ivanti

Repartez sur de nouvelles bases

Rapport sur l'état de la cybersécurité en 2023

Alors que les entreprises aspirent à une protection renforcée contre les cyberattaques, le secteur peine à se débarrasser de pratiques réactives.

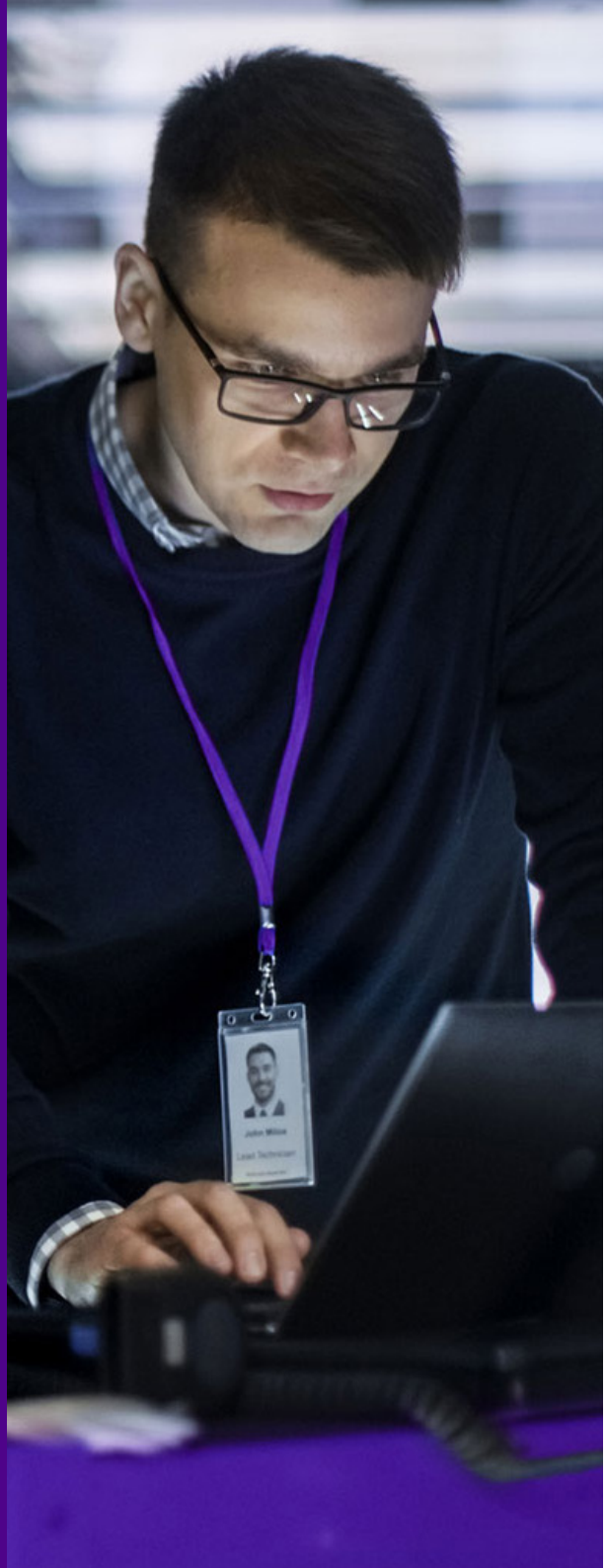
Qui est prêt à parier un kopeck sur la sécurité de son entreprise ?

Nous avons interrogé 1 356 dirigeants et professionnels de sécurité sur la capacité de leur entreprise à empêcher une faille de sécurité dommageable.

Seriez-vous capable de parier un kopeck sur les protections que vous avez mises en place ?

1 professionnel interrogé sur 5 nous a répondu « non ».

ivanti



L'état de la cybersécurité est-il donc si mauvais, que 20 % refusent de parier même un kopeck sur leurs protections en cybersécurité ?

Quand une entreprise embauche les bonnes personnes, achète la bonne technologie, et adopte tous les bons processus et procédures, mais ne peut pas parier sur la force de sa sécurité IT, quelque chose ne tourne pas rond. Cela signifie qu'il est peut-être temps de repartir sur de nouvelles bases et de repenser son approche de la cybersécurité.

Dans le cadre de notre série d'études sur l'état de préparation de la cybersécurité (State of Cybersecurity Preparedness), nous avons interrogé plus de 6 550 professionnels pour mieux comprendre les problématiques auxquelles les entreprises sont confrontées : des menaces de cybersécurité émergentes aux restrictions budgétaires, en passant par les couches de technologies et les processus utilisés pour assurer leur protection.

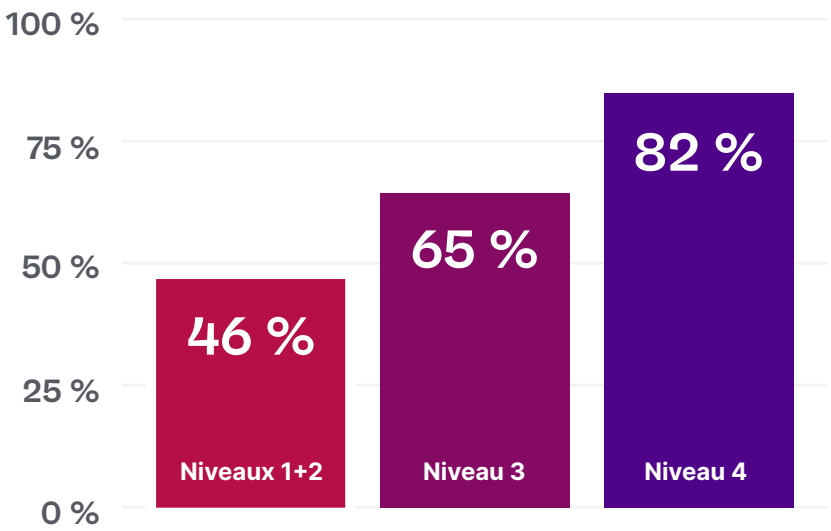
Nous avons en outre examiné le problème sous trois angles différents : dirigeants et hauts responsables de l'entreprise, professionnels de la sécurité et main-d'œuvre intellectuelle. Nous avons aussi abordé le sujet des vulnérabilités inquiétantes constatées au niveau des dirigeants.

Notre objectif ? Comprendre comment les responsables de sécurité peuvent être à la fois optimistes concernant leur propre état de préparation (et ils le sont) et peu disposés à parier un kopeck sur leur propre système de sécurité. Nous expliquons par ailleurs comment repartir sur de nouvelles bases pour changer d'approche et adopter une stratégie et des pratiques de cybersécurité efficaces et proactives.

Sommaire :

Les dirigeants sont optimistes sur le niveau de préparation de leur organisation.

Q : Comparativement à l'an dernier, vous sentez-vous mieux ou moins bien préparé à lutter contre les attaques de cybersécurité ?



« Je me sens mieux préparé à me défendre que l'an dernier. »

Les groupes de maturité de la cybersécurité sont décrits page 24.

01

La sécurité dans un monde hyperconnecté

Une récente enquête de PwC a révélé que « dans les plans de résilience pour 2023, une cyberattaque catastrophique est le principal scénario envisagé car il mettrait à l'épreuve l'ensemble du comité de direction : deux tiers des dirigeants considèrent la cybercriminalité comme la menace la plus importante pour l'année à venir. »[1]

Que signifie exactement se préparer, dans un monde où les vulnérabilités et même les menaces inconnues ne cessent de se multiplier ? Commençons par examiner le paysage de la cybersécurité en 2023.

ivanti

Les budgets de cybersécurité augmentent pour faire face à des menaces plus importantes et plus dommageables

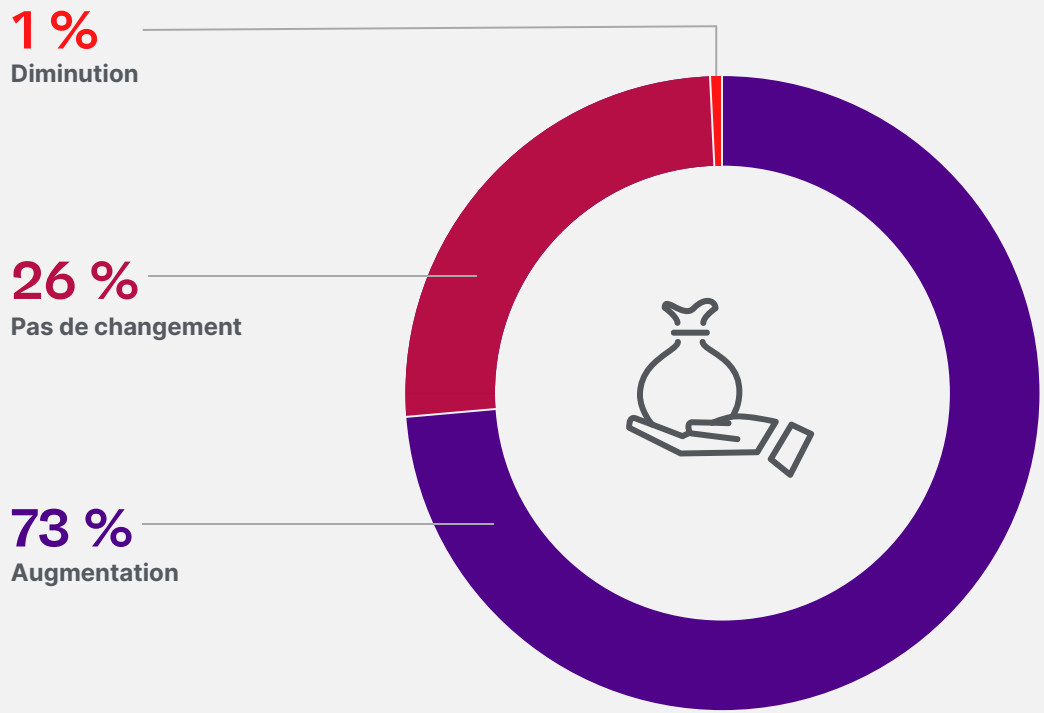
Parmi les professionnels de la sécurité et les dirigeants interrogés, 71 % prévoient une augmentation de leur budget de cybersécurité en 2023, ce qui représente en moyenne, une hausse de 11 %. Selon l'association Society for Human Resource Management, c'est environ trois fois l'augmentation de budget prévue pour les rémunérations pour 2023.[2]

Lesley Salmon, CIO mondial chez Kellogg, explique au Wall Street Journal : « Si on me demandait de restreindre mon budget, j'épargnerais la cybersécurité de toute coupe budgétaire. »[3]

L'augmentation moyenne de budget prévue pour 2023 est de 11 %, bien au-delà de l'inflation prévue pour la même période.

