CISCO
SECURE

Étude sur les objectifs en matière de sécurité

Volume 2

Optimiser les cinq bonnes pratiques clés en matière de sécurité

Sommaire

Rappel : les 5 facteurs de réussite

L'étude Cisco 2021 sur les objectifs en matière de sécurité visait à mesurer les points essentiels dans la gestion de la cybersécurité. À cette fin, nous avons examiné 25 bonnes pratiques de sécurité et testé leur corrélation avec la réalisation de 11 objectifs du programme. Vous pouvez consulter ces corrélations entre bonnes pratiques et objectifs via une visualisation interactive sur le site web de l'étude Cisco 2021 sur les objectifs en matière de sécurité, ou télécharger le rapport complet.

Lors des tests, nous avons découvert que 5 bonnes pratiques sur 25 se démarquaient pour leur contribution totale à la réussite du programme de sécurité sur l'ensemble des objectifs mesurés.

Les pages qui suivent traitent des cinq facteurs clés de réussite du programme de sécurité et visent à identifier les stratégies qui optimisent leur efficacité. Les « cinq facteurs de réussite » sont :

Remplacement proactif des technologies	L'entreprise a mis en place une stratégie d'actualisation proactive de ses technologies pour disposer constamment des meilleures solutions IT et dispositifs de sécurité disponibles.
Technologie bien intégrée	Les technologies de sécurité sont bien intégrées et fonctionnent efficacement ensemble.
Réponse rapide aux incidents	Les fonctionnalités de réponse aux incidents permettent d'analyser et de corriger rapidement et efficacement les incidents.
Détection précise des menaces	Les fonctionnalités de détection des menaces offrent une visibilité précise sur les événements liés à la sécurité potentiels sans angles morts majeurs.
Reprise rapide après sinistre	Les fonctionnalités de reprise d'activité réduisent l'impact des incidents et assurent la résilience des services de l'entreprise affectés.

La grande efficacité de ces bonnes pratiques soulève des questions. Pourquoi sont-elles essentielles à la réussite de l'entreprise ? Quels facteurs les rendent plus ou moins efficaces ? Comment l'entreprise doit-elle appliquer ces bonnes pratiques pour optimiser ses résultats ? Telles sont les questions auxquelles nous allons tenter de répondre dans ce nouveau volume de notre étude sur les objectifs des entreprises en matière de sécurité.

Les pages qui suivent traitent des cinq facteurs clés de réussite du programme de sécurité et visent à identifier les stratégies qui optimisent leur efficacité. Pour cela, nous avons mené une enquête indépendante en double aveugle auprès de plus de 5 100 professionnels de l'IT et de la cybersécurité dans le monde entier. Nous analysons les données, en tirons les conclusions et partageons les points à retenir pour permettre à votre entreprise d'améliorer sa sécurité.

Principales conclusions

Nous avons interrogé plus de 5 100 professionnels de l'IT et de la cybersécurité dans 27 pays sur l'approche adoptée par leur entreprise pour mettre à jour et intégrer son architecture de sécurité, détecter et gérer les menaces, et rester résiliente en cas de sinistre. Comme vous pouvez l'imaginer, ils nous ont ainsi communiqué un très grand nombre d'informations, de difficultés, de stratégies et de réussites. Nous avons analysé chaque réponse de différentes manières et tiré les principales conclusions présentées ci-dessous.

Mettre à jour et intégrer l'architecture

- Un département IT moderne et bien intégré contribue à la réussite globale du programme, plus que tout autre contrôle et toute autre bonne pratique en matière de sécurité.
- Les nouvelles architectures cloud sont beaucoup plus faciles à actualiser régulièrement pour s'adapter à l'évolution de l'activité.
- Les entreprises qui s'appuient principalement sur un seul fournisseur doublent leurs chances de créer une pile technologique intégrée.
- Les technologies de sécurité intégrées sont sept fois plus susceptibles de donner lieu à des niveaux élevés d'automatisation des processus.

Détecter les cybermenaces et réagir

- Les programmes de sécurité reposant sur un ensemble solide de collaborateurs, de processus et de technologies sont 3,5 fois plus efficaces que ceux reposant sur des ressources moins performantes.
- Les équipes externalisées de détection et de traitement des menaces sont perçues comme plus performantes, alors que le délai moyen de réponse des équipes internes est plus court (6 jours contre 13 jours).
- Les équipes qui s'appuient largement sur la collecte d'informations sur les menaces sont deux fois plus susceptibles de déployer des capacités robustes de détection et de traitement des menaces.
- L'automatisation multiplie par plus de deux les performances des collaborateurs moins expérimentés et permet avec quasi certitude (95 %) aux équipes les plus solides de mettre en place une sécurité performante.

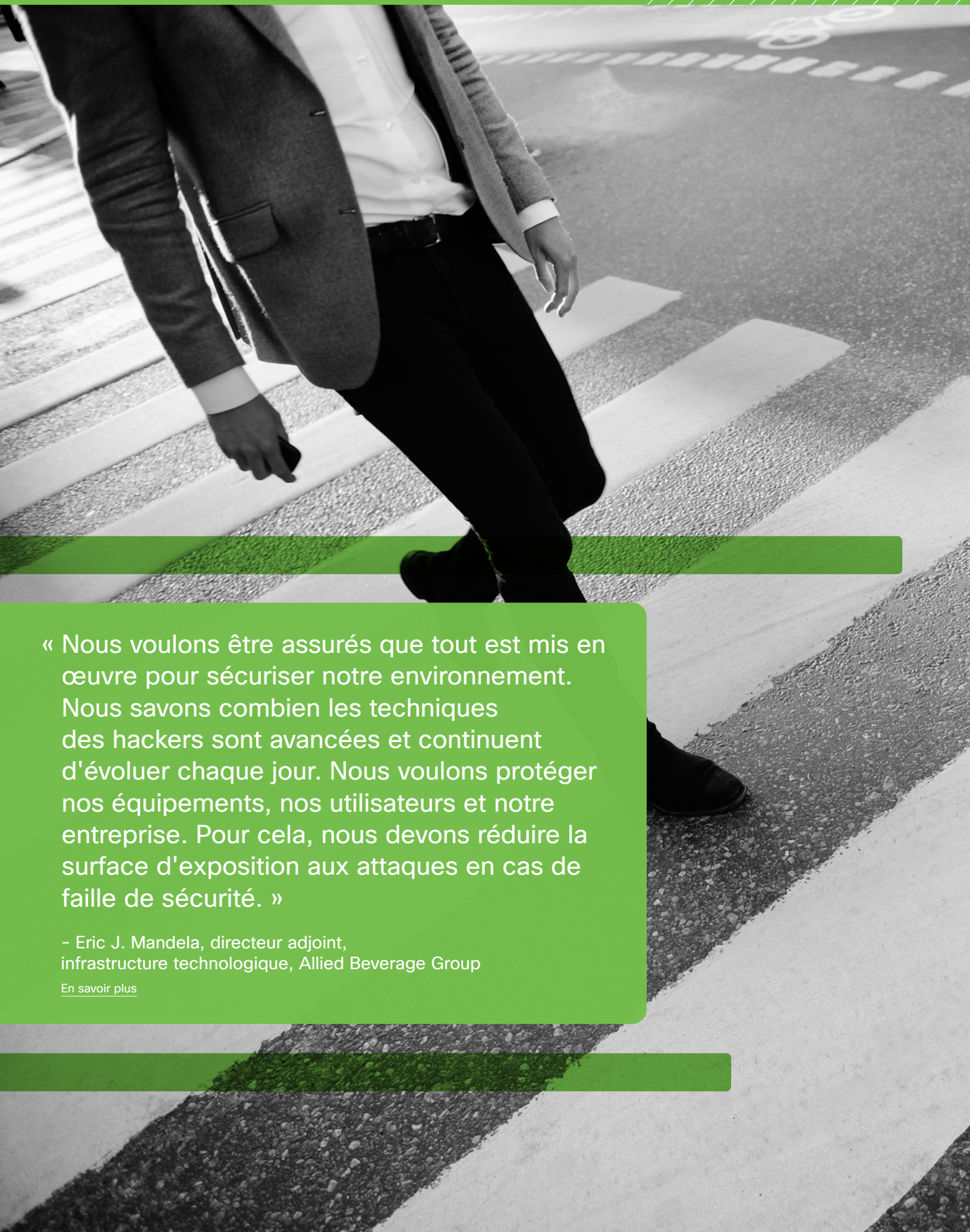
Assurer la résilience en cas de problème majeur

- Les entreprises qui supervisent la continuité de l'activité et la reprise après sinistre au niveau de leur conseil d'administration sont les plus susceptibles (11 % au-dessus de la moyenne) d'avoir mis en place des programmes performants.
- La probabilité d'assurer la résilience ne s'améliore que lorsque les capacités de continuité de l'activité et de reprise après sinistre couvrent au moins 80 % des systèmes stratégiques.
- Les entreprises qui testent régulièrement leurs capacités de reprise d'activité et de reprise après sinistre de plusieurs façons ont 2,5 fois plus de chances d'assurer leur résilience.
- Les entreprises qui intègrent des tests d'« ingénierie du chaos » sont deux fois plus susceptibles d'atteindre des niveaux élevés de résilience.

À propos de l'étude

Échantillonnage	Participants	Analyse
Cisco a fait appel au cabinet d'études YouGov pour mener une enquête entièrement anonyme dans le courant de l'année 2021, suivant une technique d'échantillonnage aléatoire stratifié.	5 123 professionnels de l'IT, de la cybersécurité et de la protection des données de 27 pays ont répondu à l'enquête. Vous pouvez consulter les données relatives aux participants en annexe.	Le Cyentia Institute a analysé les données de l'enquête de manière indépendante pour le compte de Cisco et a généré tous les résultats présentés dans cette étude.

5 123 professionnels de l'IT, de la cybersécurité et de la protection des données de **27** pays ont répondu à l'enquête



« Nous voulons être assurés que tout est mis en œuvre pour sécuriser notre environnement. Nous savons combien les techniques des hackers sont avancées et continuent d'évoluer chaque jour. Nous voulons protéger nos équipements, nos utilisateurs et notre entreprise. Pour cela, nous devons réduire la surface d'exposition aux attaques en cas de faille de sécurité. »

– Eric J. Mandela, directeur adjoint,
infrastructure technologique, Allied Beverage Group

En savoir plus

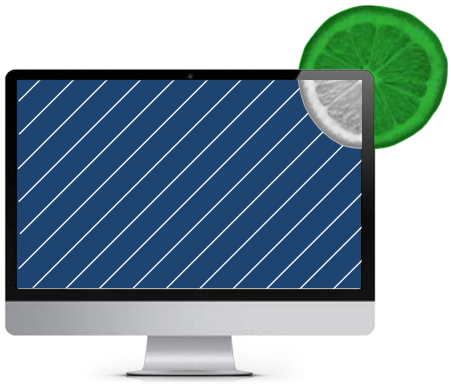
Stratégies de remplacement proactif des technologies

Notre étude précédente avait conclu qu'une approche proactive du remplacement des technologies IT et des systèmes de sécurité afin de disposer constamment de solutions de pointe contribuait plus que toute autre stratégie à la réussite d'un programme de cybersécurité. Ce n'est pas rien dans la mesure où les 25 bonnes pratiques testées étaient toutes considérées comme utiles. Dans cette étude, nous avons donc cherché à savoir ce qui fait l'efficacité de cette bonne pratique.

