ivanti

Rapport sur l'état de la cybersécurité des gouvernements

4 mesures importantes pour agir et impulser le changement en 2023

S'inscrit dans la série Ivanti de rapports sur l'état de la cybersécurité.

Le bon moment ? Maintenant

Les attaques récentes contre des réseaux hospitaliers, des systèmes logistiques internationaux et même des élections démocratiques représentent une menace fondamentale pour la sécurité publique et la gouvernance.

Mais ce n'est que le début.

Avec les progrès rapides de l'IA générative et des « deepfakes », la diffusion de ransomwares va prendre des formes encore plus crédibles… et donc, plus dangereuses.

Les gouvernements du monde entier en ont pris conscience. Les initiatives de l'administration Biden, ainsi que les directives de la Commission européenne, trahissent le nouvel état d'urgence mondiale visant à protéger les actifs et les infrastructures critiques contre les cyberattaques.

Ivanti a interrogé plus de 800 fonctionnaires gouvernementaux pour comprendre :

- Le comportement des collaborateurs et leur attitude envers la cybersécurité
- L'impact d'une organisation du travail flexible et hybride dans le secteur public
- L'opinion des professionnels de la cybersécurité sur les menaces émergentes et les technologies de sécurité

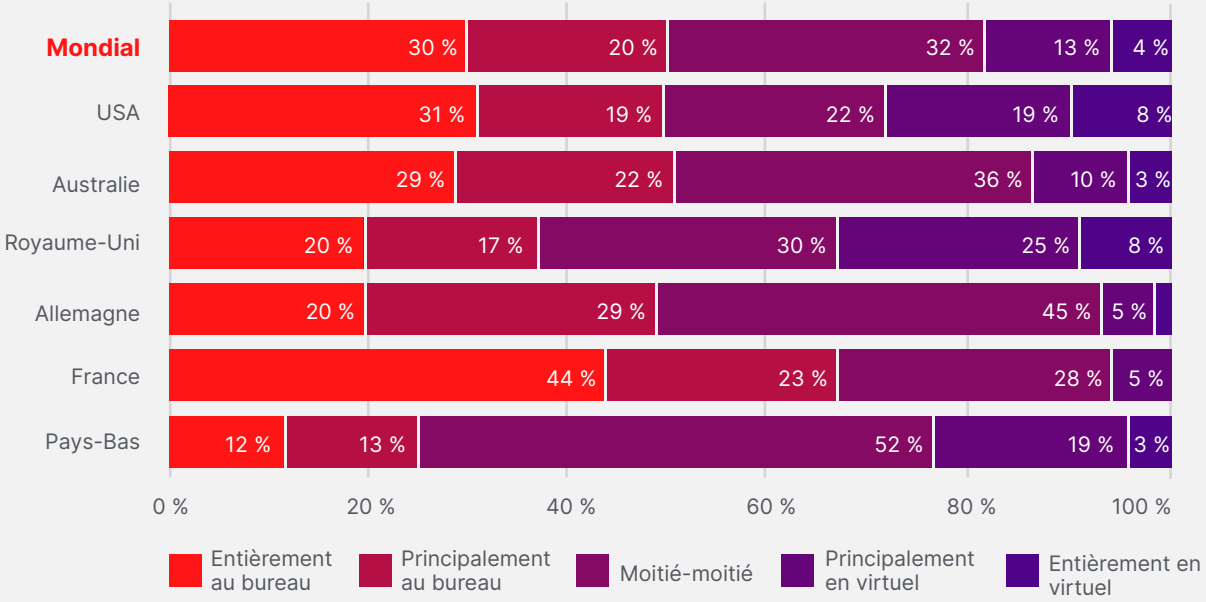
Pourquoi cette extrême urgence ?

Il ne s'agit pas seulement de nouveaux modes d'attaque et de directives gouvernementales très médiatisées. La nature même du travail des entités gouvernementales a complètement changé en seulement quelques années (sans aucune planification d'un tel bouleversement). Le travail hybride a ouvert une frontière de vulnérabilité supplémentaire.

Une nouvelle réalité

70 % des fonctionnaires travaillent en virtuel au moins une partie du temps.

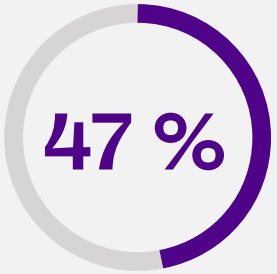
Q: Parmi ces réponses, laquelle décrit le mieux le mode de travail des personnes occupant des postes de bureau dans votre organisation ?



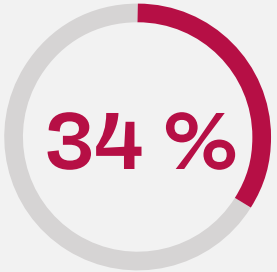
**Les résultats pour les différents pays ne donnent pas forcément un total de 100 % en raison des erreurs d'arrondi.*

De nouveaux risques

La multiplication des périphériques, des utilisateurs et des lieux de travail renforce la complexité et ajoute de nouvelles vulnérabilités.



des professionnels de la sécurité dans le monde disent manquer de visibilité sur l'ensemble des utilisateurs, périphériques, applications et services de leurs réseaux.



des fonctionnaires gouvernementaux que nous avons interrogés utilisent le même mot de passe (ou des mots de passe similaires) sur plusieurs périphériques.

Sommaire :

