État de la Machine Identity Management 2023

Ponemon INSTITUTE

KEYFACTOR

Avant-propos

Les défis de la gestion des identités et des accès (IAM) ne cessent de croître. L'évolution permanente du lieu de travail - employés travaillant à distance, taux de rotation élevés et pressions économiques toujours présentes alors que la pandémie s'atténue - crée un environnement turbulent pour les personnes chargées de la gestion des identités et des accès.

L'une des réponses a été la croissance rapide et continue des machines au sein de la main-d'œuvre. Cela s'est traduit par une augmentation du nombre de serveurs, d'appareils IoT, de conteneurs, d'applications et d'appareils d'utilisateurs finaux, alors que les entreprises s'efforcent d'améliorer la réactivité des clients tout en améliorant l'efficacité.

L'année dernière, j'ai observé que les forces qui alimentent cette croissance de la main-d'œuvre machine n'allaient faire que s'accélérer. Je ne suis pas devin ; les tendances sont très claires.

Pourtant, à mesure que ces entreprises intègrent des machines dans leurs écosystèmes, il devient de plus en plus difficile de les identifier et de leur fournir une identité (puis de la gérer). Plus de 60 % des personnes interrogées dans le cadre de notre troisième rapport annuel sur l'état de la gestion des identités machine, réalisé en collaboration avec l'Institut Ponemon, ont déclaré ne pas savoir combien de clés et de certificats ils possédaient, soit 7 % de plus que l'année dernière. L'adoption de la confiance zéro, que ce soit au sein d'une agence gouvernementale ou d'une entreprise, l'utilisation accrue d'appareils IoT et l'adoption de services basés sur le cloud sont autant de facteurs qui favorisent le déploiement de clés, PKI et de certificats.

Par conséquent, trouver des moyens de relever le défi et de réduire la complexité de l'environnement PKI est l'une des principales priorités de cette année.

Et de nouveaux défis apparaissent. Les inquiétudes concernant un monde post-quantique, où les ordinateurs quantiques ont le potentiel de briser les algorithmes cryptographiques actuels, augmentent, et le fait de comprendre que la plupart des fournisseurs de cryptographie devront migrer vers de nouveaux fournisseurs résistants aux quanta pousse les entreprises à repenser la PKI et à investir dans la gestion des certificats afin de répondre à ces inquiétudes.

Ce ne sont là que quelques-unes des conclusions du rapport de cette année. Il est clair que le paysage de la gestion des identités et des accès continue d'évoluer rapidement et que les entreprises s'efforcent de suivre le rythme de ces changements.

Mais il y a des signes de progrès. Plus que jamais, les entreprises comprennent l'importance d'avoir une stratégie globale de gestion de l'information et de la mobilité (MIM) qui peut être appliquée à l'ensemble de leur entreprise. Elles reconnaissent notamment l'importance de la visibilité sur l'utilisation et la distribution de la PKI et d'un inventaire de tous les actifs.

Le rapport 2023 sur l'état de la gestion des identités des machines reflète de nombreuses expériences quotidiennes que Keyfactor rencontre en engageant les responsables de la sécurité, les développeurs et les ingénieurs à identifier les obstacles organisationnels à une gestion efficace des identités - à la fois pour les humains et les machines. Il met également en lumière les défis et les solutions possibles auxquels sont confrontées les entreprises de toutes tailles. Nous espérons que vous le trouverez aussi instructif et utile que nous le sommes pour les travaux et recherches passionnants que nous menons dans ce domaine.

Chris Hickman
Responsable de la sécurité (CSO)

Table des matières

Résumé

Introduction

Bienvenue dans le troisième rapport annuel sur l'état de la gestion des identités des machines, un examen approfondi du rôle de la PKI et des identités des machines dans l'établissement de la confiance numérique et la sécurisation des entreprises modernes.

Dans le domaine général de la gestion des identités et des accès (IAM), la gestion des identités des machines (MIM) se concentre sur la gestion des identités des appareils et des charges de travail, telles que les certificats X.509, les informations d'identification SSH, les clés de signature de code et les clés de chiffrement.

Dans ce rapport, nous explorons les résultats d'une enquête menée indépendamment par le Ponemon Institute et publiée par Keyfactor, la solution de sécurité « identity-first » pour les entreprises modernes. Le rapport donne un aperçu de la manière dont les entreprises déploient et gèrent les PKI et les identités machine, ainsi que des défis et des risques qui sont au cœur de leurs préoccupations, alors que le rôle des PKI et des identités machine continue d'évoluer et de se complexifier.

Cette année, nous avons analysé les réponses à l'enquête de 1 280 personnes en Amérique du Nord, en Europe, au Moyen-Orient et en Afrique (EMEA). Les personnes interrogées travaillent dans tous les domaines de l'entreprise informatique, de la sécurité de l'information à l'infrastructure, aux opérations et au développement.

Les résultats de l'enquête de cette année montrent qu'une stratégie efficace de gestion des identités des machines est essentielle pour garder une trace de toutes les machines et s'assurer que chacune d'entre elles dispose d'une autorisation d'accès appropriée. Comme le montre cette étude, la responsabilité du déploiement et de la gestion des PKI est dispersée au sein des entreprises. L'une des conséquences de l'absence de responsabilité claire est que moins de la moitié (47 %) des entreprises disposent d'une stratégie à l'échelle de l'entreprise pour la gestion des PKI et des identités des machines. Seuls 31 % des répondants affirment que leur entreprise dispose d'un groupe de travail mature sur l'identité des machines.

1,280

Répondants à l'enquête

12

Secteurs d'activité

2

Régions du monde

Les résultats de l'enquête de cette année montrent que les stratégies de confiance zéro, les appareils IoT et les services cloud favorisent l'utilisation de la PKI, des clés et des certificats numériques dans l'entreprise. Cependant, le raccourcissement des cycles de vie des certificats a rendu beaucoup plus difficile le suivi de l'émission et de la gestion des certificats. De plus, 53 % des personnes interrogées déclarent que leur entreprise ne dispose pas d'un personnel et de ressources suffisants pour assurer le déploiement de la PKI. En bref, cette croissance entraîne des défis importants et la plupart des entreprises n'ont pas assez de membres d'équipe pour suivre le rythme du changement et les défis présentés par l'infrastructure PKI d'entreprise d'aujourd'hui.

La nécessité croissante de réduire la complexité de l'infrastructure PKI est un thème récurrent de l'étude. Pour la première fois, la principale priorité stratégique des entreprises en matière de sécurité numérique est de réduire la complexité de leur infrastructure PKI, ce qui représente une augmentation de 50 % en 2021 à 58 % cette année. Soixante-quatorze pour cent des répondants, soit une augmentation par rapport à 61 % en 2021, déclarent que leur entreprise déploie davantage de clés cryptographiques et de certificats numériques. En conséquence, cela a considérablement augmenté la charge opérationnelle des équipes de leur entreprise, selon 72 % des répondants, contre 62 % en 2021. L'un des principaux enseignements du rapport de cette année est que la complexité est de plus en plus reconnue comme l'ennemi d'une infrastructure PKI sécurisée et qu'elle rend les entreprises vulnérables aux violations de données. L'augmentation exponentielle du nombre et de la variété des machines nécessitant des clés et des certificats différents contribue à cette complexité.

L'évolution permanente du lieu de travail - employés travaillant à distance, taux de rotation élevés et pressions économiques toujours présentes alors que la pandémie s'atténue - crée un environnement turbulent pour les personnes chargées de la gestion des identités et des accès.

Résumé

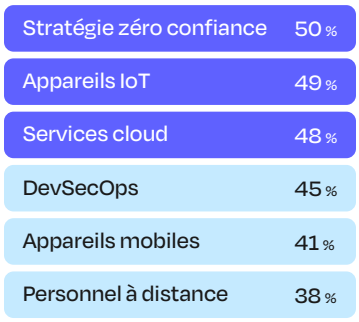
Principales conclusions

Les principaux résultats décrits ici sont basés sur l'analyse par Keyfactor des données de recherche compilées par l'Institut Ponemon.

La PKI pour l'IoT et DevOps est en hausse

La tendance au WFH décline après la pandémie

La PKI continue d'être un élément essentiel de la stratégie zéro confiance et de la sécurité du cloud. Cependant, on observe une augmentation notable de l'utilisation de la PKI pour sécuriser les environnements DevSecOps et IoT émergents, le nombre de répondants indiquant que l'IoT est une tendance majeure passant de 43 % en 2021 à 49 % en 2023. Le DevSecOps a également gagné en importance, 40 % des personnes interrogées déclarant qu'il s'agit d'un cas d'utilisation prioritaire en 2021, contre 45 % cette année.



La pénurie de compétences s'aggrave

Les experts en PKI sont difficiles à trouver et à retenir

Les RSSI et les équipes de sécurité sont aux prises avec une pénurie de main-d'œuvre, qui se répercute sur la stratégie de la PKI et de l'identité machine. En fait, les personnes interrogées déclarent que le manque de personnel qualifié et l'excès de changement et d'incertitude sont les deux plus grands défis auxquels leurs équipes sont confrontées aujourd'hui. En effet, 53 % des personnes interrogées déclarent qu'elles n'ont même pas assez de personnel pour déployer et maintenir leur PKI de manière efficace, contre 50 % en 2022.

▲53 %

Déclarent ne pas avoir assez de personnel pour déployer et maintenir leur PKI

La PKI décentralisée est la nouvelle norme

La prolifération des CA est un sérieux défi

La PKI est omniprésente, différentes équipes utilisant différents outils pour émettre des certificats - des AC internes et des certificats auto-signés aux PKI basées sur le cloud et aux AC intégrées dans les outils DevOps. En moyenne, les personnes interrogées estiment avoir 9 solutions différentes d'AC et de PKI utilisées au sein de l'entreprise. Sans surprise, la réduction de la complexité de l'infrastructure PKI est devenue la principale priorité stratégique pour la gestion de l'identification des machines en 2023, les équipes s'efforçant de reprendre le contrôle et d'empêcher la prolifération d'AC non conformes et non fiables.

9

Nombre moyen de solutions PKI et d'autorités de certification (CA) différentes utilisées au sein des entreprises

▲256 000

Nombre moyen de certificats approuvés en interne au sein des entreprises

Plus de certificats, plus de problèmes

Si vous ne pouvez pas les gérer

Pour la troisième année consécutive, le nombre moyen de certificats approuvés en interne (c'est-à-dire les certificats émis par une PKI privée interne) a augmenté de manière significative, passant de 231 063 en 2021 à 255 738 en 2023. Avec plus de certificats, les équipes responsables de la PKI luttent pour maintenir la visibilité et le contrôle. Soixante-deux pour cent des répondants déclarent ne pas savoir exactement combien de clés et de certificats ils possèdent, contre 53 % des répondants en 2021.

77 %

Déclarent que leur entreprise a connu au moins deux pannes importantes causées par des certificats expirés au cours des 24 derniers mois

Les pannes frappent durement les entreprises

Que se passe-t-il lorsque les certificats expirent de manière inattendue ?

S'ils ne sont pas suivis ou ignorés, les certificats expirent de manière inattendue, entraînant l'arrêt du fonctionnement des applications et des services. La plupart des personnes interrogées (77 %) déclarent avoir connu au moins deux de ces incidents au cours des 24 derniers mois. Les pannes liées aux certificats ne sont pas des incidents anodins : 55 % des personnes interrogées déclarent que ces pannes ont gravement perturbé les services en contact avec la clientèle. Par ailleurs, 50 % des personnes interrogées déclarent que ces événements ont entraîné des perturbations majeures pour les utilisateurs internes ou un sous-ensemble de clients.

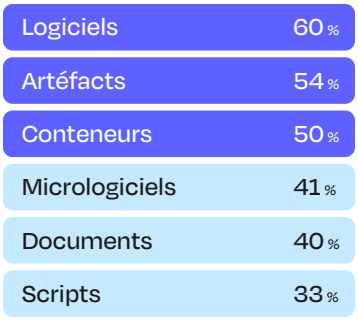
3,79 heures

Temps moyen nécessaire aux équipes pour identifier, remédier et récupérer les pannes liées aux certificats.

Le temps de rétablissement (TTR) est lent

Sans visibilité ni automatisation

Que se passe-t-il lorsqu'une panne survient ? Selon les personnes interrogées, il faut en moyenne près de 4 heures pour identifier et remédier à une panne de certificat, ce qui implique d'identifier la cause première, de trouver le certificat expiré, puis de le réémettre et de le fournir à tous les services concernés. Les personnes interrogées indiquent qu'en moyenne 11 employés sont directement impliqués dans la remédiation de ces pannes lorsqu'elles se produisent, ce qui les détourne de leurs priorités et les oblige à se consacrer à des tâches de réponse aux incidents.



L'utilisation de la signature de code se développe

Plus seulement pour les logiciels

La définition du « code » est en train de changer. Alors que les équipes passent à une infrastructure définie par les développeurs et les logiciels, elles signent bien plus que des livrables logiciels. Selon les personnes interrogées, les cas d'utilisation de la signature vont des logiciels et des microprogrammes aux artefacts, aux scripts et aux conteneurs. Pratiquement toutes les entreprises signent des logiciels sous une forme ou une autre, mais les réponses sont basées sur le point de vue individuel de chaque personne interrogée.

▲68 %

Ils déclarent que leur entreprise stocke des clés de signature de code dans un HSM

Les clés de signature de code sont vulnérables

Mais les pratiques de sécurité s'améliorent

Les récents incidents liés au vol et à l'utilisation abusive de clés de signature de code soulignent la nécessité de les protéger contre les attaquants potentiels. Malheureusement, plus de la moitié des personnes interrogées (56 %) déclarent ne pas avoir confiance dans leur capacité à protéger les clés contre le vol ou l'utilisation abusive. Alors que de nombreuses entreprises stockent encore des clés sensibles sur des serveurs ou des postes de travail, où elles sont vulnérables aux attaques, 68 % des personnes interrogées déclarent avoir adopté les meilleures pratiques en matière d'utilisation d'un HSM pour générer et stocker les clés, soit une augmentation de 17 % par rapport à 2021.

Seulement

▼22 %

Déclarent que le manque de soutien de la part de la direction est un sérieux problème

Les dirigeants sont attentifs

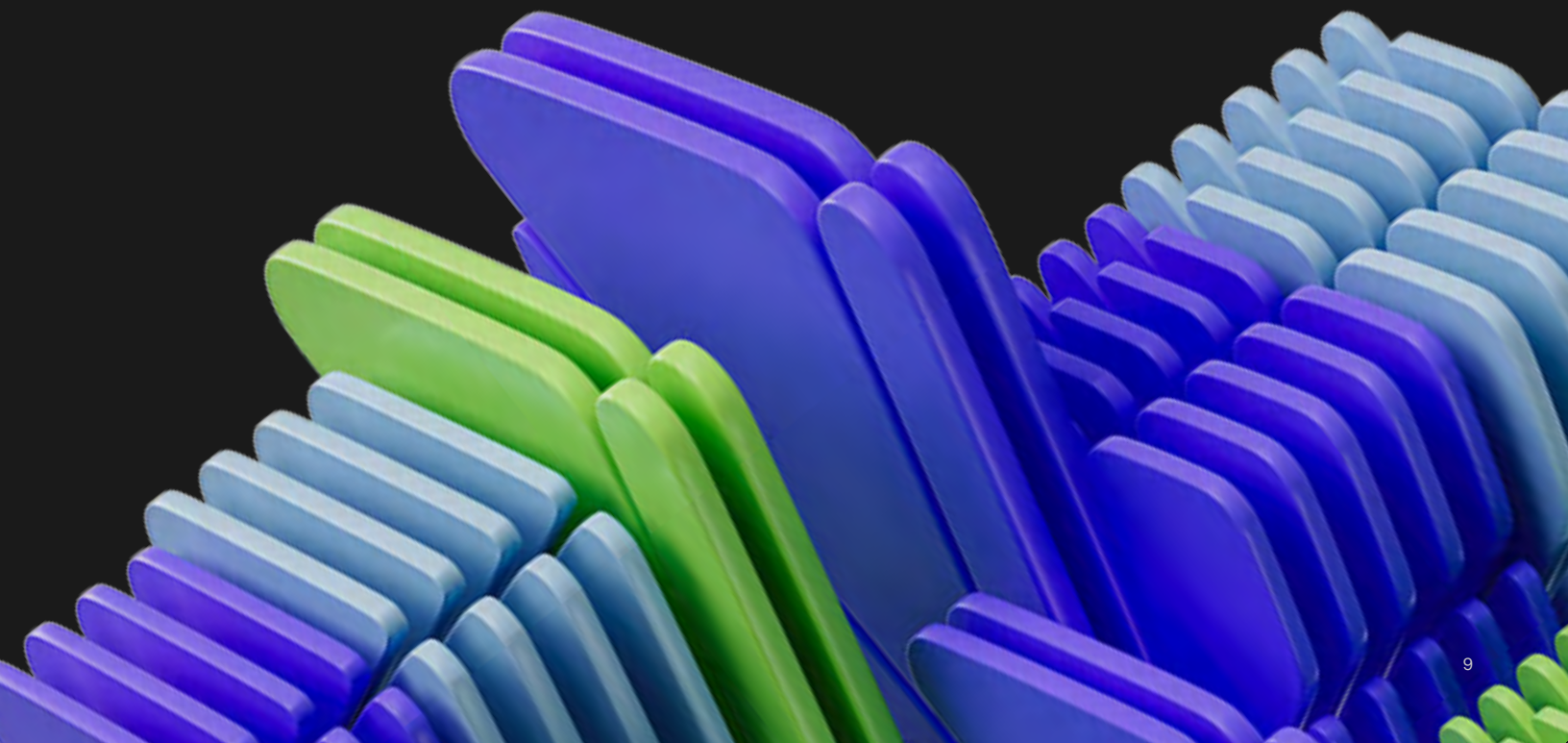
L'identité des machines n'est pas seulement un problème technique

Sans le soutien de la direction, les priorités seront toujours ailleurs. La bonne nouvelle, c'est que seulement 22 % des personnes interrogées déclarent que le manque de soutien de la direction a été un problème sérieux dans la mise en place d'une stratégie d'entreprise pour la PKI et la gestion des identités machine, ce qui représente une baisse significative par rapport aux 36 % des personnes interrogées en 2021. En résumé, les dirigeants sont de plus en plus conscients de la nécessité d'investir dans les bons outils, les bonnes personnes et les bons processus pour la gestion des identités machine.

Résultats complets

Dans cette section, nous analysons les résultats complets de la recherche. Nous avons organisé les sujets dans l'ordre suivant :

1. Stratégies et tendances en matière de PKI et de gestion des identités machine
2. Pratiques de gestion des PKI et des certificats
3. Pratiques de signature de code
4. Pratiques de gestion des identités SSH
5. L'impact des pannes, de l'utilisation abusive des clés et de l'échec des audits



Résultats complets

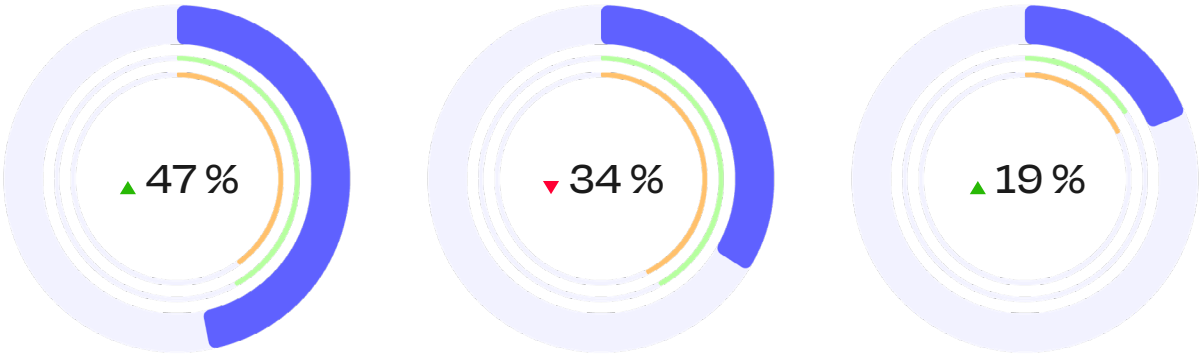
Stratégies et tendances en matière de PKI et de gestion des identités machine

La gestion des identités machine gagne du terrain, mais des obstacles organisationnels se dressent sur sa route. Comme le montre la figure 1, 47 % des personnes interrogées déclarent disposer d'une stratégie globale de gestion des PKI et des identités des machines, telles que les clés, les certificats et les secrets, ce qui représente une augmentation par rapport aux 40 % de 2021.

