SOPHOS

CYBERSÉCURITÉ : LE DÉFI HUMAIN

Résultats d'une enquête indépendante menée auprès de 5 000 responsables informatiques dans 26 pays

Livre blanc Sophos Octobre 2020

Introduction

Le rôle des professionnels expérimentés dans le domaine de la cybersécurité n'a jamais été aussi important. Si les progrès de l'automatisation et des technologies ont joué un rôle crucial dans le renforcement des cyberdéfenses des entreprises, les programmes de sécurité véritablement efficaces requièrent toujours la présence d'experts humains.

L'importance de ces professionnels de la sécurité est due en grande partie à l'évolution des cyberattaques. Derrière chaque menace se cache un cybercriminel, et les attaques avancées d'aujourd'hui combinent souvent des technologies pointues avec du pilotage en direct. Pour se protéger contre ces attaques manuelles, il faut un savoir-faire humain.

Notre enquête exhaustive fournit un aperçu inédit de l'état des compétences et des ressources en matière de cybersécurité à travers le monde. Elle lève le voile sur la réalité de la cybersécurité pour les équipes informatiques et les défis auxquels ces dernières sont confrontées sur le plan humain.

L'étude présente également un aperçu unique du rapport observé entre les entreprises victimes d'un ransomware et leurs pratiques de la cybersécurité au quotidien.

À propos de l'enquête

Sophos a chargé le cabinet Vanson Bourne, spécialiste indépendant en études de marché, de mener une enquête auprès de 5 000 responsables IT en janvier et février 2020. Sophos n'a joué aucun rôle dans la sélection des participants et toutes les réponses ont été fournies de manière anonyme.

PAYS	NB DE RÉPONDANTS
Australie	200
Belgique	100
Brésil	200
Canada	200
Chine	200
Colombie	200
République tchèque	100
France	300
Allemagne	300

PAYS	NB DE RÉPONDANTS
Inde	300
Italie	200
Japon	200
Malaisie	100
Mexique	200
Pays-Bas	200
Nigeria	100
Philippines	100
Pologne	100

PAYS	NB DE RÉPONDANTS
Singapour	200
Afrique du Sud	200
Espagne	200
Suède	100
Turquie	100
EAU	100
Royaume-Uni	300
États-Unis	500

Pour chaque pays, 50 % des répondants sont issus d'entreprises comptant entre 100 et 1 000 employés et 50 % sont issus d'entreprises comptant entre 1 001 et 5 000 employés. Les répondants couvrent un large éventail de secteurs industriels, tant publics que privés.

SECTEUR	NB DE RÉPONDANTS
IT, technologies et télécoms	979
Commerce, distribution et transport	666
Manufacture et production	648
Services financiers	547
Secteur public	498
Services commerciaux et professionnels	480
Construction et immobilier	272
Énergie, pétrole/gaz, services publics	204
Médias, loisirs et divertissement	164
Autre	542

Résumé

Les équipes IT progressent dans de nombreux domaines

- **Les équipes IT sont au top au niveau de l'installation des correctifs.** Les 3/4 des équipes IT installent, en général, les correctifs au niveau des postes de travail, des serveurs, des applications et des ressources connectées à Internet dans la semaine suivant leurs publications. Les serveurs et les actifs sont corrigés assez rapidement, avec 39 % des répondants les corrigeant dans les 24 heures.
- **La prévention est une priorité.** En moyenne, les équipes informatiques consacrent près de la moitié de leur temps (45 %) à la prévention, puis 30 % sont consacrés à la détection et les 25 % restants à la réponse.
- **Les responsables informatiques se tiennent régulièrement informés sur l'évolution de la cybersécurité.** La majorité (72 %) déclare être, avec leurs équipes, à jour ou en avance sur les menaces de cybersécurité. Seulement 11 % pensent qu'ils sont nettement en retard.

L'amélioration de la cybersécurité nécessite des ressources humaines, lesquelles font cruellement défaut

- **Il existe un besoin urgent en matière de traque des menaces dirigée par des experts.** 48 % des personnes interrogées ont déjà intégré cette activité dans leurs procédures de sécurité et 48 % supplémentaires prévoient de la mettre en œuvre d'ici un an.
- **La pénurie de compétences en cybersécurité impacte directement la mise œuvre d'une protection efficace.** Plus d'un quart (27 %) des responsables ont déclaré que leur capacité à trouver et à retenir des professionnels de la sécurité qualifiés était le plus grand défi dans la mise en place d'une stratégie de cybersécurité, tandis que 54 % affirment qu'il s'agit, pour eux, d'un défi majeur.

Les entreprises changent leurs façons de mettre en œuvre la sécurité

- **L'externalisation de la sécurité informatique évolue rapidement.** 65 % sous-traitent aujourd'hui tout ou partie de leurs activités de cybersécurité. Et on estime que ce pourcentage devrait passer à 72 % d'ici 2022. Le pourcentage d'entreprises qui utilisent exclusivement du personnel interne diminuera de 34 % à 26 %.
- **L'amélioration de l'efficacité opérationnelle est une priorité majeure.** Quatre personnes interrogées sur dix (39 %) pensent qu'améliorer l'efficacité et l'évolutivité des opérations est l'une des grandes priorités cette année.

Les victimes de ransomware ont des comportements et des attitudes qui diffèrent de celles n'ayant pas été touchées

- **Les victimes de ransomware sont plus exposées aux infections provenant de tiers.** 29 % des entreprises touchées par un ransomware au cours de l'année passée avaient permis à 5 fournisseurs, voire plus, de se connecter directement à leur réseau, contre seulement 13 % pour celles qui n'ont pas été touchées.
- **Les ransomwares érodent la confiance des professionnels.** Les responsables informatiques dont les entreprises ont été touchées par un ransomware sont près de trois fois plus susceptibles de se sentir « nettement en retard » sur les cybermenaces que ceux dont l'entreprise n'a pas été ciblée (17 % contre 6 %).
- **Être pris pour cible accélère la mise en œuvre de la traque des menaces dirigée par des experts.** 43 % des entreprises victimes d'un ransomware prévoient de mettre en œuvre cette activité dans les 6 mois, contre 33 % pour celles qui n'ont pas subi d'attaque.
- **Les victimes ont découvert l'importance d'avoir des professionnels de la cybersécurité qualifiés.** Plus d'un tiers (35 %) des victimes de ransomware ont déclaré que le recrutement et la rétention de professionnels qualifiés étaient leur plus grand défi en matière de cybersécurité, contre seulement 19 % pour les entreprises qui n'ont pas été touchées.

Les équipes IT progressent dans de nombreux domaines

Commençons par une bonne nouvelle : Les équipes informatiques maîtrisent de nombreux aspects de la cybersécurité. Ils parviennent à mener de front tous leurs projets et, ce faisant, à protéger leurs entreprises contre une multitude de menaces.