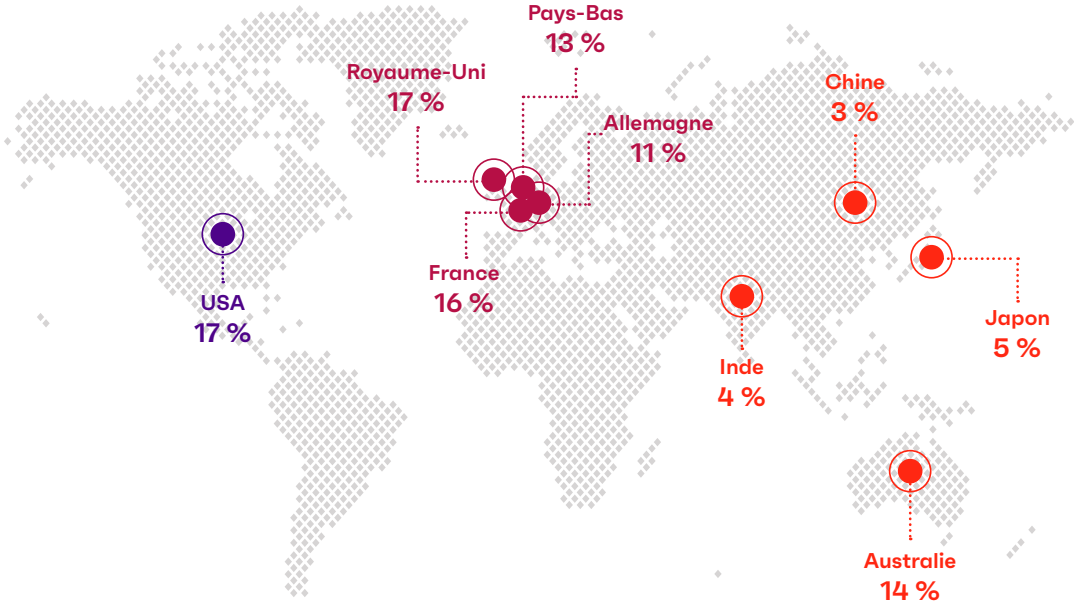
ivanti

Méthodologie

Ivanti a interrogé plus de 6 500 dirigeants, professionnels de la cybersécurité et collaborateurs de bureau au cours du 4e trimestre 2022 pour comprendre les menaces d'aujourd'hui et savoir comment les entreprises se préparent aux menaces futures encore inconnues. C'était l'objet de notre publication, Repartez sur de nouvelles bases : *Rapport sur l'état de la cybersécurité en 2023*.

Les informations collectées ici reposent sur les réponses d'un sous-ensemble de ces personnes : les collaborateurs de bureau travaillant pour les gouvernements du monde entier (803 au total), ainsi que des professionnels de la cybersécurité de plusieurs secteurs.

Fonctionnaires gouvernementaux interrogés (n=803)



01

Aucune « culture de responsabilité »

ivanti

Problème actuel

L'attitude « ce n'est pas mon travail » compromet la cybersécurité des gouvernements

Le désengagement des collaborateurs menace réellement la sécurité des entreprises. Selon le Partnership for Public Service, les scores d'engagement et de satisfaction dans le secteur public sont inférieurs de 15 points à ceux des collaborateurs du secteur privé.[1]

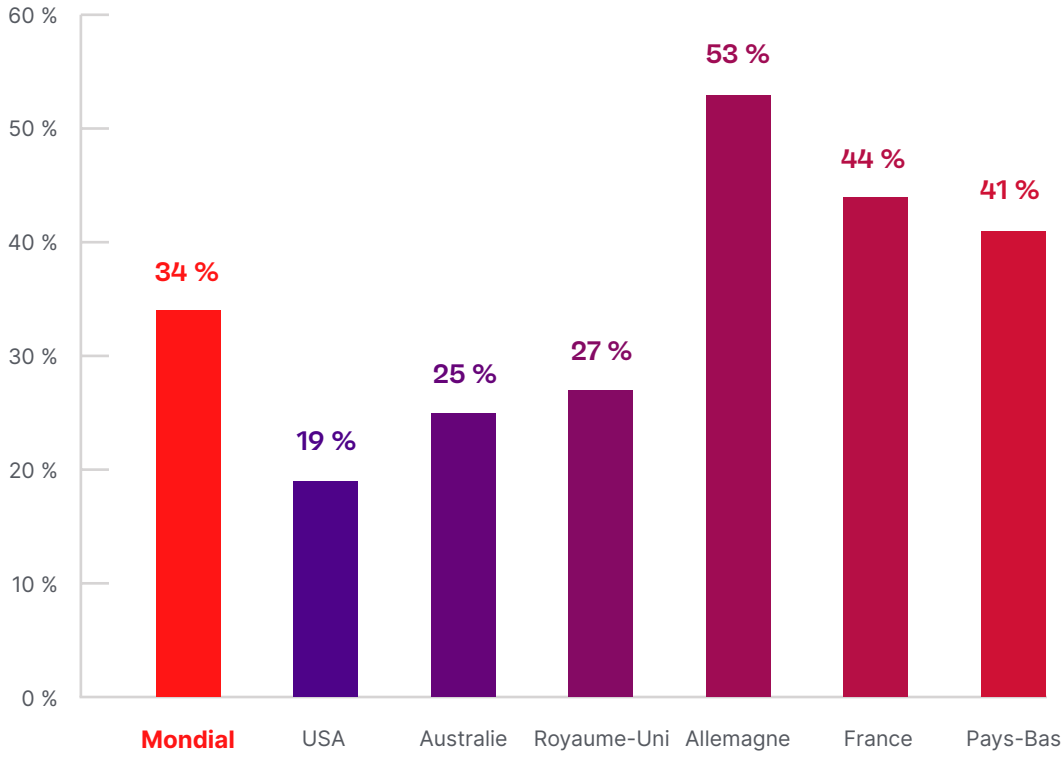
Et ce faible engagement signifie que les collaborateurs ne se sentent pas concernés ni responsables de la santé de l'organisation dans son ensemble.

Les recherches d'Ivanti le montrent : une grande partie des fonctionnaires dans le monde pense que leurs actions n'ont pas d'impact sur la sécurité.

Au Royaume-Uni, 27 % des collaborateurs du gouvernement disent que leurs actions n'ont aucun impact sur la capacité de leur organisation à se prémunir des cyberattaques ; en Allemagne, ce chiffre atteint 53 %.

Les collaborateurs pensent-ils que leurs propres actions comptent ?

Q: Pensez-vous que vos actions ont un impact sur la capacité de votre organisation à se protéger des cyberattaques ?



« Mes actions n'ont aucun impact sur la capacité de mon organisation à se protéger des cyberattaques. »

Certains fonctionnaires ne signalent pas les activités suspectes.

17 % ont peur de signaler à l'équipe de cybersécurité une erreur qu'ils ont faite au travail.

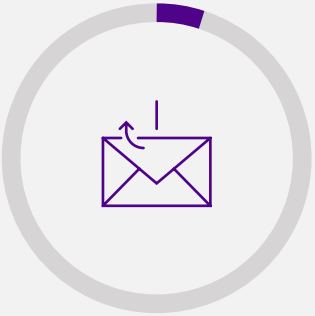
36 % n'ont pas signalé un e-mail d'hameçonnage reçu au travail.

21 % disent qu'ils ne s'inquiètent pas d'un éventuel piratage de lors organisation.

L'hameçonnage des employés gouvernementaux est un prélude aux cyberattaques

30 %

disent avoir été victimes d'hameçonnage



5 %

ont été victimes d'une tentative d'hameçonnage, soit en cliquant sur un lien, soit en envoyant de l'argent.