Pour étudier plus en détail les stratégies de remplacement des technologies, nous avons commencé par évaluer rapidement l'état de l'infrastructure. Nous avons demandé aux participants quelle proportion de leurs technologies de sécurité actives était obsolète. En moyenne, 39 % des technologies de sécurité utilisées par les entreprises sont considérées comme obsolètes. Près de 13 % des participants affirment qu'au moins 8 outils de sécurité sur 10 sont vieillissants.

L'intérêt d'une stratégie de remplacement proactif des technologies apparaît donc clairement. Bien sûr, les nouvelles technologies apportent des fonctionnalités avancées pour lutter contre les menaces en constante évolution. Mais ce n'est pas là leur seul avantage. Nous le verrons en continuant à explorer les réponses aux questions.

En moyenne, 39 % des technologies de sécurité utilisées par les entreprises sont considérées comme obsolètes.



Les caractéristiques de l'infrastructure ont-elles un impact sur les projets d'actualisation des systèmes ?

Dans l'étude initiale, nous avions supposé que les architectures cloud plus modernes étaient plus efficaces, car elles étaient plus faciles à gérer et intégraient des mesures de sécurité natives. Pour tester cette hypothèse, nous avons demandé aux participants de décrire globalement leur infrastructure technologique en choisissant parmi les critères suivants :

- Cloud ou on-premise
- Moderne ou obsolète
- Consolidée ou distribuée

Ces caractéristiques architecturales distinctes contribuent-elles à l'efficacité du remplacement des technologies ? Selon la Figure 1, c'est effectivement le cas. **Les entreprises disposant d'architectures modernes, consolidées et gérées dans le cloud sont deux fois plus susceptibles de faire état de fortes capacités de remplacement de leurs technologies que celles utilisant des systèmes obsolètes, distribués et on-premise.** Toutefois, avant de présenter ce graphique lors de la prochaine réunion sur votre stratégie de migration vers le cloud, notez que les entreprises qui utilisent principalement des environnements on-premise restent plus performantes que la moyenne, à condition d'avoir modernisé leur infrastructure IT.

Bien sûr, la stratégie de remplacement de vos technologies sera plus facile à mettre en œuvre avec des solutions cloud natives, mais le problème de l'obsolescence est le plus urgent à régler. Si l'actualisation de votre ancienne infrastructure est de plus en plus complexe, mieux vaut migrer vers une nouvelle architecture que moderniser l'ancienne. Bien sûr, ce n'est pas toujours possible ni rentable avec vos infrastructures existantes et stratégiques, mais le principe n'en est pas moins valable.

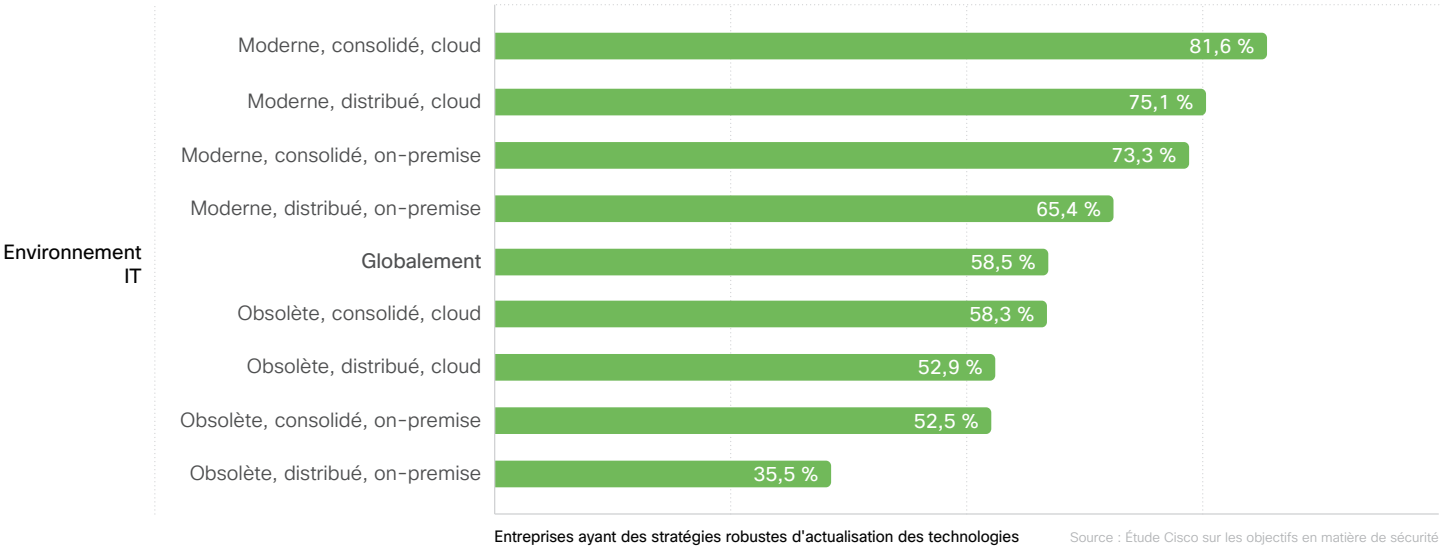
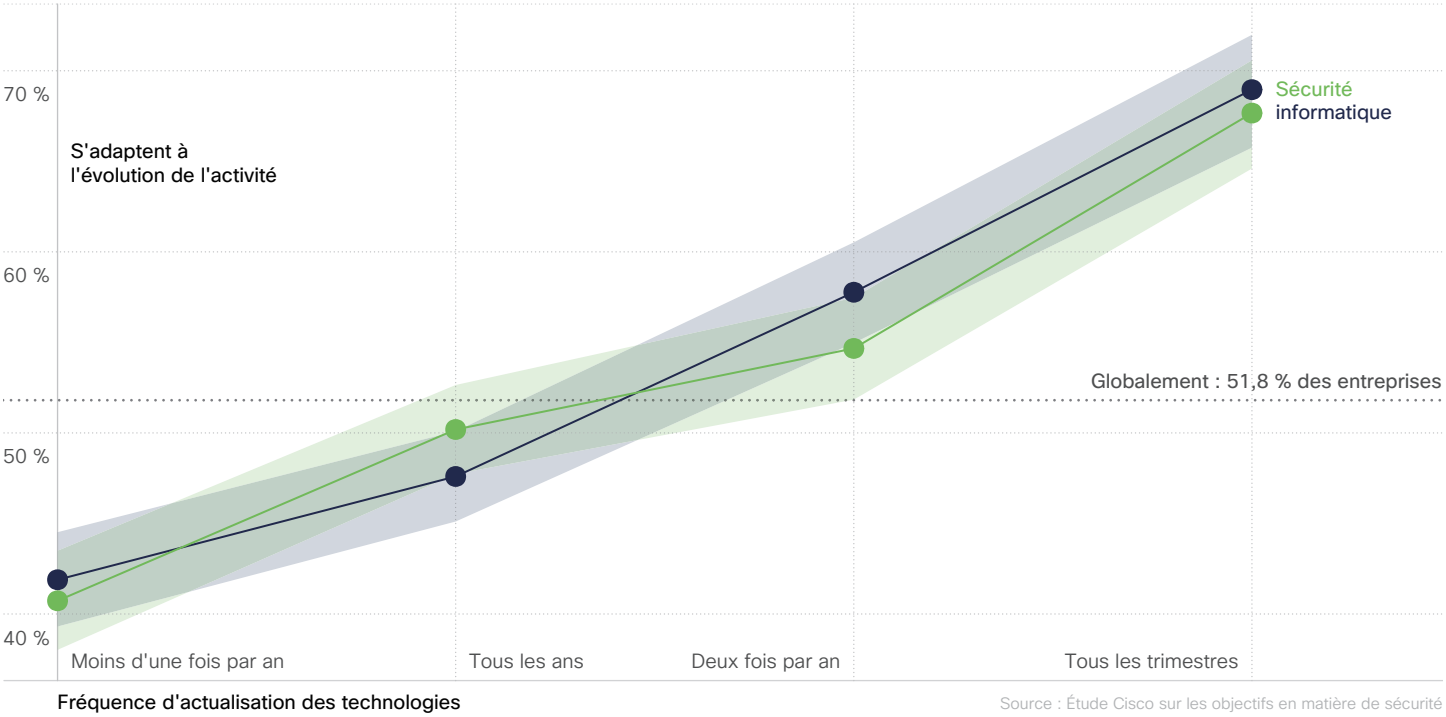


Figure 1 : Effet des caractéristiques de l'architecture IT sur les capacités de remplacement des technologies

81,6 % des entreprises disposant d'architectures modernes, consolidées et gérées dans le cloud font état de fortes capacités de remplacement des technologies

Les mises à niveau fréquentes permettent-elles d'adapter la sécurité à l'évolution de l'activité de l'entreprise ?

Selon l'étude 2021 sur les objectifs en matière de sécurité, mettre en place un programme de sécurité qui s'adapte aux exigences et au développement de l'activité est l'objectif le plus fortement corrélé avec une stratégie de remplacement proactif des technologies. Cette corrélation entre la pratique et l'objectif est d'ailleurs la plus forte de l'étude.



Source : Étude Cisco sur les objectifs en matière de sécurité

Figure 2 : Effet de la fréquence de remplacement des technologies sur la capacité du programme de sécurité à s'adapter à l'évolution de l'activité de l'entreprise[1]

Nous avons interrogé les entreprises sur la fréquence de leurs mises à niveau des systèmes IT et de sécurité, et avons comparé leurs réponses à la capacité annoncée de leur programme de sécurité à s'adapter à l'évolution des besoins de l'entreprise. Y a-t-il une relation entre ces deux variables ? Oui, nous avons constaté une amélioration constante de cet objectif clé à mesure que la cadence des mises à niveau augmentait. **Dans l'ensemble, les entreprises qui mettent à niveau leurs technologies IT et de sécurité chaque trimestre sont environ 30 % plus susceptibles de s'adapter parfaitement à l'évolution des besoins de l'entreprise que celles qui n'effectuent les mises à niveau qu'à plusieurs années d'intervalle.** Cela peut-être une source de motivation pour votre équipe IT.

[1] Dans certaines figures tout au long du rapport apparaît un pourcentage global pour certaines bonnes pratiques et certains objectifs (« Globalement »). Cette valeur représente la valeur moyenne de toutes les réponses obtenues à une série de questions donnée. Vous pouvez vous y référer pour comprendre quelles entreprises font mieux que la moyenne et lesquelles ne sont pas à la hauteur. Certains graphiques reflètent également les incertitudes sous forme de barres d'erreur ou de zones ombrées. Lorsque ces zones chevauchent la ligne « Globalement », cela signifie que nous ne pouvons pas déduire si tel aspect d'un programme de sécurité a un impact sur l'objectif ou la bonne pratique que nous examinons.

Qu'est-ce qui doit motiver le remplacement des technologies ?

