Rapport 2022

Trois étapes pour passer à un niveau supérieur de cybersécurité

kaspersky BRING ON THE FUTURE

EN SAVOIR PLUS : KASPERSKY.COM

Trois étapes pour passer à un niveau supérieur de cybersécurité

Une nouvelle étude menée auprès de 750 responsables de grandes entreprises met en évidence trois étapes pour être mieux préparé face à une cyberattaque.

La menace de la cybersécurité pèse à l'heure actuelle plus lourdement que jamais sur les entreprises. Les chercheurs dans le domaine de la technologie de l'institut Gartner déclarent que les nouveaux modèles de ransomwares sont à eux seuls le plus gros risque émergeant auquel doivent faire face les entreprises de nos jours, plus important que la pandémie et l'interruption de la chaîne d'approvisionnement.

Toutefois, une nouvelle étude effectuée par Kaspersky en collaboration avec Longitude, une société du Financial Times, montre que les entreprises ne sont pas préparées.

Moins d'une sur 10 est très bien préparée pour gérer des cyberattaques perpétrées par des

9 %	7 %	6 %
Professionnels de la cybercriminalité	**Pirates isolés**	**États**

L'étude a porté sur 750 responsables d'entreprises dans le monde entier pour examiner leur approche de la cybersécurité. Les personnes interrogées, qui représentent des entreprises dans de nombreuses régions et secteurs d'activité comportant au moins 1 000 employés, étaient celles qui connaissaient la stratégie de cybersécurité de leur société.

Entreprises non préparées pour les cyber-attaques

« La plupart des personnes ne sont pas préparées du tout », déclare Shawnee Delaney, PDG de **Vaillance Group**, spécialiste des menaces internes, basé aux États-Unis. « Tous les jours, quelque chose change : il apparaît de nouveaux virus plus dangereux, une nouvelle technique ou un nouveau mode opératoire. Il est impossible de tenir la cadence avec tous ces éléments, cela est épouvantable pour tout le monde. »

Delaney est davantage préparée que la moyenne, avec les informations d'identification de sécurité de son entreprise et ses antécédents au sein de la Defense Intelligence Agency, qui mène des opérations de renseignements clandestines dans le monde.

Selon l'étude de Kaspersky, la raison principale pour laquelle les entreprises ne sont pas préparées vient du fait qu'elles dépendent de technologies anciennes qui sont vulnérables aux menaces actuelles. Elles manquent également de ressources financières pour recruter ou consulter des professionnels compétents en matière de sécurité.

Le risque est réel, et les entreprises ne sont pas préparées. Que peuvent-elles faire ? L'étude de Kaspersky indique trois choses qu'il est possible de changer pour améliorer la sécurité.

Étape 1 :

Diversifier davantage les équipes de cybersécurité

La diversité et l'inclusion font partie des priorités des entreprises, en partie grâce à des mouvements comme #MeToo et Black Lives Matter. Il existe également une solide étude de cas à ce sujet. L'étude réalisée par le conseil en gestion McKinsey & Company montre que **les sociétés qui se situent dans le quartile supérieur pour la diversité des genres ont une probabilité supérieure à 25 % de présenter une rentabilité supérieure à la moyenne** par rapport à celles qui se trouvent dans le quartile inférieur.

62 %

Dans l'étude de Kaspersky, la plupart des entreprises (62 %) sont convaincues que la création d'une équipe de cybersécurité plus diverse et plus inclusive sera un élément important au cours des deux prochaines années.

Elles ont raison de se concentrer sur cela, car il reste encore un long chemin à accomplir. Les chiffres émanant du National Cyber Security Center, au Royaume-Uni, révèlent que **85% des professionnels travaillant dans le domaine de la cybersécurité sont des blancs, et 66 % sont des hommes**.

L'étude de Kaspersky montre que les équipes de cybersécurité ont tout à gagner en augmentant la diversité et l'inclusivité.