Pourquoi c'est important

Un véritable ouragan de cybersécurité menace toutes les entités gouvernementales

Des vecteurs de menace multiples et efficaces

Le secteur public est particulièrement vulnérable aux attaques, en raison de la taille et de la valeur de la cible qu'il représente. Au cours de l'année écoulée, les groupes de pirates sponsorisés par des États, comme APT29, se sont tous révélés des ennemis redoutables et évoluant rapidement.[2]

Un contenu numérique « synthétique » en évolution rapide

Grâce à l'IA générative, les emails d'hameçonnage sont devenus parfaits, d'autant qu'ils sont personnalisés en fonction des vulnérabilités de chaque cible.[3]

Encore plus inquiétant : les deepfakes menacent la crédibilité du journalisme et des élections démocratiques partout dans le monde.[4]

Les contraintes budgétaires et les silos organisationnels ruinent les efforts de sécurité

Le Government Accountability Office (GAO) des États-Unis affirme que 60 % de ses recommandations en matière de cybersécurité n'ont pas été implémentées lors de la dernière décennie.[5]

Un fort taux de désengagement des collaborateurs

L'engagement moyen des fonctionnaires fédéraux américains est de 64,5 %, soit 14 points de moins que dans le privé.[6]

72 %

des fonctionnaires n'ont jamais contacté l'équipe Sécurité pour poser une question ou exprimer une inquiétude.

ivanti

Comment réagir

Faites de la sécurité une responsabilité partagée par tous les collaborateurs

Les responsables de la sécurité ne peuvent pas obliger les collaborateurs à se soucier de la cybersécurité, mais ils peuvent influencer leur attitude au fil du temps en investissant dans une culture de sécurité positive et en la développant.

Qu'est-ce qui définit une culture de sécurité positive ?

Ouverture

Les collaborateurs sont à l'aise pour poser des questions à l'équipe Sécurité.

Intégration

Les responsabilités de sécurité sont partagées ; chaque collaborateur a un rôle à jouer.

Sécurité

Les collaborateurs n'hésitent pas à signaler les incidents ou les erreurs.

Répétition

La formation est fréquente, répétée et attrayante.

Stratégie

La sécurité est un actif, indispensable à la réussite de l'entreprise.

Étapes suivantes

Auditez, impliquez et optimisez l'expérience de vos collaborateurs pour une culture de sécurité positive

1

Audit

Interrogez les collaborateurs pour définir une baseline, et documentez les comportements et attitudes actuels. Les résultats vous aideront à identifier les faiblesses spécifiques de votre organisation et à dégager une feuille de route vers le changement.

2

Implication

Échangez avec les dirigeants de l'entreprise pour obtenir leur soutien et leur adhésion. Les dirigeants donnent le ton, mais représentent aussi l'un des groupes les plus à risque.

Pour en savoir plus sur les risques de cybersécurité que présentent les dirigeants, consultez la page 19 (Les attaques de whaling dans les entités gouvernementales).

3

Optimisation

Un changement culturel n'est jamais « fait une fois pour toutes ». C'est un processus continu, qui exige de surveiller les métriques de performances clés, d'écouter les collaborateurs et de corriger le tir si nécessaire.

02

(Mauvaise) gestion des mots de passe : le « niveau zéro » de la sécurité

ivanti

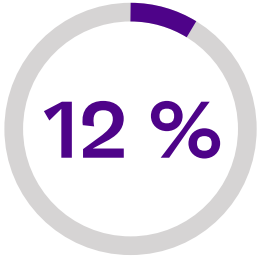
Problème actuel

Le manque de cyberhygiène (y compris les mauvaises habitudes concernant les mots de passe) hante les entités gouvernementales

Les experts de la sécurité tirent la sonnette d'alarme concernant les risques liés aux mots de passe depuis plus de dix ans. Pourtant, la plupart des entreprises, y compris les entités gouvernementales, adoptent encore parfois une approche laxiste en matière de gestion des mots de passe. Les recherches Ivanti dévoilent toute une gamme de mauvaises habitudes chez les fonctionnaires interrogés.

ivanti

Erreurs des gouvernements concernant l'accès aux mots de passe

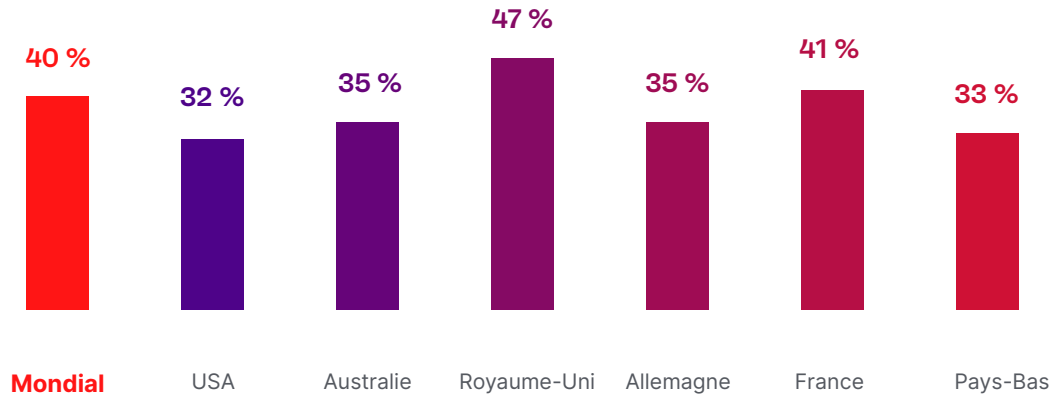


des fonctionnaires admettent avoir accès à des informations sensibles dont ils n'ont pas besoin dans le cadre de leur travail.

1 sur 3

pense que les mots de passe qu'il utilisait dans son ancien travail fonctionnent toujours.

Pourcentage des fonctionnaires gouvernementaux qui utilisent le même mot de passe pendant plus d'un an



Pourquoi c'est important

L'équilibre entre sécurité et facilité d'utilisation

Le « Shadow IT » et autres solutions de contournement sont les ennemis des entreprises sécurisées. Lorsque les collaborateurs trouvent une mesure de sécurité inefficace ou lourde, ils cherchent un moyen de la contourner, généralement dangereux.