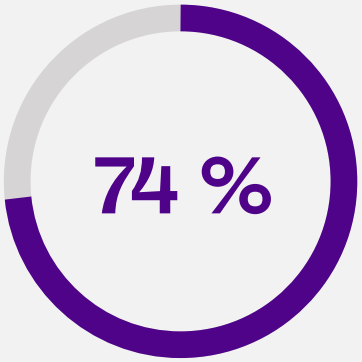
Les budgets de cybersécurité augmentent.

Q : Prévoyez-vous une augmentation ou une diminution de votre budget de cybersécurité en 2023, par rapport à 2022 ?

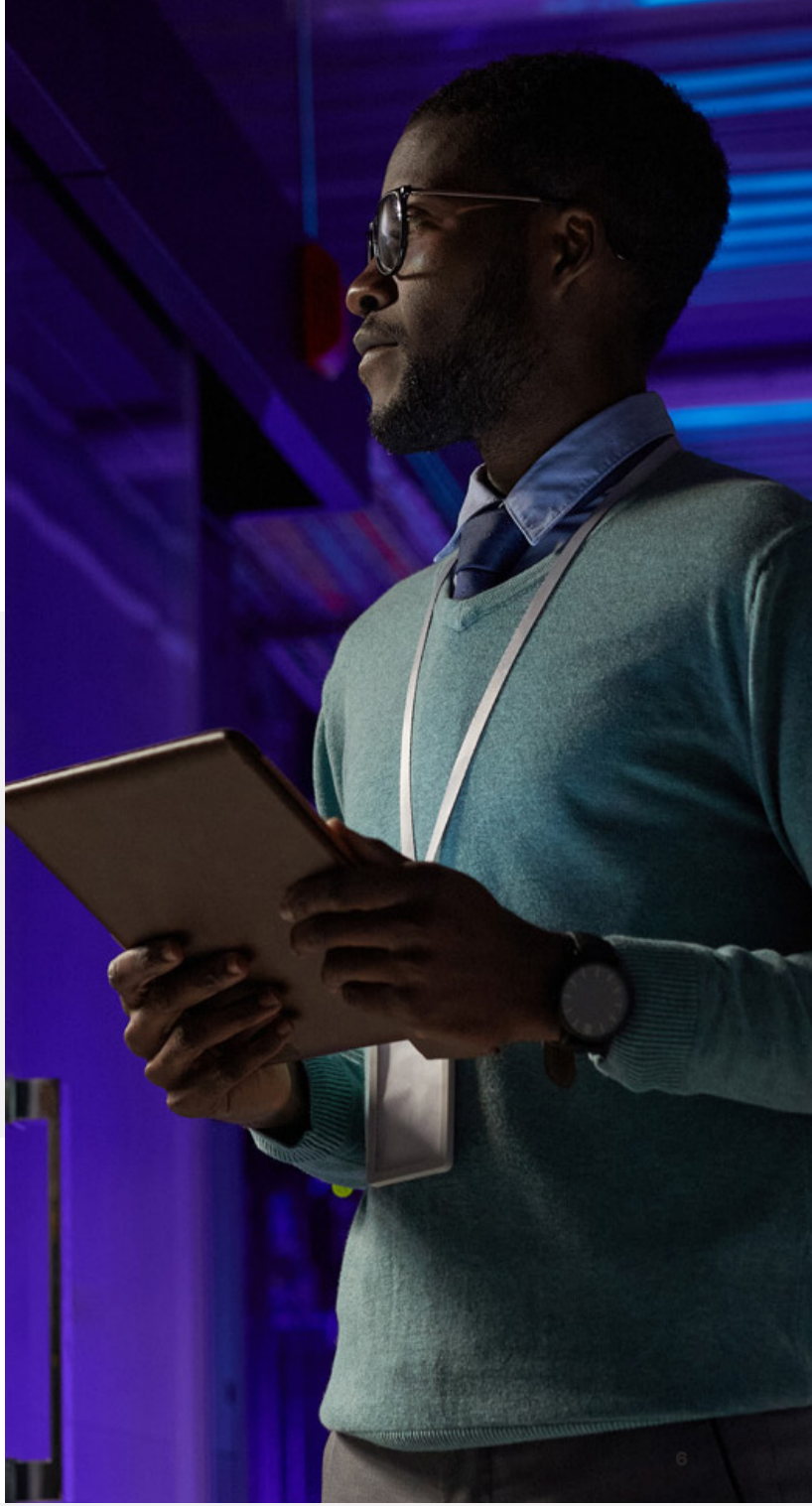


Près de 3/4 des professionnels de la sécurité interrogés par Ivanti provisionnent des fonds pour les failles de sécurité. Ces « fonds d'urgence » représentent environ 16 % du budget global de la cybersécurité - une somme importante.

Le rapport IBM « Cost of a Data Breach 2022 » révèle que le coût de récupération des systèmes après une fuite de données peut facilement atteindre une somme à 7 chiffres. Une entreprise dépense en moyenne 4,35 millions de dollars pour s'en remettre. Les secteurs comme la santé et la banque paient le plus lourd tribut.[4]



déclarent allouer leur budget aux failles de sécurité. Le « fonds d'urgence » pour ces failles représente en moyenne 16 % du budget de cybersécurité global.



Une sécurité entravée par une pile technologique complexe et un déficit de compétences en sécurité

La « complexité de la pile technologique » et le « déficit de compétences en sécurité » sont les principaux obstacles à l'excellence que citent les professionnels de la sécurité et les dirigeants, loin devant le « manque de budget ».

Complexité de la pile technologique

Les professionnels de la sécurité disent utiliser en moyenne six outils et programmes de cybersécurité distincts.

Charlie Bell, Security Chief chez Microsoft, affirme que l'accumulation d'un nombre trop important de plateformes de sécurité crée ce qu'il appelle une « sorte de solution Frankenstein ». Comme M. Bell l'explique, « le problème, c'est que chaque fois qu'on colle plusieurs éléments, cela laisse des joints[ ] et ce sont ces joints que les pirates attaquent ».[5]

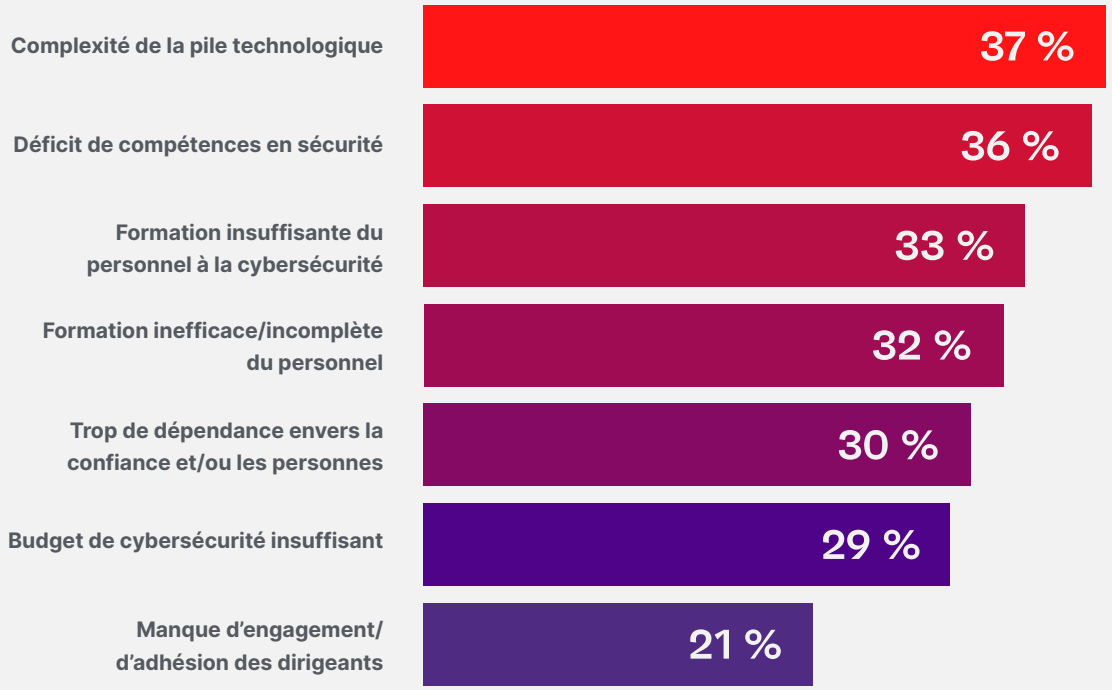
Déficit de compétences en sécurité

Pour les professionnels de la sécurité, le « déficit de compétences » est de très loin la plus grande difficulté, citée par 39 % des professionnels interrogés.

Cela rejoint les conclusions de nombreuses autres études, notamment un récent rapport d'ISC2 qui révèle que le déficit mondial de main-d'œuvre en cybersécurité a augmenté de 26,2 % en 2022 par rapport à 2021, et que 3,4 millions de travailleurs supplémentaires sont nécessaires pour protéger efficacement les actifs.[6]

La complexité et le déficit de compétences sont les plus grands défis.

Q : Parmi ces obstacles sévères à l'excellence de la cybersécurité, lesquels concernent votre entreprise ?



La course à l'atténuation des risques de la supply chain

La transformation digitale des entreprises apporte avec elle des risques démesurés pour la supply chain. Il en va de même de tous les gains d'efficacité qui découlent d'une supply chain hautement connectée.