Les identités des machines, par opposition aux identités humaines ou d'utilisateur, deviennent un élément de plus en plus important du paysage de la gestion des identités et des accès (IAM). Cependant, la figure 2 montre qu'il n'est toujours pas clair qui détient la stratégie de gestion des identités et des accès (IAM), sans parler de la place qu'occupent les identités des machines.

Figure 1

Votre entreprise dispose-t-elle d'une stratégie à l'échelle de l'entreprise pour la gestion des PKI et des identités des machines ?



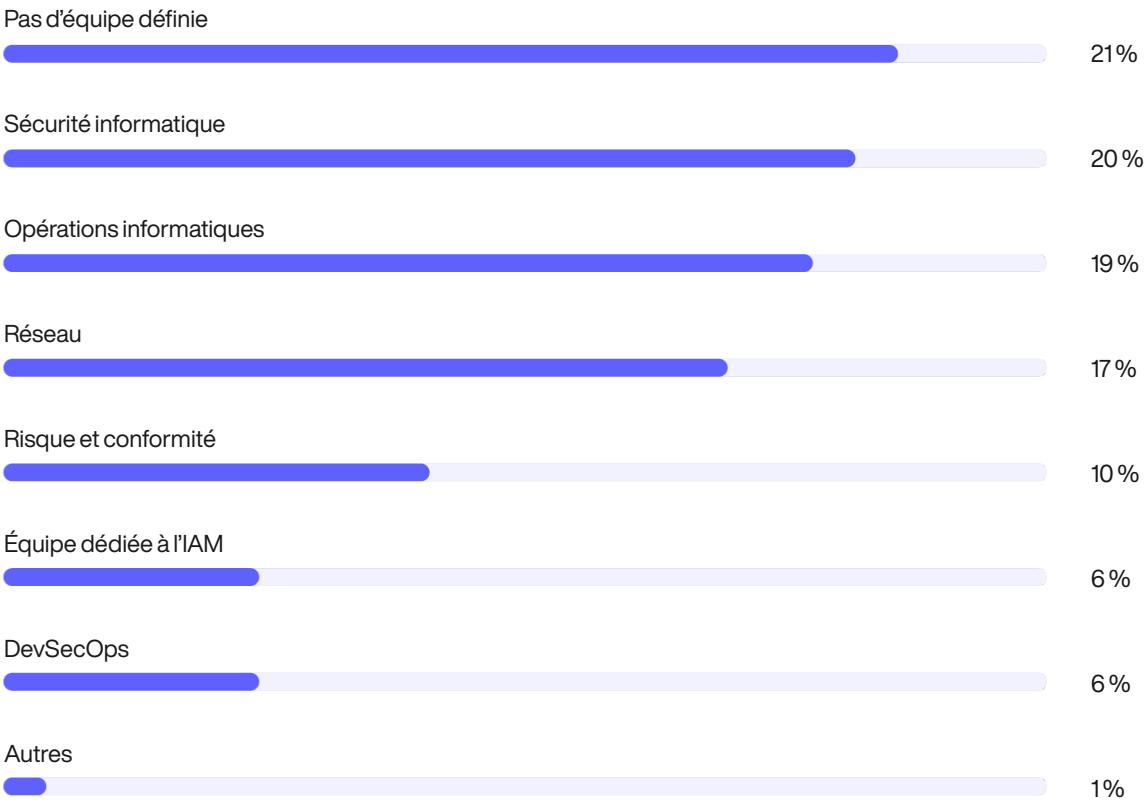
Nous disposons d'une stratégie globale de gestion des identités des machines appliquée de manière cohérente à l'ensemble de l'entreprise.

Nous disposons d'une stratégie de gestion des identités machine limitée à certaines applications ou cas d'utilisation.

Nous n'avons pas de stratégie de gestion des identités des machines

Figure 2

Qui est responsable de la gestion des identités et des accès (IAM) au sein de votre entreprise ?

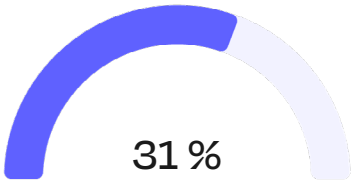


Un groupe de travail sur l'identité des machines pourrait être la solution. Si un développeur ou un ingénieur demande comment obtenir un certificat lors du déploiement d'un nouveau service, qui consulte-t-il ? La réponse est qu'ils ont besoin de l'avis de plusieurs équipes pour rassembler les bonnes informations et prendre les bonnes décisions, ce qui pourrait inclure PKI, I&O, DevOps et IAM. En résumé, cela nécessite une collaboration interfonctionnelle.

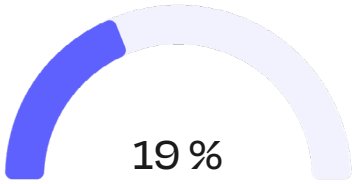
Une fois constitué, un groupe de travail interfonctionnel sur l'identité des machines peut définir des lignes directrices et des meilleures pratiques pour l'émission et la gestion de certificats et d'autres identifiants de machines, prendre des décisions en matière d'outillage et définir des politiques claires. Comme le montre la figure 3, 50 % des personnes interrogées déclarent que leur entreprise dispose d'un groupe de travail sur l'identité des machines, à différents niveaux de maturité.

Figure 3

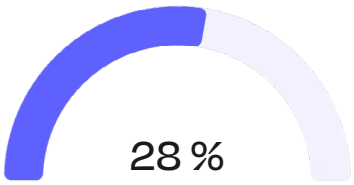
Votre entreprise dispose-t-elle d'une équipe ou d'un groupe de travail dédié à la PKI et à la gestion des identités machine ?



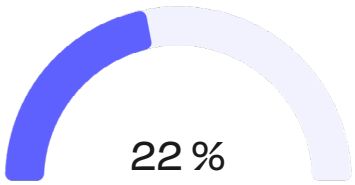
Oui, nous disposons d'un groupe de travail mature sur l'identité des machines qui assure le leadership, la recherche, la mise en œuvre, la stratégie, l'appropriation et les meilleures pratiques.



Oui, mais notre groupe de travail sur l'identité des machines est encore immature.



Non, mais nous prévoyons de mettre en place une équipe ou un groupe de travail sur l'identité des machines dans les six prochains mois.



Non, et nous ne prévoyons pas de mettre en place une équipe ou un groupe de travail sur l'identité des machines.

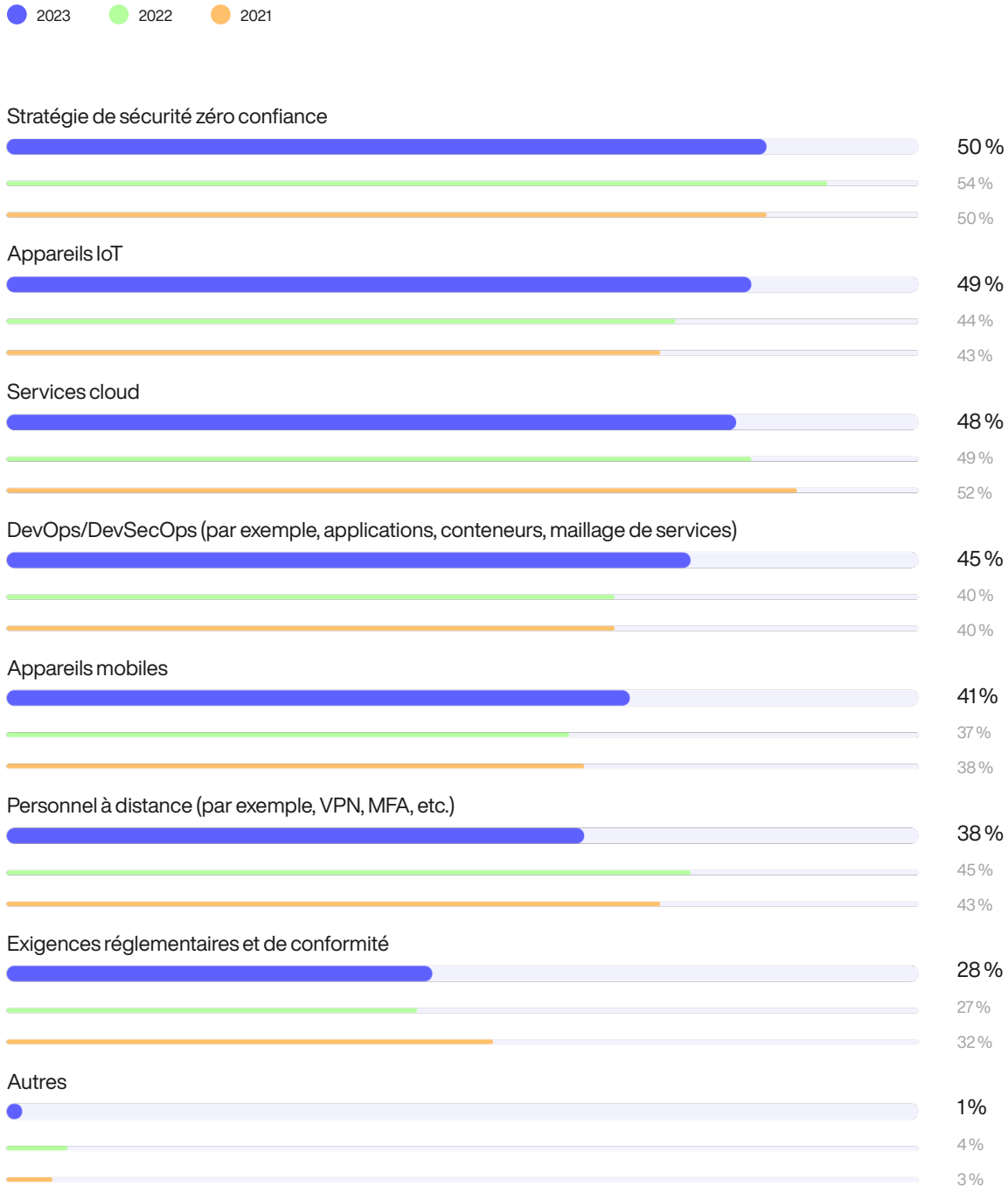
L'IoT et le DevOps sont les cas d'utilisation qui connaissent la croissance la plus rapide pour la PKI et les identités de machine. La figure 4 montre les tendances les plus importantes qui déterminent le déploiement de la PKI, des clés, des certificats et d'autres secrets. La stratégie de confiance zéro et les services basés sur le cloud restent les principales tendances pour la PKI, conformément aux résultats des années précédentes.

Les appareils IoT (49 % des répondants) et DevOps/DevSecOps (45 % des répondants) représentent les tendances à la croissance la plus rapide, contre respectivement 43 % et 40 % des répondants en 2021. À l'inverse, l'importance de la main-d'œuvre à distance a diminué, passant de 43 % des répondants en 2021 à 38 % des répondants dans le rapport de cette année, probablement en raison d'un changement de priorités après la pandémie.

Figure 4

Les tendances et les cas d'utilisation les plus importants pour le déploiement de la PKI, des clés, des certificats et d'autres secrets

Trois réponses possibles



L'industrie technologique est en pleine mutation et la demande de talents en matière de cybersécurité continue de dépasser les ressources disponibles.

Découvrez trois stratégies pour faire face à la pénurie de main-d'œuvre dans le domaine de la cybersécurité.

En savoir plus ↗

La pénurie de compétences et l'incertitude restent les principaux défis auxquels sont confrontées les équipes ; la fragmentation des outils devient un problème plus important. La figure 5 présente une liste de six défis liés à la mise en place d'une stratégie à l'échelle de l'entreprise pour la gestion des PKI et des identités machine. Nous avons demandé aux personnes interrogées d'indiquer les deux principaux défis auxquels leur entreprise est confrontée.

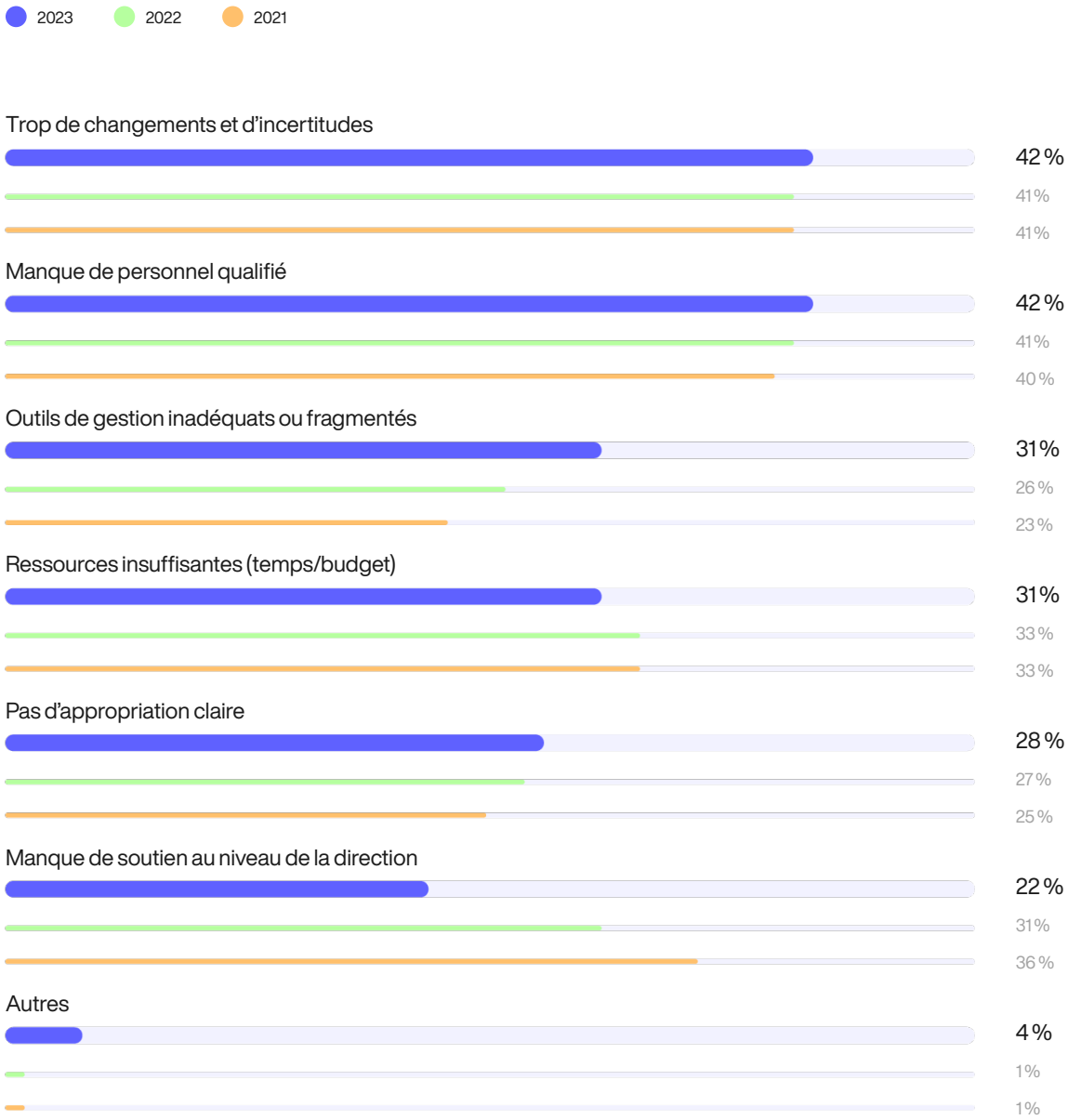
Quarante-deux pour cent des personnes interrogées déclarent que le manque de personnel qualifié et l'excès de changement et d'incertitude sont les principaux défis, ce qui est cohérent avec les années précédentes. Toutefois, on constate une augmentation notable du nombre de répondants qui déclarent que des outils de gestion inadéquats et fragmentés constituent un défi majeur, passant de 23 % des répondants en 2021 à 31 % des répondants dans le rapport de cette année.

Sur une note positive, il semble que les dirigeants soient de plus en plus conscients de la nécessité d'une gestion des identités machine et qu'ils la soutiennent, puisque seulement 22 % des personnes interrogées déclarent que le manque de soutien de la part de la direction est un défi majeur, contre 36 % des personnes interrogées en 2021.

Figure 5

Principaux défis liés à la mise en place d'une stratégie à l'échelle de l'entreprise pour la gestion des PKI et des identités des machines

Deux réponses possibles



Plus de certificats créent plus de problèmes, si les entreprises ne peuvent pas les suivre ou les gérer efficacement. Comme le montre la figure 6, 72 % des personnes interrogées déclarent que l'utilisation croissante des clés et des certificats a considérablement augmenté leur charge opérationnelle, contre 62 % des personnes interrogées en 2021.

À mesure que le volume de certificats augmente au sein des entreprises, la visibilité devient également un sérieux défi. Soixante-deux pour cent des personnes interrogées déclarent ne pas savoir exactement combien de clés et de certificats (y compris auto-signés) leur entreprise possède, contre 53 % des personnes interrogées en 2021. La mauvaise configuration des clés et des certificats est également une préoccupation croissante.

En juin 2022, le NIST a choisi le premier groupe d'algorithmes qui feront partie de sa norme cryptographique post-quantique, qui devrait être finalisée d'ici deux ans. Quarante-huit pour cent des personnes interrogées se disent préoccupées par leur capacité à s'adapter à ces algorithmes post-quantiques, contre 44 % l'année dernière, avant l'annonce du NIST.

Figure 6

Perceptions et préoccupations concernant la gestion des identités des machines

Réponses à la fois « tout à fait d'accord » et « d'accord »

figure 6 Cont.

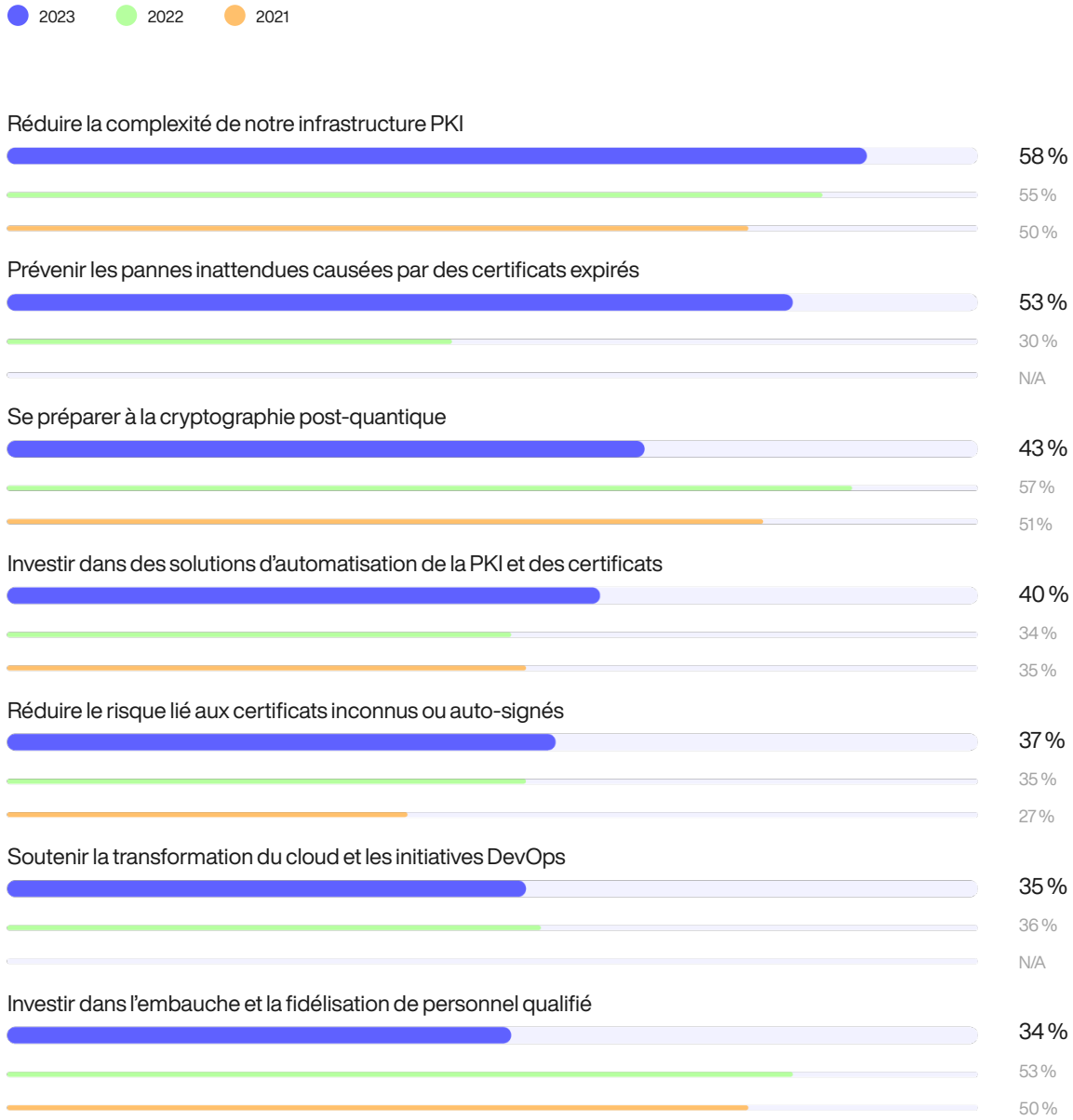
La réduction de la complexité de la PKI, la prévention des pannes liées aux certificats et la préparation à la cryptographie post-quantique figurent en tête de liste des priorités stratégiques. La figure 7 présente une liste de sept priorités stratégiques pour la gestion des identités machine. Nous avons demandé aux répondants d'indiquer les trois premières priorités.