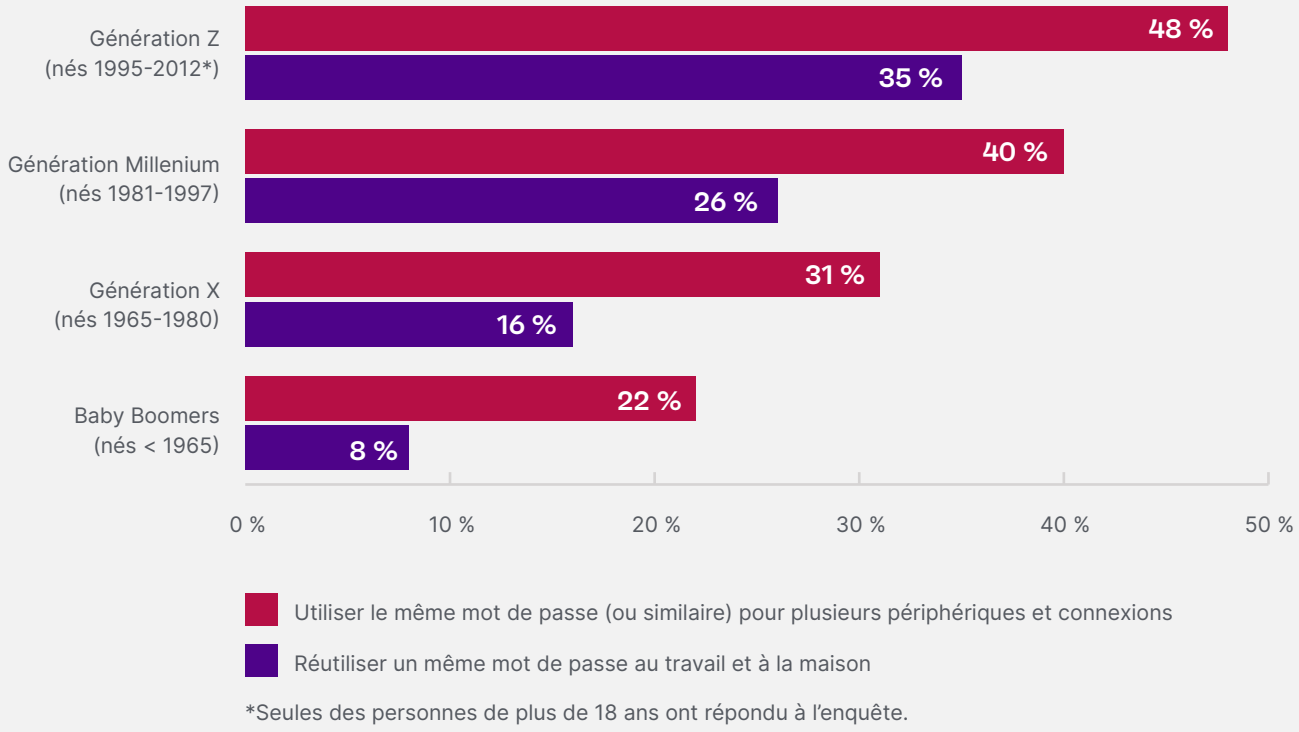
Les mots de passe constituent le niveau zéro des contournements de sécurité par les collaborateurs. Dans tous les secteurs, les collaborateurs continuent à utiliser des post-its, des surnoms, des dates de naissance… ou le célèbre code impossible à craquer : « 12345 ».

Les entités gouvernementales ont besoin de solutions de sécurité tellement pratiques et simples que les collaborateurs ne cherchent même pas à les contourner.

Le mythe des « natifs du numérique »

Vous pensez que vos collaborateurs les plus jeunes maîtrisent mieux la sécurité des mots de passe ? Ce n'est pas ce que montrent les chiffres.

Q: Lorsqu'on vous a demandé de créer un mot de passe au travail, lesquelles de ces opérations avez-vous exécutées ces deux dernières années ?



*Seules des personnes de plus de 18 ans ont répondu à l'enquête.

Comment réagir

Investissez dans la DEX (Expérience numérique des collaborateurs) pour renforcer la sécurité

Les équipes de sécurité doivent évaluer les nouvelles stratégies ou technologies du point de vue de l'expérience numérique des collaborateurs (DEX), et se demander « L'expérience utilisateur final va-t-elle encourager les solutions de contournement ou autres comportements déconseillés pour plus de praticité ? Et si oui, cela vaut-il la peine de prendre le risque ? »

Étapes suivantes

Implémenter des expériences conviviales tout en assurant la sécurité

1 Ciblez les solutions de contournement à haut risque

- Collaborateurs qui contournent la sécurité au nom de la praticité
- Dirigeants qui réclament des exceptions aux règles de sécurité

2 Priorisez les technologies orientées DEX

- Mise en place d'expériences centrées sur l'utilisateur (moins de friction = meilleure conformité)
- Élimination de l'intervention humaine lorsque c'est possible
- Interdiction des exceptions

Répercussions dans le monde réel

Implémentation d'une architecture Zero Trust (ZTA) et remarques sur la DEX

Qu'elles utilisent l'authentification à deux facteurs, des jetons ou des données biométriques, les entreprises comme les entités gouvernementales doivent prioriser (et s'engager à appliquer) un modèle d'accès le moins privilégié pour tous les collaborateurs, avec une stratégie d'architecture Zero Trust (ZTA).

Avec le ZTA, les solutions IT et Sécurité interagissent pour vérifier en continu l'état de la sécurité et de la conformité, en octroyant à chaque collaborateur uniquement le niveau d'accès nécessaire.

Entre autres avantages pour la sécurité, cet accès limité garantit la sécurité d'une entité tout en permettant des modalités de travail flexibles.

Après tout, si un collaborateur est victime d'une attaque par hameçonnage, le pirate ne peut accéder qu'aux options limitées dont dispose ce collaborateur.

Cependant, le ZTA peut s'avérer excessivement lourd pour les opérations quotidiennes (pour les collaborateurs) et la maintenance (pour le personnel IT), ce qui encourage l'utilisation du Shadow IT et balaie tous les avantages du ZTA.

C'est pourquoi les entités gouvernementales qui envisagent le ZTA doivent s'appuyer sur :

- Une automatisation stratégique qui signale les périphériques inconnus, émet une alerte en cas de comportement suspect et applique un délai de temporisation aux privilèges utilisateur.
- Des playbooks et des arbres de décision IT pour gérer les demandes de permissions et les requêtes courantes.
- Des instructions intuitives et faciles d'accès pour permettre aux utilisateurs finaux de « trouver de l'aide par eux-mêmes » avant de soumettre un ticket IT.