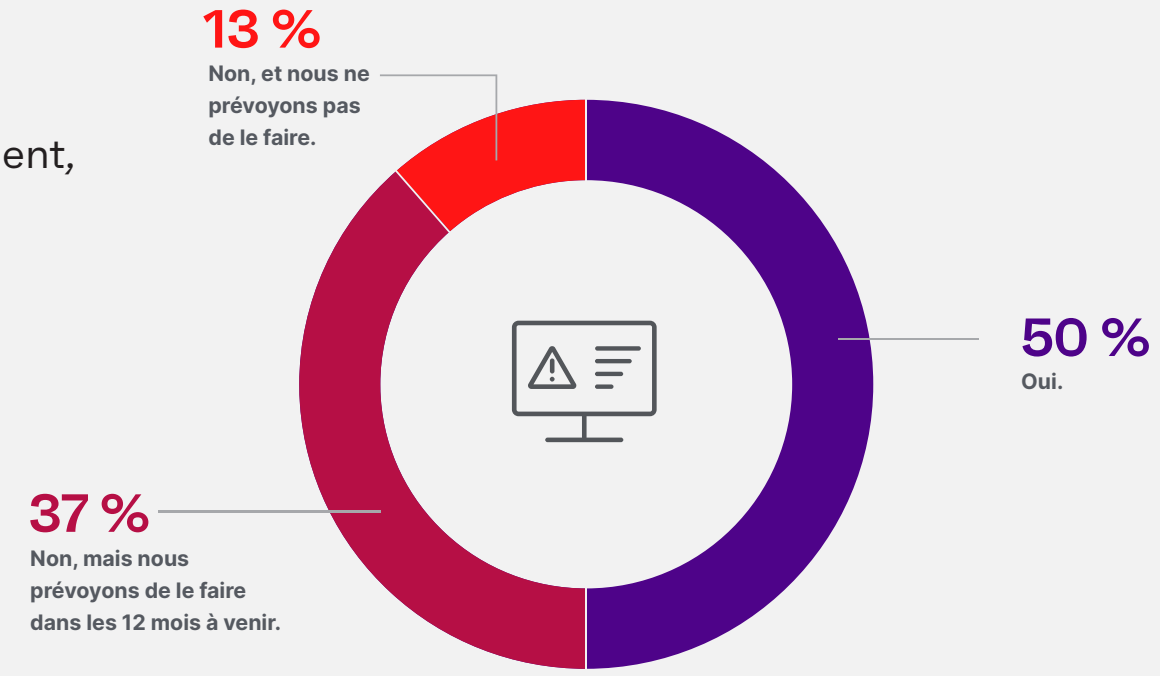
« Comme les chaînes d'approvisionnement sont aujourd'hui fortement interconnectées, une menace visant un seul des partenaires (un fournisseur tiers, par exemple) constitue une menace pour l'ensemble de la chaîne d'approvisionnement », dit Shaun McAlmont, Chief Executive Officer chez Ninjio.[7]

Certains CISO (responsables de la sécurité des systèmes d'information) s'empressent de doter leurs organisations de solutions pour identifier et atténuer les vulnérabilités de la supply chain, mais la majorité est encore à la traîne.

Dans l'étude menée par Ivanti, moins de la moitié (47 %) disent avoir déjà identifié les systèmes et composants tiers les plus vulnérables dans leur supply chain logicielle, mais 35 % prévoient de gérer ce risque dans les 12 prochains mois. 46 % classent les menaces visant la supply chain au niveau « Élevé » ou « Critique » pour 2023.

Les risques de la chaîne d'approvisionnement, un sujet de préoccupation croissante

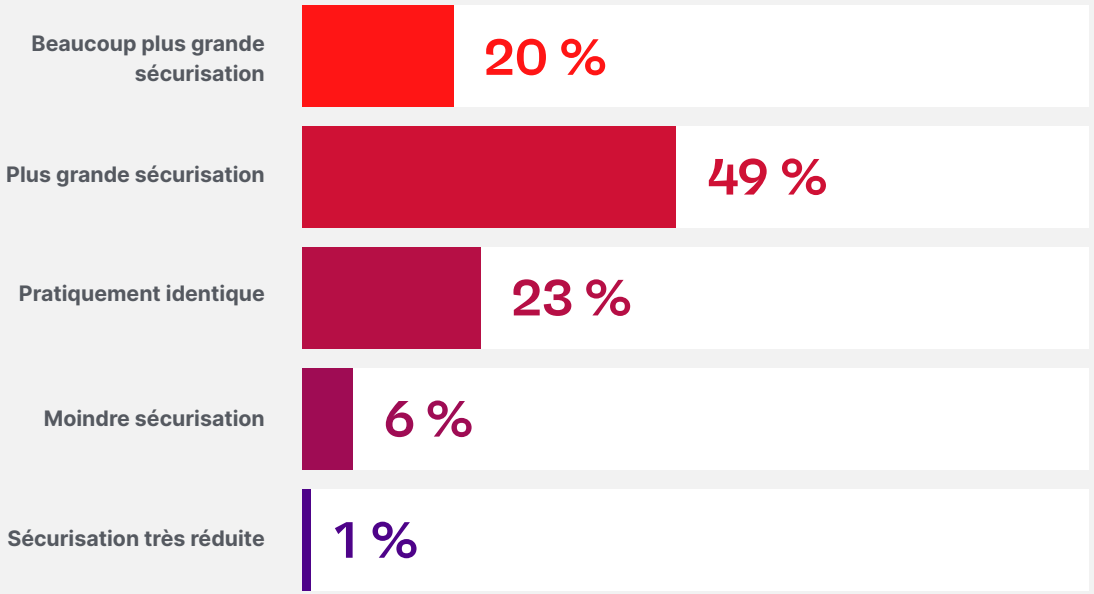
Q : Votre équipe a-t-elle identifié les systèmes/composants tiers les plus vulnérables de votre supply chain logicielle et ceux qui auront le plus d'impact sur l'entreprise en cas d'attaque ?



Les risques liés au Cloud sont-ils exagérés ?

Les systèmes Cloud, un atout pour la sécurité

Q : Compte tenu des risques de sécurité et des opportunités d'un environnement Cloud, considérez-vous que la sécurisation de vos systèmes augmentera ou baissera significativement après l'adoption de systèmes et/ou d'un stockage Cloud ?



Plus de 2 professionnels sur 3 (68 %) affirment que leurs systèmes sont nettement plus sécurisés depuis l'adoption de systèmes et/ou d'un stockage Cloud.

Autrement dit, malgré l'idée fausse que les systèmes Cloud exposent les entreprises à des risques de cybersécurité au-delà de l'acceptable, les dirigeants et les professionnels de la sécurité que nous avons interrogés pensent, après en avoir évalué les risques et les opportunités, que l'environnement Cloud assure une meilleure sécurité.

« Pour les responsables IT modernes, la nouvelle pierre angulaire de leurs systèmes est d'assurer une expérience numérique des collaborateurs qui soit à la fois positive et sécurisée » affirme Andy Stone, Chief Technology Officer chez Pure Storage. « En utilisant le Cloud de manière sécurisée et efficace, les entreprises permettent à leurs collaborateurs de travailler partout où ils le souhaitent et sur tous les périphériques. À l'ère du tout numérique, l'incapacité à passer au Cloud en toute sécurité freine sensiblement la croissance d'une entreprise. »

02

Points sensibles de la cybersécurité en 2023

Quelles sont les principales menaces pour 2023 d'après les experts en cybersécurité ? Comment les entreprises se préparent-elles aux attaques, à la fois connues et inconnues ?

ivanti

Manque de préparation et d'expérience

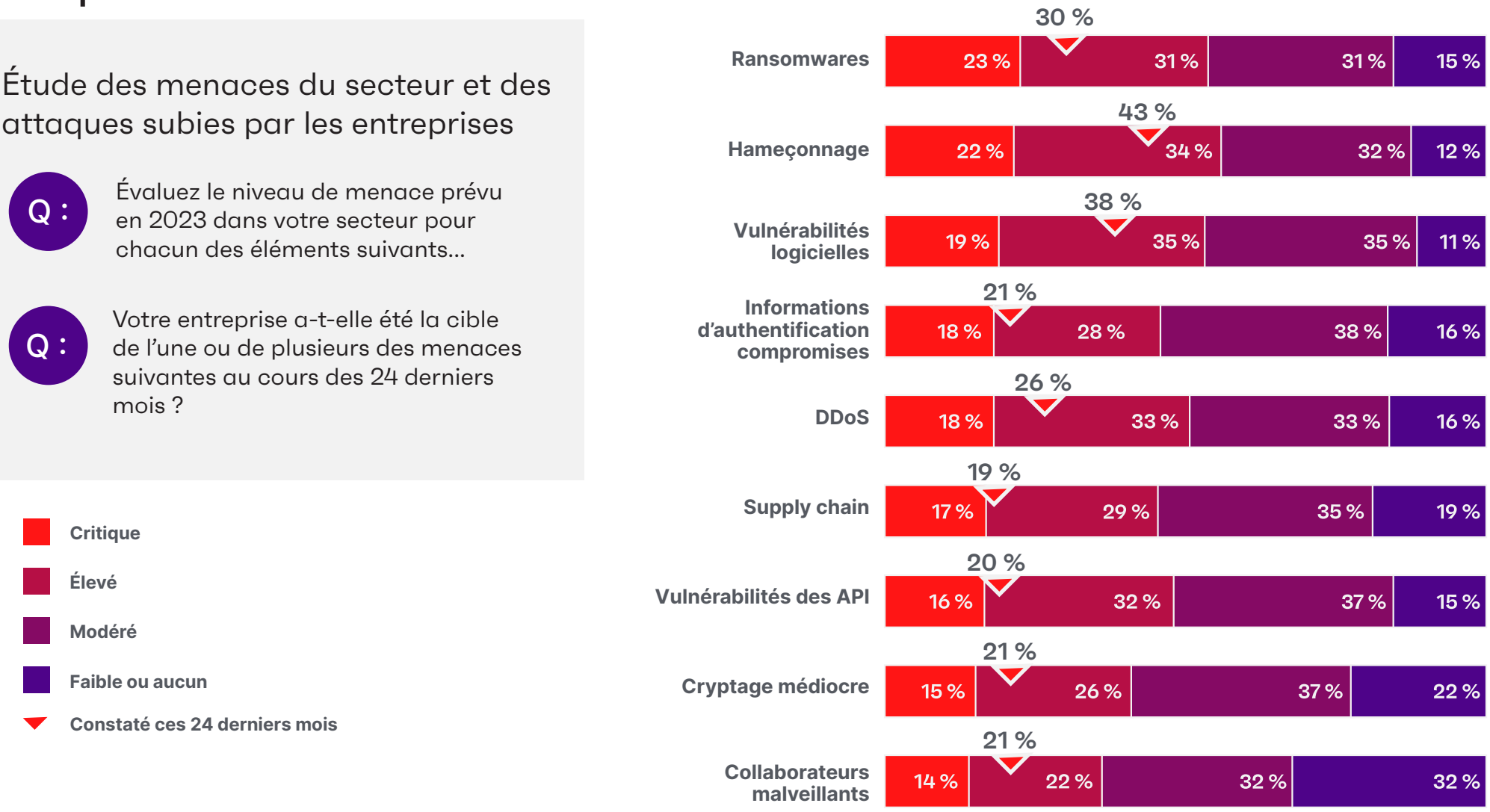
Les professionnels interrogés citent l'hameçonnage (ou « fishing »), les ransomwares et les vulnérabilités logicielles comme les principales menaces pour le secteur.