Nous avons établi que les mises à niveau fréquentes contribuaient au bon fonctionnement de l'entreprise, mais qu'est-ce qui doit motiver ces mises à niveau ? Nous avons demandé aux participants de sélectionner les principales motivations pour le remplacement des technologies de sécurité dans leur entreprise, et leurs réponses se répartissent en trois grandes catégories :

- **Fournisseur :** le calendrier est déterminé par un fournisseur SaaS ou fait partie d'un plus vaste projet de consolidation du fournisseur (motivation la plus courante)
- **Proactive :** selon un calendrier prédéterminé ou lorsque de nouvelles fonctionnalités ou scénarios justifient une mise à niveau (deuxième motivation la plus courante)
- **Réactive :** en cas d'incident, lorsque la technologie devient obsolète ou pour satisfaire aux exigences de conformité (motivation la moins courante)

Ces motivations sont certes intéressantes, mais nous voulons surtout savoir si elles sont en corrélation avec une approche plus robuste du remplacement des technologies. La réponse se trouve dans la Figure 3. Elle indique que les projets de remplacement des technologies sont plus efficaces lorsque les fournisseurs technologiques les gèrent (ou du moins sont activement impliqués dans leur réalisation). **Moins de la moitié des entreprises ayant une approche réactive font état de fortes capacités de remplacement des technologies, contre près des deux tiers des entreprises qui se synchronisent sur les cycles de remplacement des fournisseurs.**

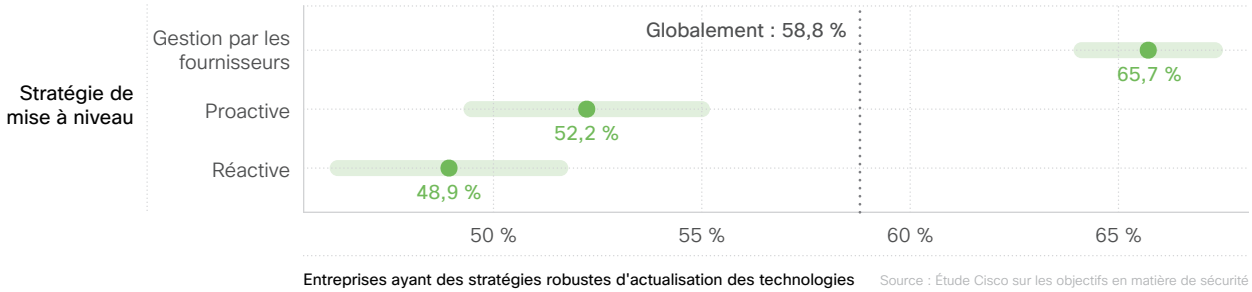


Figure 3 : Effet des principaux motifs de mise à niveau sur les capacités de remplacement des technologies de sécurité

Les informations provenant d'un fournisseur de produits IT et de solutions de sécurité peuvent être suspectées de manquer d'objectivité. Mais nous pouvons vous assurer que nous n'avons en aucun cas influencé cette conclusion. L'enquête a été menée par un cabinet d'études indépendant réputé ; les participants ne savaient pas que Cisco l'avait commandée et les données ont été analysées par le respectable Cyentia Institute, qui a obtenu les résultats présentés dans la Figure 3. Pour faire bonne mesure, nous sommes très prudents dans l'interprétation de ces résultats.

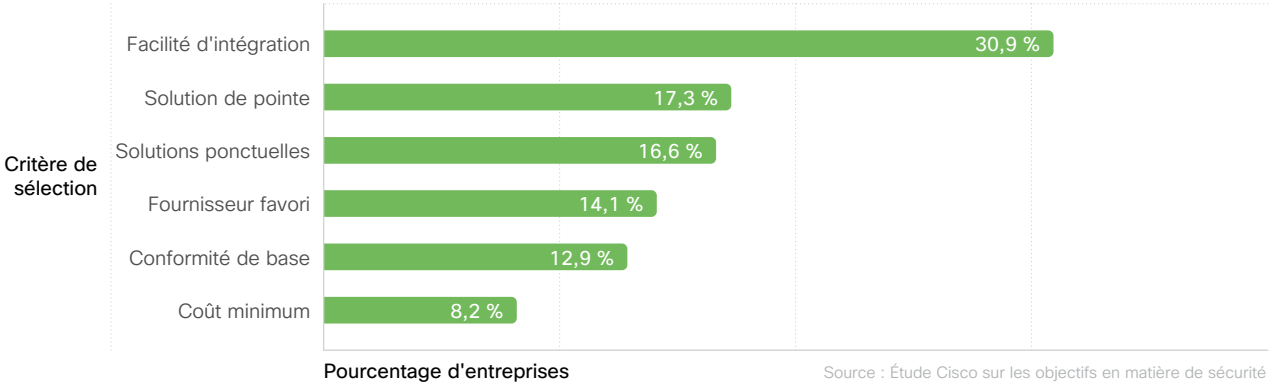
Selon nous, les améliorations attribuées aux approches motivées par les fournisseurs peuvent être liées au fait que les architectures cloud/SaaS sont plus favorables aux mises à niveau fréquentes. Nous remarquons également qu'il est moins question de l'efficacité des fournisseurs que d'obstacles internes et de problèmes politiques à éviter pour ne pas entraver le calendrier de remplacement des technologies.

Comme le chantent Rob Base et DJ EZ Rock, tout devient possible lorsqu'on est deux. Et cela est également le cas en matière d'architecture de sécurité. Mettez en place votre stratégie de remplacement en tirant parti de l'inertie de vos partenaires technologiques pour atteindre vos objectifs.

65,7 % des entreprises synchronisées sur les cycles d'actualisation des fournisseurs font état de fortes capacités de remplacement des technologies

Fonctionnalités ou compatibilité : qu'est-ce qui motive la mise à niveau ?

La section précédente traitait des scénarios qui incitent les entreprises à mettre à niveau leurs technologies. Nous allons maintenant voir pourquoi elles choisissent une solution plutôt qu'une autre. La Figure 4 présente les critères de sélection des participants à l'enquête. Le critère principal est l'intégration réussie avec les technologies existantes. Viennent ensuite les solutions qui offrent des fonctionnalités de pointe ou qui répondent à des besoins particuliers. Étonnamment, la réduction des coûts n'apparaît qu'en dernier.



Source : Étude Cisco sur les objectifs en matière de sécurité

Figure 4 : Principaux critères de sélection lors du remplacement des produits de sécurité

Mais ces critères ont-ils un impact sur la mise en œuvre d'un programme de sécurité performant ? Pour répondre à cette question, nous avons regroupé les critères de sélection de la Figure 4 en trois catégories :

- **Minimum :** solution à moindre coût ; conformité de base
- **Facilité d'intégration :** intégration avec les technologies existantes ; recours aux fournisseurs favoris
- **Fonctionnalité :** solutions de pointe ; solutions ponctuelles

Nous avons ensuite comparé ces catégories au score agrégé créé pour chaque entreprise en fonction de son niveau de réussite pour les 11 objectifs en matière de sécurité. La valeur absolue du score n'a pas de signification particulière, mais elle fournit un point de comparaison pour les différentes stratégies d'actualisation des technologies. **Comme le montre la Figure 5, les entreprises qui donnent la priorité à l'intégration et aux fonctionnalités atteignent davantage les objectifs que celles qui choisissent des produits en se basant sur des critères comme le moindre coût ou le respect des exigences de conformité de base. Mais l'approche axée sur l'intégration est la seule clairement plus performante que la moyenne.**

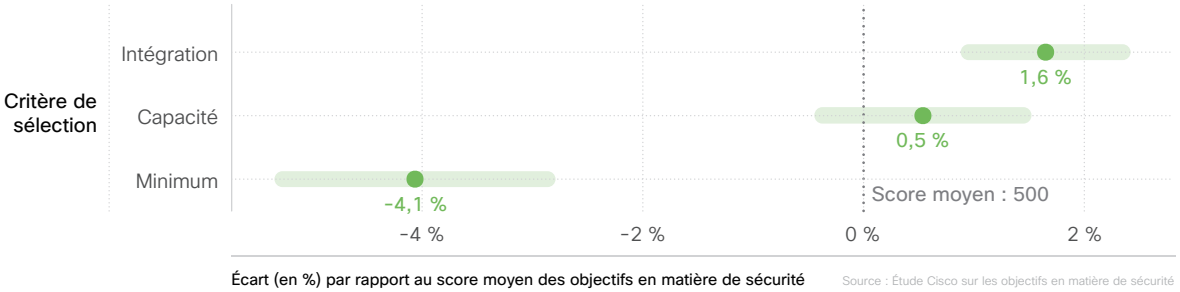


Figure 5 : Effet des critères de sélection des technologies sur le score global des objectifs en matière de sécurité

Notez que les écarts sont relativement faibles en termes de réussite globale du programme. C'est sans doute parce que ces résultats tiennent compte des priorités et des bonnes pratiques globales du programme de sécurité. C'est pourquoi il est également intéressant d'étudier plus en détail les raisons du choix d'un produit plutôt qu'un autre. Si vous avez des difficultés à classer les fonctionnalités lors du remplacement ou de la mise à niveau des solutions de sécurité, c'est qu'il est préférable de privilégier la compatibilité et les fonctionnalités plutôt que la réduction des coûts.

Qu'est-ce que le score des objectifs en matière de sécurité ?

Nous avons demandé aux participants quel était le niveau de réussite de leur entreprise par rapport à 12 objectifs du programme de sécurité. La première édition de notre étude sur les objectifs des entreprises en matière de sécurité analysait ces données en détail. Nous allons également examiner certaines d'entre elles individuellement dans cette nouvelle édition. Mais nous avons aussi créé un score agrégé qui indique le niveau de réussite de chaque entreprise par rapport aux 12 objectifs, afin de mesurer la performance globale du programme de sécurité. Nous l'appelons « score des objectifs en matière de sécurité » et nous y faisons référence à plusieurs reprises dans ce rapport.

Pour obtenir le score, nous avons utilisé une technique statistique appelée « théorie de la réponse aux items ». Cette technique nous permet de noter les entreprises en fonction de leurs résultats aux différents objectifs, tout en tenant compte du fait que certains objectifs sont plus difficiles à atteindre que d'autres. Cette technique éprouvée permet de créer des scores de test standardisés. La valeur absolue du score n'a pas de signification particulière, mais elle fournit un point de comparaison entre les programmes.

« Les RSSI doivent être à la fois des influenceurs et des formateurs. Pour être aussi efficaces que possible, nous devons être à l'avant-garde des décisions stratégiques prises dans nos entreprises. Mais pour convaincre les utilisateurs de l'importance de la sécurité, de la nécessité de réaliser de bons investissements pour la mettre en place et de notre nécessaire implication à tous les niveaux de l'entreprise, nous devons également les former. La plupart des dirigeants ne maîtrisent pas la sécurité. Nous devons donc les informer à chaque étape du processus sur tous les types de risque induits par chaque prise de décision. »

Helen Patton, consultante RSSI, Cisco @CisoHelen

Découvrez le point de vue d'Helen sur l'évolution du rôle du RSSI dans cet épisode de notre podcast de témoignages sur les solutions de sécurité

Bonne intégration des technologies de sécurité

Selon notre dernière édition de l'étude, les technologies de sécurité bien intégrées qui fonctionnent efficacement avec une infrastructure IT plus vaste contribuent à la réussite de tous les objectifs du programme. Nous avons posé une série de questions afin de mieux cerner les facteurs expliquant cela, en commençant par les intentions ayant motivé l'intégration des technologies de sécurité.