Ressources supplémentaires concernant le ZTA et la DEX

- Publication spéciale NIST 800-207 (« Zero Trust Architecture »)
- Rapport 2022 : De la nécessité d'améliorer l'expérience digitale des collaborateurs
- Premiers pas avec la DEX : principaux points à prendre en compte pour offrir une expérience numérique de qualité aux collaborateurs
- L'expérience collaborateur à l'ère de l'Everywhere Workplace : pourquoi le département IT doit-il être à l'avant-garde

03

Formation pour tous : l'importance du facteur humain dans les lacunes de cybersécurité des entités gouvernementales

ivanti

Problème actuel

Les inégalités de formation à la cybersécurité mettent à mal les défenses des gouvernements

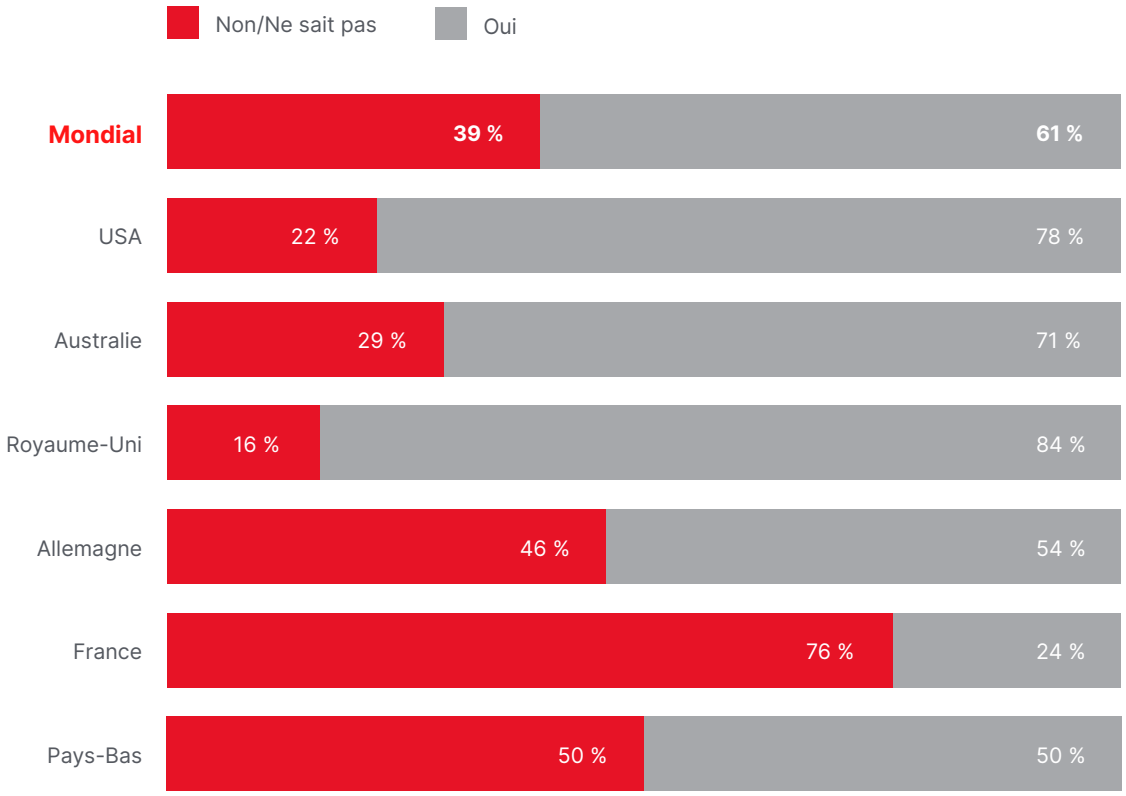
Les technologies de sécurité et d'automatisation assurent une puissante protection de première ligne, mais la formation des collaborateurs pour qu'ils soient les yeux et les oreilles de l'organisation en matière de sécurité est une ligne de défense secondaire indispensable. Les études Ivanti montrent que, dans le secteur public, la formation ne concerne pas l'ensemble des collaborateurs.

27 %

27 % seulement des fonctionnaires se disent « très bien préparés » à reconnaître et à signaler les menaces de type malware et hameçonnage au travail.

La formation pour tous ? On en est très loin.

Q: « Votre organisation dispense-t-elle une formation obligatoire à la cybersécurité ? »



Pourquoi c'est important

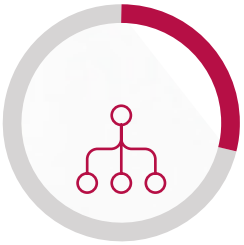
Les fonctionnaires et sous-traitants des gouvernements signalent une formation très rare ou insuffisante, malgré les réglementations

Le rapport « Repartez sur de nouvelles bases : Rapport sur l'état de la cybersécurité en 2023 » sur les professionnels de la sécurité dans le monde entier montre qu'une grande partie des entreprises sont bien loin des niveaux souhaités en matière de formation des collaborateurs aux risques de cybersécurité et aux processus de signalement.

Dans une entité gouvernementale, l'erreur d'une seule personne peut entraîner des dommages involontaires et catastrophiques, avec des incidences sur les administrés.

32 %

des professionnels de la sécurité disent que la formation inefficace ou incomplète des collaborateurs représente un frein significatif à l'excellence de la cybersécurité dans leur organisation.



29 %

des organisation dans le monde ne demandent pas à leurs partenaires et/ou fournisseurs de suivre une formation à la cybersécurité… ce qui est dangereux pour les entités gouvernementales qui travaillent avec des sous-traitants.

Données du rapport
Repartez sur de nouvelles bases : Rapport sur l'état de la cybersécurité en 2023

Répercussions dans le monde réel

Les attaques de whaling dans les entités gouvernementales

Les attaques de whaling (aussi connues sous le nom de whalephishing ou hameçonnage à la baleine) utilisent des tactiques d'ingénierie sociale pour viser des cibles à forte valeur et à haut risque, les « baleines ». Les cibles habituelles de l'hameçonnage à la baleine sont les chefs de division, les personnalités publiques et les directeurs financiers… ou même leurs assistants ou le personnel administratif de la division visée.

Après avoir trompé leur cible en faisant croire qu'une communication est légitime, les acteurs de la menace obtiennent des informations d'identification, des informations sensibles ou même des autorisations frauduleuses de virement bancaire.

Ce type d'accès passe souvent inaperçu et n'est pas signalé pendant longtemps, ce qui permet aux groupes APT de rôder sur le réseau de l'entité gouvernementale pendant des mois, voire des années.[7]

Et les études montrent que ce sont précisément les personnes avec le plus haut niveau d'accès aux informations et réseaux sensibles qui ont les plus mauvaises habitudes de sécurité.

Les hauts responsables sont bien plus sujets aux comportements de sécurité dangereux que les autres collaborateurs.

Plus d'un dirigeant sur 3 a déjà cliqué sur un lien d'hameçonnage, soit quatre fois plus que le collaborateur de bureau moyen !