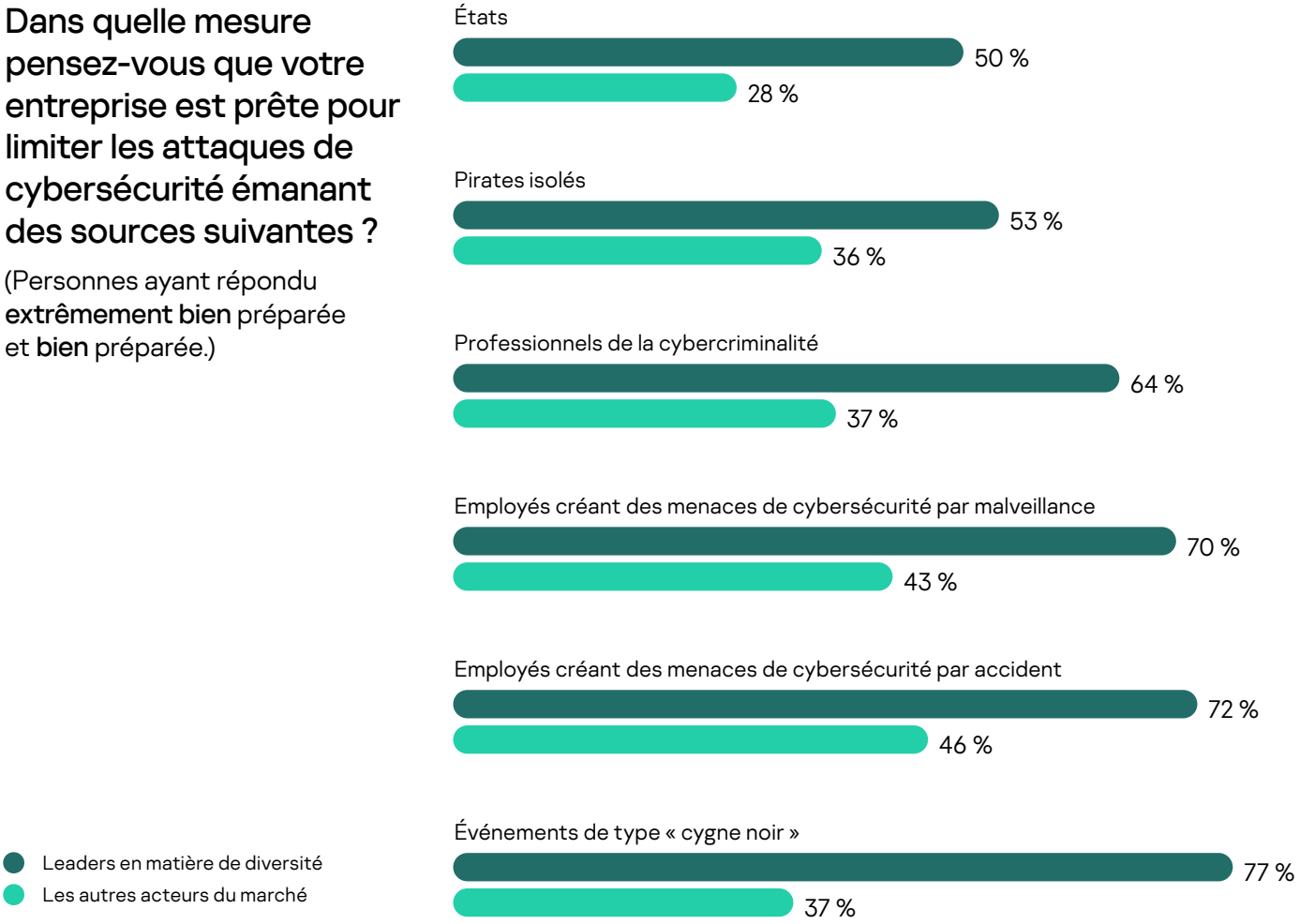
20 %

Une personne interrogée sur 5 est fermement convaincue que son entreprise améliore de manière active la diversité et l'inclusion dans ses équipes de cybersécurité.

Les données montrent que ce petit groupe, que Kaspersky appelle « Leaders en matière de diversité », est beaucoup mieux préparé pour faire face à diverses des attaques de cybersécurité.