Lorsque l'on examine les attaques réelles subies par les entreprises, l'hameçonnage et les vulnérabilités logicielles dépassent très largement les autres risques.

Étude des menaces du secteur et des attaques subies par les entreprises

Q : Évaluez le niveau de menace prévu en 2023 dans votre secteur pour chacun des éléments suivants...

Q : Votre entreprise a-t-elle été la cible de l'une ou de plusieurs des menaces suivantes au cours des 24 derniers mois ?



Un participant à l'enquête explique :

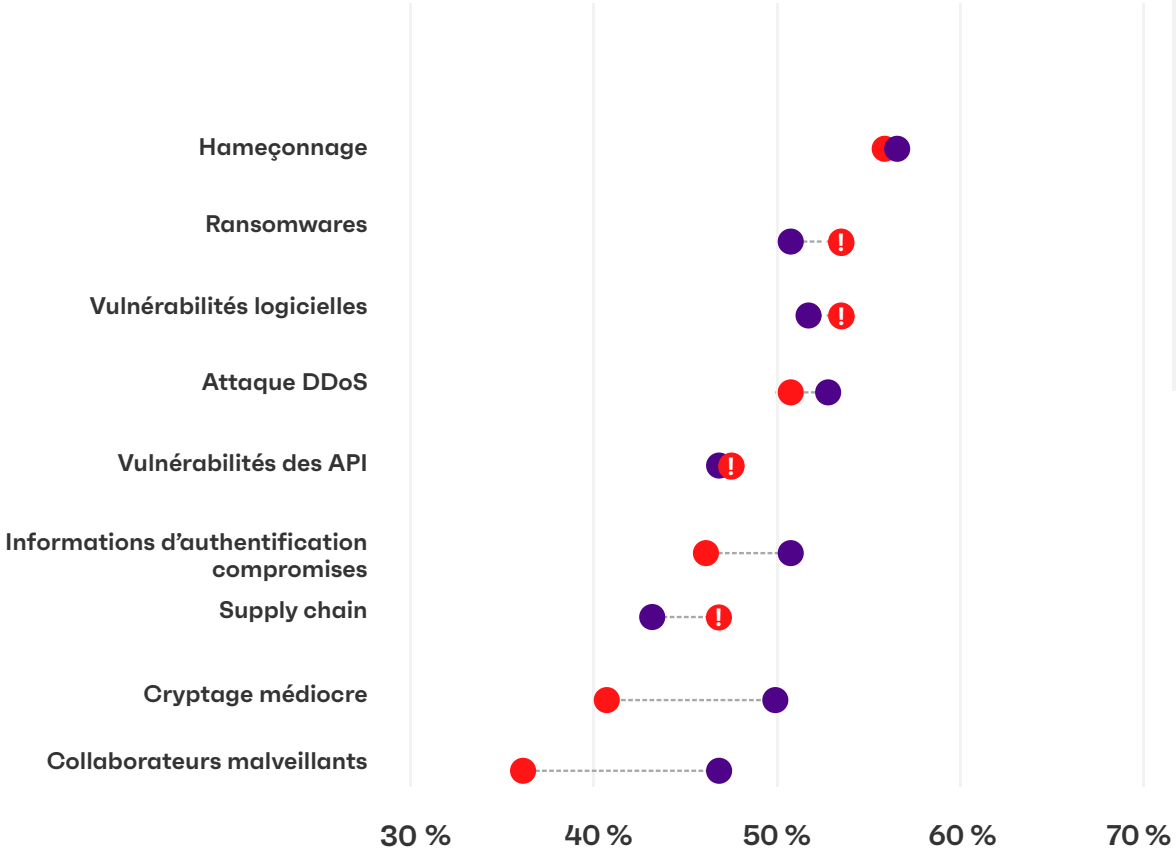
« Nous avons subi quelques tentatives d'hameçonnage avancées et les collaborateurs ignoraient totalement qu'ils étaient ciblés. Ce type d'attaque est devenu tellement plus sophistiqué au cours des deux dernières années… même nos collaborateurs les plus expérimentés tombent dans le piège. »

Malgré la diversité des menaces, une grande partie des personnes interrogées se disent prêtes à faire face au paysage croissant des menaces. Environ la moitié se disent « tout à fait préparées » à affronter ces myriades de menaces, notamment les ransomwares, le cryptage médiocre, les collaborateurs malveillants et les vulnérabilités logicielles.

Un point sensible : les vulnérabilités de la supply chain. 42 % seulement se disent vraiment prêts à se protéger des menaces visant la supply chain, bien que 46 % classent ces menaces au niveau Élevé.

Ce risque n'est qu'une des nombreuses menaces « inversées », pour lesquelles le niveau de préparation est inférieur au niveau de menace estimé.

Menaces de sécurité et niveau de préparation



Q : Évaluez le niveau de menace prévu en 2023 dans votre secteur pour chacun des éléments suivants…

Q : À quel point votre entreprise est-elle préparée à chacun des types de menace de cette liste ?

- Niveau de menace Élevé + Critique
- « Tout à fait prête »
- Menace inversée

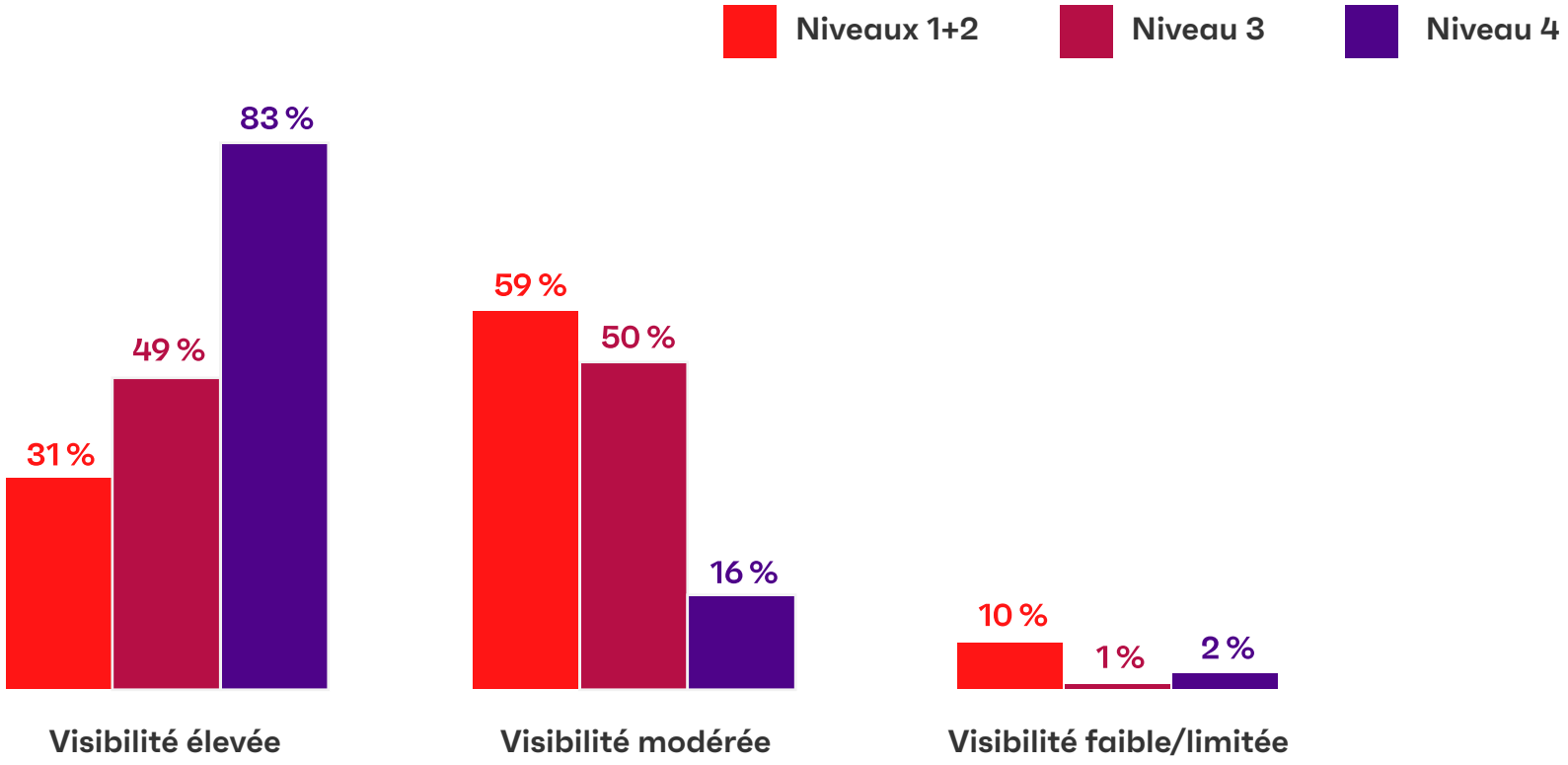
Les garde-fous attendus font cruellement défaut

Un peu plus de la moitié des dirigeants et des professionnels de la sécurité (52 %) déclarent bénéficier d'une « visibilité élevée » sur chaque utilisateur, périphérique, application et service de leur réseau.