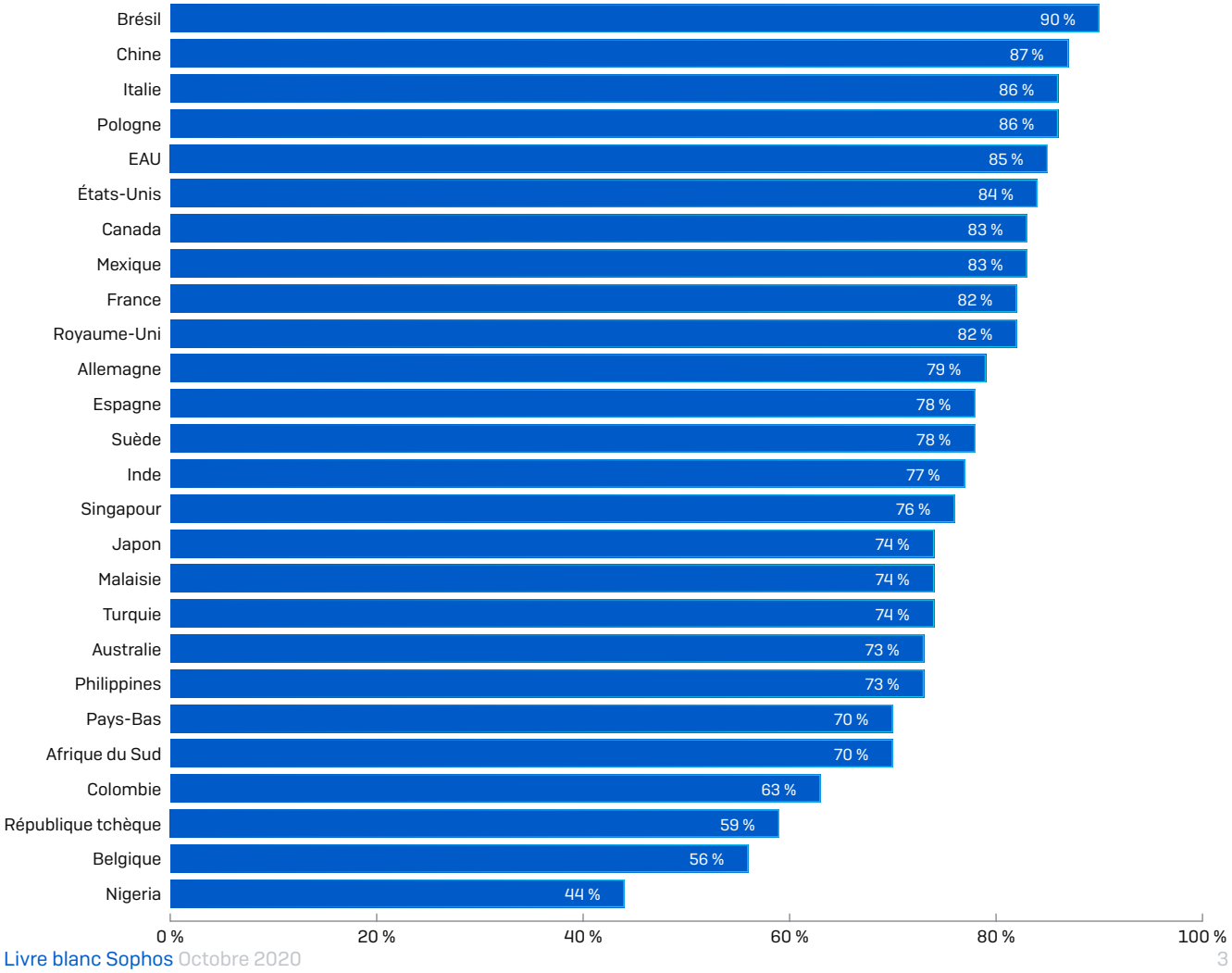
Les équipes IT sont au top au niveau de l'installation des correctifs

« Patchez au plus tôt. Patchez régulièrement. » est un mantra familier des experts en sécurité, et les équipes informatiques y attachent une grande importance. Les répondants sont conscients de la nécessité d'appliquer rapidement les correctifs ; beaucoup d'entre eux le faisant dans les 24 heures suivant la publication, et les 3/4 dans la semaine. Les serveurs et les ressources connectées à Internet sont corrigés assez rapidement : 39 % des répondants les corrigent dans les 24 heures.

	PATCHÉS SOUS 24 HEURES	PATCHÉS SOUS UNE SEMAINE	PATCHÉS SOUS UN MOIS
Postes	36 %	41 %	14 %
Serveurs	39 %	38 %	14 %
Applications	36 %	40 %	15 %
Ressources connectées à Internet	39 %	38 %	14 %

Cependant, 22 % admettent qu'il leur faut plus d'une semaine pour appliquer les correctifs ; les personnes interrogées au Nigeria, en Belgique et en République tchèque étant celles qui mettent le plus de temps à les appliquer.

Pourcentage de répondants qui patchent les postes de travail dans la semaine suivant leur publication

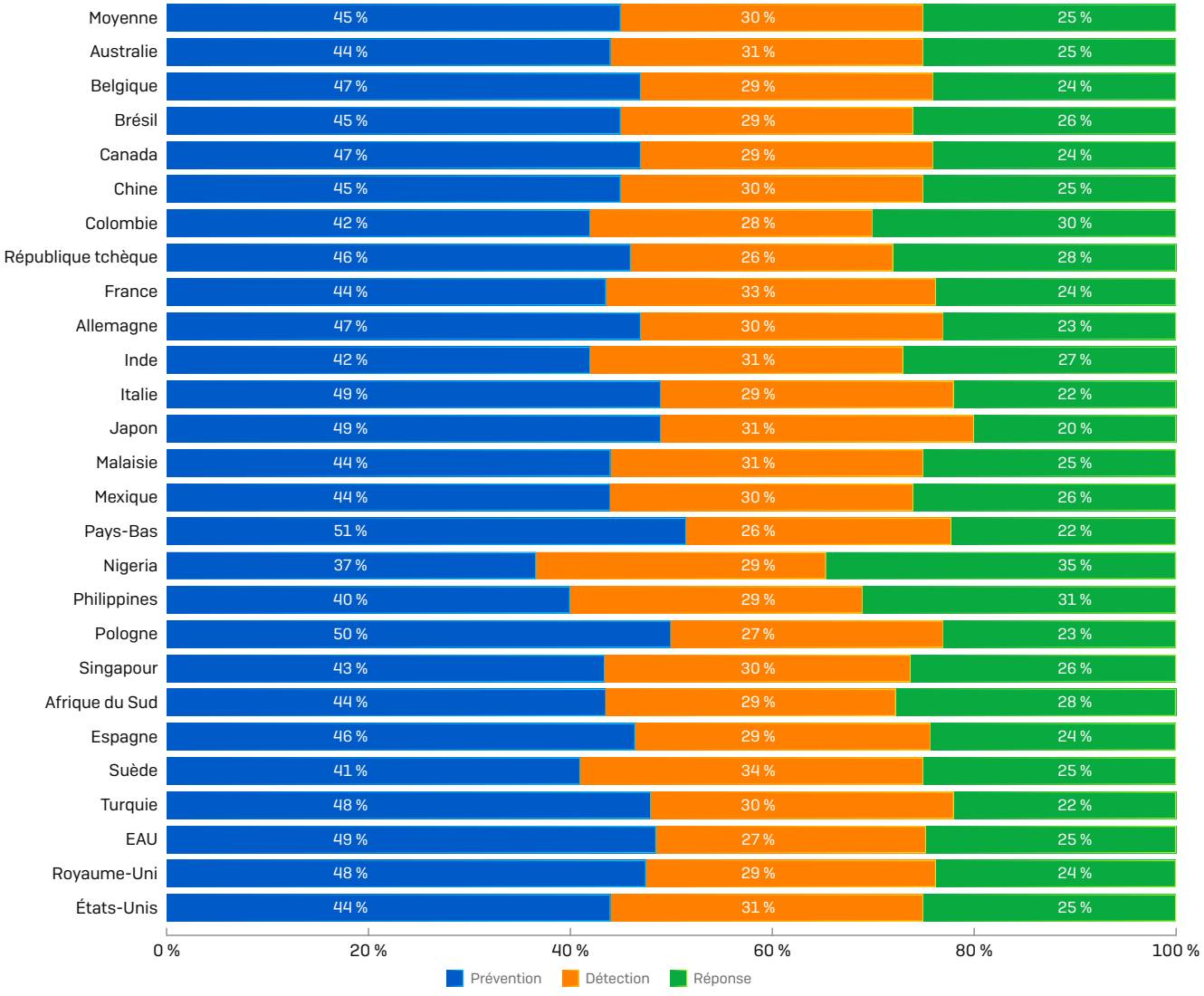


Priorité à la prévention

En moyenne, les équipes informatiques consacrent près de la moitié de leur temps (45 %) à la prévention, puis 30 % sont consacrés à la détection et les 25 % restants à la réponse. Les données ont révélé quelques variations géographiques parmi les pays étudiés : les équipes informatiques aux Pays-Bas déclarent consacrer le plus de temps à la prévention (51 %), les équipes suédoises passent le plus de temps à la détection (34 %) et les entreprises nigérianes déclarent le plus grand pourcentage de temps consacré à la réponse (35 %).