Dans quelle mesure pensez-vous que votre entreprise est prête pour limiter les attaques de cybersécurité émanant des sources suivantes ?

(Personnes ayant répondu **extrêmement bien** préparée et **bien** préparée.)



Les Leaders en matière de diversité de Kaspersky ont également été plus rapides à tirer les leçons de la pandémie. Ils ont davantage tendance que les autres à planifier une crise majeure à travers une formation aux cyber-incidents du monde réel (68 % des Leaders en matière de diversité, contre 54 % pour les autres acteurs du marché).

« La diversité est un impératif stratégique pour tout le secteur. Nous savons qu'il s'agit non seulement de la meilleure chose à faire, mais également que le fait de faire appel à des groupes variés de personnes nous apporte une manière plus équilibrée de penser à la façon dont nous pouvons gérer le risque de cybersécurité. »

Darren Argyle, directeur de la stratégie du groupe en matière de risques de sécurité des informations, Standard Chartered

Il existe plus de

3 millions

de postes vacants dans le domaine de la cybersécurité au niveau mondial, selon l'organisation des professionnels de la cybersécurité (ISC)[2].

Darren Argyle, directeur de la stratégie du groupe en matière de risques de sécurité des informations de la banque internationale Standard Chartered, pense que l'amélioration de la diversité dans les équipes peut aider à pourvoir les postes vacants.

En 2021, Standard Chartered a lancé son programme CAP (Cyber Acceleration Programme). À ce jour, environ 50 femmes y ont participé. Un programme de « développement des compétences et d'évolution », CAP, propose à des femmes débutantes et de niveau intermédiaire des modules à leur propre rythme sur le thème de la cybersécurité et du leadership. En haut des modules d'apprentissage, des groupes atteignant jusqu'à 10 femmes sont affectés à des responsables expérimentés en cybersécurité et sont soumis à un programme de tutorat de 12 semaines.

« Nous créons un cadre de leadership dans lequel les femmes peuvent s'impliquer. Elles travaillent sur des modèles de postes dans le secteur, qui sont principalement occupés par des femmes, sur des domaines qu'elles souhaitent développer. »

Darren Argyle, directeur de la stratégie du groupe en matière de risques de sécurité des informations, Standard Chartered

Étape 2 :