Seulement 48 % disent exécuter leur programme de découverte des actifs au moins une fois par semaine.

Les entreprises leaders font état d'une bonne visibilité des actifs.

Q : Quel est le degré de visibilité de votre entreprise sur chaque utilisateur, périphérique, application et service de votre réseau ? (Par niveau de maturité de la cybersécurité)

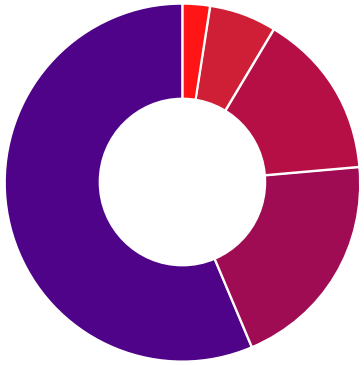


Presque tous les répondants affirment avoir mis en place un processus formel de déprovisionnement, et la grande majorité (68 %) disent que le déprovisionnement des collaborateurs qui quittent l'entreprise est réalisé sous trois jours ouvrables. (Pour les fournisseurs extérieurs, 81 % disent que le processus est exécuté sous 5 jours ouvrables.)

Pourtant, les professionnels de la sécurité nous disent aussi que les instructions de déprovisionnement sont ignorées un tiers du temps… aveu étonnant, compte tenu de l'exposition que cela implique.

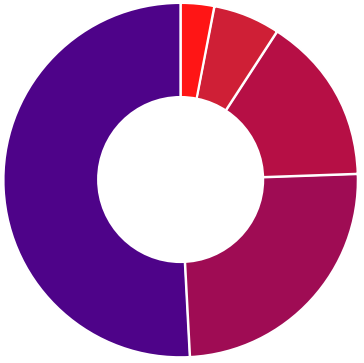
Pour le déprovisionnement, de bons protocoles mais des résultats mitigés

Q : Quelle est votre rapidité de déprovisionnement des informations d'authentification d'un collaborateur lorsqu'il quitte l'entreprise ?



- **2 %** Nous n'avons pas de processus formel pour le déprovisionnement
- **5 %** Ne sait pas
- **12 %** Plus de 7 jours
- **16 %** 4-7 jours
- **45 %** 2-5 jours ouvrables

Q : À quelle vitesse déprovisionnez-vous les informations d'authentification d'un fournisseur tiers, d'un consultant et/ou d'un sous-traitant à la fin de son contrat ou à la résiliation du service ?



- **2 %** Nous n'avons pas de processus formel pour le déprovisionnement
- **4 %** Ne sait pas
- **10 %** Plus de 7 jours
- **16 %** 4-7 jours
- **33 %** 2-3 jours ouvrables

La prolifération des informations d'authentification zombies

Encore plus flagrant : 45 % des personnes interrogées disent soupçonner que d'anciens collaborateurs et sous-traitants ont toujours un accès actif aux systèmes et fichiers de l'entreprise, que ce soit parce que les instructions de déprovisionnement n'ont pas été suivies correctement ou parce que les applis tierces offrent toujours un accès masqué, même une fois les informations d'authentification désactivées.

« Très souvent, les grandes entreprises ne tiennent pas compte de l'énorme écosystème d'applis, de plateformes et de services tiers qui maintiennent un accès bien après la fin de contrat d'un collaborateur » déclare le Dr Srinivas Mukkamala, Chief Product Officer chez Ivanti. « Nous appelons cela des informations d'authentification zombies, et un nombre choquant de professionnels de la sécurité (et même de dirigeants) ont toujours accès aux systèmes et données de leur ancien employeur. »

45%

des professionnels de la sécurité soupçonnent ou ont la certitude que d'anciens collaborateurs et sous-traitants ont toujours un accès actif aux systèmes ou fichiers, que ce soit par des noms d'utilisateur, des informations de connexion ou des mots de passe toujours actifs.

Les instructions de déprovisionnement ne sont suivies que 68 % du temps.

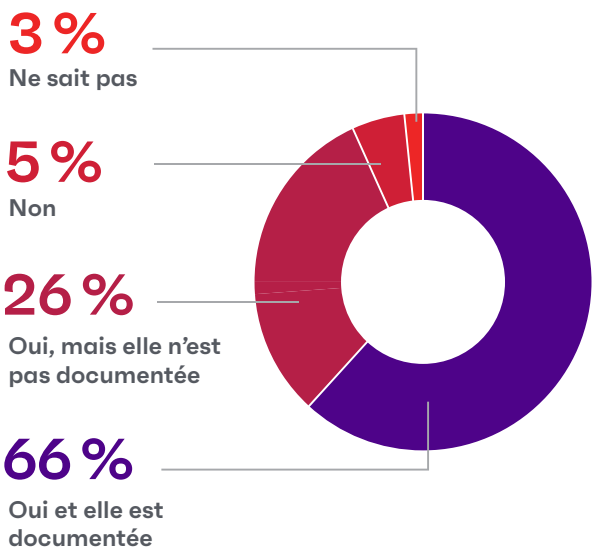
ivanti

Si tous les correctifs sont prioritaires, aucun n'est traité en priorité

92 % des répondants disent disposer de méthodes pour prioriser les vulnérabilités auxquelles appliquer des correctifs, bien que plus d'un quart d'entre eux affirment que les méthodes en question ne sont documentées nulle part.

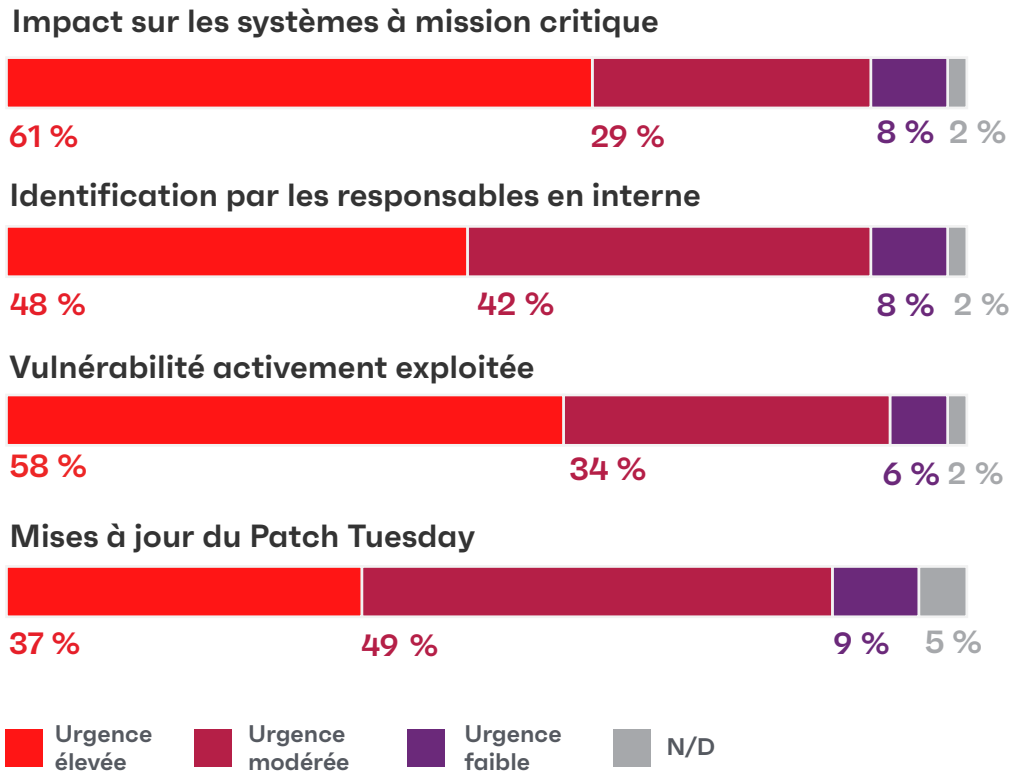
En fait, lorsqu'on leur demande les types de correctifs à prioriser, les professionnels de la sécurité disent que tous les types sont prioritaires… si bien qu'en réalité, aucun ne l'est.

Q : L'équipe de cybersécurité dispose-t-elle d'une méthode pour prioriser les vulnérabilités auxquelles appliquer des correctifs ?



Une gestion des correctifs enlisée dans la philosophie du « tout urgent »

Q : Comment priorisez-vous les correctifs de vulnérabilité à appliquer ?



En ne permettant pas à l'équipe Sécurité d'identifier clairement les priorités, cette approche du « tout urgent » est génératrice de stress et peut entraîner des burnouts.

Une enquête mondiale menée par IBM auprès de 1 100 agents de support chargés des incidents montre que 68 % d'entre eux déclarent qu'on leur affecte souvent deux incidents ou plus à la fois. Comme l'explique l'étude, « le travail semble faire des ravages : ils sont presque autant (64 %) à avoir demandé l'aide d'un spécialiste de la santé mentale pour insomnie, burnout ou anxiété. »[8]

Une enquête plus ancienne d'Ivanti montre les mêmes difficultés : lorsqu'on leur demande quelles sont les causes du turnover, les professionnels IT citent avant tout autre problème une trop forte charge de travail (41 %) et des attentes irréalistes envers l'équipe (34 %).[9]

03

Le danger des attaques de whaling

On parle d'attaque de whaling ou d'hameçonnage à la baleine lorsque les cyberpirates utilisent des techniques personnalisées de « spearphishing » ou harponnage pour chasser les « baleines », c'est-à-dire les cibles significatives à forte valeur, comme les PDG, les politiciens ou les hauts fonctionnaires. Cette technique est aussi communément appelée la fraude au président.