Selon les personnes interrogées, le motif le plus courant d'intégration des technologies de sécurité est l'amélioration de l'efficacité de la supervision et des audits. Nous comprenons cela très bien. Il est en effet difficile d'avoir à contrôler un grand nombre de consoles ou de tableaux de bord pour comprendre ce qui se passe sur le réseau. L'intégration de technologies de sécurité est également motivée par la simplification de la collaboration et de l'automatisation (plus d'informations suivront à ce sujet). Nous avons comparé ces motivations aux niveaux d'intégration des technologies et aux objectifs du programme, mais la corrélation n'était pas très étroite. Peut-être que le « quoi » ou le « comment » comptent plus que le « pourquoi » lors de l'intégration des technologies de sécurité ? Creusons un peu plus ces questions.

Selon les personnes interrogées, le motif le plus courant d'intégration des technologies de sécurité est l'amélioration de l'efficacité de la supervision et des audits.

Vaut-il mieux acheter ou concevoir pour réussir l'intégration des technologies ?

L'étude précédente nous a appris que l'intégration des technologies de sécurité permettait d'atteindre les objectifs. Mais quel est le meilleur moyen de mettre en place une pile technologique hautement intégrée ? L'acheter toute prête ? La concevoir pour s'adapter ? Ou simplement laisser les choses se faire naturellement ? Voyons si nous pouvons le déterminer.

Nous avons demandé aux entreprises quelle était leur approche classique de l'intégration des technologies de sécurité. Leurs réponses sont présentées dans la Figure 6. **Globalement, plus des trois quarts d'entre elles préfèrent acheter des solutions intégrées que les concevoir.** Parmi ces entreprises, plus de 40 % choisissent des technologies proposant des intégrations clés en main dans l'infrastructure existante. Et plus de 37 % vont plus loin et préfèrent s'approvisionner en solutions auprès d'un fournisseur unique afin de les intégrer de façon native ou dans une plateforme plus vaste. Un peu plus de 20 % des entreprises souhaitent concevoir elles-mêmes les intégrations, à condition que le produit soit adapté à leurs besoins. Rares sont celles qui adoptent une approche de laisser-faire.

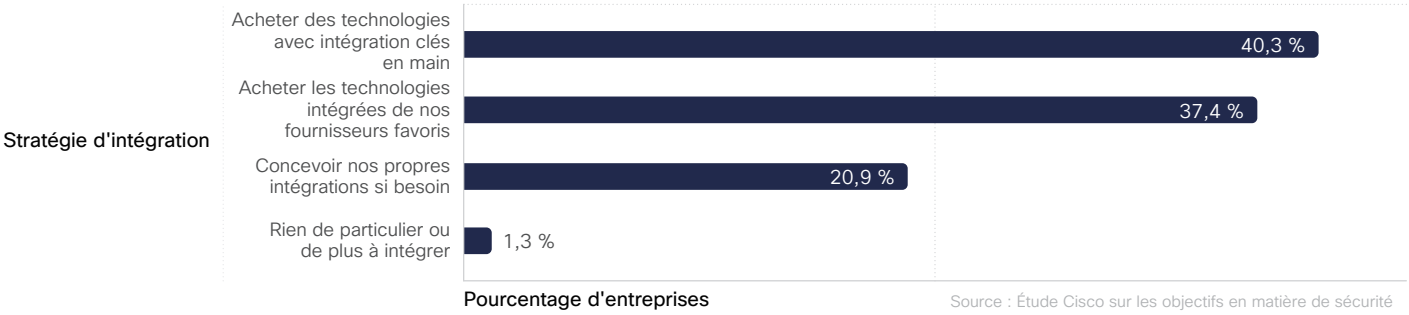


Figure 6 : Les approches courantes des entreprises en matière d'intégration des technologies de sécurité

Globalement, plus de **3/4** des entreprises préfèrent acheter des solutions intégrées plutôt que les concevoir

La Figure 7 évalue si l'une ou l'autre de ces approches de l'intégration fait la différence. Une fois encore, les bénéfices de la collaboration avec les fournisseurs pour assurer l'actualisation et l'intégration des technologies sont mis en avant. **Comme le montre le graphique, le choix d'un fournisseur privilégié est deux fois plus susceptible de favoriser la bonne intégration des technologies de sécurité qu'une approche non interventionniste (~ 69 % contre ~ 31 %).** En outre, selon notre étude, cette constatation reste la même quelle que soit la taille de l'entreprise, bien que les bénéfices de l'utilisation d'un fournisseur favori soient légèrement supérieurs pour les PME que pour les grandes entreprises.

Bien sûr, vous pouvez une nouvelle fois vous dire que cette conclusion tombe bien pour une entreprise proposant une gamme complète et intégrée de solutions de sécurité. Nous sommes effectivement ravis que ce résultat confirme la stratégie de Cisco… mais rappelons qu'il s'agit d'une étude en double aveugle et que nous n'avons eu aucune influence sur son résultat.

Le sort des entreprises qui n'ont rien fait de plus pour intégrer les technologies de sécurité n'est pas surprenant. **Mais la surprise vient du fait qu'il n'y a pratiquement aucune différence entre les entreprises qui achètent des produits proposant une intégration clés en main et celles qui conçoivent elles-mêmes leurs intégrations.** Un peu moins de la moitié (~ 49 %) des entreprises utilisant chacune de ces approches font état de niveaux d'intégration élevés.

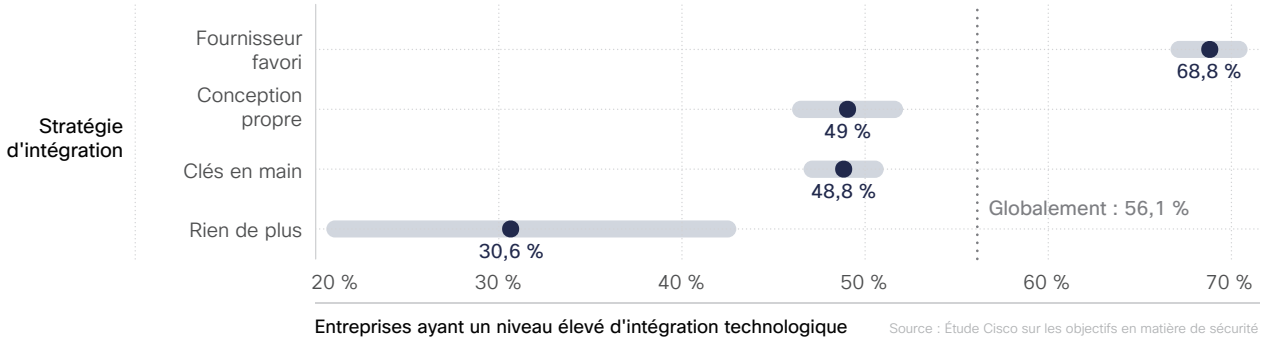


Figure 7 : Effet des approches d'intégration courantes sur le niveau d'intégration des technologies de sécurité

Le cloud pour faciliter l'intégration

Beaucoup d'entreprises ont du mal à décider si elles doivent lancer (ou étendre) des projets d'intégration des technologies de sécurité dans le cloud ou on-premise. Si tel est votre cas, nous disposons de données pour vous aider dans votre choix. La bonne nouvelle, c'est que de nombreux participants à l'enquête font état de bons résultats à la fois dans les environnements on-premise et cloud. Il apparaît cependant beaucoup plus facile de réaliser une intégration technologique poussée dans le cloud.

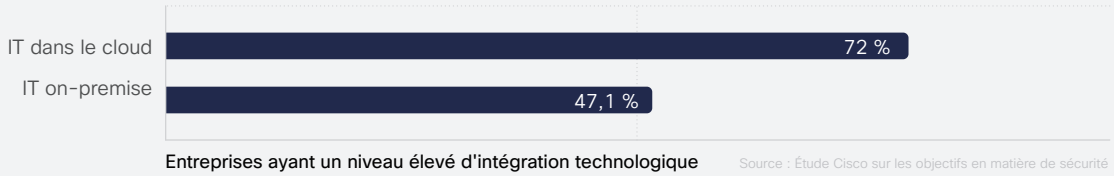


Figure 8 : Effet des environnements cloud et on-premise sur le niveau d'intégration des technologies de sécurité

L'intégration facilite-t-elle l'automatisation ?

Comme indiqué au début de cette section, l'automatisation n'est pas la motivation la plus courante de l'intégration des technologies. Mais 44 % des entreprises la voient comme un facteur positif. Motivations mises à part, existe-t-il des preuves que l'intégration réussie des technologies améliore effectivement l'automatisation des processus de sécurité ? La Figure 9 montre que c'est effectivement le cas.

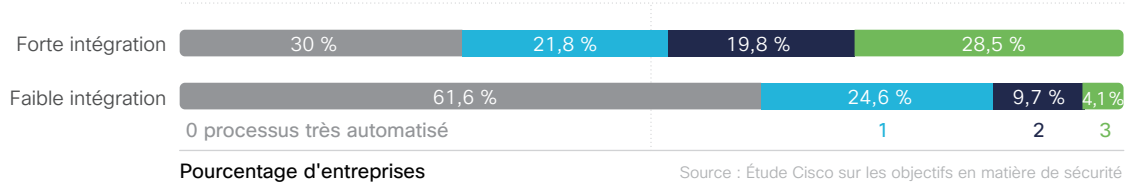


Figure 9 : Effet de l'intégration des technologies sur l'ampleur de l'automatisation des processus de sécurité

Dans la Figure 9, les deux barres horizontales distinguent les entreprises en fonction de leur niveau d'intégration des technologies de sécurité (importante ou faible). Les segments de couleur représentent le nombre de processus de sécurité majeurs (surveillance des événements, analyse des incidents et riposte) pris en charge dans le cadre d'un dispositif d'automatisation mature. La proportion d'entreprises sans automatisation est deux fois plus élevée que celle dont les capacités d'intégration sont faibles. **À l'inverse, les entreprises disposant de technologies de sécurité bien intégrées sont près de sept fois plus susceptibles d'atteindre des niveaux élevés d'automatisation de l'ensemble des trois processus (4,1 % contre 28,5 %).** C'est effectivement une motivation convaincante !

Quelles fonctions doivent être intégrées ?

Ensuite, nous avons demandé aux participants quel était leur niveau d'intégration des technologies prenant en charge les cinq fonctions principales du cadre relatif à la cybersécurité (CSF) du NIST. Ils ont répondu en désignant les technologies sur une échelle allant de très fragmentées (technologies en silos qui fonctionnent principalement de manière isolée) à hautement intégrées (technologies coordonnées qui fonctionnent comme une unité fonctionnelle). Ensuite, nous avons créé un modèle pour déterminer leur effet sur le score des objectifs en matière de sécurité de chaque entreprise.

Les résultats indiqués dans la Figure 10 sont relativement homogènes pour les cinq fonctions. **La défragmentation et l'intégration de toutes les fonctions du CSF NIST se traduisent par une augmentation de la réussite des programmes de sécurité (+ 11 à ~ 15 %).** Ainsi, la réponse à notre question est que toutes les fonctions doivent être intégrées. Mais si vous vous demandez par où commencer, sachez que la haute intégration de la fonction « Identifier » génère le meilleur résultat.