Bien que l'équilibre entre la prévention et la détection soit une approche sensée de la cybersécurité, le fait de consacrer un temps considérable à la réponse suggère généralement que les incidents ne sont pas bloqués. Un temps élevé consacré à la réponse indique que les entreprises connaissent un grand nombre d'incidents ou que ceux-ci ne sont détectés qu'à un stade tardif, ou une combinaison des deux.

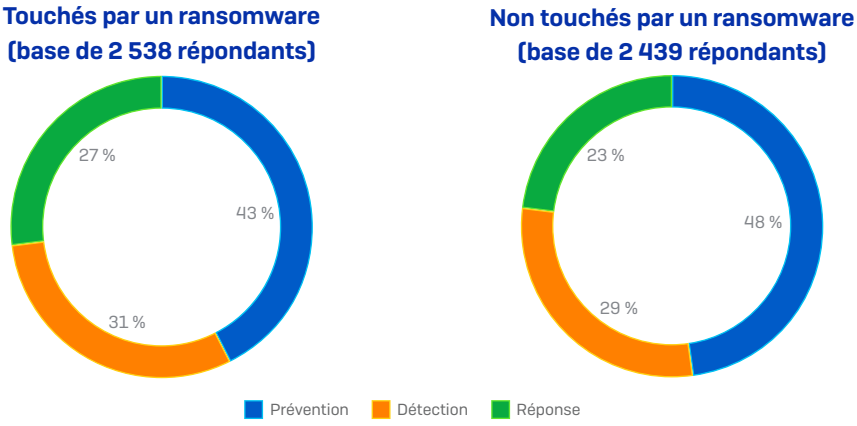
Répartition du temps entre prévention, détection et réponse



En raison des arrondis, il arrive que la somme des totaux ne soit pas égale à 100 %.

Les victimes de ransomware consacrent moins de temps à la prévention et plus de temps à la réponse

51 % des répondants ont admis que leur entreprise avait été touchée par un ransomware au cours des douze derniers mois. Ces entreprises se concentraient davantage sur la détection et la réponse que celles qui n'ont pas été victimes d'un ransomware. À l'inverse, les entreprises qui n'ont pas été touchées consacraient plus de temps à la prévention que celles qui en ont été victimes.



Il se peut que cette attention accrue portée à la prévention ait aidé les entreprises qui n'ont pas été touchées à prévenir les attaques : pour obtenir les meilleures défenses il faut mettre en œuvre la meilleure protection. En même temps, les victimes de ransomware peuvent être plus attentives à la nature complexe des attaques avancées et donc consacrer plus de ressources à la détection des signes avant-coureurs d'une attaque imminente et à leur réponse.

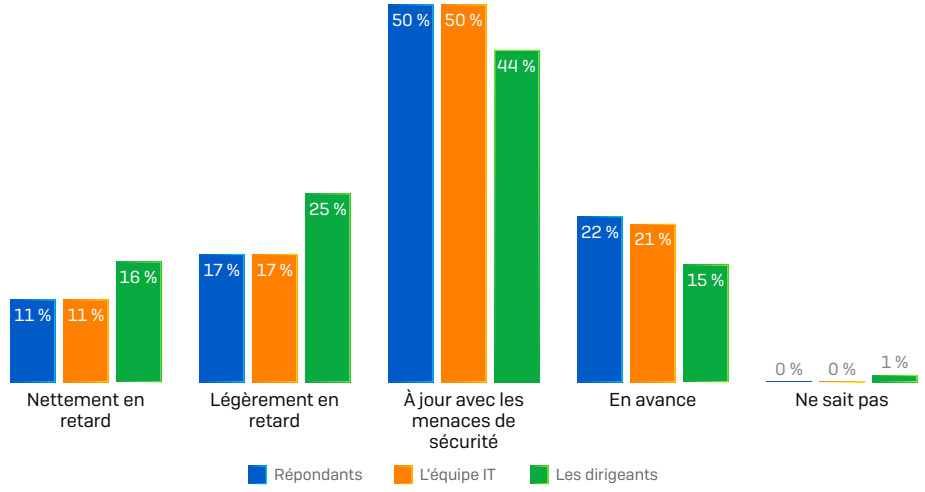
Pour savoir comment identifier précocement si vous êtes la cible d'une attaque de ransomware, consultez l'article des SophosLabs '5 signes qui indiquent que vous êtes la cible d'une attaque de ransomware'.

Les responsables IT se tiennent régulièrement informés sur l'évolution de la cybersécurité

Malgré l'évolution rapide des cybermenaces, les professionnels de l'informatique pensent qu'ils parviennent à se tenir informés sur les nouvelles tendances. La majorité des responsables informatiques (72 %) déclarent être, avec leurs équipes, à jour ou en avance sur les cybermenaces. Sur les 28 % de responsables qui se sentent en retard, 17 % estiment qu'ils sont seulement un peu en retard et 11 % qu'ils sont nettement en retard.

Ces chiffres masquent des variations géographiques notables : les répondants de Pologne, du Mexique et de Turquie sont les plus susceptibles de dire qu'ils se sentent en avance sur les cybermenaces (39 %, 34 % et 31 % respectivement), tandis que ceux du Nigeria (60 %), de Suède (57 %) et d'Allemagne (49 %) sont les plus susceptibles de dire qu'ils sont en retard. Il convient de noter que ces données sont les perceptions des répondants (et qu'il y a donc probablement un impact culturel) et non une mesure de l'état réel des entreprises.

Dans quelle mesure les répondants pensent-ils que les membres de leur entreprise sont à jour en matière de cybersécurité



Si les responsables informatiques sont globalement convaincus qu'eux-mêmes et leur équipe sont à jour, 41 % d'entre eux estiment que leurs dirigeants sont en retard (25 % légèrement en retard, 16 % très en retard). Cet écart est compréhensible à bien des égards (les dirigeants sont rarement spécialisés dans la cybersécurité), mais il met en évidence le défi que doivent relever les équipes informatiques pour leur faire comprendre les risques de cybersécurité et les investissements durables à engager.

Les attaques de ransomware entament la confiance des professionnels

En analysant minutieusement les données, nous constatons que les attaques de ransomware entament considérablement la confiance des responsables informatiques et de leurs équipes, au-delà de toute répercussion sur l'activité de l'entreprise.

Près de trois fois plus de responsables IT dont l'entreprise a été touchée par un ransomware au cours de l'année passée estiment qu'ils ont un « retard important » sur les cybermenaces, par rapport à ceux dont l'entreprise n'a pas été touchée (17 % contre 6 %). Cette baisse de confiance se répercute sur la perception qu'ont les responsables de leur équipe informatique et des dirigeants, comme l'illustre le tableau ci-dessous.