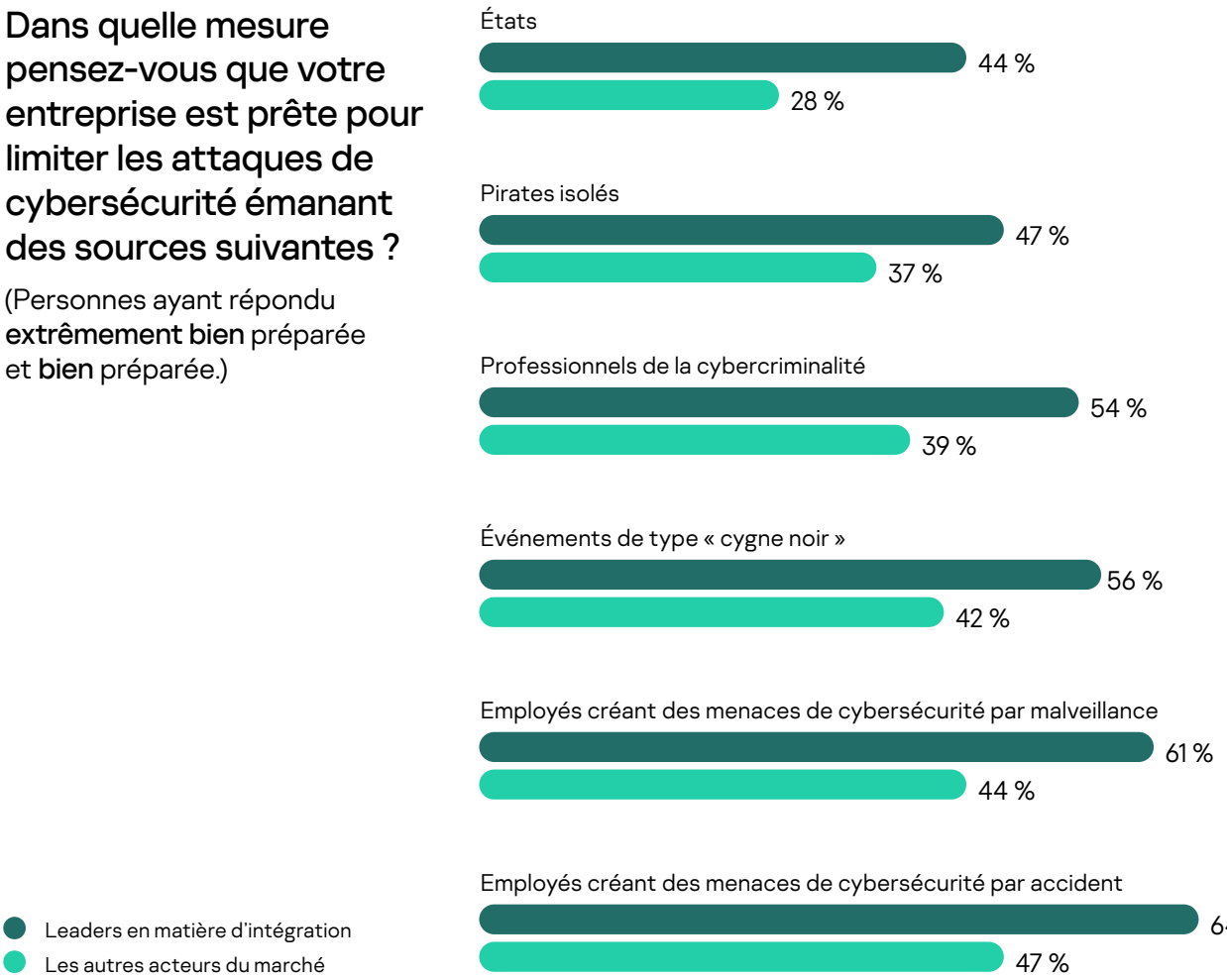
Intégrer étroitement les cadres supérieurs aux équipes de cybersécurité

Les cadres supérieurs (direction) ont des attributions étendues et de haut niveau, alors que les professionnels de la cybersécurité se concentrent sur les détails des cyber-menaces. Ce ne sont pas des partenaires évidents. Toutefois, l'étude de Kaspersky fait apparaître que lorsque les entreprises élaborent des liens forts entre ces deux catégories de personnes, elles obtiennent de meilleurs résultats en matière de sécurité.

Un quart (26 %) des personnes interrogées est convaincu qu'une forte intégration entre les cadres dirigeants et les équipes de cybersécurité sera très importante au cours des deux prochaines années. Les données montrent que ce petit groupe que Kaspersky appelle Leaders en matière d'intégration est mieux préparé pour gérer les cyberattaques.

Dans quelle mesure pensez-vous que votre entreprise est prête pour limiter les attaques de cybersécurité émanant des sources suivantes ?

(Personnes ayant répondu **extrêmement bien** préparée et **bien** préparée.)



Le géant de l'informatique au Royaume-Uni, **Softcat**, met étroitement en phase ses cadres supérieurs et ses équipes de cybersécurité. La responsabilité des risques (notamment la cybersécurité) relève en dernier ressort de son PDG, Graeme Watt. « Je suis la partie prenante essentielle pour la sécurité au sein du conseil d'administration. Le directeur des systèmes d'information relève directement de moi, et l'équipe de la sécurité des informations est sous sa responsabilité », déclare-t-il. « Je suis la personne vers laquelle se tourne le conseil d'administration pour tout ce qui touche aux risques de cybersécurité, mais je n'établis pas tous les rapports moi-même. Je fais venir le directeur des systèmes d'information aux réunions du conseil d'administration lorsque nous évoquons les risques en matière de cybersécurité. »

L'entreprise se soumet à un examen approfondi de l'état de sa cybersécurité auprès de nombreuses sources. En tant qu'entreprise publique, elle fait l'objet d'un audit externe. Elle dispose de ses propres audits internes. En tant que société informatique qui propose des services et des produits de sécurité, sa réputation auprès des clients dépend de ses propres normes de sécurité.