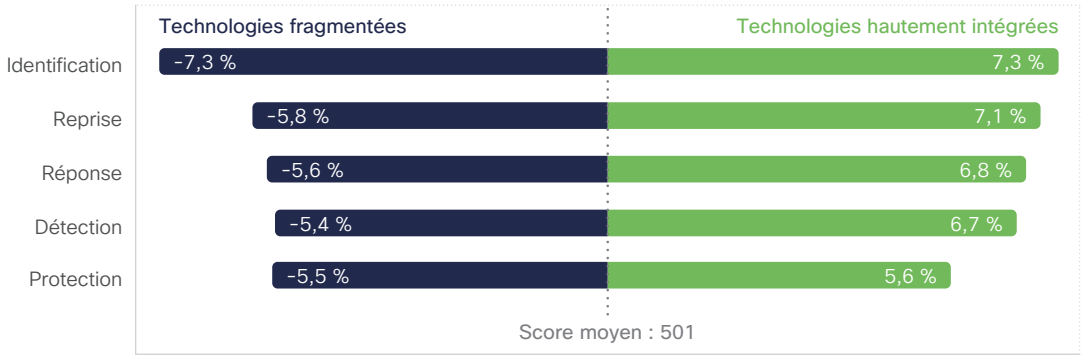


Figure 10 : Effet de l'intégration des fonctions du CSF NIST sur le score global des objectifs en matière de sécurité

Difficile de ne pas faire le lien entre ce fait et ce que nous avons appris dans la section précédente, à savoir que la supervision, l'audit et la collaboration sont les principales motivations de l'intégration des technologies. D'où l'importance fondamentale d'une bonne visibilité sur l'ensemble de l'environnement de l'entreprise. Il est tout à fait logique qu'une approche fragmentée visant à « développer une connaissance organisationnelle pour gérer les risques liés à la cybersécurité au niveau des systèmes, des personnes, des ressources, des données et des fonctionnalités » (comme indiqué dans le CSF) ne donne pas les résultats attendus. Nous aborderons ce thème plus en détail dans la section « Détection des menaces et réponse aux incidents ».

À propos de l'intégration, de l'identification et des informations

Outre le graphique que nous venons de présenter, les données de cette étude révèlent une relation cruciale entre l'intégration, l'identification et les informations. Lorsque vous n'êtes pas informé de la présence d'une ressource ou d'une menace qui n'a pas été identifiée, vous ne vous doutez pas qu'il est nécessaire de mettre en place une défense adaptée avant qu'il soit trop tard.

La Figure 11 illustre bien ce concept. Nous avons comparé le niveau d'intégration de la fonction « Identifier » du CSF NIST déclaré par chaque entreprise avec sa capacité à détecter les menaces rapidement et avec précision. **Les entreprises qui disposent de systèmes hautement intégrés pour identifier les ressources et les risques critiques disposent de fonctionnalités de détection des menaces bien plus robustes (+ 41 %).** Lutter contre la fragmentation et contre les menaces se fait donc de manière symétrique.

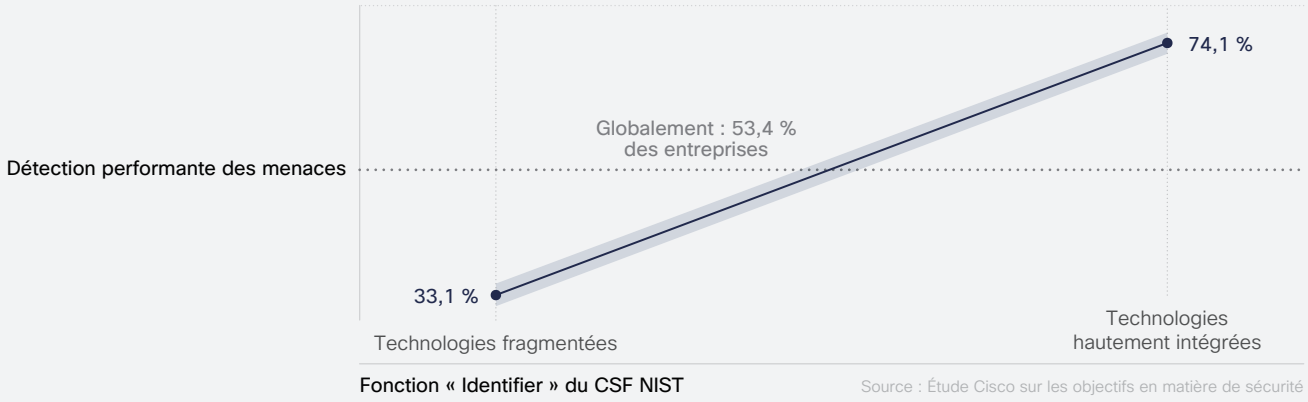


Figure 11 : Effet de l'intégration de la fonction Identifier du CSF NIST sur les fonctionnalités de détection des menaces

Les entreprises qui disposent de systèmes hautement intégrés pour identifier les ressources et les risques critiques disposent

+41 %

de fonctionnalités de détection des menaces bien plus robustes.

« L'automatisation permet à nos ingénieurs de réagir rapidement aux nouvelles menaces. Nous pouvons maintenant nous focaliser sur la mise en œuvre des concepts de sécurité au lieu de mettre à jour les règles et de surveiller le réseau 24 h/24 et 7 j/7. Cisco analyse les données et extrait les informations dont nous avons besoin pour mieux sécuriser et entretenir notre infrastructure. C'est une parfaite combinaison entre l'intelligence humaine et l'intelligence de la machine. »

Steve Erzberger, DSI, Frankfurter Bankgesellschaft (Schweiz) AG

En savoir plus

Développement des capacités de détection des menaces et de réponse aux incidents

Cette section couvre deux bonnes pratiques distinctes en matière de sécurité qui valident les cinq facteurs de réussite. La détection des menaces et la réponse aux incidents font partie des opérations de sécurité qui touchent à la fois les collaborateurs, les processus et les technologies. Ce point commun appelait des questions communes. Pour cette étude, nous avons donc analysé les trois dans la même section.

92 % des entreprises dotées d'effectifs, de processus et de technologies solides disposent de fonctionnalités avancées de détection et de traitement des menaces.

Donner la priorité aux collaborateurs, aux processus ou aux technologies ?

Commençons notre enquête par l'étude des collaborateurs, des processus et des technologies. Les fonctions de sécurité sont souvent décrites comme une combinaison de ces trois éléments, en particulier dans le domaine de la détection des menaces et de la réponse aux incidents. Mais est-ce qu'un élément de ce trio est plus important que les autres ? Vous nous voyez venir. Passons à l'analyse.

En bas de la Figure 12, nous voyons qu'un quart seulement des entreprises dont les programmes connaissent des manques au niveau des collaborateurs, des processus et des technologies ont confiance dans leurs opérations de sécurité. Lorsque l'un de ces trois éléments est plus performant (collaborateurs, processus ou technologies), ce pourcentage augmente de 60 à 64 %. La tendance semble être un peu plus forte lorsque ce sont les collaborateurs, mais le chevauchement des intervalles de confiance ne nous permet pas de l'affirmer complètement. Le point important à retenir, c'est que chacun de ces éléments constitue un bon point de départ pour développer de meilleures fonctionnalités de détection des menaces et de réponse aux incidents.

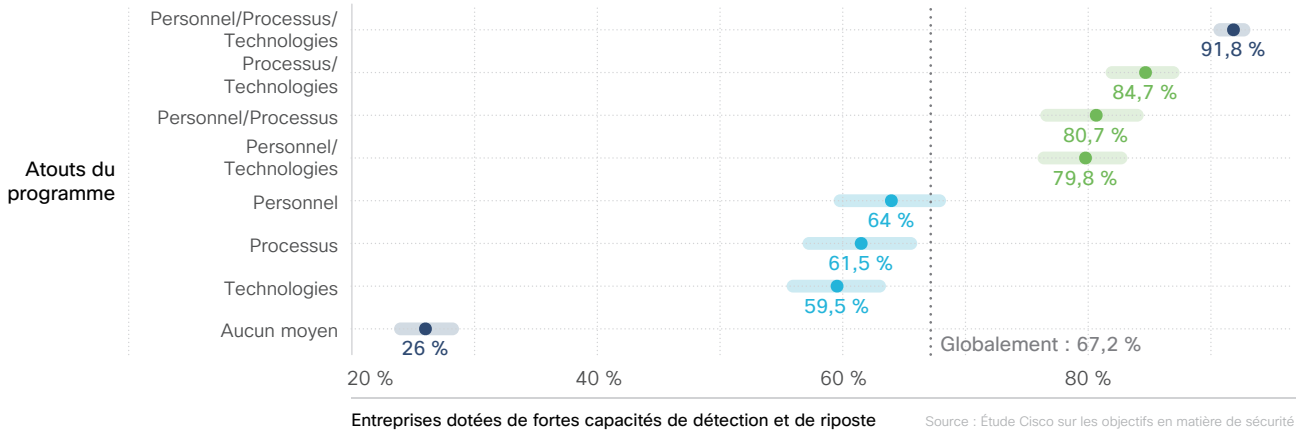


Figure 12 : Effet des collaborateurs, des processus et des technologies sur les fonctionnalités de détection des menaces et de réponse aux incidents

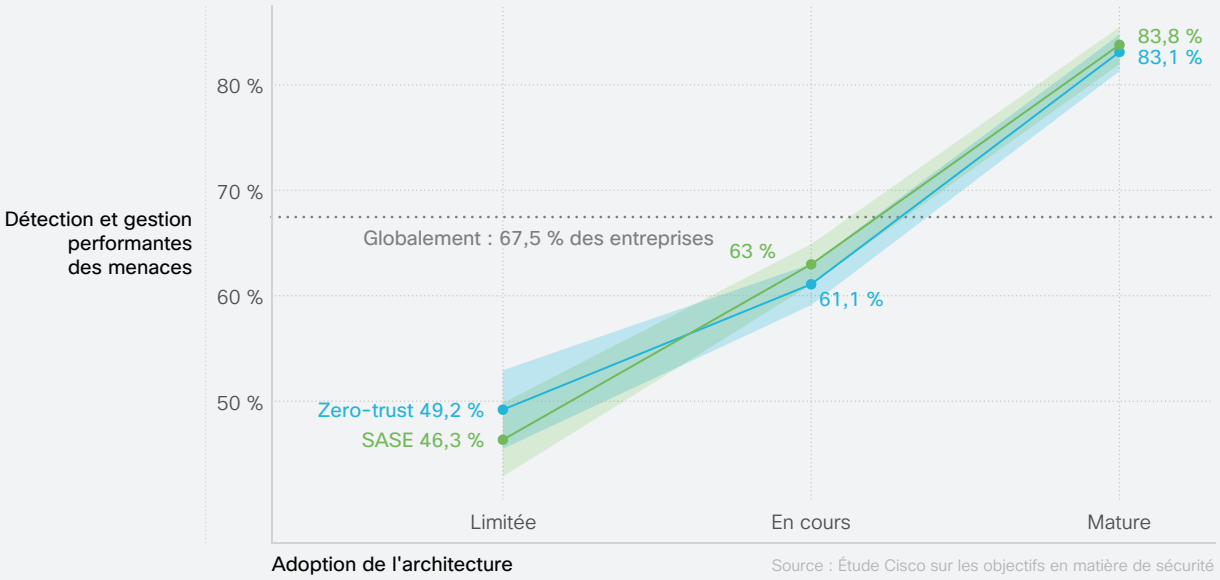
Toujours d'après la Figure 12, le renforcement de deux de ces éléments se traduit par des programmes de sécurité plus performants que la moyenne et améliore les fonctionnalités d'environ 15 à 20 % par rapport aux entreprises qui renforcent un seul de ces éléments. Peu importe lesquels vous choisissez d'associer parmi les collaborateurs, les processus et les technologies. Il suffit d'en avoir deux sur trois. N'est-il pas rassurant de savoir que vous pouvez adapter librement la feuille de route des opérations de sécurité de votre entreprise ?