	NETTEMENT EN RETARD SUR LES CYBERMENACES (%)	À JOUR SUR LES CYBERMENACES (%)
Responsables IT (répondants)		
Touchés par un ransomware	17 %	43 %
Non touchés par un ransomware	6 %	57 %
Équipes IT (perception des répondants)		
Touchés par un ransomware	15 %	43 %
Non touchés par un ransomware	6 %	58 %
Dirigeants (perception des répondants)		
Touchés par un ransomware	20 %	39 %
Non touchés par un ransomware	11 %	49 %

Là encore, il est important de rappeler que ces réponses sont la perception du répondant plutôt qu'une mesure de la réalité. Il se peut que le fait d'être touché par un ransomware les rappelle à la réalité et que, grâce à leur expérience, les victimes de ransomware aient une bien meilleure compréhension de la situation.

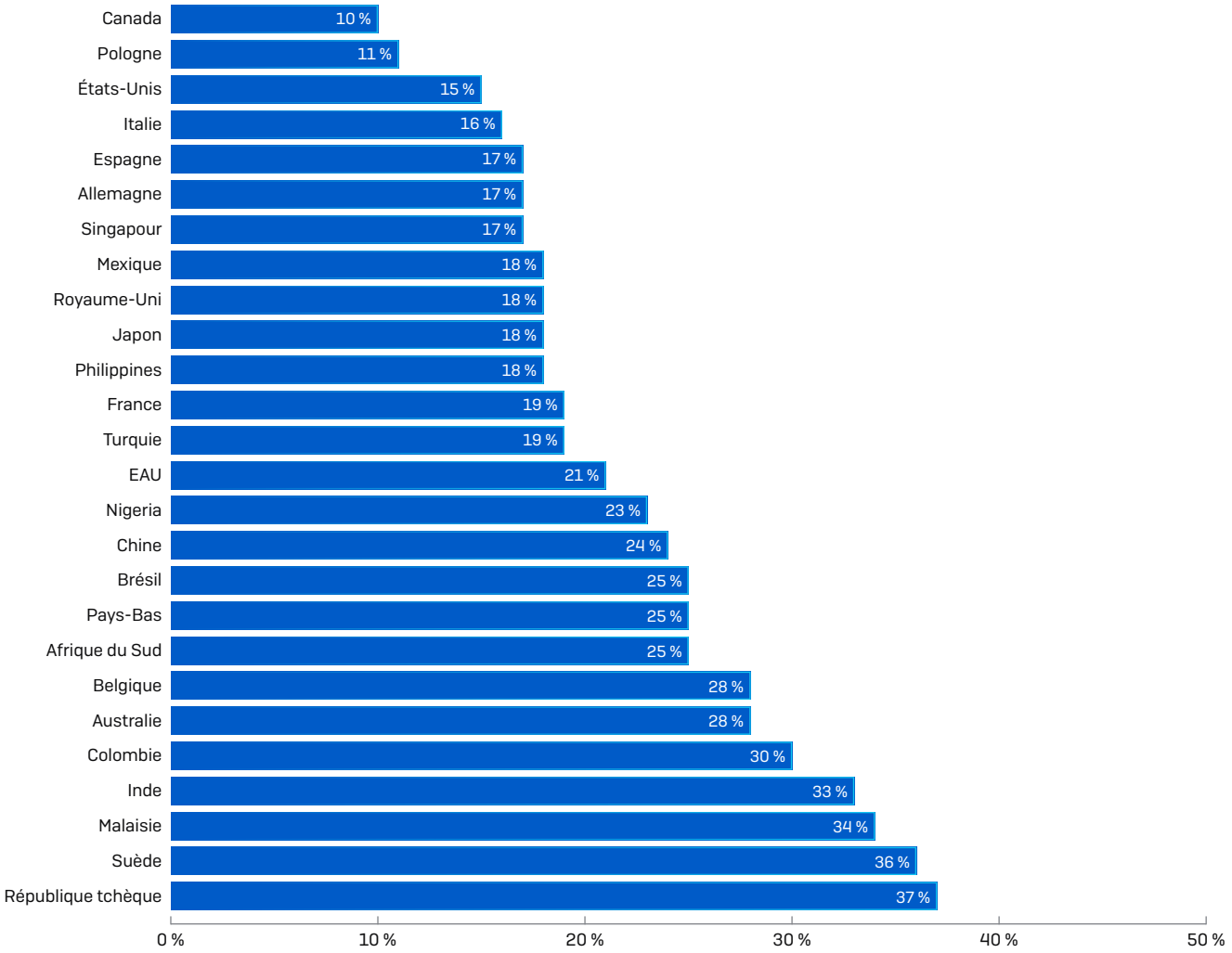
L'amélioration de la cybersécurité nécessite des ressources humaines, lesquelles font cruellement défaut

Bien que les équipes informatiques remportent de nombreuses batailles, la guerre est loin d'être gagnée. Malgré les meilleurs efforts des responsables informatiques et de leurs équipes, les cybermenaces restent un défi permanent. À tel point qu'un peu plus de la moitié des répondants (51 %) ont déclaré que réduire le risque de cyberattaque était une priorité pour les douze prochains mois. Les raisons semblent évidentes lorsqu'on examine en détail la grande variété de défis de sécurité auxquels les équipes sont confrontées.

En effet, elles font face à un déluge de cyberattaques, avec des menaces venant de toutes parts et ayant des cibles variées. Comme nous l'avons vu dans une précédente enquête, 51 % des répondants ont été touchés par un ransomware l'année dernière et les cybercriminels ont réussi à chiffrer les données dans 73 % de ces attaques*. La sécurité du Cloud est également un défi : 70 % des entreprises hébergeant des données et des ressources dans le Cloud public ont connu un incident de sécurité au cours de l'année passée.

Un autre défi auquel les équipes sont confrontées est la sécurisation des fournisseurs tiers qui peuvent se connecter directement à leur réseau, comme les services comptables ou les prestataires de services informatiques. En moyenne, les répondants déclarent permettre à 3 fournisseurs de se connecter à leurs systèmes. Cependant, un répondant sur cinq (21 %) (et ce chiffre passe à un tiers, voire plus, en République tchèque, en Inde, en Malaisie et en Suède) permet à 5 fournisseurs ou plus de se connecter. À l'inverse, au Canada et en Pologne, seul un répondant sur dix a déclaré avoir 5 fournisseurs ou plus avec un accès à distance.

Pourcentage d'entreprises avec 5 fournisseurs ou plus qui peuvent se connecter directement au réseau



Permettre à des fournisseurs tiers de se connecter au réseau offre des bénéfices commerciaux certains, mais cela introduit aussi un risque de sécurité. Plus le nombre de fournisseurs pouvant se connecter est élevé, plus les équipes informatiques sont face à des difficultés et à une charge de travail importante.

Les victimes de ransomwares sont plus exposées aux infections provenant de tiers

Parmi les entreprises touchées par des ransomwares au cours de l'année passée, 29 % avaient permis à 5 fournisseurs, voire plus, de se connecter directement à leur réseau, contre seulement 13 % pour celles qui n'ont pas été touchées. Les fournisseurs tiers ont été utilisés comme méthode d'entrée pour 9 % des victimes, ce qui en fait clairement un vecteur d'attaque majeur.

S'il existe de nombreuses raisons commerciales valables de permettre à des sociétés extérieures de se connecter à votre réseau, il ressort de notre enquête qu'il est crucial de sécuriser votre chaîne d'approvisionnement. Être doté d'une cybersécurité forte doit être un critère essentiel pour quiconque cherche à se connecter à votre réseau.