Alors que les entreprises s'appuient de plus en plus sur la PKI et les certificats numériques pour authentifier les charges de travail et les appareils, il est clair que les équipes s'efforcent de maintenir la visibilité et le contrôle. Sans surprise, les personnes interrogées déclarent que leurs principales priorités sont de réduire la complexité de l'infrastructure PKI (58 %) et de prévenir les pannes causées par des certificats expirés (53 %). Quarante-trois pour cent des personnes interrogées déclarent que la préparation à la cryptographie post-quantique est également une priorité absolue.

Figure 7

Priorités stratégiques pour la gestion des PKI et des identités machine en 2023

Trois réponses possibles



*Remarque : des options de réponse supplémentaires ont été incluses dans l'enquête de 2022 et 2023.

Pratiques de gestion des PKI et des certificats

La PKI décentralisée est la nouvelle norme. Selon les répondants, il y a en moyenne 9 autorités de certification (AC) et PKI différentes utilisées au sein des entreprises.

Comme le montre la figure 9, les répondants déclarent que leur PKI comprend généralement un mélange de PKI privées internes (50 %), d'AC intégrées aux outils DevOps (35 %), de certificats auto-signés (33 %), de services PKI gérés (33 %), de services d'AC privés dans le cloud (31 %), ainsi que de services d'AC publics (25 %).

L'époque où une ou deux autorités de certification se trouvaient derrière les quatre murs du centre de données est révolue. Aujourd'hui, différentes équipes utilisent plusieurs déploiements d'AC et de PKI pour soutenir différents niveaux de confiance, cas d'utilisation et exigences en matière de sécurité et de performance. Bien que nécessaire, cette situation engendre de nouveaux risques et défis, car la PKI devient de plus en plus fragmentée et complexe, d'où la nécessité d'un contrôle et d'une consolidation, dans la mesure du possible.

Figure 8

Combien de PKI et d'autorités de certification (AC) différentes sont utilisées au sein de votre entreprise ?

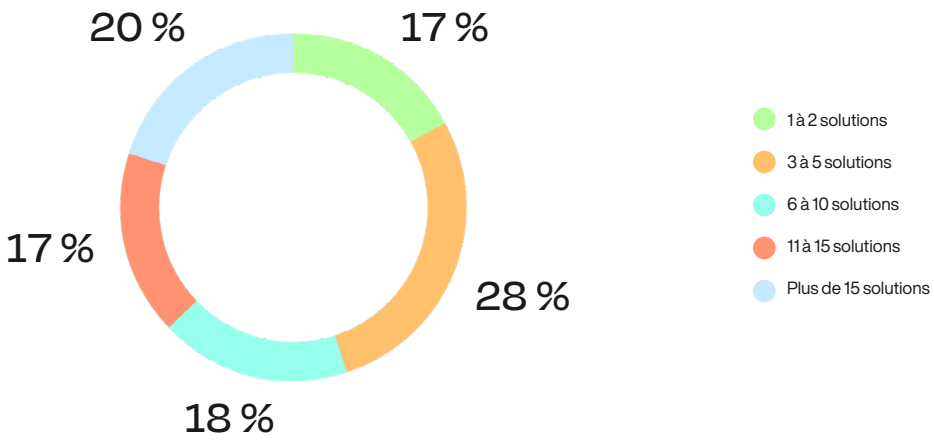
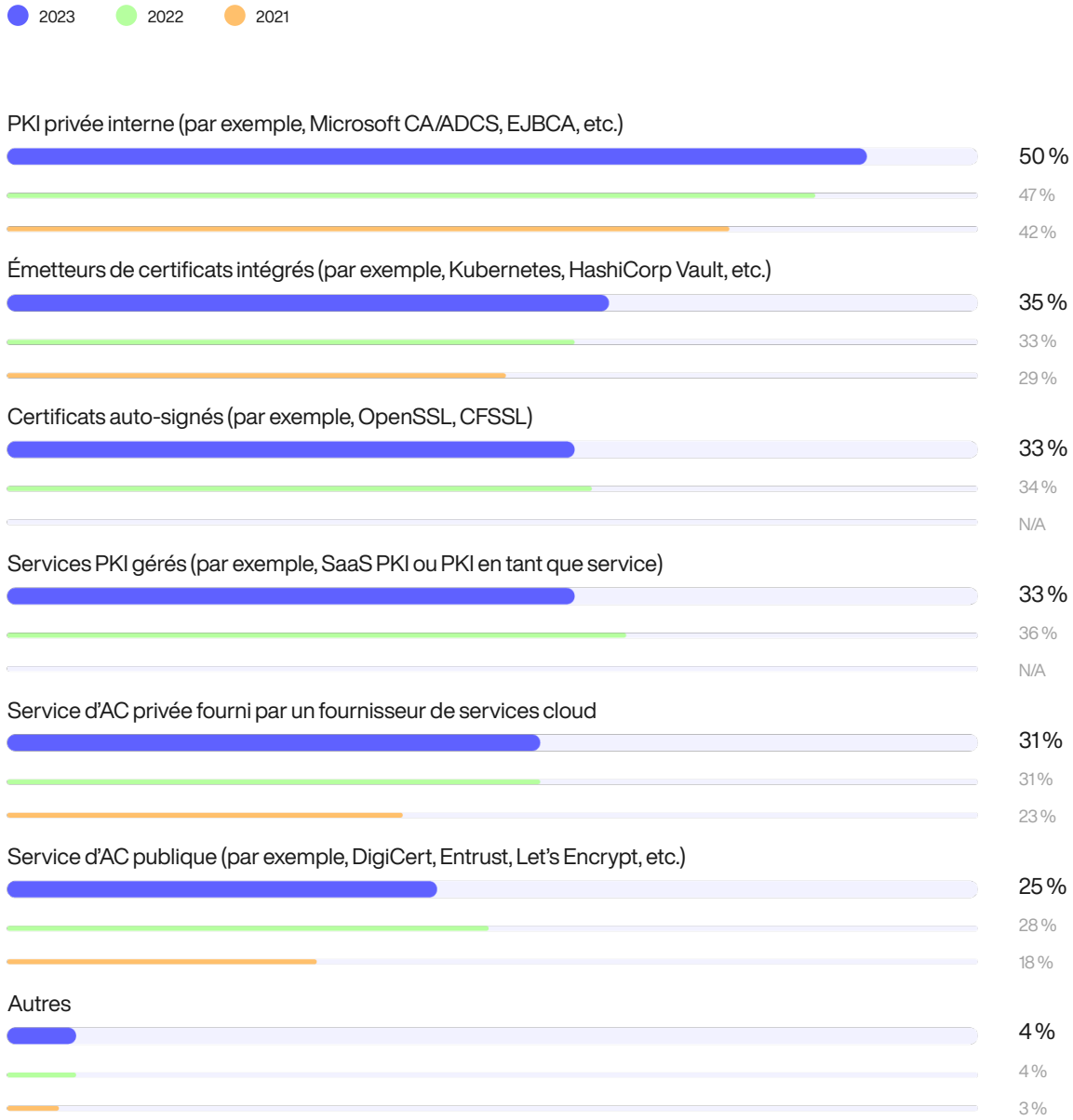


Figure 9

Parmi les solutions de PKI et d'autorité de certification (AC) suivantes, lesquelles sont déployées dans votre entreprise ?

Plusieurs réponses possibles

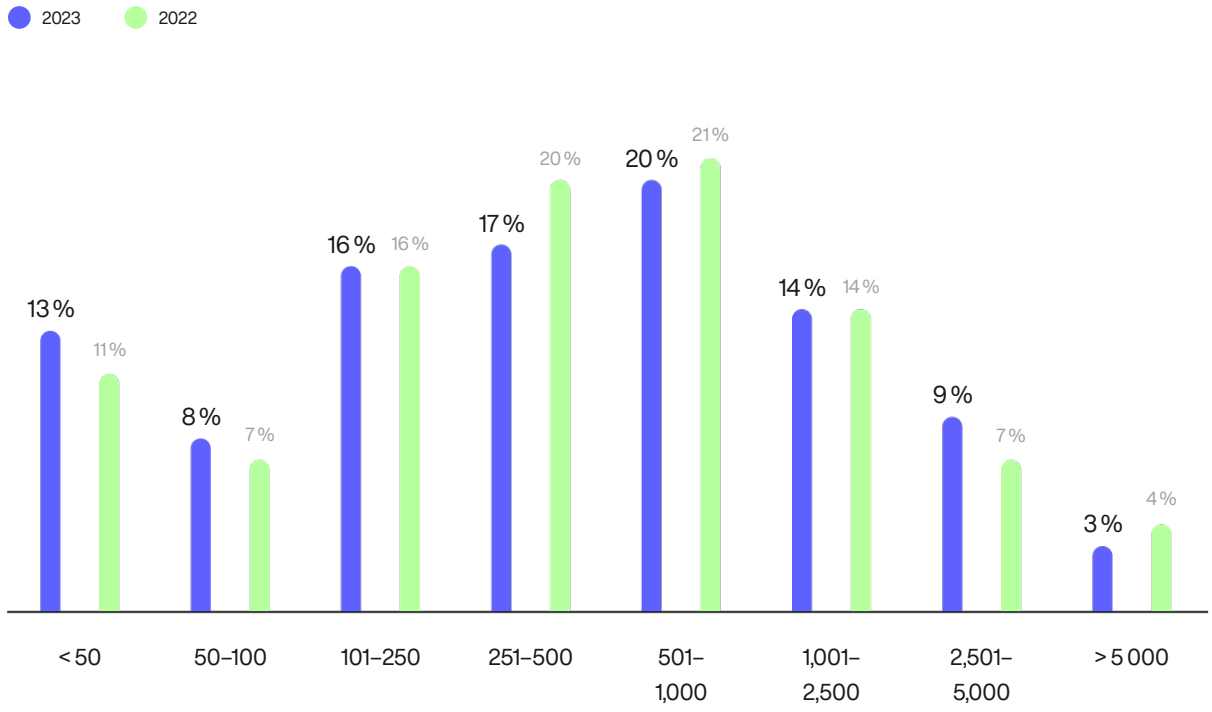


*Remarque : des options de réponse supplémentaires ont été incluses dans l'enquête de 2022 et 2023.

Le volume de certificats de confiance internes augmente rapidement. Selon les répondants, les entreprises représentées dans cette étude ont en moyenne 255 714 certificats de confiance internes (c'est-à-dire émis par une PKI interne) et 1 024 certificats SSL/TLS émis publiquement (c'est-à-dire émis par un fournisseur SSL/TLS ou une AC publique). Le nombre moyen de certificats approuvés en interne a augmenté de manière significative au cours de l'année écoulée, avec une moyenne de 235 084 en 2022.

Figure 10

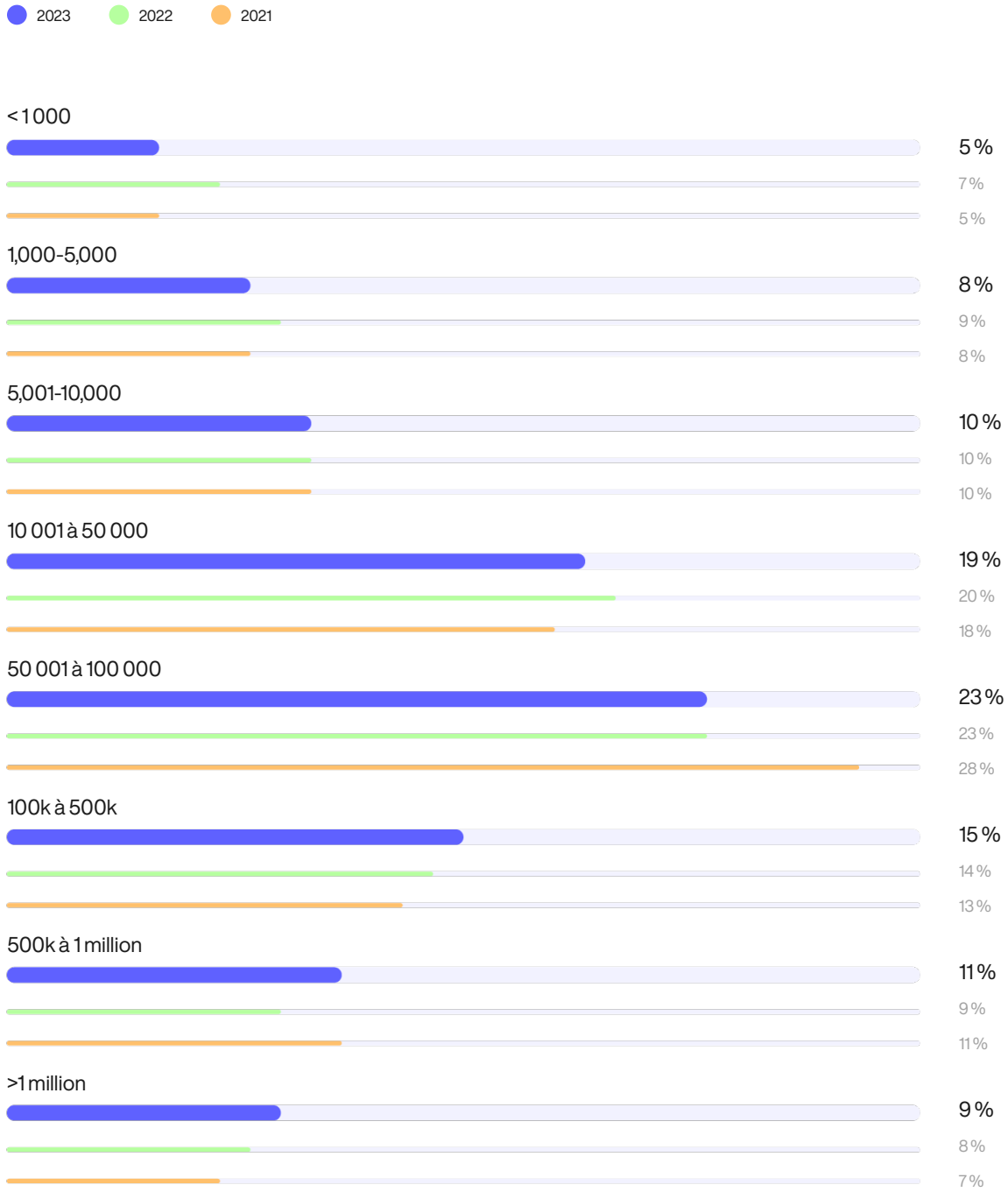
Combien de certificats SSL/TLS publics votre entreprise possède-t-elle ?



*Remarque : cette question ne figurait pas dans l'enquête de 2021.

Figure 11

Combien de certificats de confiance internes votre entreprise possède-t-elle ?



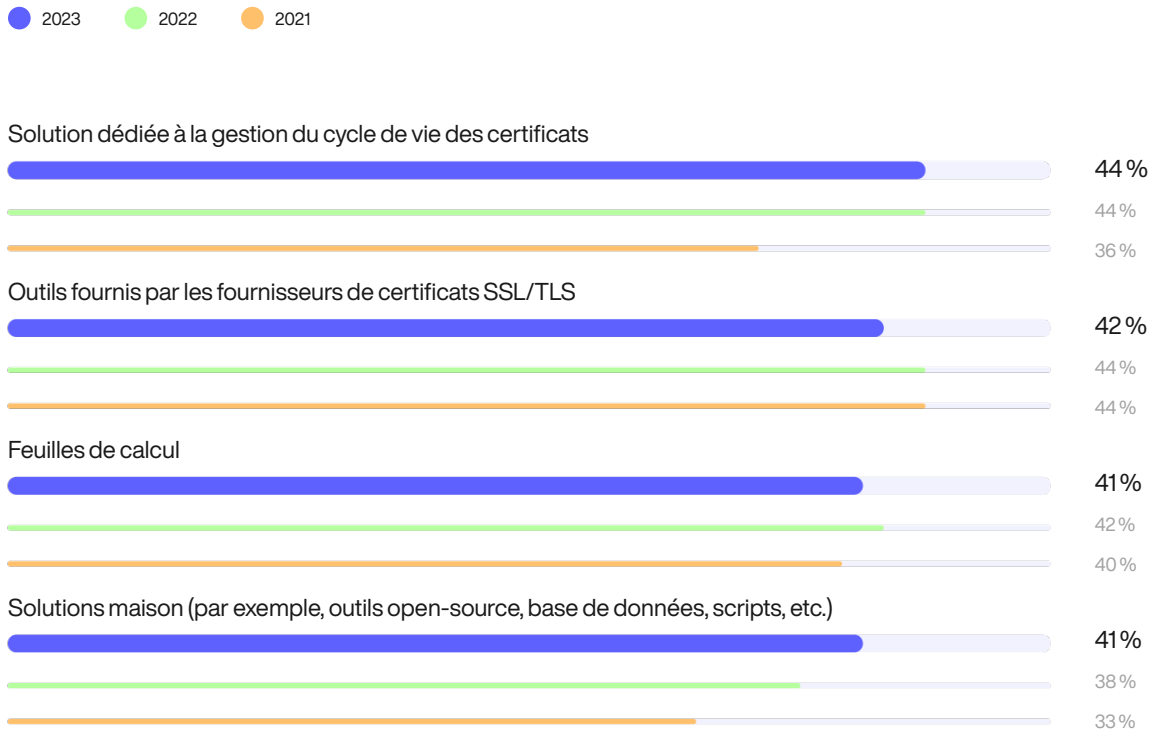
*Note : la valeur moyenne extrapolée de 2022 a été corrigée. Le nombre moyen de certificats approuvés en interne par les entreprises était de 235 084 en 2022, et non de 267 620 comme indiqué précédemment.

Comment les certificats sont-ils gérés ? La figure 12 montre que de nombreuses entreprises s'appuient encore sur un ensemble de solutions disparates et manuelles pour gérer les certificats numériques. Quarante et un pour cent des répondants utilisent des feuilles de calcul et/ou des outils maison, et 42 % des répondants utilisent des outils fournis par leur fournisseur de certificats SSL/TLS. L'utilisation de solutions maison pour gérer les certificats a augmenté de façon constante d'une année sur l'autre, passant de 33 % des répondants en 2021 à 41 % en 2023.

Figure 12

Comment votre entreprise assure-t-elle le suivi et la gestion des certificats ?

Plusieurs réponses possibles



Le manque de personnel et de ressources dans le domaine de la PKI reste un problème. La PKI n'est pas seulement un logiciel, c'est une infrastructure critique. Sans les compétences et l'expertise adéquates, il est difficile de la configurer, de la déployer et, surtout, de la maintenir correctement tout au long de sa durée de vie. Comme le montre la figure 13, plus de la moitié des personnes interrogées déclarent ne pas disposer de suffisamment de personnel et de ressources pour déployer et maintenir efficacement la PKI, ce qui représente une tendance relativement constante d'une année sur l'autre au cours des trois dernières années.