Près d'1/4 des dirigeants utilisent des dates de naissance faciles à mémoriser dans leurs mots de passe.

Les dirigeants sont bien plus susceptibles de garder les mêmes mots de passe pendant plusieurs années que les autres collaborateurs. En fait, 1/4 des dirigeants interrogés le font.

Les dirigeants sont cinq fois plus susceptibles de partager leur mot de passe avec des personnes extérieures à l'entreprise.

*Ces statistiques s'appliquent aux dirigeants de tous les secteurs, y compris du secteur public, comme le montre le rapport *Repartez sur de nouvelles bases : Rapport sur l'état de la cybersécurité en 2023*

Comment réagir

Mettre en place une formation pour tous les collaborateurs gouvernementaux afin de limiter les risques tout en améliorant les comportements

L'une des meilleures façons d'atteindre les informations sensibles accessibles aux « baleines » (ou utilisateurs à privilèges), c'est de passer par les collaborateurs qui travaillent avec des cibles à haute valeur :

- un assistant administratif influent,
- la nouvelle recrue qui attend à l'entrée,
- des sous-traitants tiers experts en visite pour la journée.

Même si ces personnes n'ont pas officiellement un accès direct aux supports de stockage et aux informations privées, elles constituent la porte d'accès idéale aux informations et supports les plus sensibles d'une entité du fait des mauvaises habitudes de sécurité adoptées par commodité, et de leur proximité avec des cibles à haute valeur.

Une bonne formation en cybersécurité couvre deux aspects :

Quoi

Les types d'attaque spécifiques, et comment les reconnaître et les repousser.

Pourquoi

Le rôle critique joué par chaque collaborateur, quels que soient son poste, son rôle et son lieu de travail.

Étapes suivantes

Une « formation pour tous » mais sans approche à « taille unique »

1

Formez des ambassadeurs

Désignez des « ambassadeurs de sécurité » très bien formés. Des personnes qui ne travaillent pas dans la sécurité mais s'y intéressent.

2

Portez une attention particulière aux collaborateurs à haut risque

Identifiez les maillons faibles de l'entreprise et développez un programme sur mesure pour chacun, en vous concentrant sur des scénarios réalistes pour l'entité gouvernementale concernée, sur la base des menaces récentes.

3

Pensez positif

Proposez des formations attrayantes qui laisseront un souvenir mémorable. Les cours magistraux ont bien sûr leur place, mais rendez l'apprentissage ludique en organisant des compétitions ou en recourant à des scénarios de gamification.

ivanti

04

Comment préparer les entités gouvernementales à l'avenir

ivanti

Problème actuel

Systèmes traditionnels, complexité de la pile technologique, silos de données, pénurie de talents...

Beaucoup pensent que les entités gouvernementales, les grandes municipalités, les organismes fédéraux ou militaires, ou les entreprises publiques, savent tout de la cybersécurité.

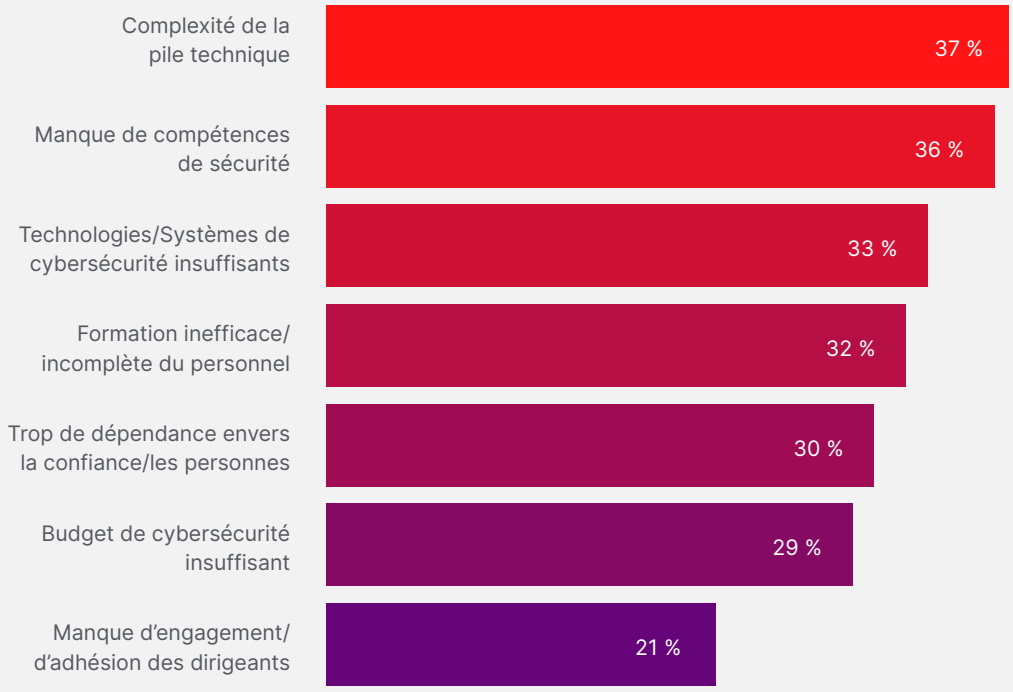
(En matière de cybersécurité, il est vrai que le secteur militaire concentre les talents les plus brillants et les technologies les plus avancées.)

En réalité, la plupart des entités gouvernementales manquent de financement durable pour investir dans :

- les talents
- les nouvelles technologies
- la formation
- la culture

Obstacles les plus fréquemment signalés à l'excellence en matière de cybersécurité dans le monde

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



Informations du rapport
Repartez sur de nouvelles bases : Rapport sur l'état de la cybersécurité en 2023