Il existe un besoin urgent en matière de traque des menaces dirigée par des experts

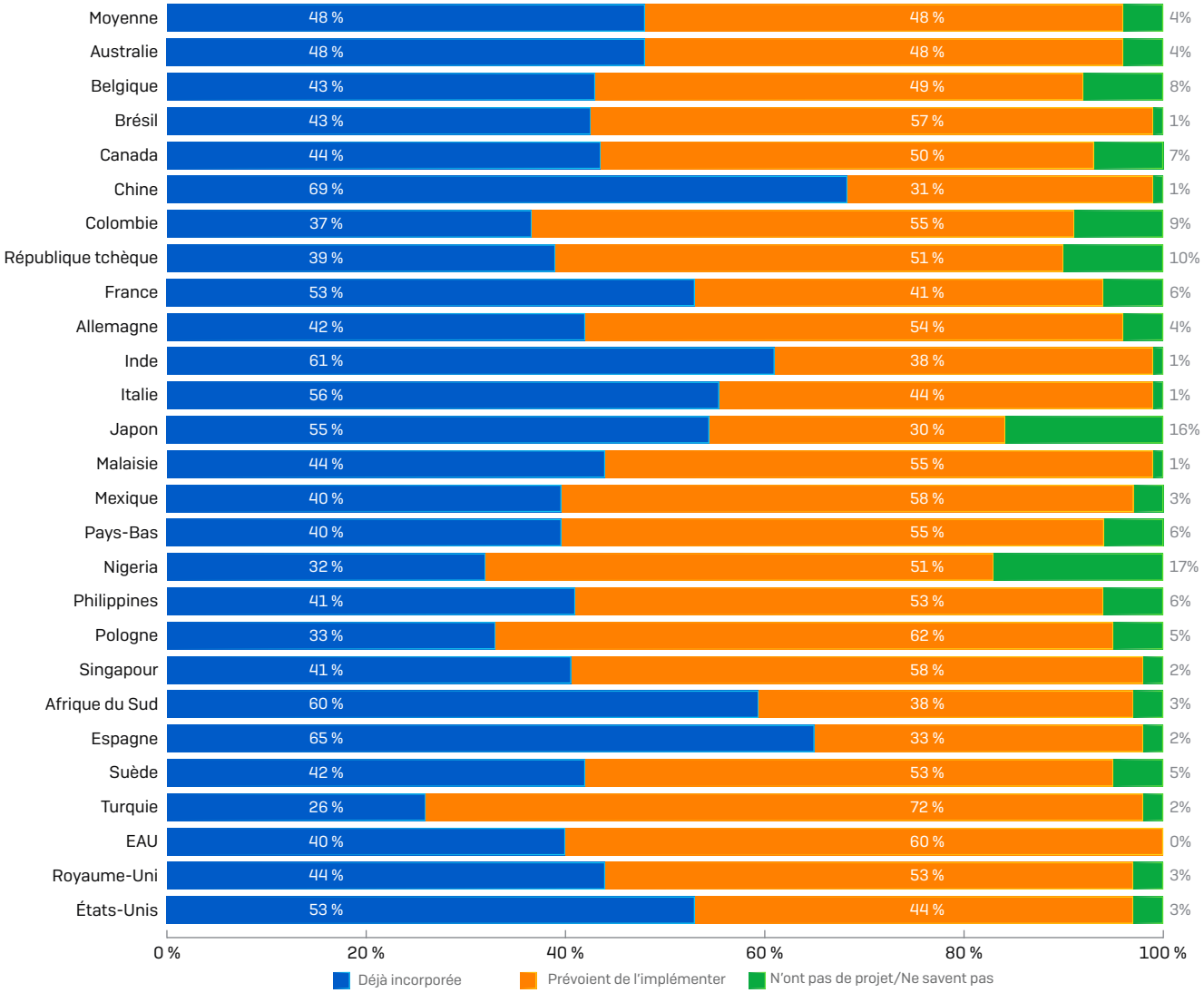
Les cyberattaques les plus dévastatrices sont généralement celles qui sont pilotées manuellement, et qui vont exploiter des outils et des processus légitimes tels que PowerShell. Le piratage en temps réel permet aux attaquants de modifier leurs tactiques, techniques et procédures (TTP) au fur et à mesure pour leur permettre de contourner les produits et protocoles de sécurité. Une fois à l'intérieur du réseau de leur victime, ils peuvent se déplacer latéralement, exfiltrer des données, installer des logiciels malveillants ou des portes dérobées en vue de futures attaques, ou encore déployer un ransomware.

Si les technologies ont un rôle important à jouer, en particulier les technologies automatisées intelligentes, la présence d'opérateurs spécialisés reste indispensable. Pour mettre fin aux attaques menées par des experts, il faut une traque des menaces menée par des experts.

Pratiquement tous les répondants reconnaissent la nécessité de cette approche : 48 % intègrent déjà la traque des menaces dans leurs procédures de sécurité afin d'identifier les activités frauduleuses qui pourraient ne pas être détectées par les outils de sécurité (par exemple SIEM, protection Endpoint, pare-feu, etc.). 48 % prévoient de l'implémenter. Les répondants sont également conscients de l'urgence de déployer cette activité. La quasi-totalité (99,6 %) des répondants qui prévoient de l'implémenter souhaite le faire dans l'année à venir.

La pratique de la traque des menaces dirigée par des experts varie considérablement selon les pays. 69 % des répondants en Chine l'ont déjà mise en œuvre, suivis de près par l'Espagne (65 %), l'Inde (61 %) et l'Afrique du Sud (60 %). À l'inverse, la Turquie est le pays qui a été le plus lent à adopter cette activité, avec seulement 26 % des répondants l'ayant déjà implémenté, le Nigeria (32 %) et la Pologne (33 %) le devançant légèrement.