Quand une « baleine » est harponnée, les pirates accèdent à des informations sensibles, autorisent des virements bancaires, voire même obligent les collaborateurs à réaliser des opérations qu'ils n'accepteraient jamais en temps normal… mais, voilà, si le big boss a donné son accord…

ivanti

Les dirigeants disent être conscients des risques de cybersécurité mais ils ont toujours des comportements à risque

Près de 9 dirigeants sur 10 (PDG, vice-présidents, directeurs, etc.) se disent prêts à reconnaître et à signaler les menaces comme les malwares et l'hameçonnage au travail.

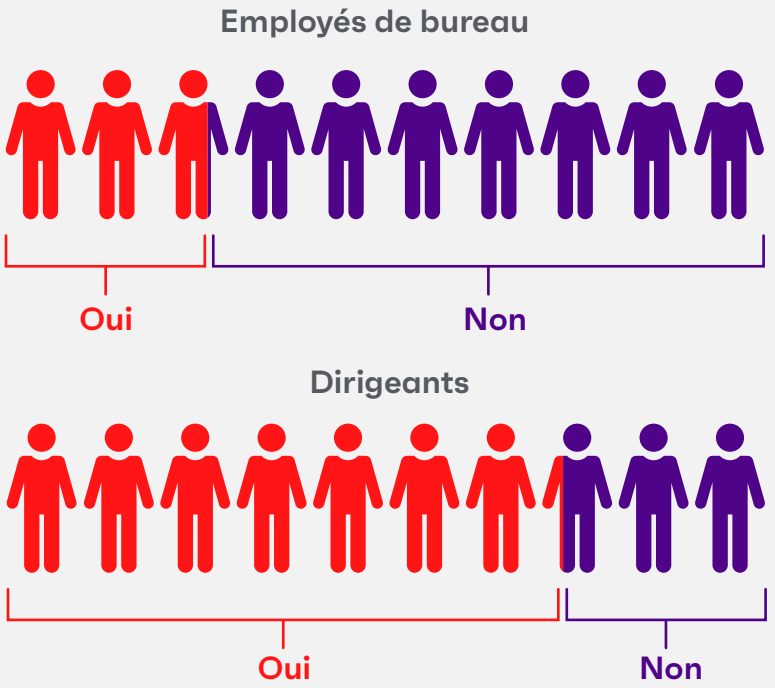
De plus, comparativement aux autres collaborateurs, ils sont beaucoup plus susceptibles d'admettre avoir contacté l'équipe Sécurité pour une question ou une inquiétude.

C'est encourageant. Cependant, nos recherches montrent que les dirigeants sont beaucoup plus enclins à signaler des interactions négatives avec l'équipe Sécurité, et qu'ils sont 1,3 fois plus susceptibles de dire qu'ils « ne se sentent pas en sécurité » en signalant des failles de sécurité.

Par ailleurs, leurs actions (ces habitudes quotidiennes que les dirigeants d'entreprises avouent) sont encore plus inquiétantes.

Les dirigeants considèrent qu'ils sont impliqués dans les efforts de sécurité de l'entreprise.

Q : Avez-vous déjà contacté un membre de l'équipe en charge de la cybersécurité pour une question ou une inquiétude liée à la sécurité ?



Les dirigeants ont des comportements plus dangereux

Les PDG, vice-présidents et directeurs (ceux que nous avons qualifiés de « dirigeants » dans notre enquête) sont plus susceptibles que le reste de la main-d'œuvre intellectuelle d'adopter des comportements de sécurité dangereux.

- Plus d'un tiers des dirigeants interrogés ont cliqué sur un lien d'hameçonnage, soit quatre fois plus que les autres employés de bureau !
- Près d'un quart des dirigeants utilisent une date d'anniversaire facile à mémoriser dans leur mot de passe.
- Les dirigeants sont bien plus susceptibles que leurs collaborateurs de garder le même mot de passe pendant des années au lieu de les mettre régulièrement à jour : ils sont 1/4 à le faire.
- Les dirigeants interrogés sont cinq fois plus susceptibles de partager leur mot de passe avec des personnes extérieures à l'entreprise.

Une attaque de whaling réussie représente une vulnérabilité beaucoup plus grande que les tentatives d'hameçonnage traditionnelles, mais de nombreuses entreprises ne considèrent toujours pas cela comme une menace unique et démesurée.

Les faits parlent d'eux-mêmes : les dirigeants (les personnes ciblées par les attaques d'hameçonnage les plus sophistiquées) sont quatre fois plus susceptibles d'être victimes d'hameçonnage que les autres employés de bureau.

On ne le répètera jamais assez : vos collaborateurs de plus grande valeur sont quatre fois plus susceptibles d'exécuter une action qui ouvre grand la porte aux pirates.

À lui seul, ce risque signifie que les entreprises doivent développer un programme de formation personnalisé et des interventions techniques pour les PDG et autres hauts responsables afin de constituer des couches de protection supplémentaires pour ces cibles particulièrement vulnérables.

Plus d'un dirigeant sur 3 (PDG, VP, directeurs, etc.) a été victime d'escroqueries par hameçonnage, soit en cliquant sur un lien frauduleux, soit en envoyant de l'argent.

04

Comment préparer les entreprises pour 2023 et au-delà

Dans le cadre de l'enquête Ivanti, l'équipe de recherche a examiné de plus près les entreprises à la pointe en matière de cybersécurité (Niveau 4 sur l'échelle de la maturité). Nous nous sommes intéressés à différentes questions : quels sont les indicateurs qui font qu'elles se distinguent et comment les autres entreprises peuvent-elles apprendre de ces leaders ?

ivanti

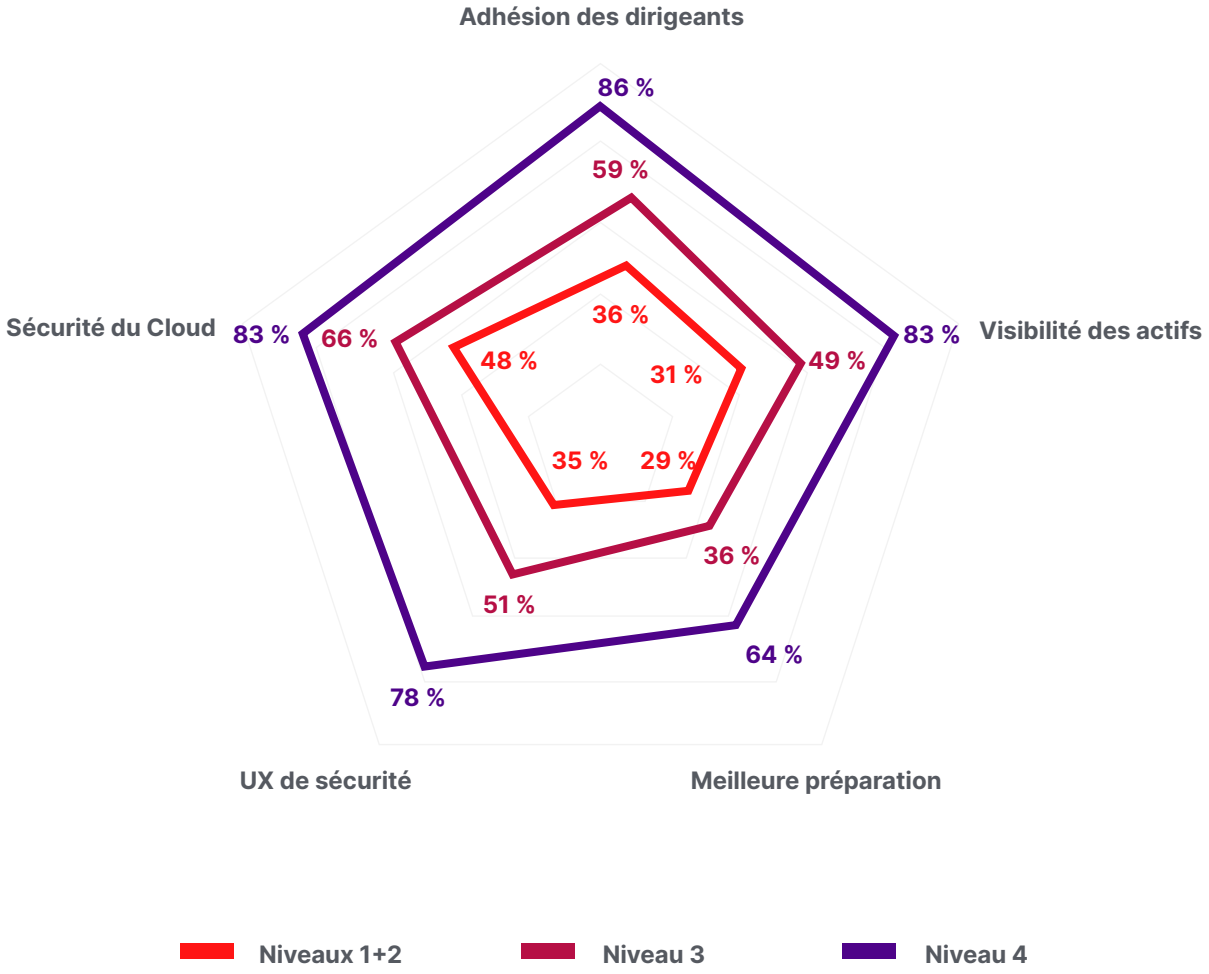
L'échelle de maturité de la cybersécurité

Nous avons demandé aux personnes travaillant dans le domaine de la cybersécurité d'évaluer le niveau de préparation de leur entreprise en matière de cybersécurité, du niveau de base (Niveau 1) aux meilleurs (Niveau 4). Nous avons ensuite comparé ces groupes pour en savoir plus sur les pratiques et comportements des entreprises de niveau 4.

Les entreprises dont la cybersécurité est la plus mature signalent une plus grande adhésion, et plus d'attention portée à la visibilité et à l'expérience utilisateur (UX).