Venons-en aux programmes d'élite présentés dans la Figure 12, qui réunissent les trois éléments pour leurs opérations de sécurité. **92 % des entreprises dotées d'effectifs, de processus et de technologies solides disposent de fonctionnalités avancées de détection et de traitement des menaces.** Leurs performances sont multipliées par 3,5 par rapport aux programmes de sécurité ne disposant d'aucun des trois éléments ! Conclusion : commencez par l'élément qui vous permet de progresser le plus, puis continuez jusqu'à la mise en place du trio gagnant.

Les entreprises dotées d'effectifs, de processus et de technologies solides multiplient par **3,5 X** leurs performances de détection et de traitement des menaces par rapport aux entreprises qui n'en ont pas

Les architectures zero-trust et SASE permettent-elles d'améliorer les opérations de sécurité ?

Nous comprenons que les critères abstraits tels qu'« avoir des technologies performantes » ne permettent pas de tirer des conclusions concrètes. C'est pourquoi nous avons posé des questions complémentaires sur certaines architectures. Nous avons interrogé les participants sur leur adoption des architectures zero-trust et SASE (sécurité au niveau des points d'accès) afin de mieux cerner l'impact de ces approches sur les capacités de détection des menaces et de réponse aux incidents (et donc sur les objectifs du programme de sécurité).



Source : Étude Cisco sur les objectifs en matière de sécurité

Figure 13 : Effet des architectures zero-trust et SASE sur les capacités de détection des menaces et de réponse aux incidents

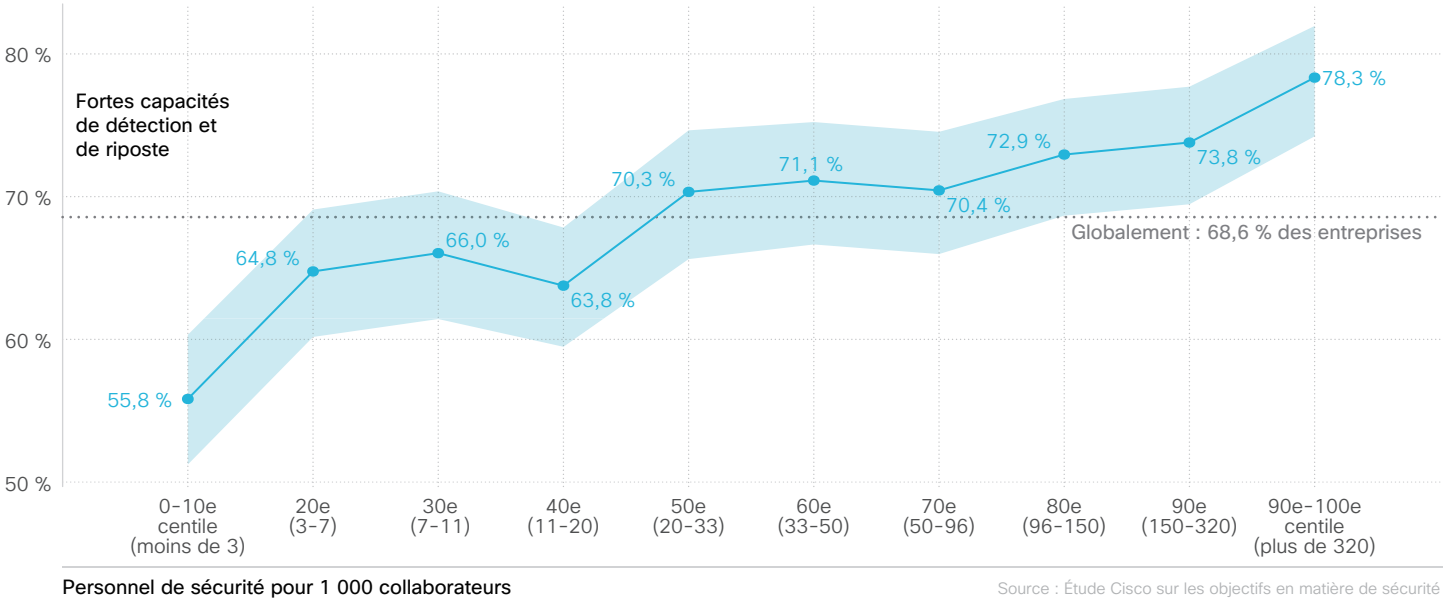
Les entreprises dont les implémentations d'architectures zero-trust ou SASE sont matures sont environ 35 % plus susceptibles de faire état d'opérations de sécurité performantes que celles dont les implémentations sont récentes.

Ces résultats corroborent les preuves partagées plus haut sur les nombreux bénéfices des architectures modernes pour les programmes de cybersécurité.

Plus on est de fous, moins il y a de risques ?

Il est indispensable de s'appuyer sur des collaborateurs compétents pour renforcer la détection des menaces et la réponse aux incidents. Mais faut-il privilégier l'ajout de nouvelles personnes ou la montée en compétences des collaborateurs en place ? Bien sûr, l'un n'exclut pas l'autre, mais la question demeure : est-ce la quantité ou la qualité qui importe le plus pour la formation d'équipes de sécurité performantes ?

Pour répondre à cette question, nous avons d'abord calculé le ratio entre le personnel dédié à la sécurité et le nombre total de collaborateurs dans l'entreprise. Nous avons ensuite comparé ce ratio aux performances de détection des menaces et de réponse aux incidents déclarées par chaque entreprise. La Figure 14 illustre le résultat de ces calculs. Bien qu'elle ne réponde pas entièrement à la question sur la quantité et la qualité, elle fournit quelques éclaircissements.



Source : Étude Cisco sur les objectifs en matière de sécurité

Figure 14 : Effet de la proportion de personnel dédié à la sécurité sur les capacités de détection des menaces et de réponse aux incidents

Le premier est qu'il y a bien une corrélation entre la proportion du personnel dédié à la sécurité et l'amélioration de la détection et du traitement des menaces. Les entreprises aux ratios les plus élevés sont un peu plus de 20 % plus susceptibles de faire état de meilleures performances que celles dont les ratios sont les plus faibles. CEPENDANT, regardez la ligne pointillée de la moyenne globale dans la Figure 14 ; elle traverse la majeure partie de l'intervalle de confiance ombré. Cela signifie que les entreprises qui ne se trouvent pas aux extrémités de l'échelle de dotation en personnel (soit la majorité des entreprises) sont tout aussi susceptibles de faire état de programmes de sécurité performants.

Comment analyser concrètement ce résultat ? Nous pouvons affirmer avec certitude que les entreprises dotées de larges équipes dédiées à la sécurité sont beaucoup plus susceptibles de disposer de fonctionnalités de détection et de traitement des menaces performantes que celles dotées d'équipes restreintes. Cela étant dit, les effectifs ne font pas disparaître à eux seuls les problèmes de sécurité et ne sont pas non plus une garantie de réussite. Par ailleurs, les écarts de ratio de personnel dédié à la sécurité n'influent pas autant sur les performances que la compétence des collaborateurs analysée à la section précédente. **Il apparaît donc que la qualité compte autant, voire plus, que la quantité pour constituer des équipes performantes de détection et de traitement des menaces.**

Les équipes de sécurité restent confrontées à une importante pénurie de personnel.

Le manque de ressources et l'augmentation des menaces entraînent un stress intense et la multiplication des burnouts chez les professionnels de la cybersécurité. Quelles mesures peuvent être prises de manière proactive afin d'assurer leur bien-être ? Dans cet e-book, nous avons demandé aux leaders du secteur et à des médecins de partager leur avis et leurs témoignages sur la gestion de la santé mentale.

Une équipe de sécurité interne, externe ou les deux ?

La réussite des opérations de sécurité ne dépend donc pas seulement des effectifs. Toutefois, les modèles de dotation en personnel ont-ils un impact sur les résultats ? Est-il préférable d'externaliser, de gérer en interne ou de partager les responsabilités en matière de détection et de traitement des menaces ? Voyons ce que révèlent les données. Cependant, sachez qu'elles sont quelque peu contradictoires sur ce point.

Nous avons interrogé les participants sur leurs modèles de dotation en personnel, puis comparé leurs réponses à l'évaluation de leurs fonctionnalités de détection des menaces et de réponse aux incidents. **Comme le montre la Figure 15, les entreprises dont les équipes sont principalement internes ou externes sont beaucoup plus susceptibles (+ 20 à 30 %, respectivement) de faire état de programmes de sécurité performants que celles ayant adopté un modèle de dotation mixte.** Étant donné que la plupart des entreprises déclarent utiliser un modèle mixte, nous avons pensé qu'il serait intéressant d'envisager cette question sous un autre angle avant de se fier aux résultats de l'enquête qui semblent être en défaveur de ce modèle.

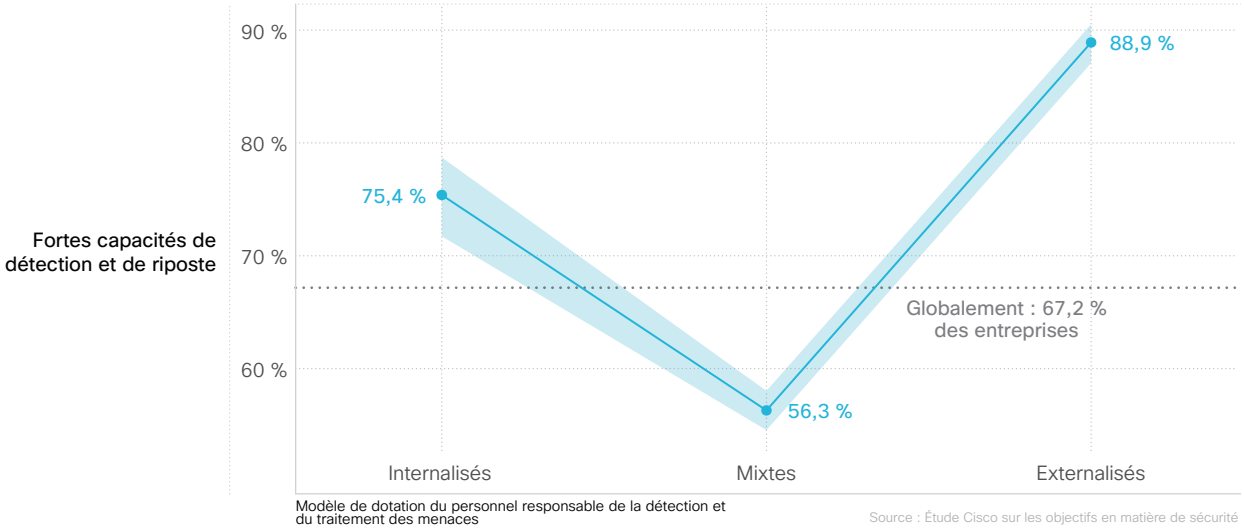


Figure 15 : Effet des modèles de dotation en personnel sur la perception des capacités de détection des menaces et de réponse aux incidents

Les entreprises dont les équipes sont principalement internes ou externes sont

20 à 30 %

plus susceptibles de faire état de programmes de sécurité performants que celles ayant adopté un modèle de dotation mixte

Nous ne nous sommes pas contentés de demander aux participants d'évaluer la performance perçue des fonctionnalités de détection des menaces et de réponse aux incidents. Nous avons aussi essayé d'obtenir d'autres mesures plus objectives à des fins de comparaison. L'une d'elles est le délai moyen de réponse ou le délai moyen de résolution ou de confinement d'un incident lié à la sécurité. L'analyse contextuelle extérieure à ce rapport montre que ces mesures concordent souvent avec les évaluations subjectives. En revanche, d'après la Figure 16, ces deux approches sont en contradiction.