Projet d'incorporer la traque des menaces dirigée par des experts

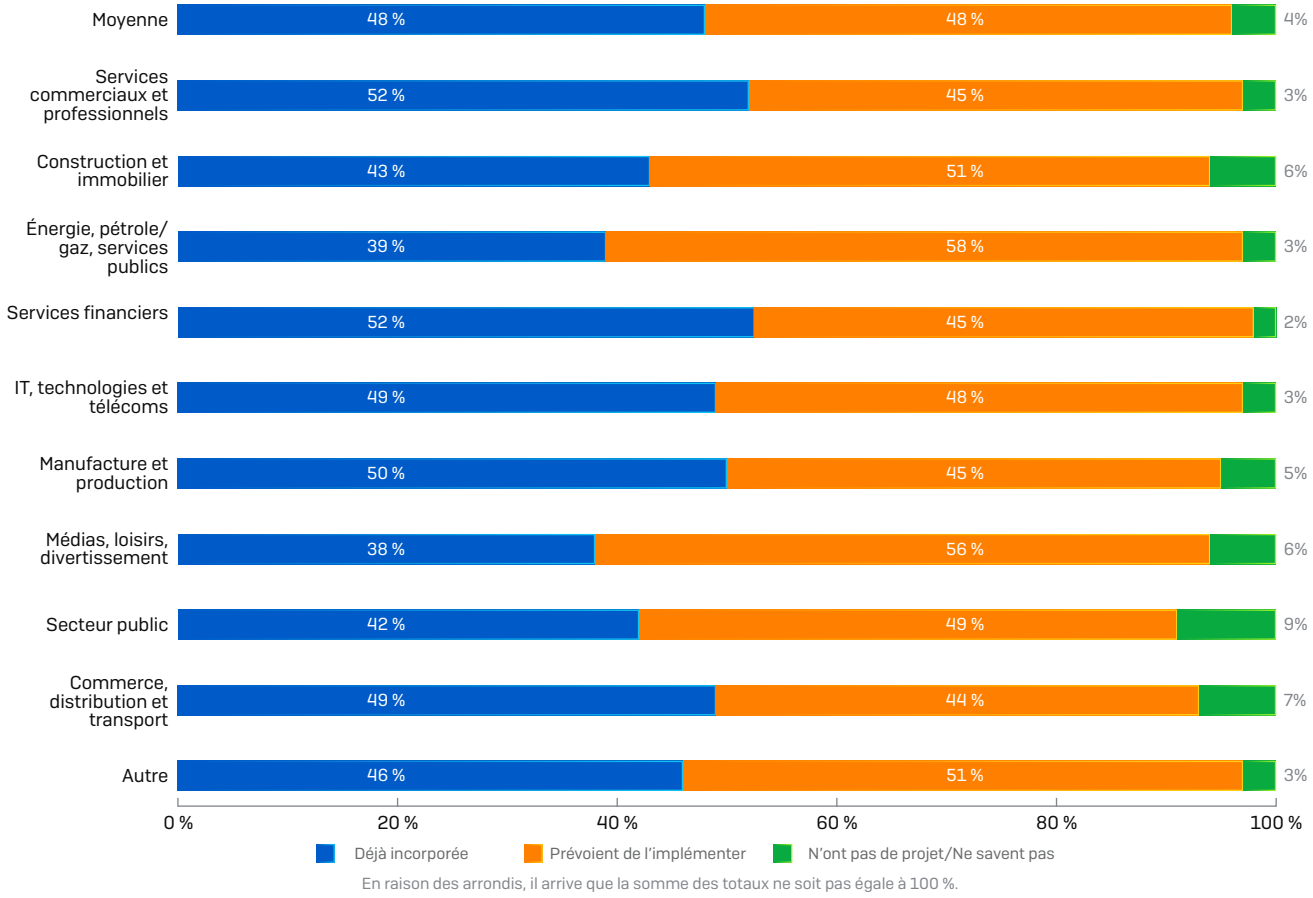


En raison des arrondis, il arrive que la somme des totaux ne soit pas égale à 100 %.

L'enquête a également révélé différents niveaux de préparation en fonction du secteur industriel. Les services commerciaux et professionnels et les services financiers sont ceux qui ont le plus adopté cette approche, 52 % des répondants de chaque secteur l'utilisant déjà.

En revanche, les répondants des secteurs des médias, des loisirs et du divertissement (38 %) ainsi que de l'énergie, du pétrole/gaz et des services publics (39 %) ont été moins nombreux à déclarer cette pratique. Étant donné que le secteur de l'énergie est une cible potentielle d'attaques par des États-nations, sa vulnérabilité est préoccupante.

Projet d'incorporer la traque des menaces dirigée par des experts selon les secteurs industriels

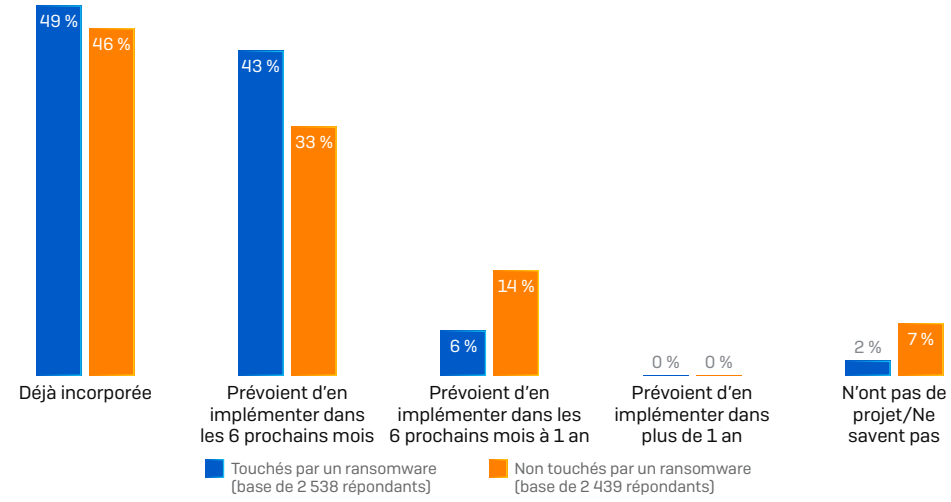


En raison des arrondis, il arrive que la somme des totaux ne soit pas égale à 100 %.

Être pris pour cible par un ransomware accélère la mise en œuvre de la traque des menaces dirigée par des experts

Le fait d'être touché par un ransomware a peu d'impact global sur le projet de l'entreprise d'intégrer la traque des menaces dirigée par des experts, mais elle accélère son implémentation. 43 % des entreprises victimes prévoient de la mettre en œuvre dans les six mois, contre 33 % pour celles qui n'ont pas subi d'attaque. Ces données suggèrent que les victimes de ransomware redoublent d'efforts pour éviter qu'un incident ne se reproduise.

Impact d'une attaque récente de ransomware sur la mise en œuvre de la traque des menaces dirigée par des experts



La pénurie de compétences en cybersécurité impacte directement la mise œuvre d'une protection efficace

81 % des personnes interrogées ont déclaré que trouver et retenir des professionnels de la cybersécurité compétents est un défi majeur pour assurer la sécurité informatique : 54 % ont déclaré qu'il s'agissait d'un défi important, tandis que plus d'un quart (27 %) ont déclaré que c'était leur plus grand défi.

Tous les pays ont fait état de difficultés à recruter du personnel informatique qualifié. En Italie (94 %), en Inde (93 %), au Brésil et en Colombie (92 % chacun), plus de neuf personnes interrogées sur dix ont déclaré que ces difficultés étaient un obstacle majeur à la protection de l'entreprise contre les cybermenaces.

Même en Afrique du Sud, le pays le moins susceptible de déclarer que le recrutement du personnel qualifié est un défi, plus de six personnes interrogées sur dix (62 %) déclarent qu'il s'agit d'un problème majeur.

Dans quelle mesure le recrutement et la rétention de professionnels compétents en cybersécurité constituent-ils un défi pour la capacité de votre organisation à assurer la sécurité informatique ?