Watt travaille en collaboration étroite avec son équipe de cybersécurité pour s'assurer que les normes sont respectées, mais l'ensemble des autres responsables de l'équipe dirigeante de Softcat a également une responsabilité pour la cybersécurité.

Notre directeur général a une approche de la sécurité côté client, il applique donc ce qu'il voit, entend et pense à notre propre entreprise. Par exemple, nous proposons des évaluations de sécurité à nos clients, et nous avons appliqué ces mêmes services à nous-mêmes. Il s'agit d'une approche extrêmement saine. »

Graeme Watt, PDG,
Softcat

Le fabricant indien **Shriram Pistons and Rings** adopte une approche similaire et maintient son expertise en matière de sécurité proche de l'équipe dirigeante. La numérisation au niveau de l'atelier de fabrication est une priorité pour l'entreprise, et elle prévoit d'utiliser largement l'Internet des objets (IoT) dans ses installations.

Son responsable en chef pour le numérique, Prashant Khairnar, embauché pour mener à bien la numérisation depuis l'atelier de fabrication jusqu'à la direction, explique que l'équipe de direction prend la sécurité très au sérieux. « Lorsque nous procédons à des évaluations de risques, la cybersécurité est toujours la préoccupation principale », déclare-t-il. « Bien sûr, je ne suis pas expert en cybersécurité, mais la personne qui gère ce secteur l'est, et travaille directement sous ma responsabilité. J'ai une approche plus stratégique, il se concentre sur la sécurité quotidienne et les problèmes techniques. »

La cybercriminalité augmente rapidement. Les données provenant des analystes du marché de la technologie de Canalys révèlent que **30 milliards d'enregistrements de données ont été dérobés dans le monde entier en 2020**, plus que le cumul des 15 années précédentes.

Evgeniya Naumova, vice-présidente exécutive de l'activité Entreprises chez Kaspersky, déclare que la hausse de la cybercriminalité a fait prendre conscience de la menace aux équipes dirigeantes. « Je pense que les cadres supérieurs et les équipes dirigeantes se sont rendu compte de l'importance de la sécurité des informations pendant la pandémie du Covid-19 », déclare-t-elle, en laissant entendre que l'augmentation des risques de sécurité liée au travail à distance a attiré l'attention des responsables. « Il y a eu un déclic, clairement visible, dans leur état d'esprit. Ils ont réalisé que cela ne se limitait pas à quelque chose à regarder de loin, mais que ce devait être le principal élément à avoir en tête. »

Étape 3 :