Pourquoi c'est important

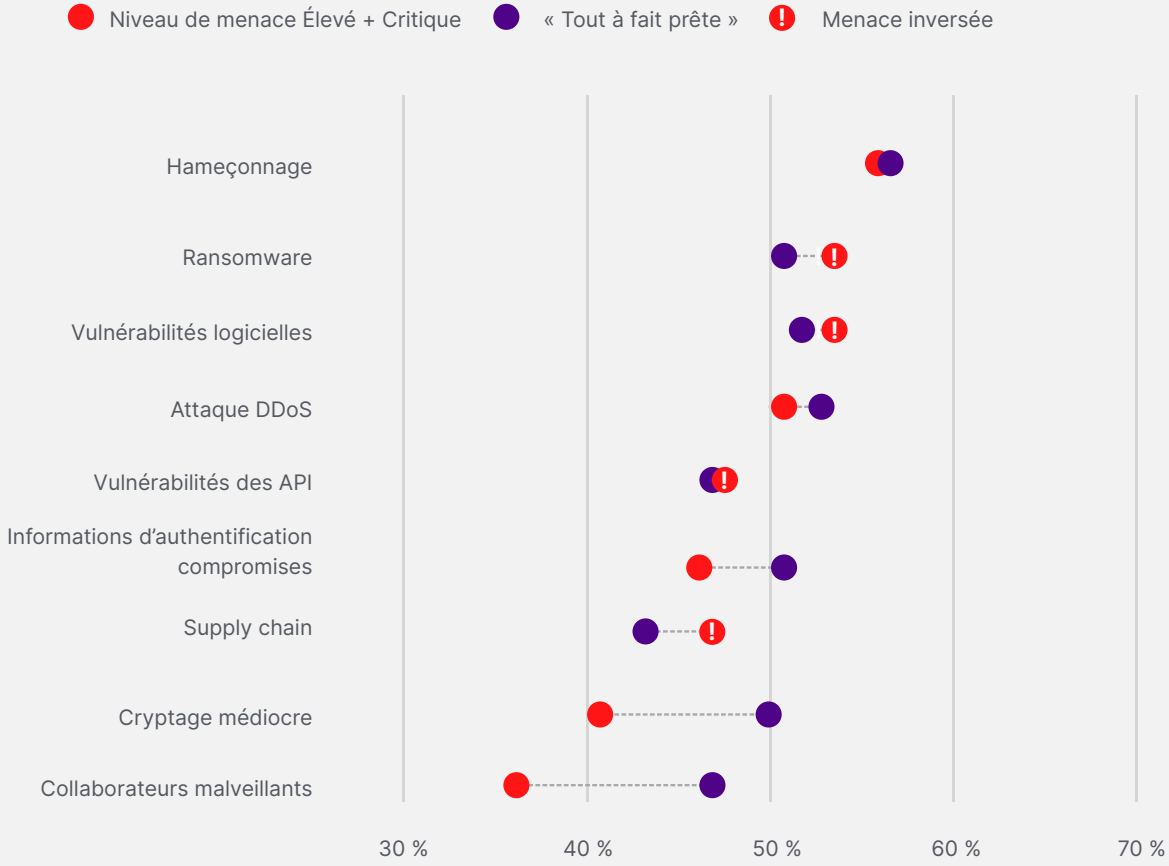
Les pirates continuent à créer des armes innovantes face à nos anciennes défenses

Selon un rapport du Government Accountability Office (GAO) des États-Unis, le gouvernement fédéral américain n'a toujours pas mis en œuvre plus de la moitié des recommandations du GAO, depuis 2010.[8]

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 ?

Menaces de sécurité et niveau de préparation



Informations du rapport
Repartez sur de nouvelles bases : Rapport sur l'état de la cybersécurité en 2023

Répercussions dans le monde réel

Le secteur public reste exposé aux pirates sponsorisés par des États

Le secteur public est particulièrement vulnérable aux attaques de cybercriminels sponsorisés par des États, car les acteurs malveillants s'attaquent à toutes les entités apparentées à ce secteur, même si elles sont très éloignées.

Pour plus de contexte sur d'autres acteurs de la menace actifs, en plus des trois présentés à droite, ainsi que sur leur méthodologie, les vulnérabilités exploitées et les attaques connues du public, lisez notre document « *Toolkit de cyberstratégie 2023* ».

« Nos systèmes énergétiques, de santé et financiers [...] sont tous confrontés à des cyber-risques provenant d'acteurs malveillants. Ce type d'attaque peut causer de graves dommages aux personnes, à notre environnement, à la sécurité nationale et surtout, à notre économie. »[8]

Marisol Cruz Cain
Director, Équipe IT et cybersécurité du GAO

Voici certains des groupes APT (Advanced Persistent Threat - Menace avancée persistante) **et cybergangs** qui visent les gouvernements mondiaux :

ALPHV

Gang cybercriminel responsable de la création, de la vente et du déploiement d'un modèle de « ransomwares en tant que service » (RaaS). Ce type de solution de piratage prête à l'emploi donne des outils à un large éventail d'acteurs malveillants.

APT29

Pirates sponsorisés par des États, lié à la branche étranger du service d'espionnage et de renseignement russe dédié aux activités d'espionnage et de renseignement.

Conti

Pirates associés à la Russie, dont le groupe a été dissous suite à la divulgation de ses manuels de formation... mais les pirates et le code associés à Conti continuent de lancer des attaques sauvages. On a reconnu les tactiques de Conti chez plusieurs groupes de cybercriminels l'an dernier.

Comment réagir

Combattez la désinformation et les attaques accélérées grâce à une technologie et une culture stratégiques

Nous vivons dans un monde où la désinformation est une force :

- Campagnes de désinformation à grande échelle sur des réseaux sociaux, alimentées par des bots
- Attaques par hameçonnage hautement crédibles, adaptées aux préférences de chaque personne
- Deepfakes qui minent le journalisme indépendant et perturbent les élections
- Ransomwares qui stoppent la logistique mondiale et la prestation des soins de santé

La désinformation et les cyberattaques peuvent faire des ravages sur la sécurité publique, le commerce mondial et la diplomatie… et même coûter des vies. Les entités gouvernementales sont particulièrement vulnérables, car elles détiennent les clés de systèmes et de messages que les acteurs malveillants cherchent à perturber et à exploiter.

Les responsables de la sécurité doivent protéger leur position en opérant avec précision : développer des stratégies, des systèmes, des outils, des formations et une gouvernance qui fonctionnent de concert pour tenir les pirates en respect.

À la différence des organisations qui agissent après avoir subi des attaques, vous devez mettre en place ces défenses en « temps de paix ».

Il faut agir, maintenant !

Étapes suivantes

Pérennisez vos piles technologiques

1

Résilience

Concevez des plans d'intervention et de récupération pour raccourcir les interruptions de service et limiter l'effet domino.

2

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).

3

Autonomie

Donnez à votre équipe de Cybersécurité davantage d'indépendance pour définir le calendrier de la sécurité. Arrêtez les réactions irréfléchies aux dernières menaces qui font la Une des journaux.

4

Gestion globale des risques

Le périmètre de sécurité doit dépasser les murs de votre organisation et inclure le travail de partout (WFE), les collaborateurs qui travaillent en mode hybride, les sous-traitants et les fournisseurs.