Ces graphiques indiquent les pourcentages des personnes interrogées qui rapportent :

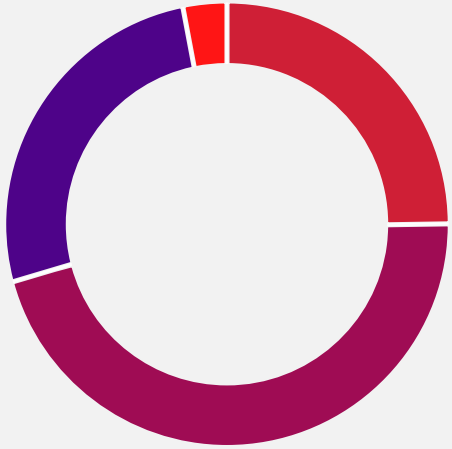
- Des dirigeants très favorables (« Adhésion des dirigeants »)
- Une bonne visibilité sur les utilisateurs, les périphériques, les applis et les services de leur réseau (« Visibilité des actifs »)
- Une bonne préparation aux menaces visant la supply chain (« Meilleure préparation »)
- Forte priorisation de l'UX des utilisateurs finaux concernant les interventions techniques liées à la cybersécurité (« UX de sécurité »)
- Davantage de sécurité dans l'adoption de leurs systèmes et/ou outils de stockage Cloud (« Sécurité du Cloud »)



Remarque : l'auto-perception est un mode de collecte des informations qui présente des limites, car les personnes interrogées peuvent ne pas être objectives lorsqu'elles évaluent leurs propres efforts. Cette autoévaluation peut expliquer en partie le nombre exceptionnellement faible de réponses de niveau 1 (c'est pourquoi nous les avons regroupées avec le niveau 2 pour ce rapport).

Nous pensons que les résultats basés sur ce modèle de maturité constituent des signaux utiles pour le domaine de la cybersécurité, mais nous demandons à nos lecteurs de garder à l'esprit les limites précédemment exprimées.

Réponses des professionnels de la cybersécurité par niveau (n=902)



4 %

Niveau 1 : Hygiène de cybersécurité élémentaire

25 %

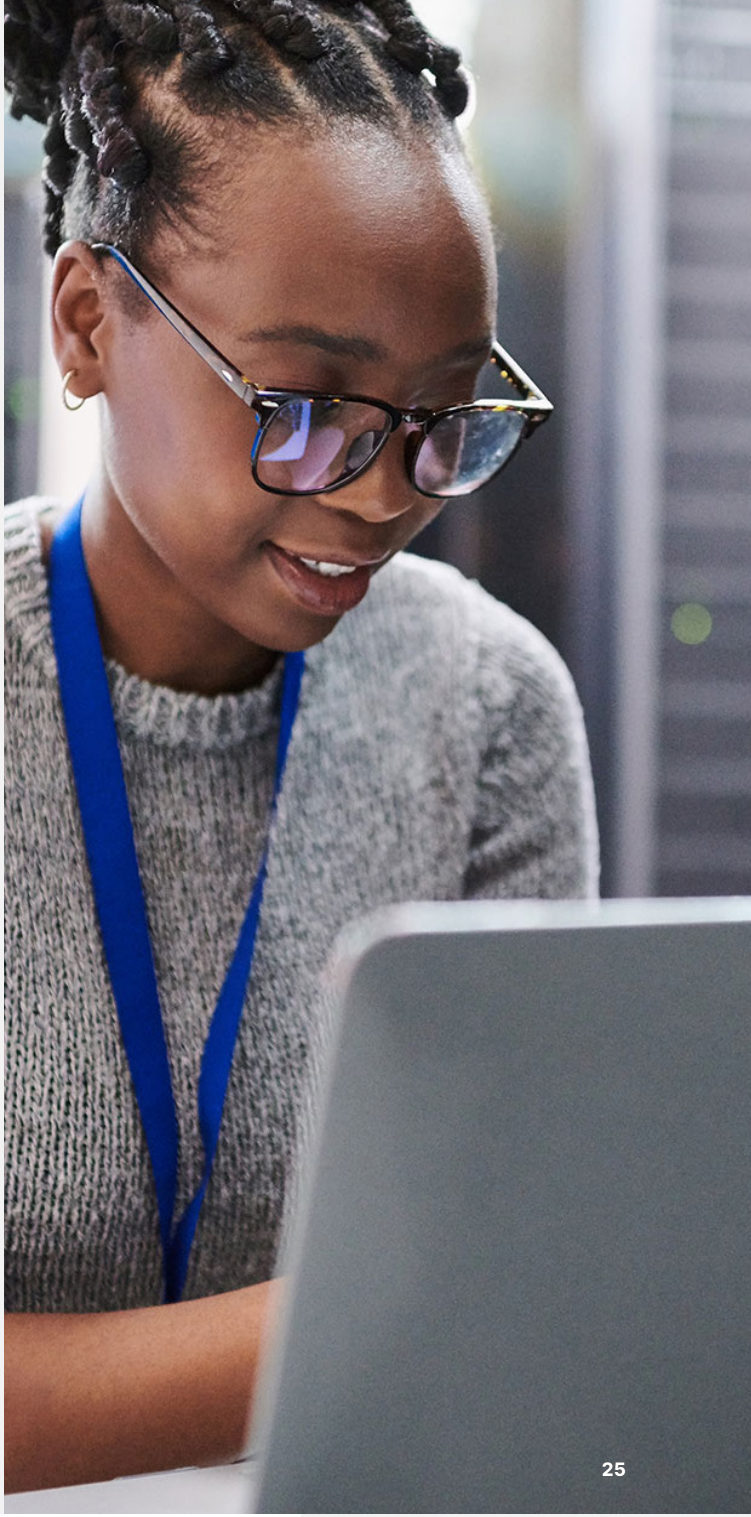
Niveau 2 : Hygiène de cybersécurité intermédiaire, avec des procédures et des stratégies établies

42 %

Niveau 3 : Hygiène de cybersécurité substantielle et proactive

29 %

Niveau 4 : Avancée, capacité prouvée à bloquer les menaces avancées



Quels sont les facteurs de différenciation des entreprises ayant une cybersécurité de niveau 4 ?

Adhésion des dirigeants : la grande majorité des entreprises qui se revendiquent de niveau 4 (86 %) disent qu'elles bénéficient de l'adhésion et du soutien des plus hauts responsables. Cette adhésion se manifeste de différentes façons : un soutien budgétaire pour renforcer les défenses, une grande autonomie pour concevoir des stratégies proactives au lieu de céder à la dernière envie du PDG quel que soit le rapport coût-bénéfice.

Visibilité des actifs : la plupart des entreprises de niveau 4 (83 %) bénéficient d'une très bonne visibilité sur les utilisateurs, les applis et les périphériques dans toute l'entreprise. En fait, elles sont 70 % plus susceptibles de le démontrer que celles de niveau 3. Avec la multiplication du nombre de périphériques et d'applis, la visibilité va être une préoccupation essentielle en 2023.

La CISA a récemment souligné cette nécessité, en publiant une nouvelle directive fin 2022 (BOD 23-01). La directrice de la CISA, Jen Easterly, explique : « En matière de réduction des risques, la première étape, pour une entreprise, consiste à connaître ce qui figure sur son réseau. »

Résilience de la supply chain : concernant la préparation de la supply chain, les entreprises de niveau 4 disent être mieux préparées que toutes les autres entreprises interrogées : 64 % déclarent être « très bien préparées » à faire face aux menaces visant la supply chain, contre seulement 36 % des entreprises de niveau 3.

« La préparation de la supply chain est un aspect auquel la plupart des entreprises ont encore du mal à s'adapter, en grande partie parce que le problème peut être extrêmement complexe » explique Michael Montoya, SVP & CISO chez Equinix. « Nous nous attendons à ce que la réduction des risques de la supply chain constitue un domaine d'investissement important en 2023, qu'il s'agisse de la mise en œuvre des nomenclatures logicielles (SBOM), du déploiement de solutions Zero Trust ou d'un contrôle d'accès complet. »

UX pour l'atténuation des risques : les meilleures entreprises savent qu'une expérience utilisateur (UX) d'excellence fait partie intégrante de la sécurité… c'est en fait un antidote au manque d'adhésion et aux solutions de contournement risquées. La plupart des entreprises de niveau 4 (71 %) disent que l'UX des utilisateurs finaux a une « priorité élevée » ou est un enjeu « à mission critique », soit 20 points de plus que les entreprises de niveau 3.

Sécurité dans le Cloud : les entreprises de niveau 4 sont bien plus enclines à affirmer que leurs systèmes basés dans le Cloud sont nettement plus sécurisés. En fait, elles sont trois fois plus susceptibles de dire que l'environnement Cloud est « bien plus sécurisé » que les entreprises de niveau 3.

> « L'inflation et les conditions macroéconomiques actuelles ont un effet d'entraînement et d'attraction sur les dépenses liées au Cloud. L'informatique Cloud va rester un bastion de sécurité et d'innovation. Sa nature agile, élastique et évolutive lui permet de soutenir la croissance lors des périodes difficiles. » — Sid Nag, Vice President Analyst chez Gartner®[11]

Une chose est certaine : les tactiques entièrement défensives ne fonctionneront pas en 2023. Michael Levin, Senior Vice President for Global Cyber Risk and Defense chez UnitedHealth Group explique ce concept au Wall Street Journal : « De nombreuses entreprises se concentrent encore sur les anciennes listes de contrôle et la conformité. “J’ai fait tout ce que vous avez demandé, je suis protégé”, au lieu de se demander “Comment me protéger ?” »[12]

N’oubliez pas que l’écrasante majorité des professionnels de la sécurité et des dirigeants nous ont dit que leur entreprise était aussi bien (voire mieux) préparée aujourd’hui qu’il y a un an. C’est ce qu’ont répondu 97 % d’entre eux ! Et pourtant, un sur cinq ne parierait pas un kopeck sur les mesures de sécurité mises en place. L’optimisme face à la réalité.

Pour faire face à des menaces qui changent sans cesse et restent encore inconnues, les entreprises doivent dépasser ce comportement réactif basé sur des règles (« J’ai fait tout ce que j’étais supposé faire »).