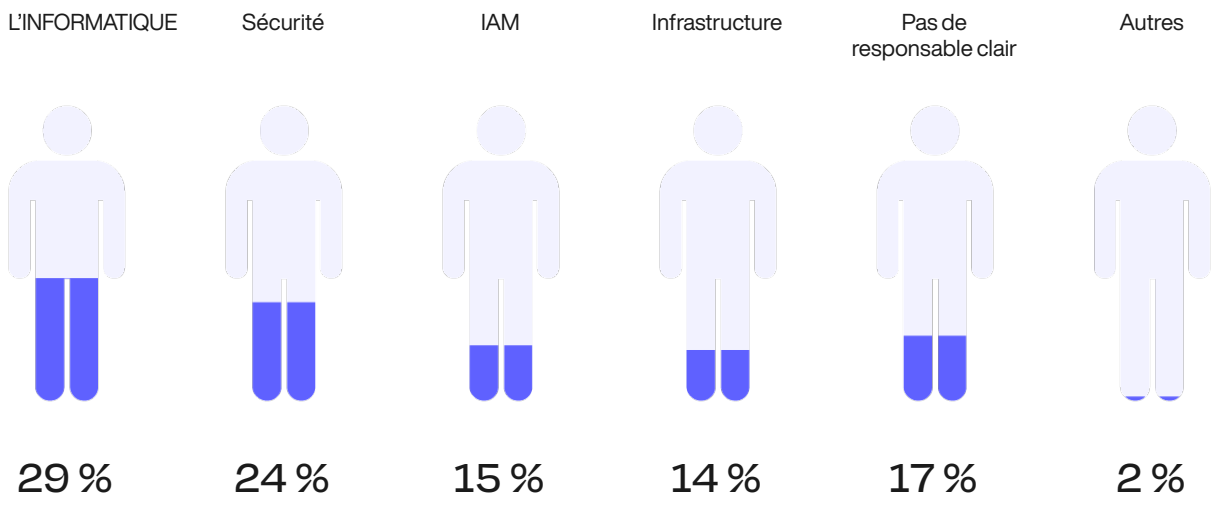
Figure 13

Selon vous, votre entreprise dispose-t-elle de suffisamment de ressources et de personnel pour déployer et maintenir une PKI efficace ?

Qui est responsable de la PKI ? La figure 14 montre les différentes équipes responsables du déploiement et de la gestion des PKI au sein des entreprises représentées dans cette étude. Les équipes informatiques et de sécurité sont le plus souvent responsables de la PKI, mais les équipes IAM et d'infrastructure ne sont pas non plus des propriétaires rares de la PKI. Dix-sept pour cent des personnes interrogées déclarent qu'il n'y a pas de propriétaire clair.

Figure 14

Qui est actuellement responsable du déploiement et de la gestion des PKI dans votre entreprise ?



*Note : cette question n'a pas été incluse dans l'enquête de 2021 ou 2022.

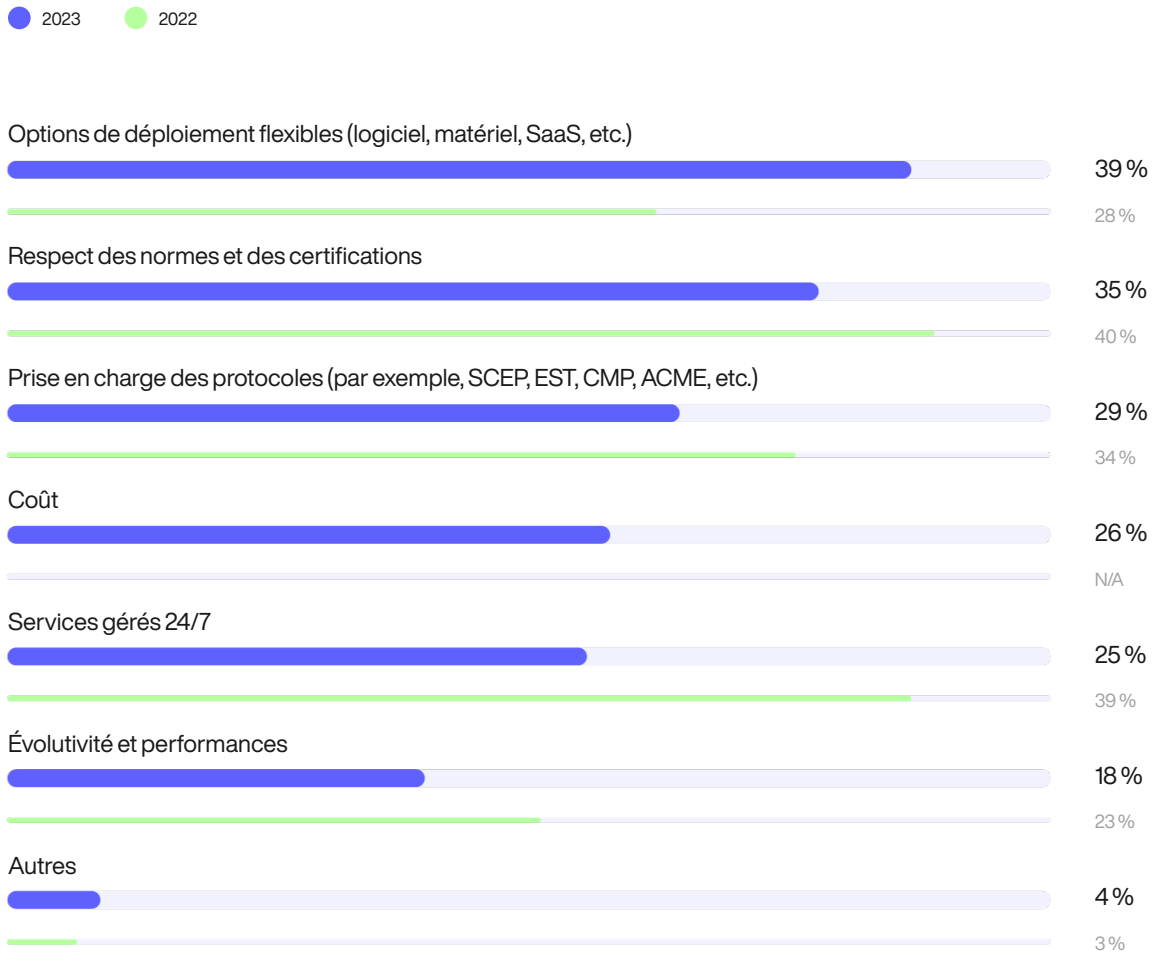
La flexibilité et la visibilité sont essentielles à la gestion des PKI et des certificats. La figure 15 énumère six caractéristiques ou facteurs jugés importants lors de l'évaluation des solutions PKI. Trente-neuf pour cent des personnes interrogées déclarent que les options de déploiement flexibles, telles que les logiciels, le matériel et la PKI fournie en mode SaaS, sont des caractéristiques essentielles, suivies par le respect des normes et des certifications (35 % des personnes interrogées) et la prise en charge des protocoles (29 % des personnes interrogées).

De même, la figure 16 montre les caractéristiques ou capacités les plus importantes des solutions de gestion des certificats. Soixante-deux pour cent des personnes interrogées déclarent qu'une visibilité complète et un inventaire de tous les certificats sont des capacités importantes. Ce n'est pas une surprise, étant donné que 62 % des entreprises ne savent pas combien de clés et de certificats elles possèdent, comme le montre la figure 6.

Figure 15

Les caractéristiques les plus importantes lors de l'évaluation des solutions PKI

Trois réponses possibles

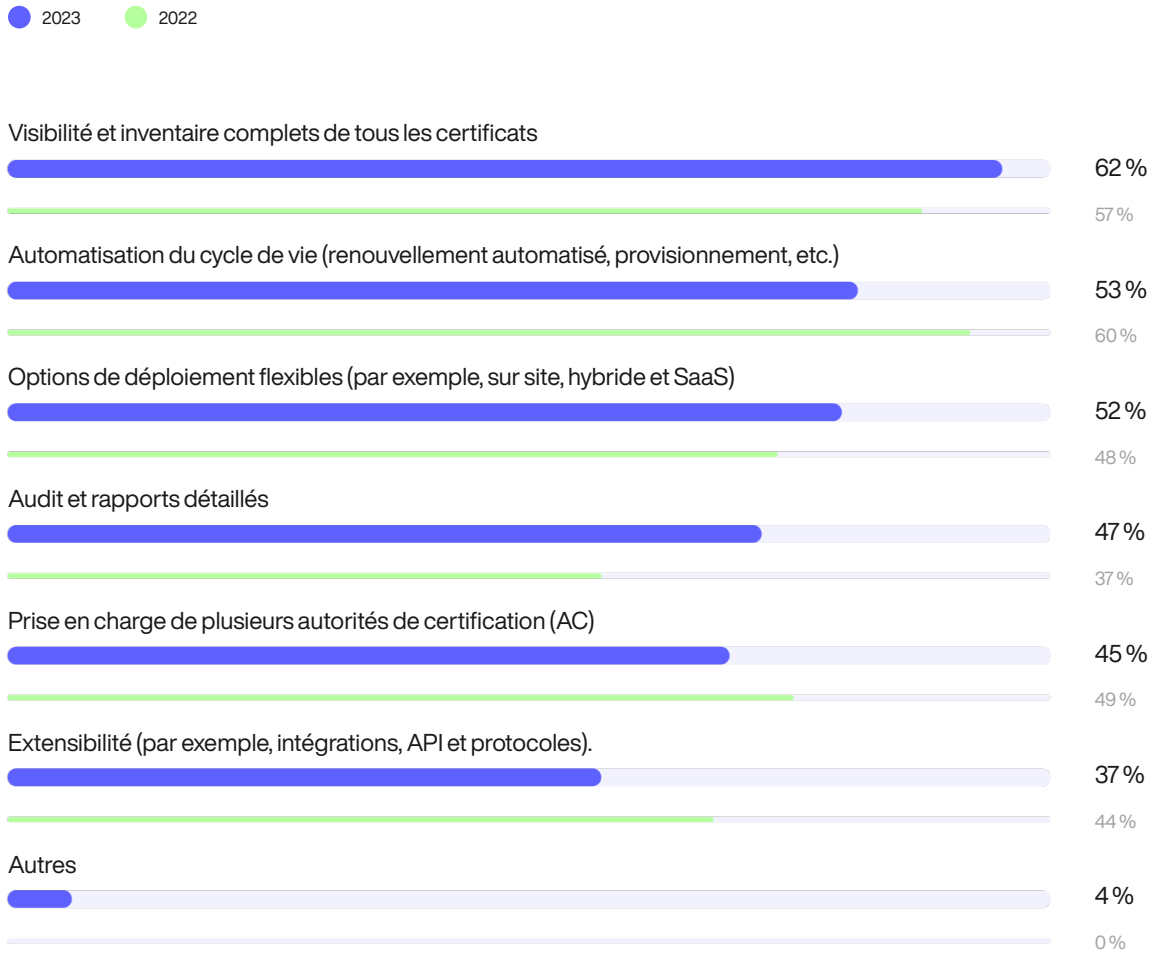


*Remarque : cette question ne figurait pas dans l'enquête de 2021.

Figure 16

Les caractéristiques les plus importantes lors de l'évaluation des solutions de gestion des certificats

Trois réponses possibles



*Remarque : cette question ne figurait pas dans l'enquête de 2021.

Pratiques de signature de code

Dans cette section, nous avons demandé aux personnes interrogées si elles étaient impliquées dans des opérations de signature de code. Les réponses des personnes qui ont déclaré ne pas être impliquées ont été exclues de l'analyse suivante.

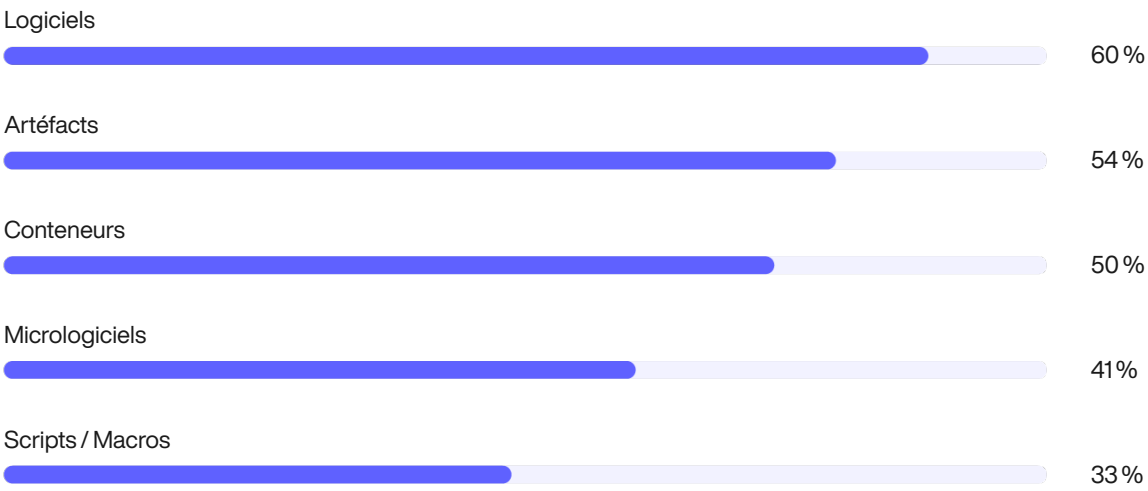
Les cas d'utilisation de la signature de code s'étendent. La définition du « code » a changé. Alors que les entreprises s'orientent vers une approche « ne faire confiance à rien, signer et vérifier tout », les équipes DevOps et de sécurité tirent parti de la signature de code non seulement pour les logiciels qu'elles livrent aux utilisateurs finaux, mais aussi pour les scripts, les conteneurs, les artefacts et l'infrastructure en tant que code utilisés tout au long du cycle de vie du développement logiciel (SDLC).

La figure 17 montre que la signature de code est le plus souvent utilisée pour les logiciels (60 % des répondants), les artefacts (54 %) et les conteneurs (50 %). Pour les entreprises qui fabriquent du matériel ou développent des microprogrammes, la signature et la vérification sont également essentielles pour activer des fonctions de sécurité telles que le démarrage sécurisé et les mises à jour OTA (over-the-air) sécurisées.

Figure 17

Quels sont les cas d'utilisation actuels de la signature au sein de votre entreprise ?

Plusieurs réponses possibles



La responsabilité de la protection et de la gestion des clés de signature de code varie. La figure 18 révèle que les entreprises représentées dans l'étude 2023 utilisent en moyenne 23 certificats de signature de code pour signer numériquement des logiciels, des artefacts, des conteneurs et d'autres actifs numériques.

Les clés privées sensibles associées aux certificats de signature de code doivent être gérées et protégées de manière sécurisée afin d'éviter toute utilisation abusive ou tout vol. Comme le montre la figure 19, la responsabilité de la gestion et de la protection de ces actifs est répartie entre les développeurs principaux et la direction (12 % des personnes interrogées), les développeurs (24 %), les opérations informatiques (29 %) et la sécurité informatique (24 %). Par ailleurs, 11 % des personnes interrogées déclarent qu'aucune fonction n'est responsable.

Figure 18

Combien de certificats de signature de code avez-vous dans votre entreprise ?

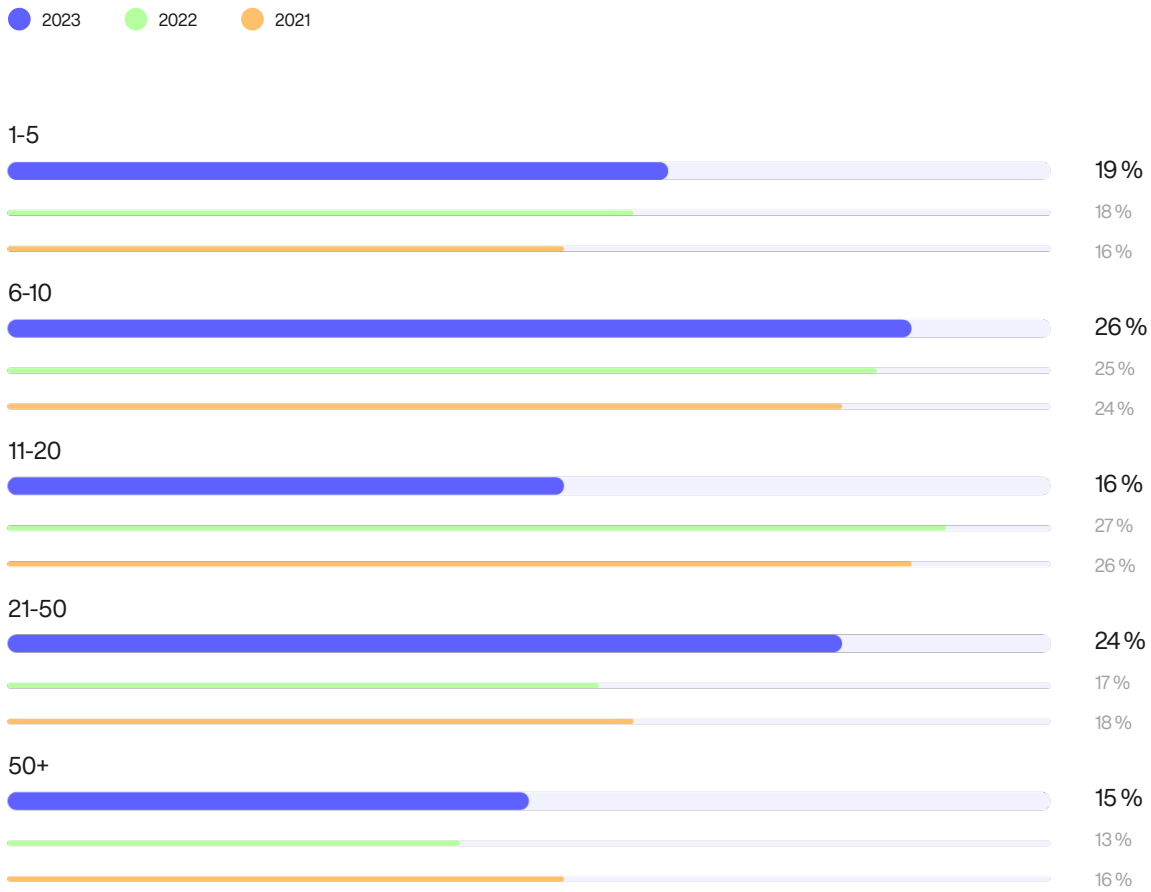
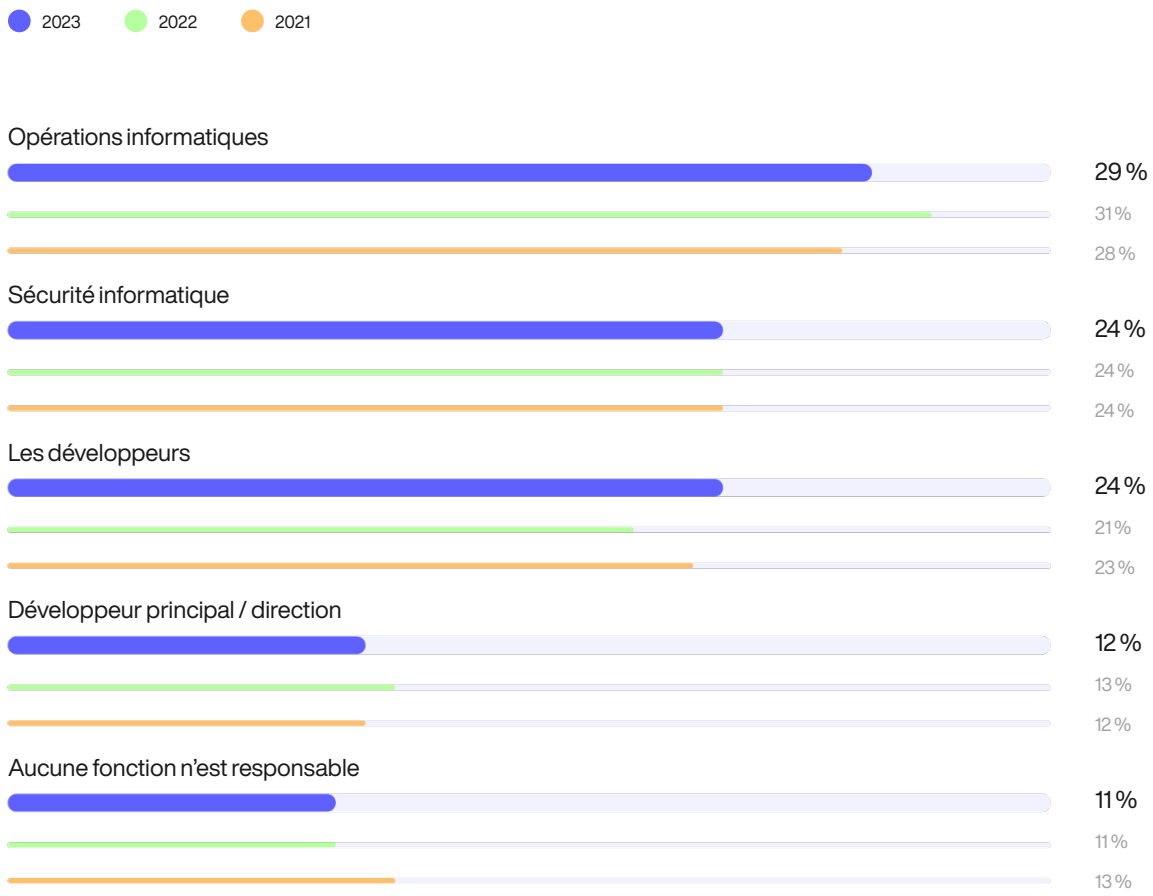


Figure 19

Qui est le plus responsable de la gestion et de la protection des clés de signature de code ?



