables de renforcer leur équipe informatique avec des compétences et des capacités non disponibles en interne, tout en offrant la flexibilité nécessaire pour s'adapter à leur modèle opérationnel souhaité.

4. Mettez tout en œuvre pour attirer les meilleurs talents au monde

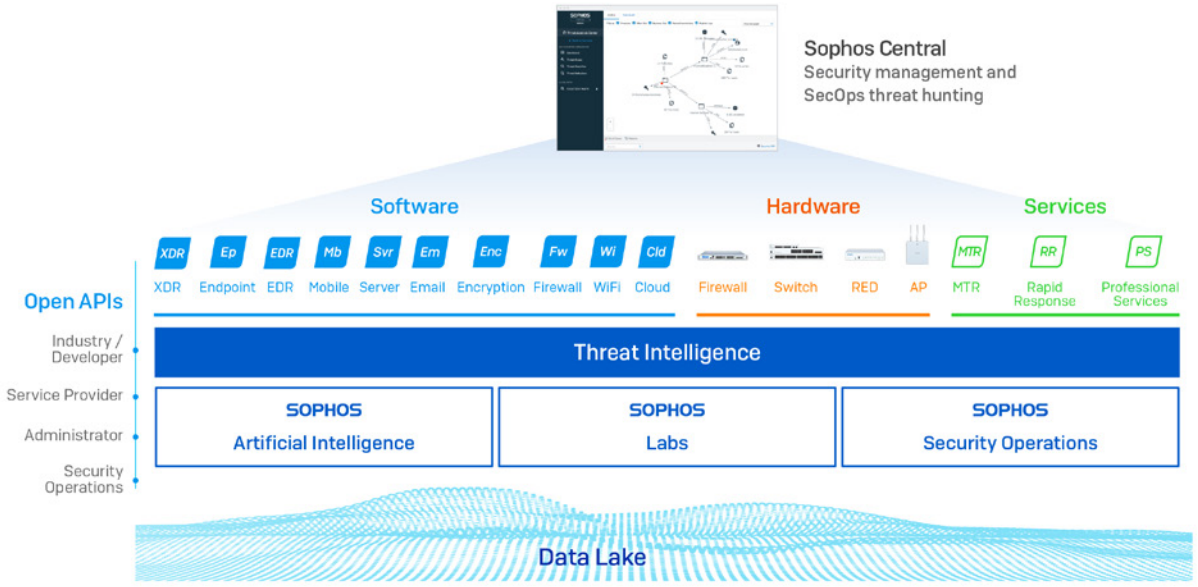
La majorité des organisations cherchent à agrandir leurs équipes informatiques, c'est pourquoi la concurrence pour attirer les meilleurs talents est féroce. En optant pour des technologies innovantes qui peuvent être gérées depuis n'importe quel endroit, vous pourrez augmenter votre vivier de talents. La pandémie nous a appris que presque tous les rôles informatiques peuvent être assumés à distance si nécessaire. De plus, en offrant des outils de haute qualité, vous augmenterez votre attrait pour les candidats les plus compétents.

5. Constituez votre équipe de cybersécurité interne

Il existe déjà une pénurie de candidats en informatique talentueux. En plus d'élargir leur bassin de talents, les entreprises doivent également mettre en œuvre des programmes internes pour développer les compétences de leur équipe informatique, tels que des stages ou des formations continues. Si l'image d'un jeune en sweat à capuche penché sur son ordinateur dans sa chambre est un stéréotype, elle rappelle aussi que de nombreuses personnes développent des compétences informatiques avancées en dehors des parcours professionnels traditionnels.

Comment Sophos peut vous aider

Sophos aide les équipes informatiques de plus de 500 000 organisations dans 150 pays à protéger leurs entreprises contre les cybermenaces.



Sophos Adaptive Cybersecurity Ecosystem (ACE)

- Nous proposons une gamme complète de **technologies de nouvelle génération** basées sur l'**intelligence artificielle**. Nos produits sont conçus pour fonctionner ensemble, en automatisant les tâches manuelles et en réduisant l'exposition aux menaces ; nous appelons cela la Sécurité Synchronisée. Les clients qui bénéficient de notre protection endpoint et pare-feu signalent systématiquement une réduction d'au moins 50 % des tâches administratives quotidiennes et une diminution des incidents de sécurité.
- **Sophos Extended Detection and Response** (XDR) et **Sophos Endpoint Detection and Response** (EDR) offrent aux équipes IT les outils dont elles ont besoin pour identifier et remédier rapidement aux menaces et aux problèmes d'hygiène informatique. Sophos EDR est le premier outil EDR conçu à la fois pour les analystes de sécurité et les administrateurs informatiques, et permet aux équipes de développer leur expertise sans ajouter de personnel.
- Toutes les technologies Next-Gen de Sophos sont administrées dans la plateforme **Sophos Central**, un outil Web qui vous permet d'employer les meilleurs talents de sécurité, peu importe où ils se trouvent.
- Les équipes **Sophos MTR (Managed Threat Response) et Sophos Rapid Response** fournissent une expertise avancée en matière de traque des menaces (Threat Hunting) et de réponse aux incidents pour soutenir les équipes internes, sous la forme d'un service entièrement managé. Vous contrôlez quand et comment les incidents potentiels sont escaladés et quelles actions de remédiation (si nécessaire) nous sommes habilités à prendre en votre nom.
- Notre protection repose sur l'intelligence sur les menaces venant de nos équipes des **SophosLabs**, **Sophos Security Operations**, **Sophos AI** et du **Sophos Data Lake**.
- Des **API ouvertes** permettent à tous les clients de bénéficier de notre expérience et de la télémétrie issues de nos partenaires du monde entier.

Pour en savoir plus sur ce que nous faisons et pour discuter des défis auxquels votre équipe est confrontée, visitez notre site Web ou contactez un représentant Sophos.

Pour en savoir plus sur ce que nous faisons et pour discuter des défis auxquels votre équipe est confrontée, visitez notre site Web ou contactez un représentant Sophos.

Sophos fournit des solutions de cybersécurité de pointe aux entreprises de toutes tailles, les protégeant en temps réel contre les menaces avancées telles que les malwares, les ransomwares et le phishing. Grâce à des fonctionnalités Next-Gen éprouvées, les données de votre entreprise sont sécurisées efficacement par des produits alimentés par l'intelligence artificielle et le Machine Learning.

2021-05-20 (WP-NP)

SOPHOS