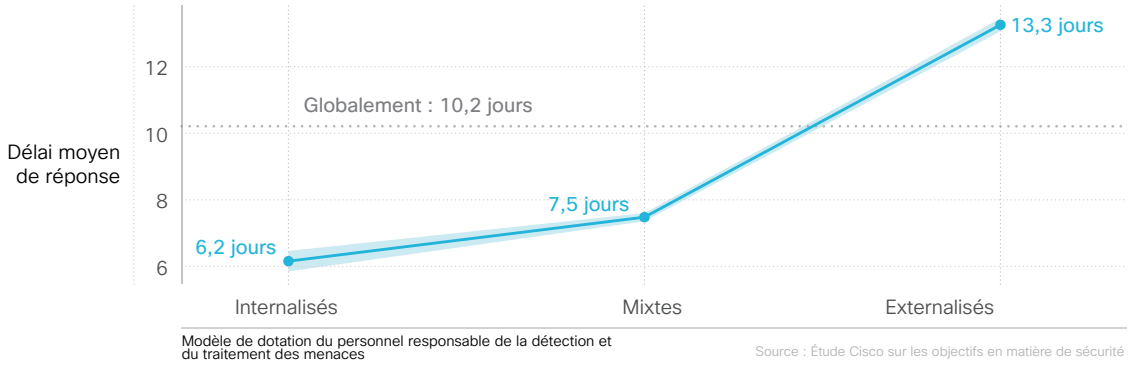


Figure 16 : Effet des modèles de dotation en personnel sur le délai moyen de réponse aux incidents liés à la sécurité[2]

D'après la Figure 16, les entreprises ayant mis en place des équipes internes de détection et de traitement des menaces divisent par plus de deux leur délai moyen de réponse par rapport aux entreprises utilisant des modèles externalisés (environ 6 jours au lieu de 13 jours). Les entreprises utilisant des modèles de dotation hybrides affichent un résultat intermédiaire (environ 8 jours). Leurs délais de réponse ne sont pas aussi rapides qu'avec des équipes internes, mais bien plus qu'avec des équipes externes.

Nous sommes donc confrontés à un dilemme. Quel angle (approche ou mesure) est le bon et surtout, lequel adopter pour choisir un modèle ? Nous allons volontairement conserver le doute et répondre « les deux » et « ni l'un ni l'autre », comme le font les données.

Bien sûr, la remédiation repose sur de nombreux éléments et dépend de nombreux facteurs. L'entreprise dépend du fournisseur pour appliquer les correctifs et corriger les vulnérabilités. Ces correctifs sont testés en laboratoire dans un environnement similaire avant d'être déployés en production. Mais beaucoup de variables entrent en jeu.

Il est difficile d'analyser les faits avec certitude. Peut-être que la collecte de données par l'intermédiaire d'une enquête nous induit en erreur. Peut-être que la différence entre le délai moyen de réponse et l'évaluation des fonctionnalités se traduit par un programme de détection des menaces et de réponse aux incidents globalement plus « performant » et des taux de remédiation plus lents. Peut-être que ces programmes sont plus lents, mais plus complets. Peut-être que la coordination avec le personnel externalisé prend plus de temps. Peut-être que le modèle externalisé induit un sentiment de confiance, la tâche étant confiée à des spécialistes. Peut-être que les opérations de sécurité subissent l'effet Dunning-Kruger. Toutes ces raisons, et bien d'autres encore, entrent certainement en ligne de compte. C'est pourquoi cette section doit vous servir à lancer des discussions plutôt qu'à prendre des décisions.

[2] Dans ce graphique, nous utilisons la moyenne géométrique, qui est plus représentative d'une valeur « type ». Le délai moyen de réponse est généralement inférieur à 2 à 3 semaines. Toutefois, pour certains participants il s'élève à plusieurs mois (ou années !). Ainsi, la moyenne géométrique nous permet de mieux représenter les valeurs « types » sans être influencés par leur ampleur.

La Threat Intelligence est-elle utile ?

En parlant d'effet Dunning-Kruger, passons maintenant à la section suivante. Nous avons interrogé les participants sur leur utilisation de la Threat Intelligence dans leur programme de sécurité. 85 % des entreprises l'utilisent, mais seulement 31 % de manière poussée. Ces informations permettent-elles d'améliorer, d'optimiser et d'accélérer la détection et le traitement des menaces ? Examinons la Figure 17.

Curieusement, la plupart des entreprises qui n'utilisent pas de Threat Intelligence pensent être assez performantes. Il semblerait que l'absence d'informations rassure. Pourtant, les résultats des entreprises qui utilisent un peu la Threat Intelligence disent l'inverse : le niveau de confiance passe de 84 à 46 %. **Les entreprises qui utilisent beaucoup la Threat intelligence ont presque deux fois plus de chances de proposer des fonctionnalités de détection et de gestion performantes que celles qui y ont moins recours. Et lorsque l'évaluation des fonctionnalités et les mesures concordent, les entreprises qui tirent le plus parti de la Threat Intelligence ont des délais moyens de réponse près de deux fois inférieurs à celles qui ne l'utilisent pas.**

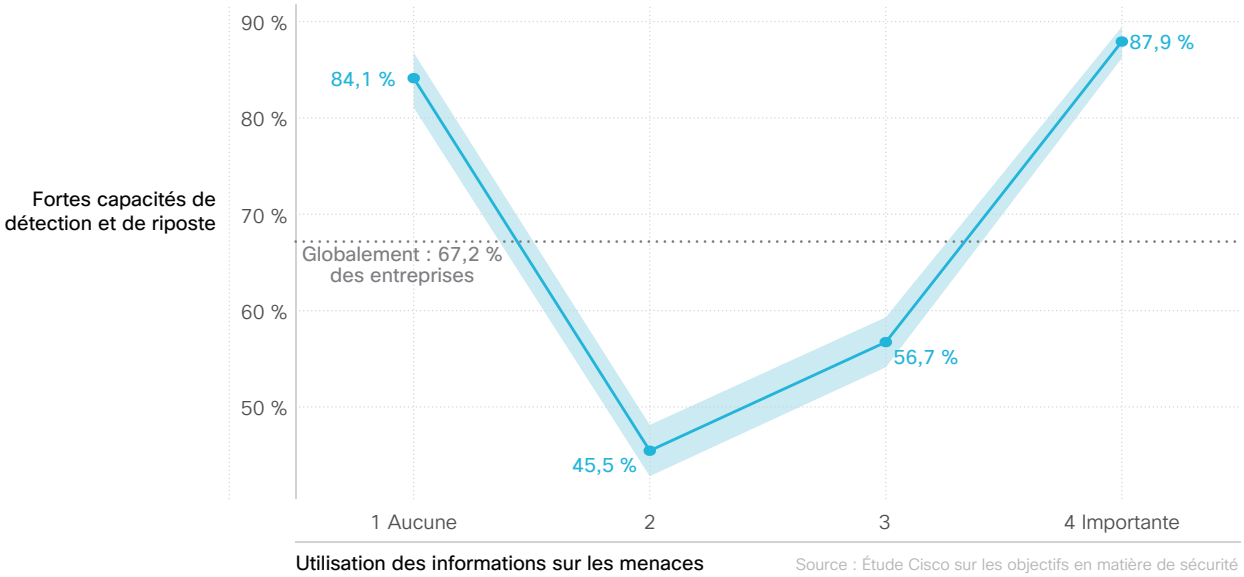


Figure 17 : Effet de l'utilisation de la cyberintelligence sur les fonctionnalités de détection des menaces et de réponse aux incidents

Le psychologue et auteur à succès Daniel Kahneman a déclaré : « Nous sommes aveugles à notre propre cécité. Nous ignorons le peu que nous savons. ». La Figure 17 montre qu'une fois que les entreprises ont des informations sur les menaces dont elles sont la cible, elles réalisent qu'elles n'en savent que très peu. L'utilisation renforcée de la Threat Intelligence restaure leur confiance. Mais ce n'est pas pour autant une confiance aveugle.

Les entreprises qui s'appuient largement sur la Threat Intelligence sont près de **2 X** plus susceptibles de faire état de fortes capacités de détection et de traitement

L'automatisation peut-elle remplacer les collaborateurs ?

Cette question peut sembler rhétorique. Mais ce n'est pas le cas. Au risque de nous attirer la fureur des professionnels de la sécurité, il est vrai que certaines données suggèrent que l'automatisation peut remplacer les collaborateurs. MAIS continuez votre lecture avant de jeter ce rapport à la poubelle.

La Figure 18 intègre certains éléments qui ont déjà été traités dans différents graphiques : personnel de sécurité et automatisation. Les deux lignes comparent deux types de programmes de sécurité. La première (ligne bleu marine) représente les entreprises qui NE disposent PAS d'une équipe interne performante, tandis que les autres sont représentées par la ligne bleue claire. Dans les deux cas, vous pouvez voir de gauche à droite l'effet de l'augmentation des niveaux d'automatisation des capacités de détection des menaces et de réponse aux incidents.