Où sont stockées les clés de signature de code ? La signature de code sans protection des clés privées expose les entreprises à de sérieux risques. Le problème est que les développeurs et les outils qu'ils utilisent doivent avoir accès à ces clés pour signer le code. Par conséquent, les clés privées sont souvent stockées dans des endroits facilement accessibles, tels que des serveurs ou des postes de travail, où elles sont exposées par inadvertance à des attaquants qui volent les clés pour signer et distribuer des codes malveillants masqués en tant que logiciels légitimes.

Comme le montre la figure 20, 68 % des personnes interrogées déclarent suivre les meilleures pratiques en stockant les clés de signature de code dans un module de sécurité matériel (HSM), ce qui représente une amélioration significative. Par ailleurs, 46 % des personnes interrogées déclarent stocker les clés de signature de code dans une carte à puce ou une clé USB amovible, qui peut être cryptée ou non. De nombreuses personnes interrogées déclarent que les clés de signature de code sont stockées de manière non sécurisée sur les serveurs de construction (39 %) et les postes de travail des développeurs (19 %).

Figure 20

Où sont stockées les clés de signature de code dans votre entreprise ?

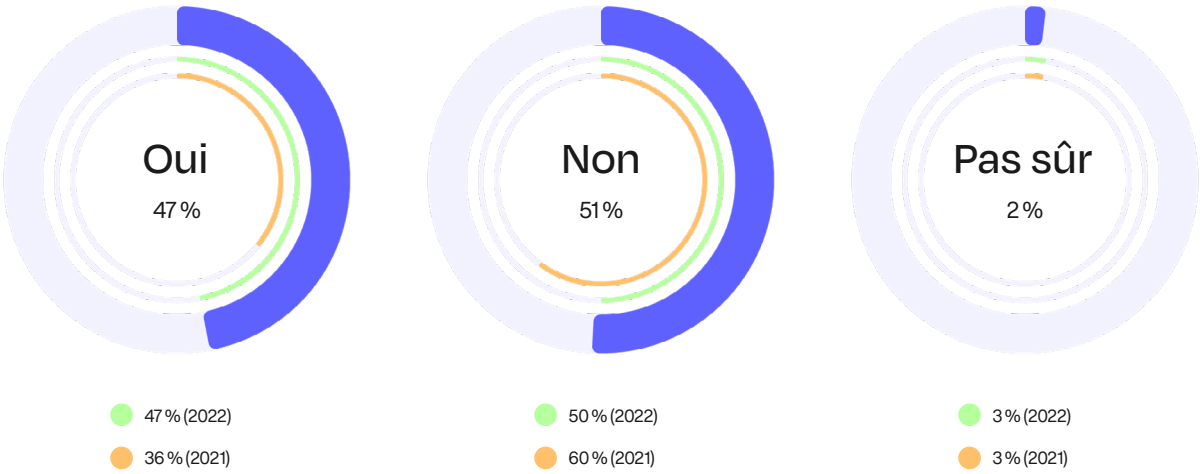
Plusieurs réponses possibles

Les entreprises ne disposent pas de contrôles d'accès formels à la signature de code. Il ne suffit pas de générer et de stocker des clés de signature de code en toute sécurité. Pour éviter tout abus ou mauvaise utilisation de la signature de code dans les environnements CI/CD dispersés et automatisés d'aujourd'hui, les entreprises doivent mettre en œuvre des politiques et des contrôles d'accès qui garantissent que seules des personnes, des machines et des outils spécifiques disposant des permissions adéquates ont l'autorisation de signer du code.

Cependant, la figure 21 montre que moins de la moitié des personnes interrogées (47 %) déclarent que leur entreprise dispose d'un contrôle d'accès formel et de processus d'approbation en place pour les clés de signature de code.

Figure 21

Votre entreprise a-t-elle mis en place des processus formels de contrôle d'accès et d'approbation pour les clés de signature de code ?

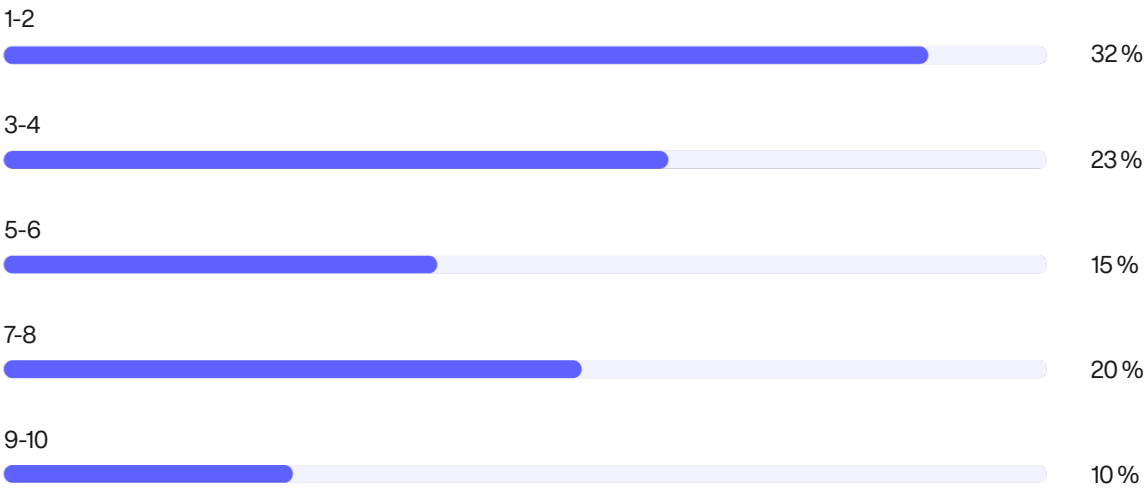


Les entreprises ne sont pas confiantes dans leur capacité à protéger les clés de signature de code. Il n'est pas surprenant que seulement 30 % des personnes interrogées se disent confiantes dans la capacité de leur entreprise à protéger les clés de signature de code contre le vol ou l'utilisation abusive (7 réponses ou plus combinées), tandis que 55 % se disent peu ou pas confiantes (< 4 réponses combinées).

Figure 22

Dans quelle mesure avez-vous confiance dans la capacité de votre entreprise à protéger les clés de signature de code contre le vol ou l'utilisation abusive par des cybercriminels ?

Sur une échelle de 1 = aucune confiance à 10 = grande confiance



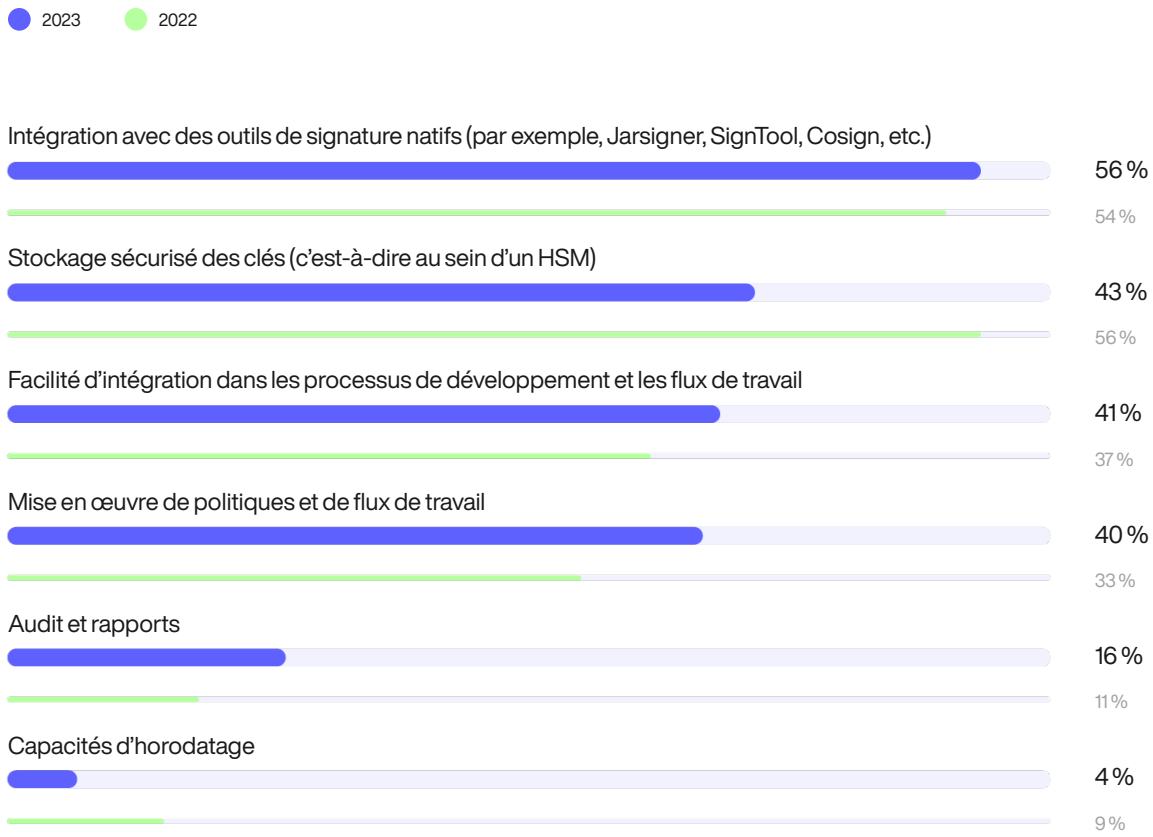
Les solutions de signature de code doivent s'intégrer aux outils et processus existants. La sécurité est indispensable, mais si les solutions de signature ne peuvent pas s'intégrer aux outils et processus existants, les développeurs ne les adopteront pas.

La figure 23 énumère six caractéristiques jugées importantes lors de l'évaluation des solutions de signature de code. Selon les personnes interrogées, les caractéristiques les plus importantes d'une solution de signature de code sont l'intégration avec les outils de signature natifs (56 %), le stockage sécurisé des clés (43 %) et la facilité d'intégration avec les processus de développement et les flux de travail (41 %).

Figure 23

Caractéristiques les plus importantes lors de l'évaluation des solutions de signature de code

Deux réponses possibles



*Remarque : cette question ne figurait pas dans l'enquête de 2021.

Pratiques de gestion des identités SSH

Dans cette section, nous avons demandé aux répondants s'ils connaissaient l'utilisation des identités SSH par leur entreprise. Les réponses des personnes ayant déclaré ne pas être au courant ont été exclues de l'analyse qui suit.

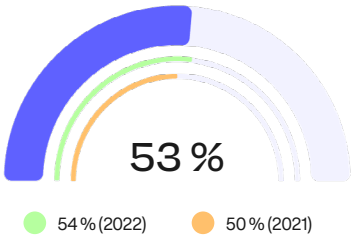
La responsabilité de la gestion des identités SSH incombe de plus en plus aux administrateurs. Lorsqu'on leur demande qui est responsable de la gestion des identités SSH, telles que les clés SSH, les certificats SSH et l'authentification par mot de passe, les personnes interrogées reconnaissent généralement qu'il s'agit d'une responsabilité partagée, en fournissant plusieurs réponses dans de nombreux cas.

Cela dit, comme le montre la figure 24, la responsabilité de la gestion des identifiants SSH se déplace vers les administrateurs de réseau et de cloud, ces deux catégories augmentant régulièrement d'une année sur l'autre.

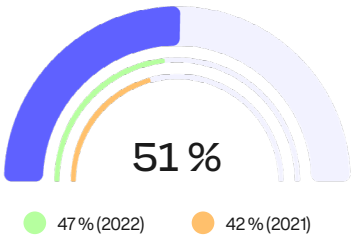
Figure 24

Qui est responsable de la gestion des identifiants SSH ?

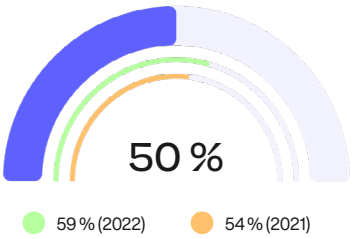
Plusieurs réponses possibles



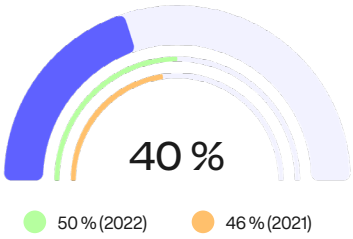
Sécurité informatique



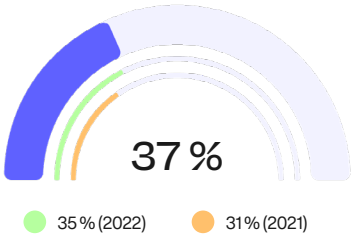
Administrateurs réseau



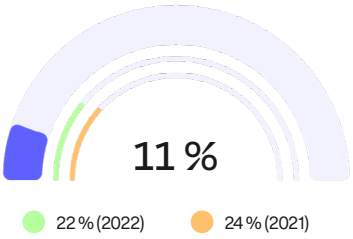
Opérations informatiques



Gestion des identités et des accès (IAM)



Administrateurs de clouds



Aucune fonction n'est responsable

Comment les identités SSH sont-elles gérées ? Cinquante-quatre pour cent des personnes interrogées déclarent que leur entreprise ne dispose pas d'une gestion centralisée des identités SSH, laissant les administrateurs gérer leurs propres clés, certificats ou mots de passe SSH. Cinquante-quatre pour cent des personnes interrogées déclarent utiliser une forme de suivi manuel. Seuls quelques répondants utilisent une solution de gestion des accès privilégiés (PAM) (26 %) ou une solution dédiée à la gestion des clés SSH (27 %).

Figure 25

Comment votre entreprise gère-t-elle les identifiants SSH ?

Plusieurs réponses possibles

La plupart des entreprises sont dans l'ignorance en ce qui concerne les identités SSH. Malgré leur utilisation répandue et leur accès privilégié, les identifiants SSH ne sont souvent pas tracés et restent inactifs sur les serveurs où les attaquants peuvent les exploiter pour accéder à des systèmes critiques et se déplacer latéralement sans être détectés.

Les personnes interrogées sont plus nombreuses à déclarer qu'elles ne disposent pas d'un inventaire précis des identifiants SSH (53 %) que celles qui affirment en disposer (41 %). Par ailleurs, 6 % des personnes interrogées se disent incertaines. Comme le montre la figure 27, seulement 51 % des personnes interrogées déclarent que leur entreprise procède à une rotation régulière (au moins une fois par an) des identités SSH, tandis que 44 % déclarent que leur entreprise procède à une rotation moins fréquente ou pas du tout.

Figure 26

Disposez-vous d'un inventaire précis des identifiants SSH dans votre entreprise ?

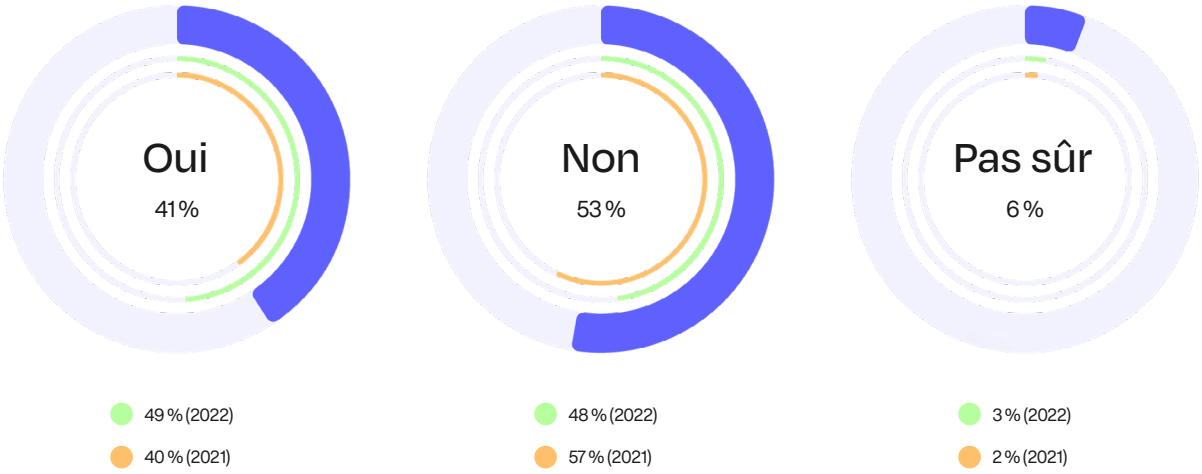
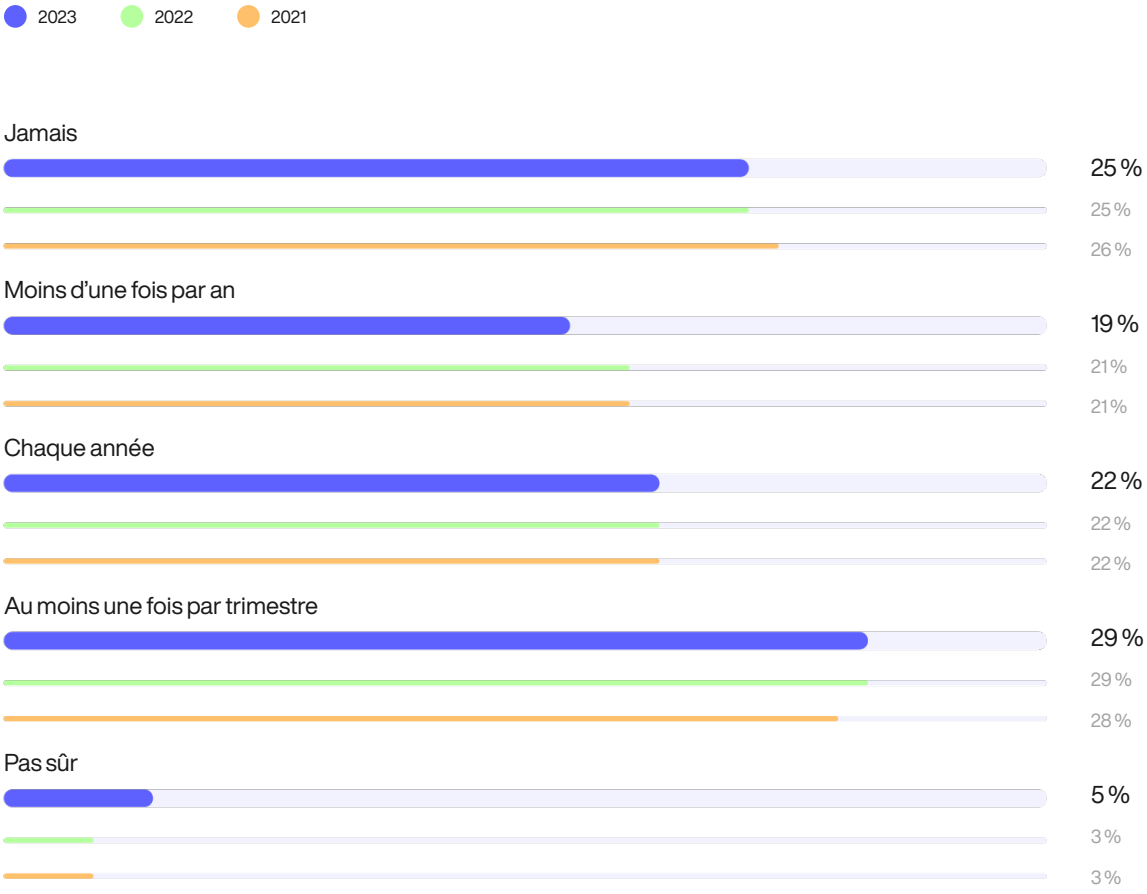


Figure 27

À quelle fréquence votre entreprise procède-t-elle à la rotation des identités SSH ?



L'impact des pannes, de la compromission des identités machine et des échecs d'audit

Chaque machine a besoin d'une identité pour s'authentifier et communiquer en toute sécurité avec d'autres appareils, charges de travail et personnes à l'intérieur et à l'extérieur de l'entreprise. Mais comme le nombre de machines augmente rapidement avec l'adoption du cloud, des appareils IoT et de la main-d'œuvre à distance, la charge d'émettre et de gérer les identités des machines pèse lourdement sur les équipes informatiques et de sécurité.