Les équipes chargées de la maturation de la cybersécurité doivent prendre en compte les considérations suivantes :

Automatisation : déployez l’automatisation pour améliorer la visibilité des actifs et mettez en place une priorisation des correctifs basée sur les risques (ce sont deux enjeux importants pour la sécurité des entreprises en 2023). Implémentez aussi une UX intelligente pour forcer les collaborateurs à adopter les bons comportements en matière de sécurité (c’est-à-dire, faire en sorte que les exceptions et les solutions de contournement causent plus de problèmes qu’elles n’en valent la peine).

Résilience : concevez des plans d’intervention et de récupération pour réduire la durée des interruptions et limiter l’effet domino, sachant que certaines attaques vont inévitablement réussir.

Autonomie : donnez à votre équipe Cybersécurité davantage d’autonomie dans l’élaboration de son calendrier. Arrêtez de réagir de façon irréfléchie face aux menaces qui font la une des journaux ou de sanctionner les équipes qui ne parviennent pas à venir à bout des listes interminables de priorités en constante évolution !

Gestion globale des risques : avec la possibilité de travailler de n’importe où, le fonctionnement en mode hybride, la collaboration avec les sous-traitants et les fournisseurs, la sécurité ne s’arrête pas à la porte de l’entreprise. Adoptez une approche risque-récompense vis-à-vis de ces acteurs, en accordant une attention particulière à vos « baleines » de sécurité comme les hauts responsables ou les fournisseurs de logiciels fortement intégrés.

Finalement, si l’on repart sur de nouvelles bases pour mieux préparer la cybersécurité et passer d’une approche réactive et défensive à une approche tournée vers l’avenir et résiliente, nombreuses sont les entreprises qui seront prêtes à parier ce fameux kopeck sur leur sécurité.

05

Méthodologie

Ivanti a interrogé plus de 6 500 dirigeants, professionnels de la cybersécurité et employés de bureau en octobre 2022. Notre objectif : comprendre les menaces d'aujourd'hui, du point de vue des professionnels de la sécurité comme de celui des autres travailleurs. Nous voulions aussi savoir comment les entreprises se préparent aux menaces futures, encore inconnues.

L'étude a été réalisée par Ravn Research et les panélistes ont été recrutés par MSI Advanced Customer Insights. Les résultats de l'enquête ne sont pas pondérés. D'autres résultats par pays sont disponibles sur demande.

Secteurs d'activité

6 %
Éducation

12 %
Services financiers

12 %
Administrations

13 %
Fabrication/transformation

3 %
Orgs caritatives/à but non lucratif

18 %
Autre, merci de préciser

8 %
Services professionnels

11 %
Vente au détail ou en gros, e-commerce

14 %
Technologie

3 %
Télécoms

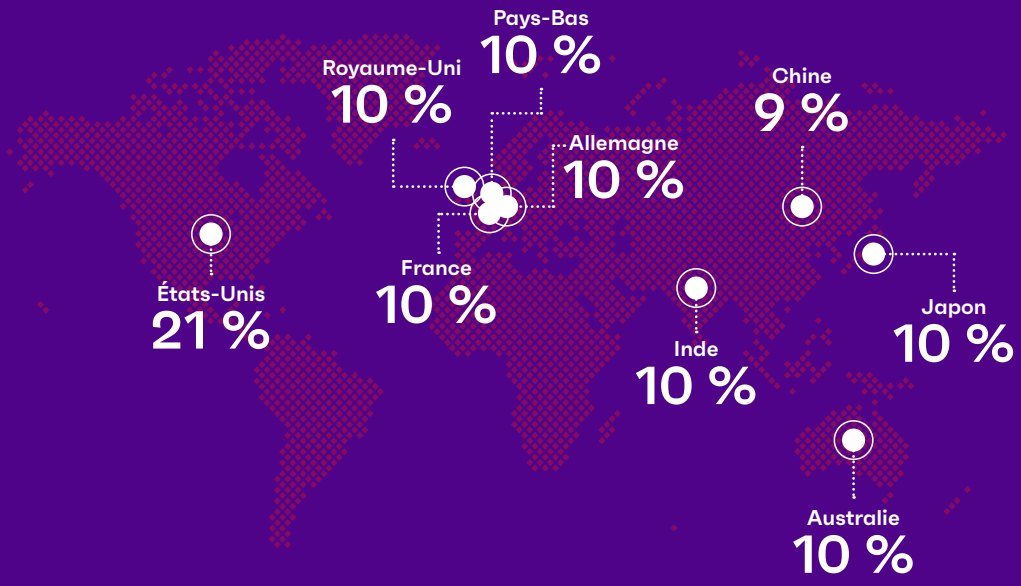
Échantillon d'enquête

Employés de bureau
5 202

Professionnels de la sécurité
902

Dirigeants
454

Pays



Références

Tous les graphiques de ce rapport ont été générés à partir des données d'enquête collectées dans le cadre de la série « Ivanti State of Cybersecurity Preparedness 2023 », comme décrit à la section « Méthodologie ».

1. PwC : « A C-suite united on cyber-ready futures: Findings from the 2023 Global Digital Trust Insights », sept. 2022. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html

2. SHRM : « 2023 Salary Budgets Projected to Stay at 20-Year High but Trail Inflation », sept. 2022 https://www.shrm.org/resourcesandtools/hr-topics/compensation/pages/2023-salary-increase-budgets-stay-trail-inflation.aspx

3. The Wall Street Journal : « Cybersecurity Tops the CIO Agenda as Threats Continue to Escalate », oct. 2022. https://www.wsj.com/articles/cybersecurity-tops-the-cio-agenda-as-threats-continue-to-escalate-11666034102

4. IBM : « Cost of a Data Breach 2022: A million-dollar race to detect and respond », juillet 2022. https://www.ibm.com/reports/data-breach

5. The Wall Street Journal : « Microsoft's New Security Chief Says It Is Time to Take Shelter in the Cloud », fév. 2022. https://www.wsj.com/articles/microsofts-new-security-chief-says-it-is-time-to-take-shelter-in-the-cloud-11645624800

6. InfoSecurity Group : « Cybersecurity Workforce Gap Grows by 26% in 2022 », oct. 2022. https://www.infosecurity-magazine.com/news/cybersecurity-workforce-gap-grows/

7. Supply Chain Brain : « Why Cybersecurity Has Never Been More Important for the Supply Chain Sector », oct. 2022. https://www.supplychainbrain.com/blogs/1-think-tank/post/35798-why-cybersecurity-has-never-been-more-important-for-the-supply-chain-sector

8. The Wall Street Journal : « Rise in Cyberattacks Stretches and Stresses Defenders », oct. 2022. https://www.wsj.com/articles/rise-in-cyberattacks-stretches-and-stresses-defenders-11664962202

9. Ivanti : « State of IT in 2021 », déc. 2021. https://www.ivanti.com/company/press-releases/2021/new-ivanti-study-finds-the-biggest-challenge-for-it-departments-is-keeping-up-with-digital-transformation-and-keeping-talent-in-technical-roles

10. CISA : « CISA Directs Federal Agencies to Improve Cybersecurity Asset Visibility and Vulnerability Detection », oct. 2022. https://www.cisa.gov/news/2022/10/03/cisa-directs-federal-agencies-improve-cybersecurity-asset-visibility-and

11. Communiqué de presse Gartner : « Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $600 Billion in 2023 » , oct. 2022. https://www.gartner.com/en/newsroom/press-releases/2022-10-31-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-600-billion-in-2023. GARTNER est une marque déposée et une marque de service de Gartner, Inc. et/ou de ses filiales aux États-Unis et dans d'autres pays, et elle est utilisée ici avec sa permission. Tous droits réservés.

12. The Wall Street Journal: « Cybersecurity Tops the CIO Agenda as Threats Continue to Escalate », Oct. 2022. https://www.wsj.com/articles/cybersecurity-tops-the-cio-agenda-as-threats-continue-to-escalate-11666034102

Informations supplémentaires sur les graphiques

Pg. 3 - Professionnels de sécurité et dirigeants interrogés : 1 356

Pg. 5 - Professionnels de sécurité et dirigeants interrogés : 1 356

Pg. 7 - Professionnels de sécurité et dirigeants interrogés : 1 356

Pg. 8 - Professionnels de sécurité interrogés : 902

Pg. 9 - Professionnels de sécurité et dirigeants interrogés : 1 341

Pg. 11 - Professionnels de sécurité interrogés : 902

Pg. 13 - Professionnels de sécurité interrogés : 902

Pg. 14 - Professionnels de sécurité et dirigeants interrogés : 1 356

Pg. 15 (« informations d'authentification d'un collaborateur ») - Professionnels de sécurité interrogés : 902

Pg. 15 (« [...] informations d'authentification d'un fournisseur tiers ») - Professionnels de sécurité interrogés : 882

Pg. 17 (« comment priorisez-vous ») - Professionnels de sécurité interrogés : 902

Pg. 17 (« une méthode pour prioriser ») - Professionnels de sécurité interrogés : 886

Pg. 20 - Dirigeants et employés de bureau interrogés : 5 656

Pg. 21 (« Plus d'un tiers ») - Dirigeants et employés de bureau interrogés : 1 949

Pg. 21 (« près d'un quart ») - Dirigeants et employés de bureau interrogés : 5 656

Pg. 21 (« les dirigeants sont bien plus ») - Dirigeants et employés de bureau interrogés : 5 373

Pg. 21 (« dirigeants interrogés » - Dirigeants et employés de bureau interrogés : 5 656

Pg. 24 (« Adhésion des dirigeants ») - Professionnels de sécurité et dirigeants interrogés : 1 356

Pg. 24 (« Visibilité des actifs ») - Professionnels de sécurité et dirigeants interrogés : 1 356

Pg. 24 (« Meilleure préparation ») - Professionnels de sécurité interrogés : 902

Pg. 24 (« UX de sécurité ») - Professionnels de sécurité interrogés : 902

Pg. 24 (« Sécurité du Cloud ») - Professionnels de sécurité et dirigeants interrogés : 1 341

Repartez sur de nouvelles bases :

Rapport sur l'état de la cybersécurité en 2023

Alors que les entreprises aspirent à une protection renforcée contre les cyberattaques, le secteur peine à se débarrasser de pratiques réactives.

ivanti

ivanti.fr
+33 (0)1 49 03 77 80
contact@ivanti.fr