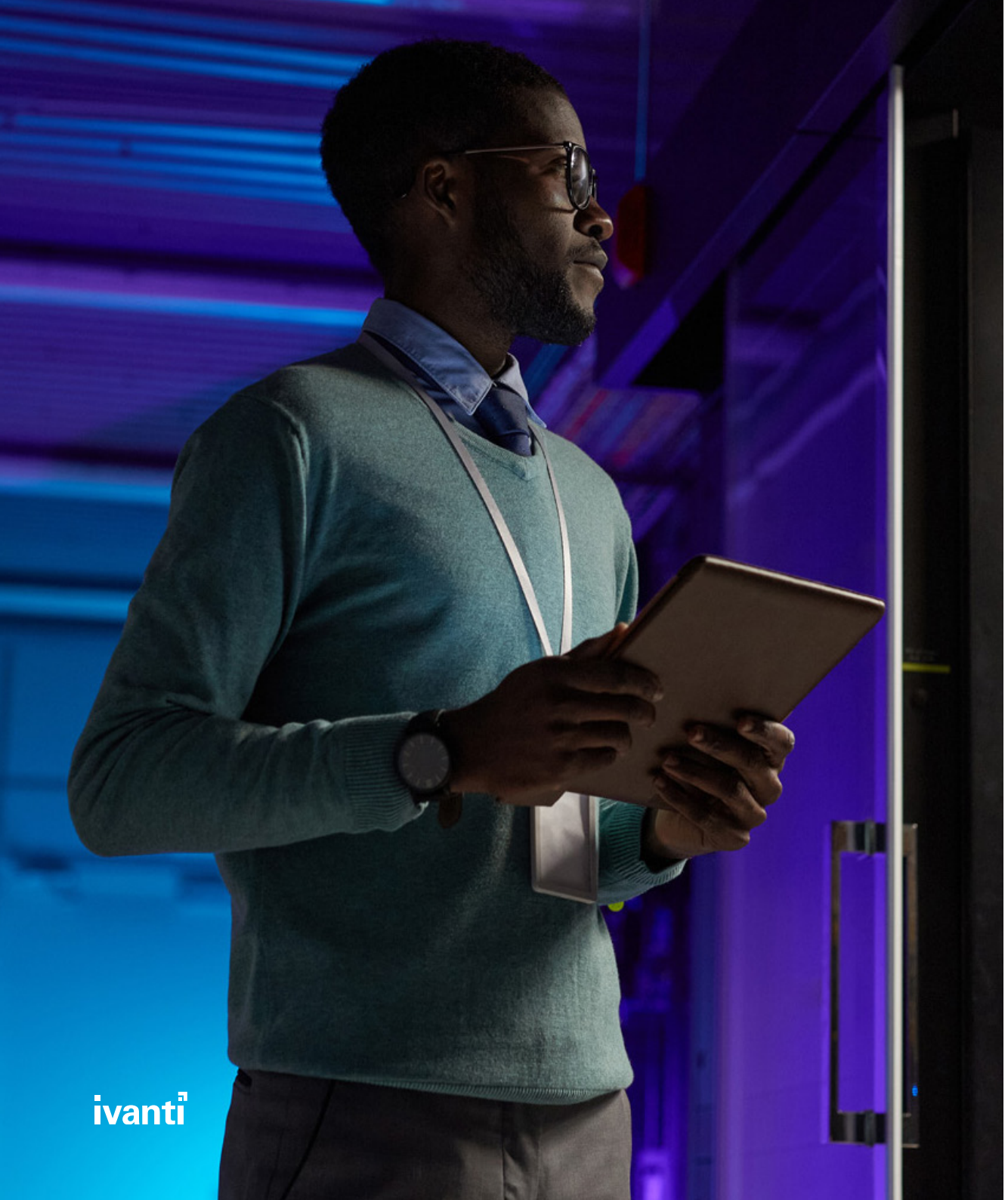
Pour en savoir plus :

« Repartez sur de nouvelles bases : Rapport sur l'état de la cybersécurité en 2023 »

L'ampleur et l'urgence de la situation obligent les entités gouvernementales à aborder la cybersécurité comme un effort d'équipe et à soutenir cet effort avec une technologie qui ne soit pas perçue comme une charge supplémentaire par les collaborateurs.

La posture de sécurité des gouvernements et entités gouvernementales pourra s'améliorer lorsque les fonctionnaires et les collaborateurs comprendront que la cybersécurité est un sujet qui les concerne et qu'ils saisiront les enjeux et leur part de responsabilité, d'autant plus si elle s'accompagne de mesures de sécurité proactives facilitant l'expérience collaborateur.

ivanti



Références

1. Partnership for Public Service: “Engaging employees at federal agencies,” July 14, 2022. https://ourpublicservice.org/blog/engaging-employees-at-federal-agencies/

2. Ivanti: “2023 Cyberstrategy Tool Kit for Internal Buy-in.” October 2022. https://www.ivanti.com/resources/v/doc/ebooks/ivi-2702-cybersecurity-tool-kit-internal-buy-in-budget-influence-non-infosec

3. Sharon Ben-Moshe, Gil Gekker, Golan Cohen / Check Point Research: “OPWNAI: AI That Can Save the Day or Hack It Away.” Dec. 19, 2022. https://research.checkpoint.com/2022/opwnai-ai-that-can-save-the-day-or-hack-it-away/

4. VOA: “Research: Deepfake ‘News Anchors’ in Pro-China Footage.” Feb. 8, 2023. https://www.voanews.com/a/research-deepfake-news-anchors-in-pro-china-footage/6953588.html

5. U.S. Government Accountability Office: “Cybersecurity High-Risk Series: Challenges in Protecting Privacy and Sensitive Data,” Feb. 14, 2023. https://www.gao.gov/products/gao-23-106443

6. Partnership for Public Service: “Employee Engagement,” July 13, 2022. https://ourpublicservice.org/our-solutions/employee-engagement/
Federal News Network: “Return-to-office plans a major cause for decline in 2021 Best Places to Work results,” July 13, 2022. https://federalnewsnetwork.com/workforce/2022/07/return-to-office-plans-a-major-cause-for-decline-in-2021-best-places-to-work-results/

7. Ivanti: “2023 Cyberstrategy Tool Kit for Internal Buy-in.” October 2022. https://www.ivanti.com/resources/v/doc/ebooks/ivi-2702-cybersecurity-tool-kit-internal-buy-in-budget-influence-non-infosec

8. U.S. Government Accountability Office: “Cybersecurity High-Risk Series: Challenges in Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight,” Jan. 19, 2023. https://www.gao.gov/assets/gao-23-106415.pdf

Rapport sur l'état de la cybersécurité des gouvernements

4 mesures importantes pour agir et impulser le changement en 2023

ivanti

ivanti.fr
33 (0)1 76 40 26 20
contact@ivanti.fr