Sans les bons outils et processus, les équipes perdent le contrôle des identités des machines. Les certificats expirent de manière inattendue, entraînant des interruptions perturbatrices pour les services et les applications. Les clés sensibles utilisées pour signer du code ou obtenir un accès privilégié à des systèmes dorsaux sont détournées par des pirates. Les auditeurs internes ou externes découvrent des lacunes dans les systèmes et les politiques qui entraînent des semaines, voire des mois, de remédiation.

Dans cette section, nous analysons la fréquence, la gravité et l'impact de ces incidents sur les risques. Nous vous présentons ici une brève analyse de ces incidents avec des exemples d'événements récents très médiatisés.

Pannes de certificats

Si un certificat inconnu ou non suivi arrive à expiration, les systèmes ou applications sur lesquels il est installé cessent de fonctionner, ce qui entraîne des temps d'arrêt et des perturbations pour les utilisateurs internes ou les services en contact avec la clientèle.

Le mégaphone se tait

Le 31 mai 2022, des millions d'auditeurs de Megaphone, une plateforme populaire d'hébergement de podcasts appartenant à Spotify, n'ont pas pu accéder à leurs émissions préférées pendant plus de huit heures après l'expiration d'un seul certificat SSL, ce qui a entraîné l'arrêt de systèmes critiques.[1] Pour chaque panne comme celle-ci qui fait la une des journaux, il y en a des milliers d'autres dont personne n'entend parler.

1 Panne massive de podcasts causée par le non-renouvellement du certificat de sécurité de Spotify

Compromission de l'identité d'une machine

Les identités machine, telles que les clés SSH, les certificats TLS et les clés de signature de code, sont des cibles de grande valeur pour les cybercriminels qui les utilisent pour signer et distribuer du code malveillant, obtenir un accès privilégié aux systèmes ou même se faire passer pour des entreprises légitimes.

Clés de signature exposées

Le 6 décembre 2022, la célèbre plateforme d'hébergement de code GitHub a signalé qu'un utilisateur non autorisé avait accédé à un référentiel contenant trois certificats de signature de code protégés par mot de passe et utilisés pour ses anciennes applications Atom et Desktop. Heureusement, GitHub a détecté la violation rapidement et a pu prendre des mesures correctives avant que des dommages ne soient causés.[2]

Échec des audits

Des résultats d'audit inattendus et la non-conformité avec les mandats réglementaires liés à la PKI, à la signature et à la gestion des certificats peuvent entraîner des amendes potentielles ou des efforts de remédiation coûteux.

De nouveaux mandats augmentent la pression

Le 2 mars 2023, l'administration Biden-Harris a publié la stratégie nationale de cybersécurité, qui, entre autres, confère davantage de responsabilités aux fabricants d'appareils IoT et aux éditeurs de logiciels pour garantir la sécurité et l'intégrité de leurs produits. Ce mandat et d'autres semblables imposeront sans aucun doute aux entreprises des exigences accrues en matière d'émission et de gestion d'identités uniques pour les appareils et de signature numérique des logiciels afin d'en garantir l'intégrité.[3]

2 Action nécessaire pour les utilisateurs de GitHub Desktop et Atom
3 Fiche descriptive :L'administration Biden-Harris annonce une stratégie nationale de cybersécurité

Qu'est-ce qui empêche les équipes informatiques et de sécurité de dormir ? Les répondants ont été invités à évaluer la gravité perçue (figure 28) et l'impact financier (figure 29) de chaque incident sur une échelle de 1 (pas grave/impact très grave) à 10 (très grave/impact très grave).

Dans l'ensemble, la gravité perçue et l'impact financier des incidents liés à l'identité des machines se sont stabilisés dans l'étude de cette année, après des augmentations significatives entre 2021 et 2022.

Les échecs d'audit restent l'incident le plus coûteux et le plus grave, 66 % des personnes interrogées déclarant que les échecs d'audit sont une préoccupation très sérieuse, et 57 % déclarant que ces incidents ont un impact financier très grave sur l'entreprise.

Figure 28

La gravité des incidents liés à l'identité des machines

Sur une échelle de 1 = pas grave à 10 = très grave. Plus de 7 réponses présentées.

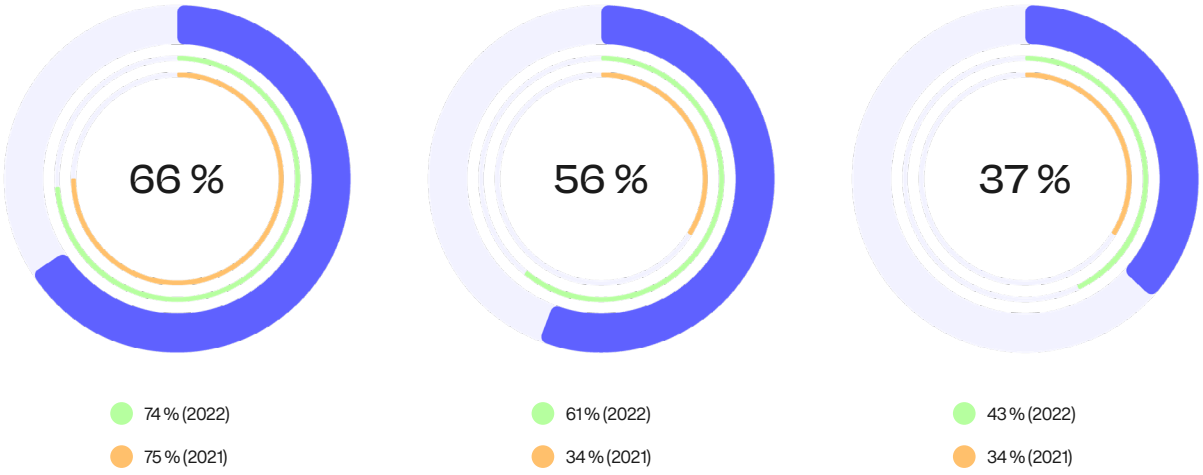
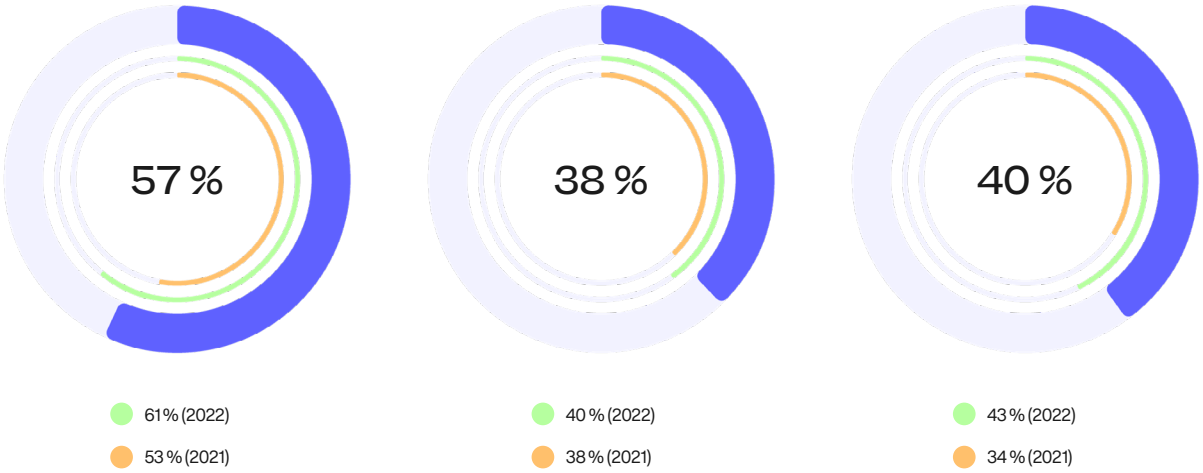


Figure 29

L'impact financier des incidents liés à l'identité des machines

Sur une échelle de 1 = aucun impact à 10 = impact très grave. Plus de 7 réponses présentées.

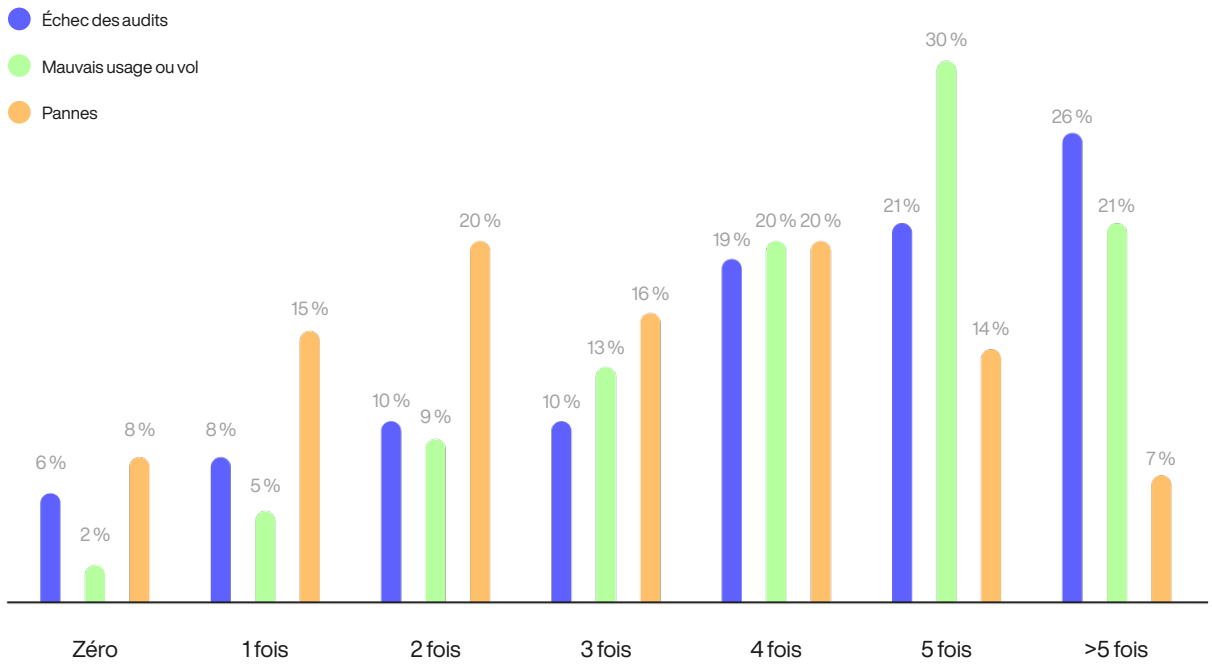


Quelle est la fréquence de ces incidents ? Les répondants ont été invités à estimer le nombre de fois où chaque incident s'est produit au cours des 24 derniers mois. Comme le montre la figure 30, l'utilisation abusive ou le vol de clés et de certificats est l'incident le plus fréquemment signalé, 93 % des personnes interrogées déclarant que leur entreprise a connu au moins deux incidents de ce type au cours des 24 derniers mois.

En moyenne, les personnes interrogées estiment que leur entreprise a connu 4,37 incidents liés au vol ou à l'utilisation abusive de clés et de certificats au cours des 24 derniers mois, suivis par les échecs d'audit (4,19 incidents) et les pannes causées par des certificats périmés (3 incidents).

Figure 30

Fréquence des incidents liés à l'identité des machines au cours des 24 derniers mois



Nombre moyen d'incidents au cours des 24 derniers mois

4.19
Échec des audits

4.37
Mauvais usage ou vol

3.00
Pannes

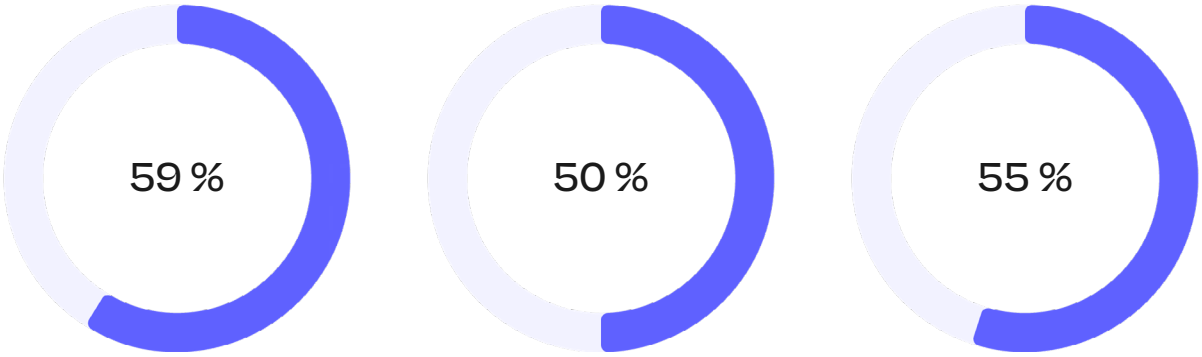
Les pannes liées aux certificats perturbent les systèmes critiques. Les pannes causées par l'expiration inattendue d'un certificat peuvent causer des ravages dans les infrastructures critiques, qu'il s'agisse d'applications destinées aux clients, de vitrines en ligne ou d'appareils et de réseaux internes.

Comme le montre la figure 31, 55 % des personnes interrogées déclarent que les pannes de certificat survenues au cours des 24 derniers mois ont entraîné des incidents graves qui ont fortement perturbé les services destinés aux clients. Cinquante autres pour cent déclarent que les pannes ont déclenché des incidents majeurs perturbant un sous-ensemble de clients ou d'utilisateurs internes, tandis que 59 % déclarent que les pannes ont entraîné des désagréments mineurs pour les clients et les utilisateurs internes.

Figure 31

Parmi les incidents suivants, lesquels se sont produits à la suite de l'expiration inattendue de certificats au cours des 24 derniers mois ?

Plusieurs réponses possibles



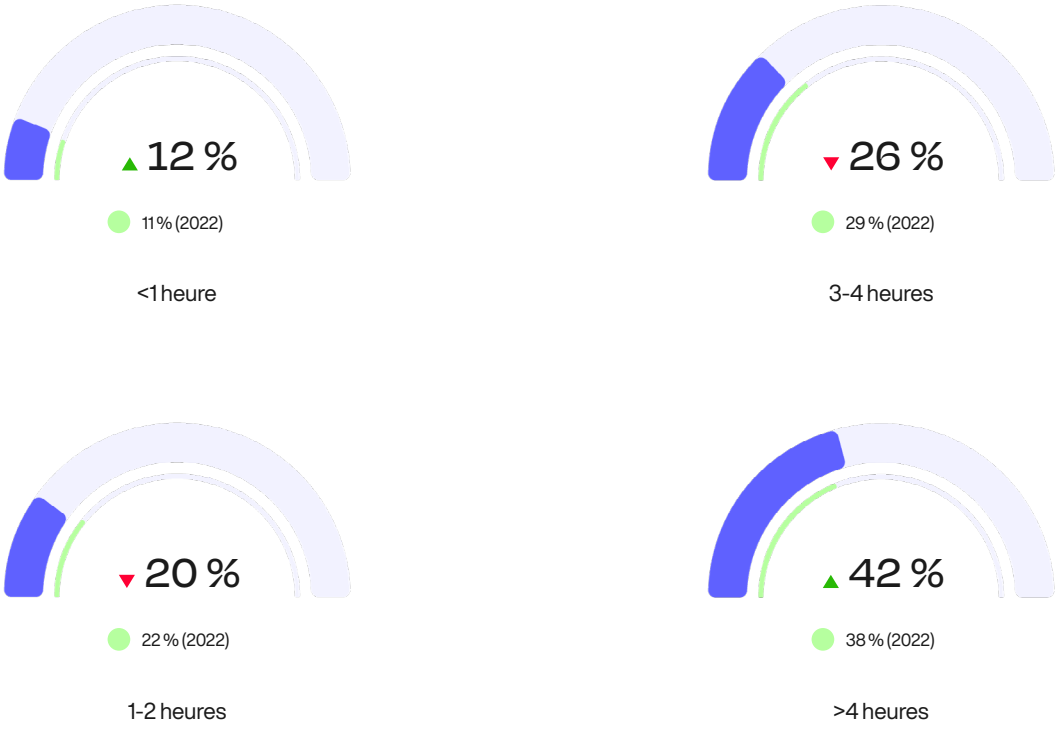
Le temps de rétablissement (TTR) d'une panne liée à un certificat est lent. Remédier à une panne liée à un certificat n'est pas aussi simple que de renouveler le certificat expiré ; cela implique d'identifier la cause première, de localiser le certificat expiré, puis de renouveler, réémettre et fournir le certificat à tous les systèmes affectés avant qu'ils ne puissent être redémarrés.

Il a été demandé aux personnes interrogées combien de temps il fallait à leurs équipes pour identifier les pannes liées aux certificats et y remédier. Comme le montre la figure 32, 42 % des personnes interrogées déclarent qu'il faut plus de 4 heures à leurs équipes pour rétablir la situation, tandis que 26 % déclarent qu'il faut entre 3 et 4 heures. En moyenne, les entreprises mettent 3,79 heures à reprendre complètement leurs activités, contre une moyenne de 3,28 heures dans l'étude de l'année dernière.

Sans visibilité sur les certificats et leur emplacement, ou sans la possibilité d'automatiser le renouvellement et le provisionnement, les équipes peuvent mettre des heures, plutôt que des minutes, à se remettre de ces incidents, sans parler de la prévention de ces incidents.

Figure 32

En moyenne, combien de temps faut-il à vos équipes pour identifier et remédier à une panne liée à un certificat ?



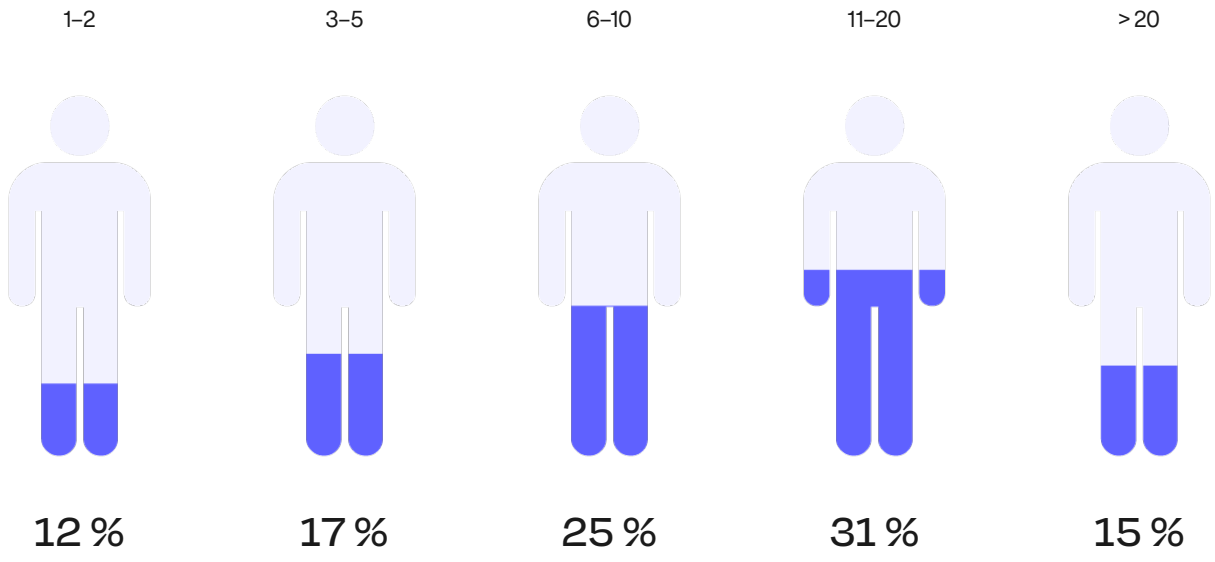
*Remarque : cette question ne figurait pas dans l'enquête de 2021.

Les pannes détournent de nombreuses équipes informatiques de leurs priorités quotidiennes. On a demandé aux personnes interrogées combien de membres du personnel sont directement impliqués dans une panne liée à un certificat, y compris ceux qui participent au diagnostic, à la résolution et à la remédiation de l'incident.

Selon les répondants, 11 personnes en moyenne sont directement impliquées dans la résolution d'une panne typique liée à un certificat, 46 % d'entre eux déclarant qu'il faut plus de 11 personnes pour y remédier.

Figure 33

Combien de membres du personnel, en moyenne, sont directement impliqués lors d'une panne typique causée par un certificat expiré ?



*Note : cette question n'a pas été incluse dans l'enquête de 2021 ou 2022.