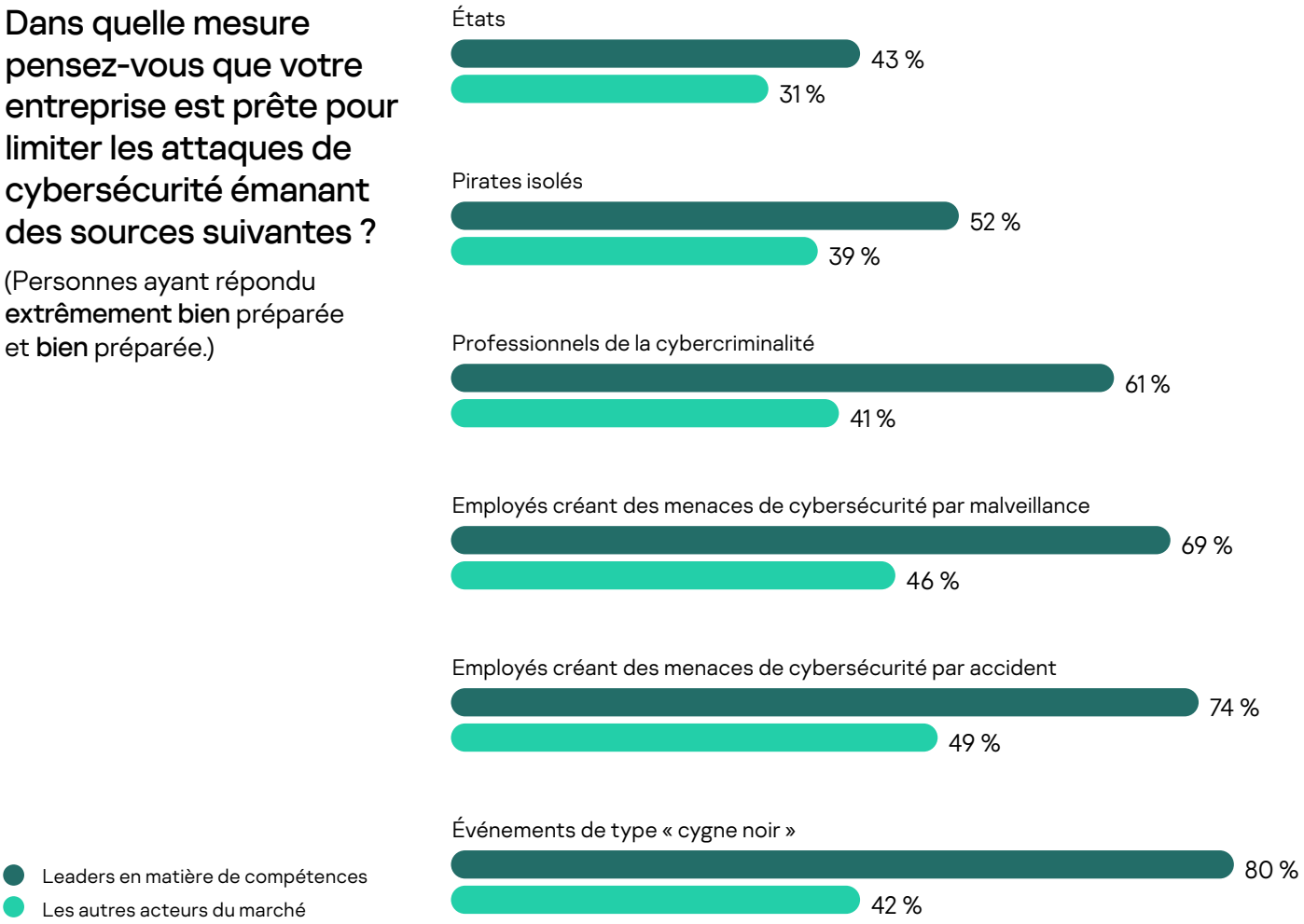
Investir dans une formation à la cybersécurité de haute qualité

Tout le monde sait qu'une équipe de cybersécurité chevronnée est essentielle pour combattre la cybercriminalité. Cependant, avec **quatre millions de postes vacants dans le monde dans le secteur de la cybersécurité**, il existe un risque considérable de pénurie.
Dans l'étude de Kaspersky, un tiers (34 %) des entreprises estime que la pénurie va s'accroître au cours des deux prochaines années.

Les compétences et les programmes de formation contribuent à combler cette carence. Toutefois, pour rester pertinents, ces programmes doivent être maintenus à jour. L'étude de Kaspersky distingue un très petit groupe d'entreprises (8 %), qui sont fermement convaincues que leur programme de formation à la cybersécurité peut suivre le rythme du paysage des menaces en évolution. Les données montrent que ce groupe, que Kaspersky nomme Leaders en matière de compétences, présente de meilleurs résultats en termes de sécurité.

Dans quelle mesure pensez-vous que votre entreprise est prête pour limiter les attaques de cybersécurité émanant des sources suivantes ?

(Personnes ayant répondu **extrêmement bien** préparée et **bien** préparée.)



La mise à jour permanente des compétences et des programmes de formation contribue finalement à faire de la sécurité une composante de la culture de l'entreprise. Selon Delaney, de Vaillance, cet aspect est essentiel. Elle pense également qu'une formation continue aux principes de base de la cybersécurité est un bon début.