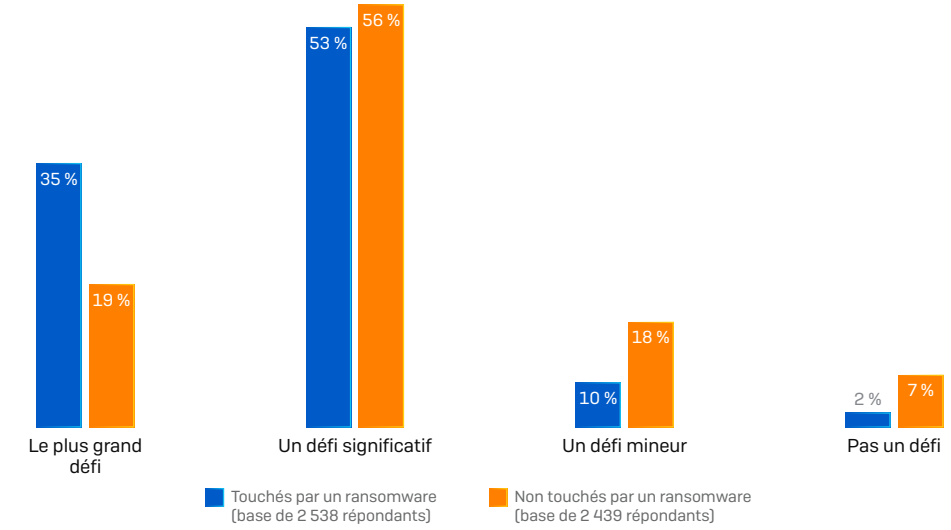
PAYS	C'EST NOTRE PLUS GRAND DÉFI	C'EST UN DÉFI IMPORTANT, MAIS PAS LE PLUS IMPORTANT	C'EST UN DÉFI MINEUR	CE N'EST PAS UN DÉFI	NE SAIT PAS
Moyenne	27 %	54 %	14 %	4 %	0 %
Australie	17 %	57 %	22 %	5 %	0 %
Belgique	24 %	52 %	24 %	0 %	0 %
Brésil	45 %	47 %	6 %	3 %	1 %
Canada	19 %	55 %	18 %	7 %	2 %
Chine	24 %	54 %	18 %	4 %	0 %
Colombie	29 %	63 %	8 %	1 %	0 %
République tchèque	33 %	47 %	18 %	1 %	1 %
France	23 %	62 %	11 %	4 %	0 %
Allemagne	19 %	63 %	14 %	5 %	0 %
Inde	58 %	35 %	6 %	1 %	0 %
Italie	28 %	67 %	5 %	2 %	0 %
Japon	35 %	44 %	17 %	4 %	1 %
Malaisie	26 %	54 %	16 %	4 %	0 %
Mexique	27 %	62 %	6 %	6 %	0 %
Pays-Bas	26 %	49 %	25 %	0 %	1 %
Nigeria	32 %	51 %	16 %	1 %	0 %
Philippines	40 %	49 %	8 %	2 %	1 %
Pologne	9 %	59 %	20 %	12 %	0 %
Singapour	17 %	72 %	10 %	2 %	0 %
Afrique du Sud	22 %	40 %	19 %	19 %	0 %
Espagne	17 %	58 %	17 %	8 %	1 %
Suède	44 %	41 %	13 %	1 %	1 %
Turquie	30 %	52 %	9 %	8 %	1 %
EAU	22 %	62 %	15 %	1 %	0 %
Royaume-Uni	14 %	64 %	20 %	2 %	0 %
États-Unis	26 %	49 %	17 %	8 %	0 %

Les victimes de ransomware ont découvert à leurs dépens l'importance d'avoir des professionnels de la cybersécurité qualifiés

Être victime d'une cyberattaque a un impact majeur sur l'attitude à l'égard du personnel de cybersécurité. Plus d'un tiers (35 %) des répondants victimes de ransomware l'année passée ont déclaré que le recrutement et la rétention de professionnels qualifiés constituaient leur plus grand défi en matière de cybersécurité, et 53 % ont déclaré qu'il s'agissait d'un défi majeur.

Inversement, parmi les entreprises qui n'ont pas été victimes d'un ransomware, seuls 19 % ont déclaré que le recrutement et la rétention de personnel qualifié étaient leur plus grand défi, soit une différence de 16 %.

Le recrutement et la rétention de professionnels compétents en cybersécurité constituent un défi pour la capacité de l'entreprise à assurer la sécurité informatique



Il est probable que plusieurs facteurs expliquent ces différentes attitudes. Premièrement, les conséquences liées au manque de compétences sont encore fraîches dans l'esprit de ceux qui ont récemment été attaqués et ont subi des pertes financières, opérationnelles et réputationnelles lourdes.

De plus, les victimes de ransomware auront invariablement analysé la source de l'attaque et identifié les failles dans leurs défenses ayant permis aux attaquants de pénétrer dans leur réseau et d'accéder à leurs données. Nombre d'entre eux auront probablement identifié le manque d'expertise humaine comme un facteur de vulnérabilité.

Le recrutement est la priorité nº 1 des responsables IT

Face à cette pénurie de compétences, les responsables informatiques font du recrutement et de la rétention de personnel qualifié leur priorité nº 1. Au total, 55 % des personnes interrogées concentreront leurs efforts dans ce domaine dans les douze prochains mois, plaçant la réduction du risque de cyberattaque en seconde position sur la liste des priorités. (Remarque : pour cette question, les répondants pouvaient sélectionner plusieurs réponses.)

Les entreprises modifient la façon dont elles assurent la cybersécurité

Les professionnels de l'informatique ne seront probablement pas surpris par l'importance du défi que représente le recrutement du personnel. Il s'agit en effet d'un problème de longue date et, s'il est encourageant de constater que les responsables en font leur priorité, l'ampleur du défi laisse penser qu'il n'existe pas de solution miracle.

De ce point de vue, les changements apportés par les responsables informatiques à la manière dont la cybersécurité est mise en œuvre et leur volonté d'améliorer l'efficacité et l'évolutivité des opérations peuvent être considérés comme une réponse directe au défi de recrutement du personnel.

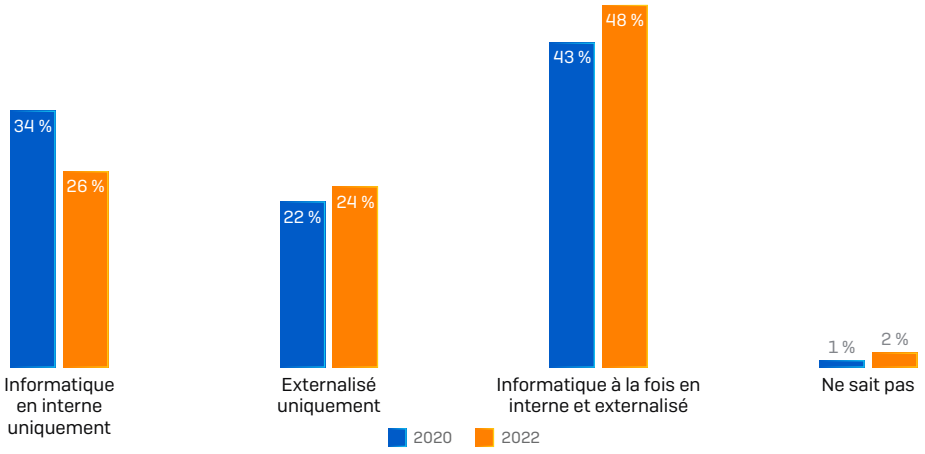
L'externalisation est en croissance rapide

L'externalisation de la cybersécurité permet aux entreprises de bénéficier de l'expertise de professionnels de la sécurité sans avoir à les embaucher. Elle permet aussi souvent d'accéder à des niveaux de compétence plus élevés que ceux dont disposent les entreprises en interne, grâce à la capacité des prestataires de services à entretenir et à développer des compétences spécialisées.

L'externalisation de la sécurité informatique est déjà la norme, avec 65 % des répondants y faisant appel : 43 % utilisent une combinaison de services internes et externes, tandis que 22 % externalisent entièrement leur cybersécurité. L'enquête a révélé des variations géographiques. Parmi les pays qui externalisent le plus, on trouve la Chine (76 %), les Émirats arabes unis (74 %), ainsi que la Malaisie et Singapour (73 % chacun), où environ 3/4 des répondants font appel à des prestataires de service. À l'opposé, en Belgique (52 %), en France (54 %) et au Nigeria (54 %), seule un peu plus de la moitié des répondants y font actuellement appel.

La tendance mondiale est à l'augmentation de l'externalisation au cours des deux prochaines années, et l'on estime que l'on devrait passer de 65 % aujourd'hui à près de 3/4 (72 %) en 2022. Le plus grand changement réside dans le pourcentage d'entreprises qui n'externalisent pas du tout leur cybersécurité : il devrait diminuer de 34 % à 26 %. Il y aura des augmentations à la fois dans le pourcentage d'entreprises qui externalisent entièrement leur cybersécurité et dans celles qui utilisent une combinaison d'expertise interne et externe.