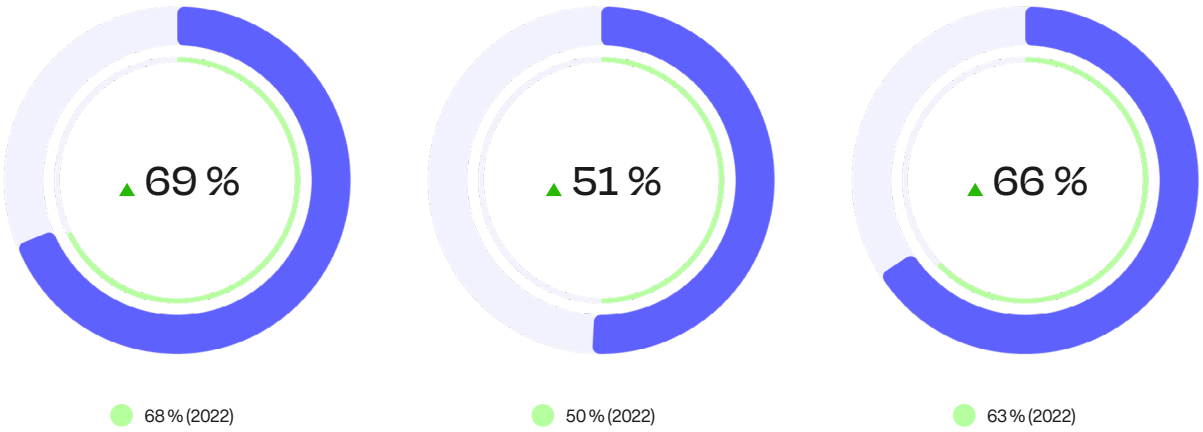
Les incidents liés à l'identité des machines devraient se poursuivre. Les répondants ont été interrogés sur la probabilité que des échecs d'audit, une utilisation abusive ou un vol de clés et de certificats, ainsi que des pannes liées à des certificats se produisent au cours des 24 prochains mois, sur une échelle allant de peu probable à très probable, en passant par assez probable et probable.

Comme le montre la figure 34, la majorité des personnes interrogées prévoient que ces incidents vont probablement ou très probablement se poursuivre au cours des 24 prochains mois. L'incident le plus probable est l'échec des audits ou le manque de conformité, suivi par les pannes de certificats et l'utilisation abusive ou le vol de clés et de certificats.

Figure 34

La probabilité que ces incidents se produisent au cours des 24 prochains mois

Réponses probables et très probables combinées



*Remarque : cette question ne figurait pas dans l'enquête de 2021.

Cinq étapes pour une gestion réussie des identités machine

Dans cette section, Keyfactor présente les étapes que les entreprises peuvent suivre pour améliorer leur stratégie de gestion des identités machine, ainsi que les ressources recommandées pour soutenir ces efforts.

Établir la propriété de l'identité de la machine.

Il est impératif de définir clairement la propriété. Dans l'étude, 78 % des répondants ont déclaré avoir un groupe de travail ou une équipe de gestion des identités machine immature ou inexistant. La technologie est une considération évidente pour la gestion des identités machine. Cependant, une mise en œuvre correcte de la technologie repose sur une base adéquate de personnes, de processus et de pratiques.

Selon Gartner, les entreprises devraient « définir la propriété des outils, des clés, des secrets et des certificats respectivement. Utiliser les conseils pour faire passer l'équipe PKI d'une structure de « gestion indirecte » à une structure de « gestion déléguée » en se concentrant sur les garde-fous et les politiques plutôt que sur la centralisation des outils »*.

Investissez dans la gestion de l'identité de votre machine.

Investir dans votre plateforme de gestion des identités machine peut aider votre entreprise à améliorer la visibilité et à accélérer la réponse aux incidents et la productivité. Automatisez et standardisez les contrôles de sécurité en les intégrant aux outils, flux de travail et applications existants.

Utilisez les meilleures pratiques établies par votre groupe de travail pour auditer votre paysage d'identité machine, déterminer les lacunes existantes et trouver des outils et des processus qui répondent aux exigences uniques des différentes équipes de votre entreprise, y compris :

- PKI et gestion des certificats
- Gestion des clés SSH
- Gestion des accès privilégiés (PAM)
- Signature de code d'entreprise
- Gestionnaires de secrets
- les systèmes de gestion des clés (KMS)
- Modules de sécurité matériels (HSM)
- Services PKI gérés

* Gartner, Solution Comparison for PKI and Certificate Management Tools, 2 mars 2021, Erik Wahlstrom, Paul Rabinovich.

Réduisez la complexité de votre infrastructure PKI.

Pour la première fois, la principale priorité stratégique en matière de sécurité numérique dans les entreprises est la réduction de la complexité de l'infrastructure PKI, une augmentation de 50 % en 2021 à 58 % dans l'étude de cette année. Davantage d'entreprises font de la prévention des pannes inattendues causées par des certificats expirés une priorité (53 % des répondants contre seulement 30 % des répondants en 2022).

Notamment, 74 % des personnes interrogées, contre 61 % en 2021, déclarent que leur entreprise déploie davantage de clés cryptographiques et de certificats numériques. En conséquence, cela a considérablement augmenté la charge opérationnelle des équipes de leur entreprise, selon 72 % des répondants, une augmentation par rapport à 62 % en 2021.

La réduction de la complexité est entravée par l'absence d'un groupe de travail mature sur l'identité des machines, soutenu par des ressources suffisantes. Seulement 31 % des personnes interrogées déclarent que leur entreprise dispose d'un groupe de travail mature sur l'identité des machines qui assure le leadership, la recherche, la stratégie de mise en œuvre, la propriété et les meilleures pratiques. En outre, 53 % des personnes interrogées déclarent que leur entreprise n'alloue pas suffisamment de ressources et de personnel au déploiement de la PKI.

Utilisez les services gérés pour combler le déficit de compétences et atténuer les effets de la pénurie de main-d'œuvre dans le domaine de la cybersécurité.

Quarante-deux pour cent des personnes interrogées dans le cadre de l'étude ont identifié le manque de compétences comme un obstacle à la mise en place d'une stratégie de cryptographie et d'identité machine à l'échelle de l'entreprise. Par ailleurs, 31 % des personnes interrogées citent le manque de ressources (temps et argent) comme un obstacle à la mise en place d'une telle stratégie.

Les experts en PKI et en cryptographie sont difficiles à trouver et encore plus difficiles à retenir. Un fournisseur de services de cryptographie ou de PKI gérés peut contribuer à réduire considérablement les coûts d'infrastructure, à atténuer les risques et à éliminer la charge opérationnelle associée à la gestion d'une infrastructure PKI en interne, en particulier en période de pénurie mondiale de main-d'œuvre.

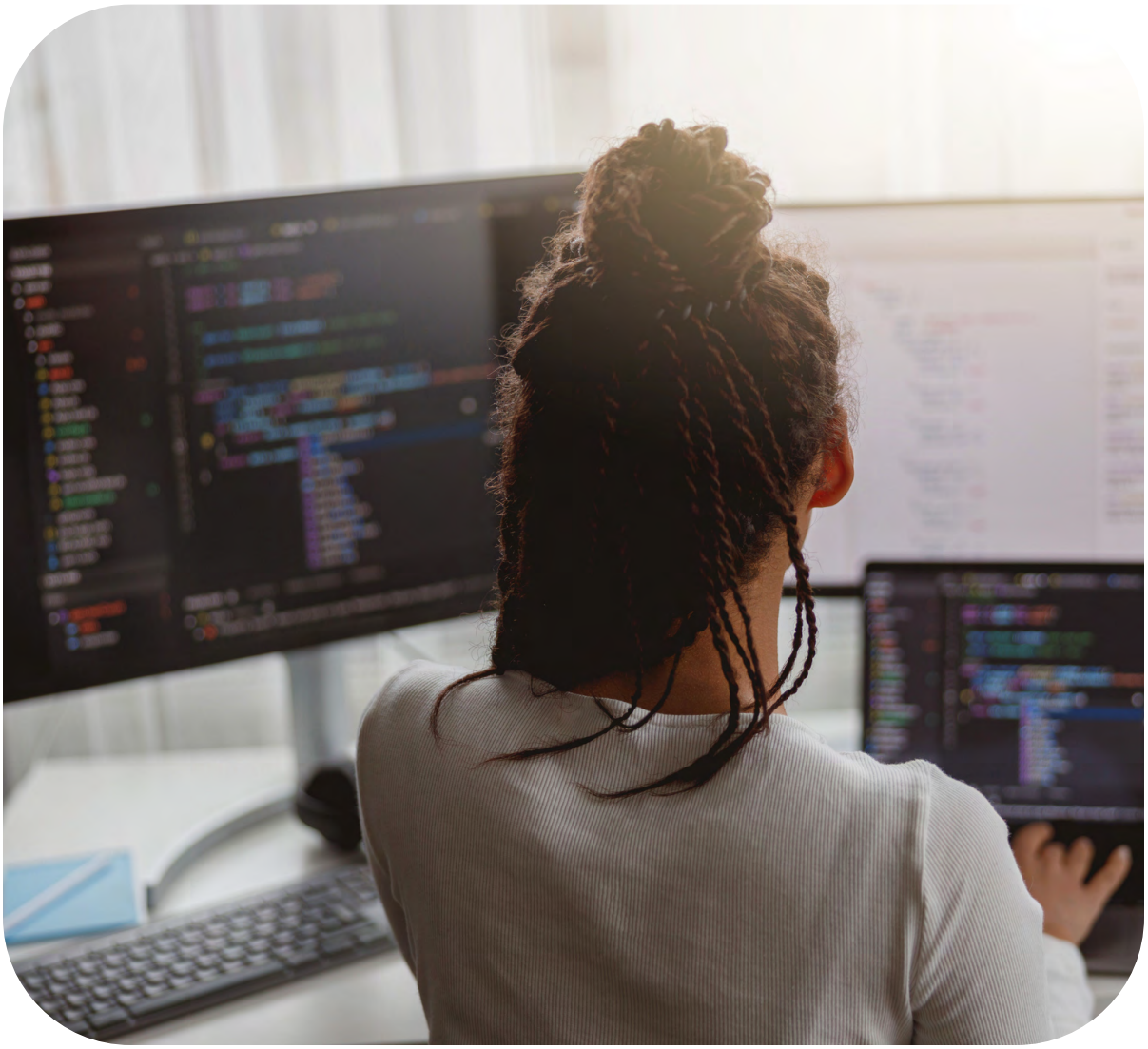
La sécurité de la signature de code devrait être un élément important des stratégies de gestion des identités machine.

La signature de code sans sécurisation des clés privées peut exposer les entreprises à des risques importants. Les développeurs de logiciels doivent souvent signer le code pour faciliter l'installation. Sans une signature de code sécurisée, les attaquants peuvent compromettre ces clés pour signer et distribuer un code malveillant aux clients d'une entreprise sous la forme d'un logiciel ou d'un microprogramme légitime.

Les répondants ont été interrogés sur leur implication dans la signature de code, et 71 % d'entre eux ont répondu qu'il s'agissait de signer numériquement le code et le logiciel. Soixante et un pour cent ont déclaré être responsables de la gestion de ces clés, et 50 % des personnes interrogées vérifient et protègent l'accès aux clés de signature de code. Selon l'étude, les répondants les plus responsables de la gestion et de la protection des clés de signature de code sont les opérations informatiques (29 %), les développeurs (24 %) et la sécurité informatique (24 %).

Les cas d'utilisation de la signature de code se multiplient : les entreprises utilisent souvent la signature de code pour les logiciels, les artefacts et les conteneurs Les meilleures pratiques en matière de signature de code incluent un processus formel de signature de code, permettant aux développeurs de signer du code depuis n'importe où tout en s'assurant que les clés restent en sécurité. Cependant, les équipes de sécurité et de développement doivent travailler en collaboration et intégrer les processus de signature de code aux outils et flux de travail existants sans avoir à franchir des étapes supplémentaires pour accéder aux clés qui sont stockées en toute sécurité. L'utilisation d'une solution de signature peut contribuer à garantir le respect d'une sécurité appropriée tout en offrant une flexibilité maximale pour signer les artefacts au moment et selon les besoins, tout en conservant une trace vérifiable pour garantir la conformité.

Dans notre monde axé sur les logiciels, la confiance est primordiale. S'assurer que les équipes de sécurité et de développement d'une entreprise travaillent ensemble pour protéger les certificats numériques et les clés utilisés pour la signature de code est essentiel pour garantir que leurs logiciels restent sûrs et fiables - ce qui fait de la signature de code un élément essentiel d'une chaîne d'approvisionnement logicielle sécurisée.

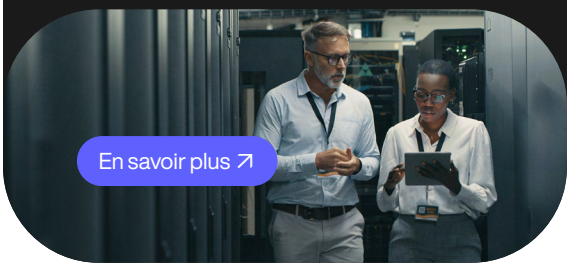


Recommandations

Ressources utiles

Trois stratégies pour surmonter la pénurie de main-d'œuvre dans le secteur de la cybersécurité

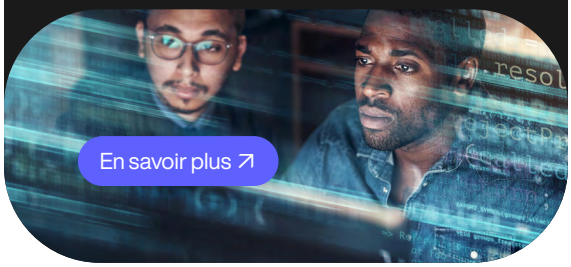
Découvrez comment faire face à la pénurie de main-d'œuvre dans le domaine de la cybersécurité et à ses conséquences grâce à des stratégies visant à aider votre équipe à faire plus avec moins, ainsi qu'à des conseils sur l'élaboration d'une analyse de rentabilité pour moderniser et automatiser votre infrastructure de clés publiques.



En savoir plus ↗

La feuille de route définitive pour la signature de code sécurisée

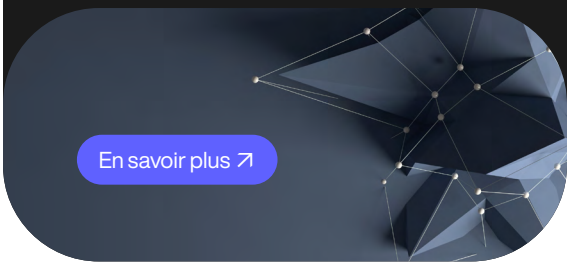
Découvrez l'importance de la signature de code sécurisée et les risques d'une mauvaise mise en œuvre. Découvrez quatre étapes pratiques pour surmonter les problèmes de sécurité et les solutions qui vous mettront sur la bonne voie.



En savoir plus ↗

Planifier la cybersécurité post-quantique

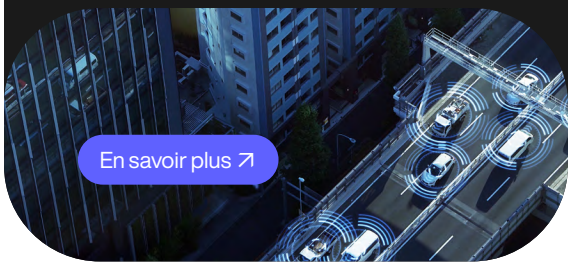
Découvrez pourquoi il est maintenant temps pour les entreprises de planifier la protection de leurs données et identités contre la menace future de l'informatique quantique.



En savoir plus ↗

Perspectives de la cybersécurité de l'IdO en 2023 et au-delà

Regardez ce webinaire à la demande avec Admir Abdurahmanovic, SVP of Strategy, Keyfactor, pour savoir comment vous préparer à l'évolution du paysage de la sécurité de l'IoT en 2023.

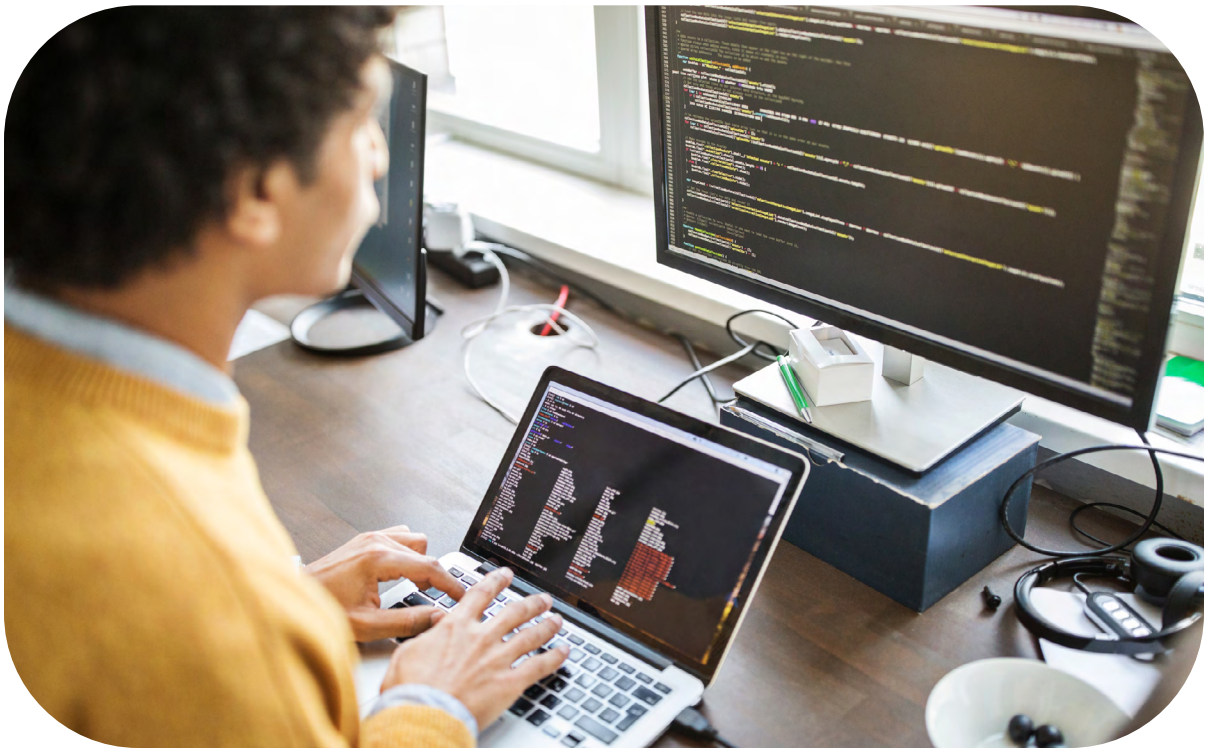


En savoir plus ↗

Méthodologie de recherche

Un échantillon de 31 817 professionnels de la sécurité informatique en Amérique du Nord et dans la région EMEA, ainsi que des entreprises dotées d'une PKI, ont été sélectionnés pour participer à cette enquête. Le tableau 1 indique 1 411 réponses au total. Les contrôles de présélection et de fiabilité ont nécessité l'élimination de 131 enquêtes. L'échantillon final se compose de 1 280 questionnaires, soit un taux de réponse de 4 %. Tous les répondants connaissent bien la PKI de leur entreprise.