« Il s'agit d'apprendre ce qu'il faut repérer, afin que la mémoire musculaire vous enseigne comment faire les bons choix en connaissance de cause. Cela est tout particulièrement important pour les personnes qui travaillent à domicile. »

Shawnee Delaney, PDG, Vaillance Group

Les Leaders en matière de compétences de Kaspersky ont davantage tendance à innover à travers leur formation.

67 %

des Leaders en matière de compétences estiment qu'il sera très important d'entreprendre une formation immersive à la cybersécurité au cours des deux prochaines années, par rapport à seulement 49 % des autres acteurs du marché.

Elle poursuit : « les employés ont besoin de maintenir leurs logiciels à jour, de comprendre ce qu'est un VPN et de savoir comment l'utiliser et ne pas avoir recours au Wi-Fi public, par exemple. Ce sont des bonnes pratiques générales en matière de cyber-hygiène qui sont essentielles pour maintenir la sécurité. »

Ils sont également plus susceptibles d'intégrer une sensibilisation à la cybersécurité dans leur processus de recrutement et d'accueil des nouveaux collaborateurs.

Une autre manière innovante de combler le manque de compétences dans les équipes de cybersécurité consiste à effectuer des recrutements auprès de concurrents, selon Argyle, de Standard Chartered. Cependant, pour cela, les entreprises doivent adapter leur manière de travailler. « Si vous examinez les compétences que nous souhaitons pour essayer d'attirer dans les entreprises dans le domaine de la cybersécurité et des technologies, bon nombre de ces compétences ne se trouvent pas nécessairement dans un autre domaine », dit-il. « Elles se trouvent dans les sociétés FinTech, les entreprises de technologies et les opérateurs de cloud. C'est la raison pour laquelle nous devons être en mesure de proposer un environnement de travail identique à celui des grandes sociétés technologiques telles que Google, Amazon ou une société FinTech. Et cela représente une manière de travailler très différente. »

Mme Naumova de Kaspersky déclare que la sécurité incombe à chaque employé. « Nous proposons des **cours de formation sur la manière de changer le comportement de toutes les personnes dans l'entreprise** », déclare-t-elle. « Il ne s'agit pas simplement d'un domaine réservé à l'équipe en charge de la sécurité des informations. Il en va de la responsabilité de tous. »

Elle ajoute que les entreprises doivent entreprendre une approche de la sécurité de bas en haut, afin que tout le monde soit informé. « Certaines entreprises disposent d'un directeur de la sécurité des informations ou d'un poste similaire au sein de leur conseil d'administration », indique-t-elle. « Elles favorisent cela, car elles comprennent qu'elles peuvent perdre leur activité en un seul jour si la sécurité n'est pas traitée correctement. »

Trois étapes créent un cercle vertueux de cybersécurité

1

Augmentent la diversité au sein des équipes de cybersécurité

2

Améliorent la collaboration avec les cadres dirigeants

3

Investissent dans des programmes de compétence de qualité.

Cependant, le développement individuel de celles-ci ne constitue pas la réponse. L'étude montre que ces facteurs sont complémentaires entre eux. Par exemple, les Leaders en matière de compétences de Kaspersky ont davantage tendance à créer des équipes de cybersécurité variées et inclusives, et à instaurer une intégration plus étroite de leurs cadres supérieurs avec leurs équipes de cybersécurité. Il s'agit d'un cercle vertueux qui augmente le degré de préparation à la cybersécurité.

Le paysage des menaces évolue rapidement, et les cybercriminels ont recours à des techniques de plus en plus sophistiquées. Les entreprises n'ont pas d'autre choix que de s'adapter à cette sophistication grâce à un degré de préparation extrêmement élevé.

kaspersky.fr

kaspersky

Actualitéssur les cybermenaces: securelist.com
Actualités sur la sécurité informatique : business.kaspersky.com
Revue destinée aux chefs d'entreprise : kaspersky.com/securefutures
Solutions de cybersécurité pour les entreprises : kaspersky.fr/enterprise-security

GBD-9212 Q1/22 V1