Comment les entreprises assurent la sécurité informatique



Ces chiffres mondiaux masquent quelques variations géographiques intéressantes :

- Les personnes interrogées en Espagne et en Inde prévoient d'augmenter la gestion de la sécurité informatique uniquement en interne. Bien que les chiffres soient relativement faibles (de 34 % à 37 % en Espagne et de 33 % à 34 % en Inde), il est intéressant de constater qu'elles prévoient d'aller à rebours de la tendance mondiale.
- Aux Philippines, près de la moitié des répondants (48 %) prévoient d'externaliser entièrement la sécurité informatique en 2022, soit un bond énorme par rapport aux 30 % d'aujourd'hui. Les autres pays qui prévoient d'externaliser entièrement leur cybersécurité sont la République tchèque, le Nigeria et la Suède (35 % chacun) et l'Australie (34 %)
- Plus de six répondants sur dix prévoient de mener une approche mixte interne/externe en Chine (67 %) et au Mexique (62 %).

Les responsables IT s'attachent à améliorer l'efficacité et l'évolutivité

Une autre réponse à la pénurie de compétences est d'exploiter au maximum celles que vous possédez déjà. Quatre personnes interrogées sur dix (39 %) pensent qu'améliorer l'efficacité et l'évolutivité des opérations est l'une des grandes priorités de cette année. Cette moyenne a été baissée par les répondants en Europe et au Japon, mais pour plus de la moitié des répondants en Chine, Malaisie et Afrique du Sud il s'agit d'une priorité fondamentale.

Conclusion

Ces informations, recueillies auprès de 5 000 responsables informatiques dans 26 pays, ont mis en lumière les défis auxquels sont confrontées les équipes informatiques lorsqu'il s'agit de gérer et d'assurer la cybersécurité. Alors que les équipes remportent de nombreuses batailles, notamment de bien gérer les correctifs et de se tenir informé de l'évolution de la cybersécurité, la guerre est loin d'être gagnée. Les professionnels de l'informatique sont confrontés à des défis sur de nombreux fronts : ransomwares, sécurité du Cloud, ou encore gestion des fournisseurs tiers qui peuvent se connecter au réseau.

Face à la croissance des attaques pilotées manuellement, la plupart des entreprises se tournent vers la traque des menaces dirigée par des experts : d'ici à la fin de 2020, 95 % des personnes interrogées espèrent la mettre en œuvre d'une manière ou d'une autre. En parallèle, les difficultés de recrutement et de rétention des professionnels de la cybersécurité constituent un facteur limitant pour la grande majorité des entreprises. Celles qui ont récemment été victimes de ransomware sont particulièrement préoccupées par les conséquences de cette pénurie de compétences sur leur capacité à assurer une cybersécurité efficace.

Il existe une corrélation évidente entre l'expérience vécue avec un ransomware et les comportements de l'équipe informatique. Les victimes de ransomware présentent un risque d'infection plus élevé via un fournisseur tiers que les autres entreprises, et elles consacrent aussi plus de temps à la remédiation, dénotant un nombre d'incidents plus important à traiter. Dans le même temps, leur expérience leur a permis de mieux comprendre l'importance de disposer de professionnels de la cybersécurité compétents, et de mettre en place plus rapidement la traque dirigée par des experts.

À la lumière de ces défis, il est encourageant de voir comment les équipes informatiques font évoluer leurs approches. Le recours à des experts externalisés devrait encore augmenter au cours des deux prochaines années, puisque près de 3/4 des entreprises externaliseront tout ou partie de leur cybersécurité d'ici 2022. L'accent est également mis sur l'amélioration de l'efficacité et de l'évolutivité des opérations dans de nombreuses régions du monde, afin de permettre aux équipes informatiques de faire plus avec les professionnels qualifiés dont elles disposent.

La cybersécurité ne connaît pas de répit. Il faut souligner l'effort considérable des équipes informatiques qui parviennent à maîtriser de nombreux aspects de la sécurité. Compte tenu de la pénurie actuelle de compétences en cybersécurité, les équipes informatiques devront trouver différents moyens d'étendre et d'améliorer leurs défenses face à l'évolution des menaces, et en particulier à l'augmentation des attaques pilotées manuellement.

Comment Sophos peut vous aider

Quelle que soit la manière dont vous souhaitez gérer votre cybersécurité, nous pouvons vous aider.

Traque des menaces dirigée par des experts 24/7

Avec Sophos Managed Threat Response (MTR), votre entreprise bénéficie de la protection 24 h/24 et 7 j/7 d'une équipe d'experts de haut niveau spécialisés dans la traque et la remédiation des menaces, qui les recherchent et les neutralisent de manière proactive en votre nom. Ces professionnels de la sécurité hautement qualifiés sont capables de détecter, et de stopper, les attaques manuelles avancées avant qu'elles ne puissent affecter votre entreprise.

Apprenez-en plus et découvrez le guide d'achat des services MDR.

Service de réponse aux incidents en temps réel

Toute entreprise confrontée à un incident actif peut déployer notre service **Rapid Response**. Notre équipe d'experts en réponse aux incidents identifiera et neutralisera rapidement la menace active. Qu'il s'agisse d'une infection, d'une compromission ou d'un accès non autorisé tentant de contourner vos contrôles de sécurité, nous avons déjà tout vu et tout stoppé avec succès.

En savoir plus

Outils avancés d'hygiène informatique et de traque des menaces

Si vous préférez traquer vous-même les menaces, Sophos EDR (Endpoint Detection and Response) vous donne les outils dont vous avez besoin pour les traquer et maintenir l'hygiène de vos opérations de sécurité informatique. Les puissantes capacités de recherche permettent à votre équipe d'identifier et de traiter de manière proactive les problèmes de sécurité et d'hygiène informatique, afin de renforcer votre protection.

Apprenez-en plus et essayez-le gratuitement.

Système de cybersécurité de nouvelle génération

Les entreprises qui déploient un système de cybersécurité Next-Gen Sophos font toutes état d'une réduction de 50 % des frais de gestion informatique. En déployant nos solutions Endpoint et Pare-feu de pointe et en administrant le tout depuis la plateforme Sophos Central, les équipes informatiques réduisent de moitié le temps passé à gérer la cybersécurité, tout en améliorant l'efficacité de leur sécurité.

Apprenez-en plus et découvrez tous nos témoignages client.

Travaux de recherche sur les ransomwares

Les SophosLabs et l'équipe Sophos MTR publient régulièrement leurs recherches sur les dernières techniques de ransomware sur le blog Sophos News.

* L'état des ransomwares 2020 Une enquête mondiale réalisée auprès de 5 000 responsables informatiques commandée par Sophos et menée par Vanson Bourne.

** L'état de la sécurité du Cloud 2020 Une enquête mondiale réalisée auprès de 3 521 responsables informatiques commandée par Sophos et menée par Vanson Bourne.

À propos de Vanson Bourne

*Vanson Bourne est un cabinet d'études de marché indépendant spécialisé dans le secteur des technologies. Sa réputation d'analyste solide et crédible repose sur des principes de recherche rigoureux et sur sa capacité à solliciter l'avis des décideurs de haut niveau dans les domaines techniques et commerciaux, dans tous les secteurs d'activité et sur l'ensemble des marchés dominants. Visitez leur site Web*www.vansonbourne.com

Équipe commerciale France
Tél. : 01 34 34 80 00
Email : info@sophos.fr

20-10-05 WPFR (DD)

SOPHOS