Exemple de réponse	Fréquence
Cadre d'échantillonnage	31,817
Nombre total de réponses	1,411
Enquêtes rejetées ou filtrées	131
Échantillon final	1,280
Taux de réponse	4 %

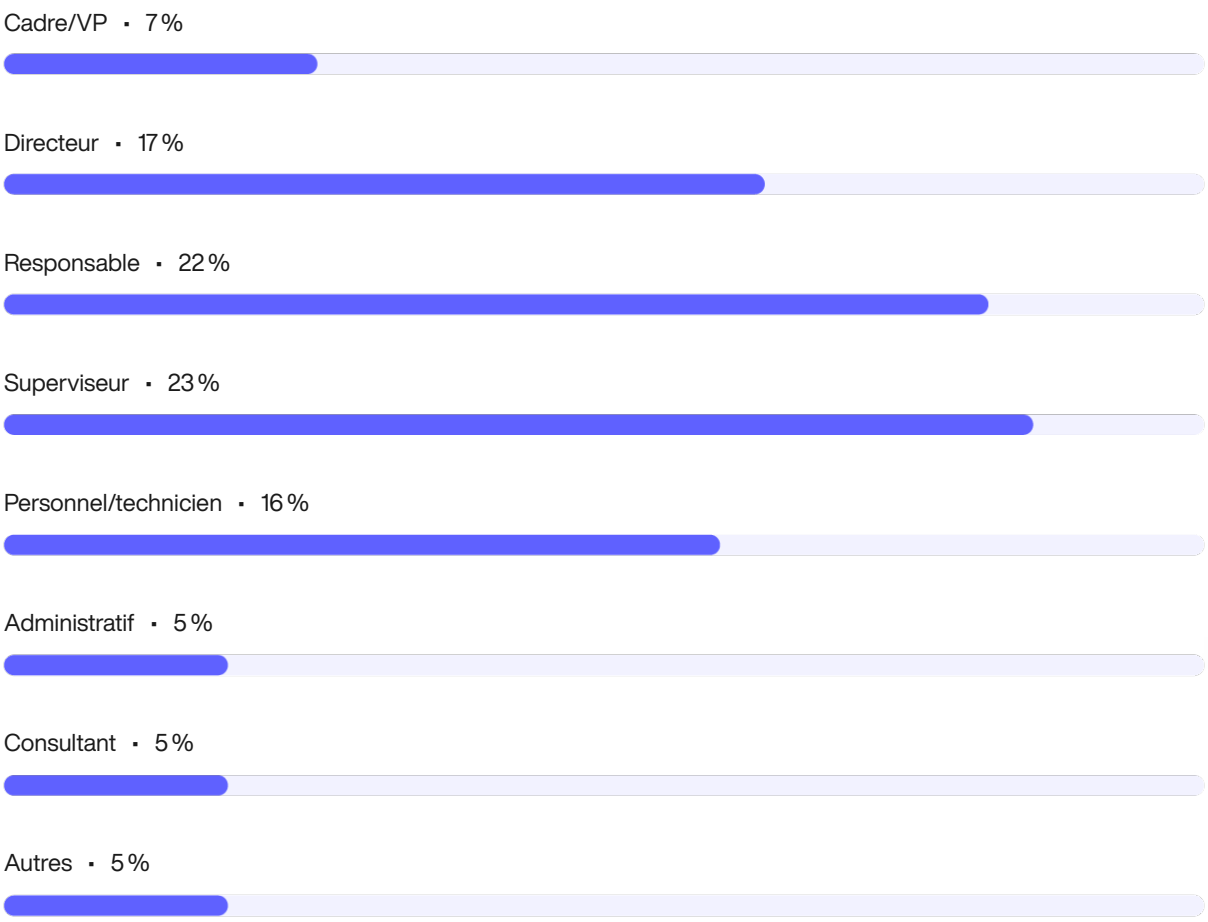


Répondants à l'enquête

Voici un aperçu des 1 280 personnes qui ont répondu à l'enquête en janvier 2023.

Figure 35

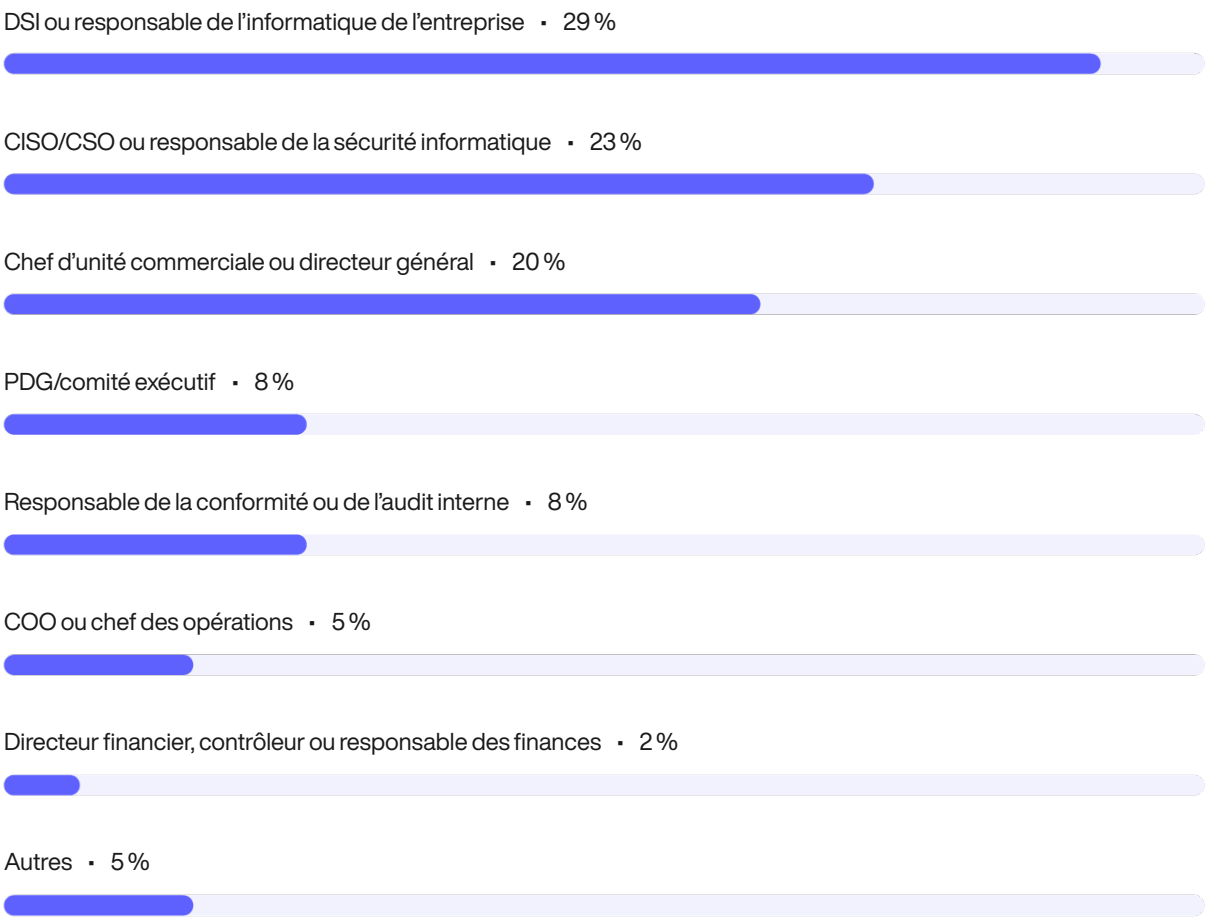
Poste actuel au sein de l'entreprise



La figure 35 indique le niveau organisationnel des répondants au sein des entreprises participantes. Par définition, plus de la moitié (69 %) des répondants se situent au niveau de l'encadrement ou à un niveau supérieur. La catégorie la plus importante (23 % des répondants) est celle des superviseurs.

Figure 36

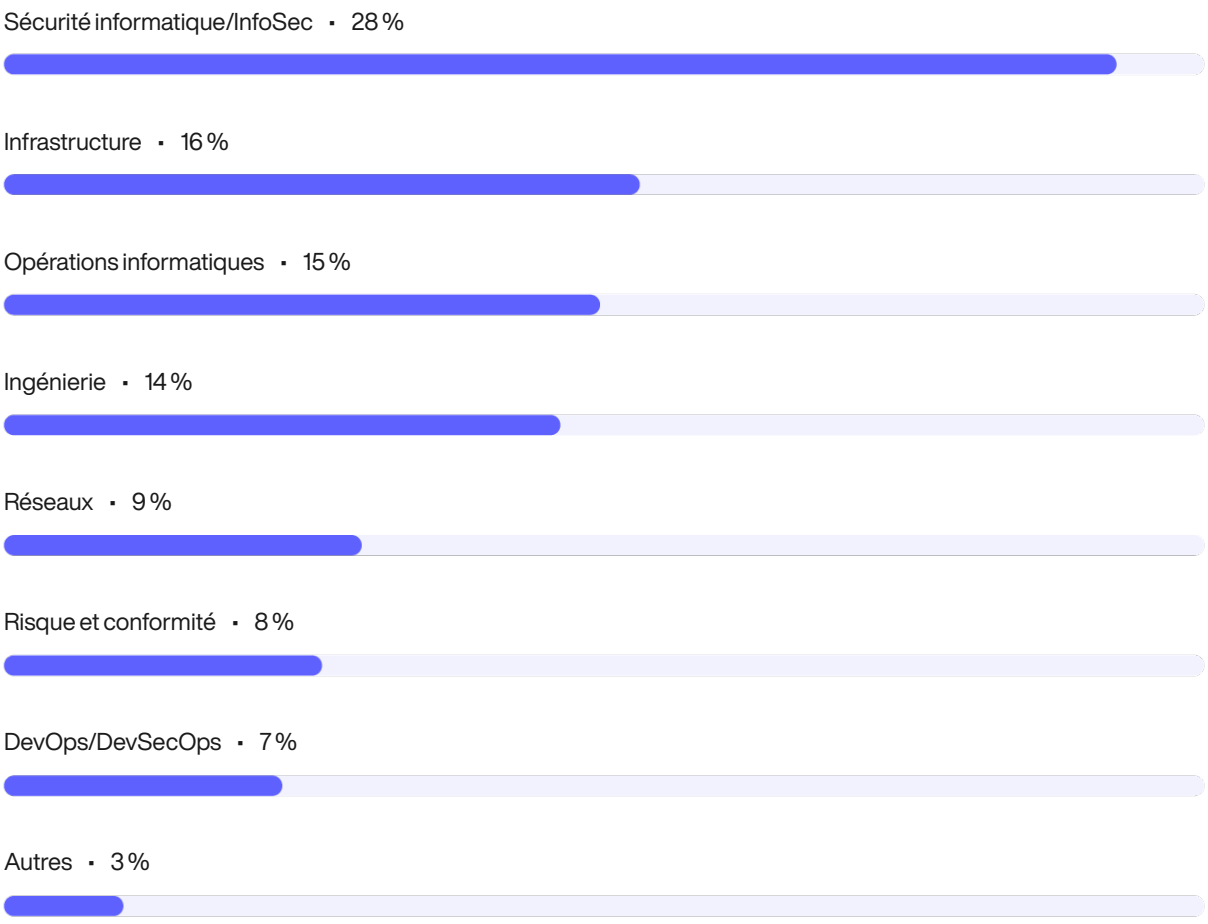
Lien hiérarchique direct



Comme le montre la figure 36, 29 % des personnes interrogées rendent compte au DSI ou au responsable de l'informatique de l'entreprise, 23 % au CISO/CSO ou au responsable de la sécurité informatique, 20 % au responsable de l'unité commerciale ou au directeur général.

Figure 37

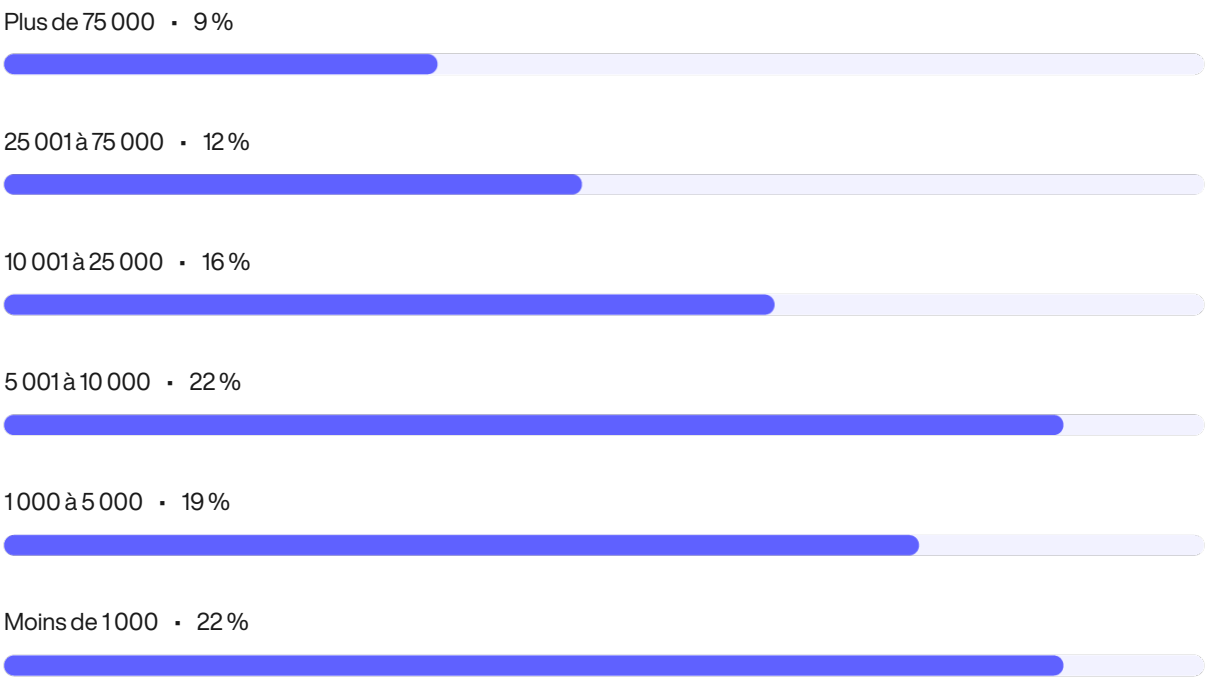
Service ou équipe des répondants



D'après la figure 37, 28 % des personnes interrogées font partie du service de sécurité informatique/Info sec. Viennent ensuite l'infrastructure (16 % des répondants), les opérations informatiques (15 % des répondants), l'ingénierie (14 % des répondants) et la mise en réseau (9 % des répondants).

Figure 38

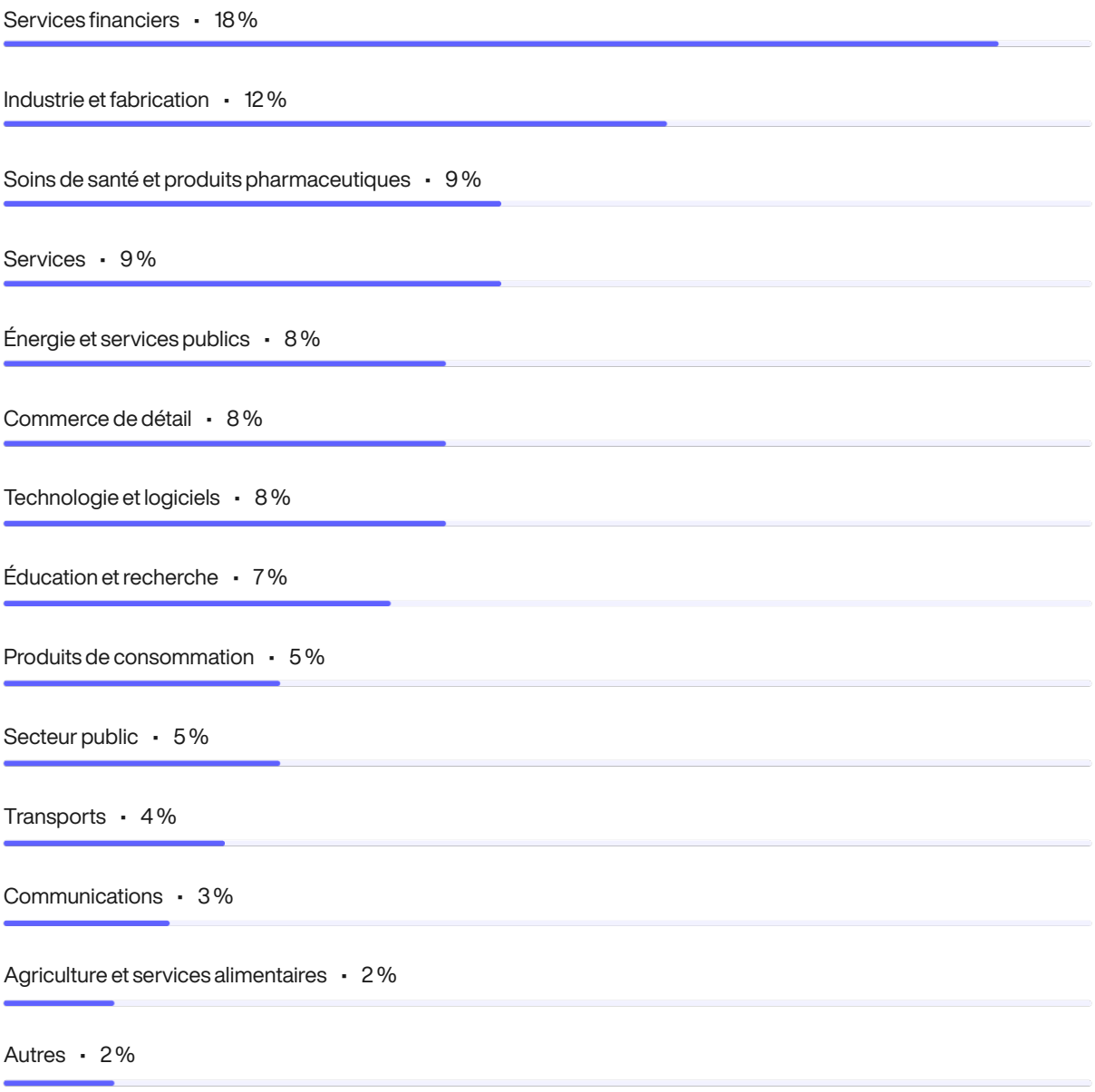
Effectifs mondiaux à temps plein



Comme le montre la figure 38, 59 % des répondants appartiennent à des entreprises dont l'effectif global est supérieur à 5 000 personnes.

Figure 39

Répartition de l'échantillon par secteur d'activité



La figure 39 présente la classification sectorielle des entreprises des répondants. Ce graphique identifie les services financiers (18 %) comme le principal secteur d'activité, qui comprend la banque, la gestion des investissements, l'assurance, le courtage, les paiements et les cartes de crédit. Viennent ensuite l'industrie et la fabrication (12 % des répondants), les soins de santé et les produits pharmaceutiques (9 % des répondants), les services (9 % des répondants), l'énergie et les services publics, la vente au détail et les technologies et logiciels (8 % des répondants chacun).

Limites de l'enquête

Les enquêtes comportent des limites inhérentes qu'il convient d'examiner attentivement avant de tirer des conclusions des résultats. Les points suivants sont des limites spécifiques qui concernent la plupart des enquêtes en ligne.

Biais de non-réponse :

Les résultats actuels sont basés sur un échantillon de réponses à l'enquête. Nous avons envoyé des enquêtes à un échantillon représentatif de personnes, ce qui a permis d'obtenir un grand nombre de réponses utilisables. Malgré les tests de non-réponse, il est toujours possible que les personnes qui n'ont pas participé soient substantiellement différentes, en termes de croyances sous-jacentes, de celles qui ont rempli l'instrument.

Biais d'échantillonnage :

La précision est basée sur les informations de contact et sur la mesure dans laquelle la liste est représentative des personnes qui connaissent la PKI de leur entreprise. Nous reconnaissons également que les résultats peuvent être faussés par des événements extérieurs tels que la couverture médiatique. Enfin, étant donné que nous avons utilisé une méthode de collecte basée sur le web, il est possible que les réponses non basées sur le web, par enquête postale ou par appel téléphonique, aboutissent à des résultats différents.

Résultats autodéclarés :

La qualité des enquêtes repose sur l'intégrité des réponses confidentielles fournies par les sujets. Bien que certains contrôles et équilibres puissent être incorporés dans le processus d'enquête, il est toujours possible qu'un sujet n'ait pas fourni des réponses exactes.

À propos du Ponemon Institute et de Keyfactor

Le rapport 2023 sur l'état de la gestion des identités machine est le fruit d'une collaboration entre Ponemon Institute et Keyfactor. La recherche est menée de manière indépendante par Ponemon Institute, et les résultats sont sponsorisés, analysés et publiés par Keyfactor.

Ponemon INSTITUTE

Le Ponemon Institute© se consacre à la promotion de pratiques responsables en matière de gestion de l'information et de la vie privée dans les entreprises et les administrations. Pour atteindre cet objectif, l'Institut mène des recherches indépendantes, forme des leaders des secteurs privé et public et vérifie les pratiques de protection de la vie privée et des données des entreprises dans une variété d'industries.

KEYFACTOR

Keyfactor apporte la confiance numérique au monde hyperconnecté grâce à la sécurité de l'identité pour chaque machine et chaque être humain. En simplifiant la PKI, en automatisant la gestion du cycle de vie des certificats et en sécurisant chaque appareil, chaque charge de travail et chaque chose, Keyfactor aide les entreprises à établir rapidement une confiance numérique à grande échelle, puis à la maintenir. Dans un monde où la confiance est nulle, chaque machine a besoin d'une identité et chaque identité doit être gérée. Pour en savoir plus, visitez keyfactor.com ou suivez @keyfactor.

Reposant sur la confiance et la sécurité, Keyfactor est fière d'être un employeur égalitaire, un partisan et un défenseur de la croissance d'un lieu de travail fiable, sûr, diversifié et inclusif.