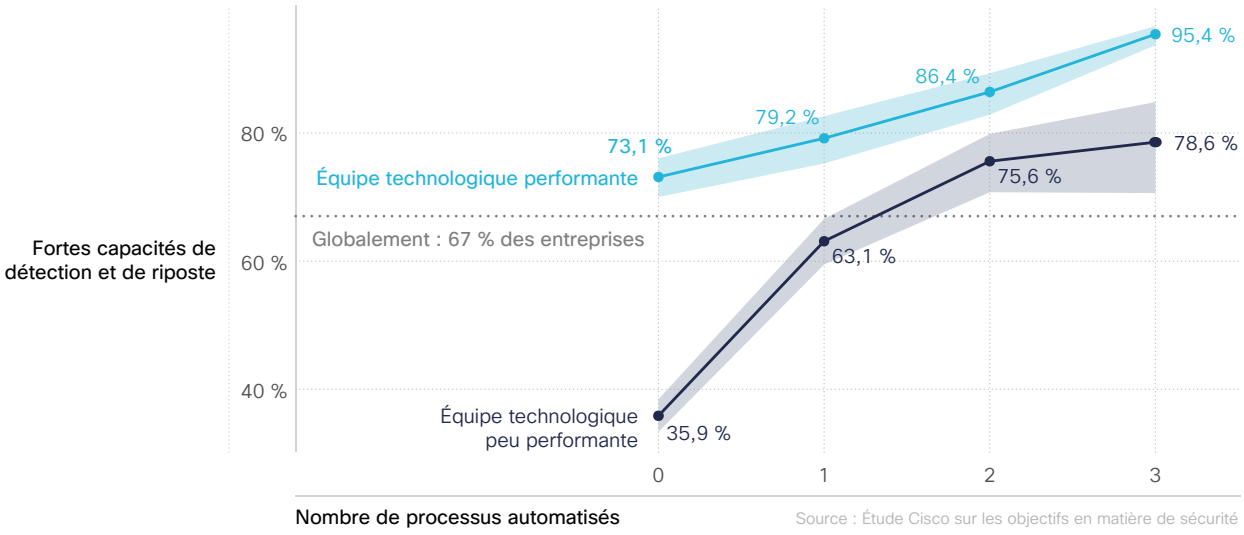


Figure 18 : Effet des effectifs et de l'automatisation sur les fonctionnalités de détection des menaces et de réponse aux incidents

Commençons par les entreprises qui n'ont pas d'équipe solide. Seul un tiers des entreprises qui ne disposent pas d'équipe de sécurité robuste et qui n'automatisent pas les principaux processus font état de fonctionnalités de détection et de gestion performantes. Ce chiffre augmente largement lorsque l'un des trois processus sur lesquels nous avons enquêté (surveillance des menaces, analyse des événements, réponse aux incidents) est automatisé. L'automatisation de deux d'entre eux entraîne une nouvelle augmentation, et l'automatisation des trois multiplie par plus de 2 les performances des équipes les moins expérimentées. **Plus des trois quarts des programmes de sécurité qui ne disposent pas de collaborateurs suffisamment performants offrent des fonctionnalités robustes grâce à des niveaux élevés d'automatisation.**

Si l'on suit l'écart entre le point le plus à droite sur la ligne bleu marine et le premier point sur la ligne bleue claire, il apparaît **qu'un programme de sécurité qui s'appuie sur des collaborateurs moins performants et sur un taux d'automatisation avancé obtient des résultats proches d'un programme s'appuyant sur des collaborateurs performants et peu d'automatisation.** En d'autres termes, une automatisation performante peut remplacer des collaborateurs performants. Nous avions donc raison.

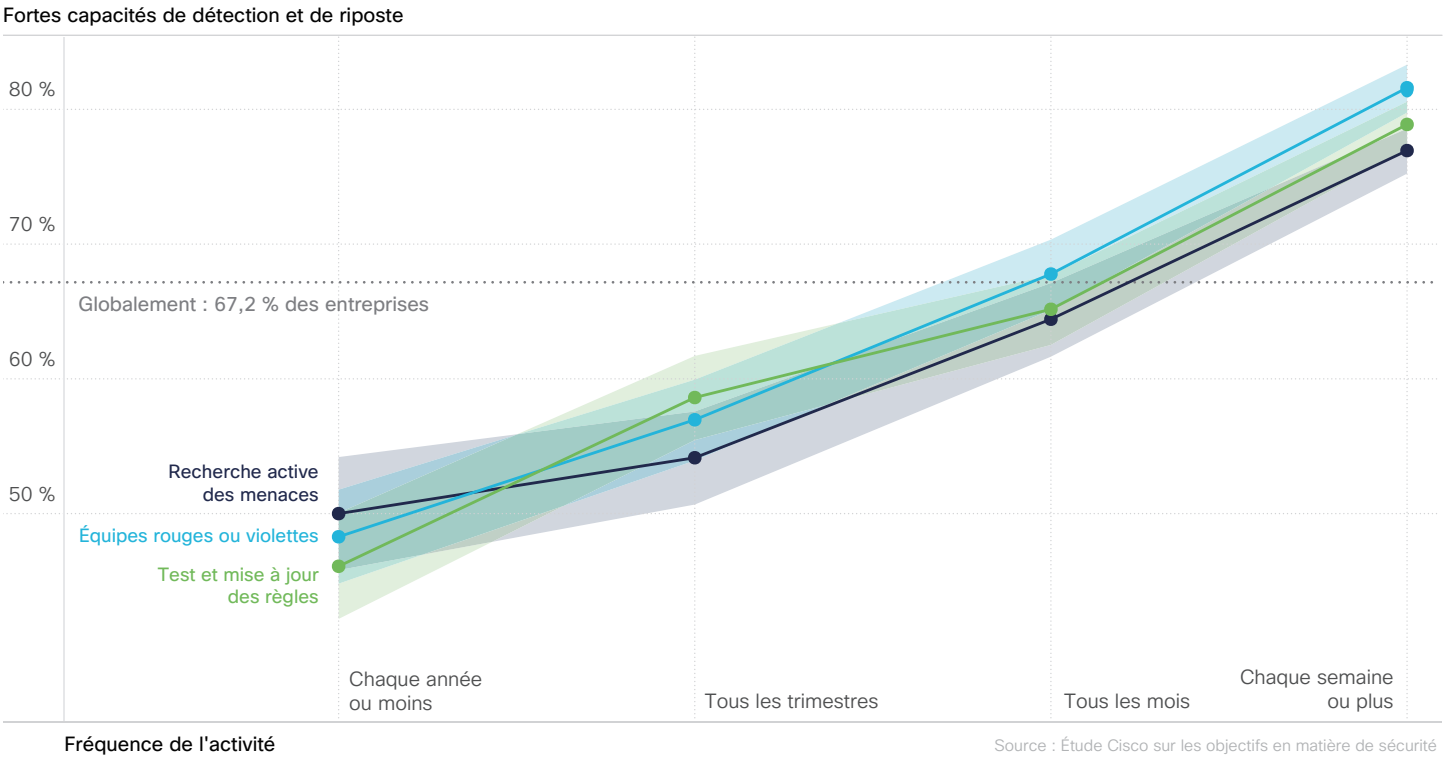
Mais ce n'est pas l'information à retenir de la Figure 18. L'évolution de la ligne bleue montre bien que les deux éléments sont importants : une équipe et une automatisation performantes. Les programmes de sécurité qui conjuguent une équipe performante ET une automatisation des principaux processus de détection et de traitement des menaces ont un taux de réussite de plus de 95 %. Ainsi, l'automatisation ne doit pas remplacer vos collaborateurs qualifiés. Elle leur permet de se concentrer sur des activités à plus grande valeur ajoutée et prioritaires.

À quelle fréquence effectuer les activités liées à la sécurité ?

De nombreuses activités menées de manière régulière permettent d'améliorer les programmes de détection et de traitement des menaces. Lors d'un sondage informel sur le sujet, trois d'entre elles sont ressorties :

- Tester et mettre à jour les règles de détection et les scénarios d'utilisation
- Rechercher des signes d'activité malveillante de façon proactive
- Organiser des exercices pour les équipes rouges et/ou violettes

Nous avons demandé aux participants à quelle fréquence leur entreprise mène chacune de ces activités, puis nous avons comparé leurs réponses à la performance déclarée de leurs fonctionnalités de détection et de traitement des menaces. La tendance qui en ressort apparaît clairement dans la Figure 19.



Source : Étude Cisco sur les objectifs en matière de sécurité

Figure 19 : Effet de la fréquence des activités sur les fonctionnalités de détection des menaces et de réponse aux incidents

La mise à jour des règles, la constitution d'équipes rouges/violettes et la recherche des menaces suivent la même trajectoire. Plus elles sont effectuées fréquemment, plus elles profitent aux programmes de sécurité. **Les entreprises qui les réalisent au moins une fois par semaine constatent une augmentation de leurs performances d'environ 30 % par rapport à celles qui les réalisent au maximum une fois par an.** Alors, à quelle fréquence votre entreprise doit-elle les effectuer ? Le plus souvent possible.

Les entreprises qui réalisent ces activités au moins une fois par semaine enregistrent près de **30 %** d'augmentation des performances

« La sécurité évolue constamment et nous devons suivre ces tendances. [Avant], nous perdions beaucoup de temps à résoudre les problèmes de sécurité et à répondre aux incidents. Maintenant que nous avons simplifié nos processus et accéléré les enquêtes, nous pouvons adopter les nouvelles tendances en matière de sécurité et intégrer des solutions innovantes qui renforcent la sécurité de l'infrastructure de notre réseau de formation. »

Bahruz Ibrahimov, ingénieur en sécurité de l'information, AzEduNet

En savoir plus

Garantie d'une reprise après sinistre et d'une résilience rapides

Il est intéressant de noter à quel point la nature « prioritaire » de différents aspects de la cybersécurité évolue au fil du temps. Après avoir été reléguées pendant quelques années à l'arrière-plan des violations de données et du cyberespionnage, la continuité de l'activité et la reprise après sinistre refont leur apparition sur le devant de la scène. Et ce n'est pas sans raison. La multiplication des ransomwares, les pannes des principaux fournisseurs d'hébergement, etc., ont forcé les entreprises à changer leur stratégie pour assurer leur résilience face aux menaces continues.

Selon l'étude 2021 sur les objectifs en matière de sécurité, la rapidité de la reprise après sinistre est le quatrième contributeur à la mise en place de programmes de sécurité efficaces. Elle montre des corrélations significatives avec les 11 objectifs, sauf un, la culture de la sécurité. Dans cet esprit, examinons les stratégies visant à optimiser l'efficacité de cette bonne pratique et à assurer la résilience.

La multiplication des ransomwares, les pannes des principaux fournisseurs d'hébergement, etc., ont forcé les entreprises à changer leur stratégie pour assurer leur résilience face aux menaces continues.

La reprise après sinistre doit-elle être supervisée par le conseil d'administration ?

Nous étions curieux de savoir qui avait la responsabilité finale de la supervision des fonctionnalités de reprise après sinistre. Il se trouve que la responsabilité est répartie de manière assez homogène entre le DSI, le RSSI et les autres membres dirigeants non spécialistes de l'IT, puisqu'un quart des processus de continuité de l'activité et de reprise après sinistre des entreprises sont chapeautés par chacun d'eux. La visibilité du conseil d'administration est un peu moins fréquente, mais elle reste présente dans 18 % des entreprises interrogées.

Lorsque nous avons comparé ces réponses à l'évaluation des fonctionnalités de continuité de l'activité et de reprise après sinistre de chaque participant à l'enquête, il est apparu que la question de la supervision présentait un réel intérêt. **Comme indiqué dans la Figure 20, les entreprises qui supervisent la continuité de l'activité et la reprise après sinistre au niveau du CA sont les plus susceptibles (11 % au-dessus de la moyenne) de déployer des programmes performants.** Les fonctions de continuité de l'activité et de reprise après sinistre chapeautées par le DSI affichent les taux les plus bas, bien inférieurs à la moyenne.

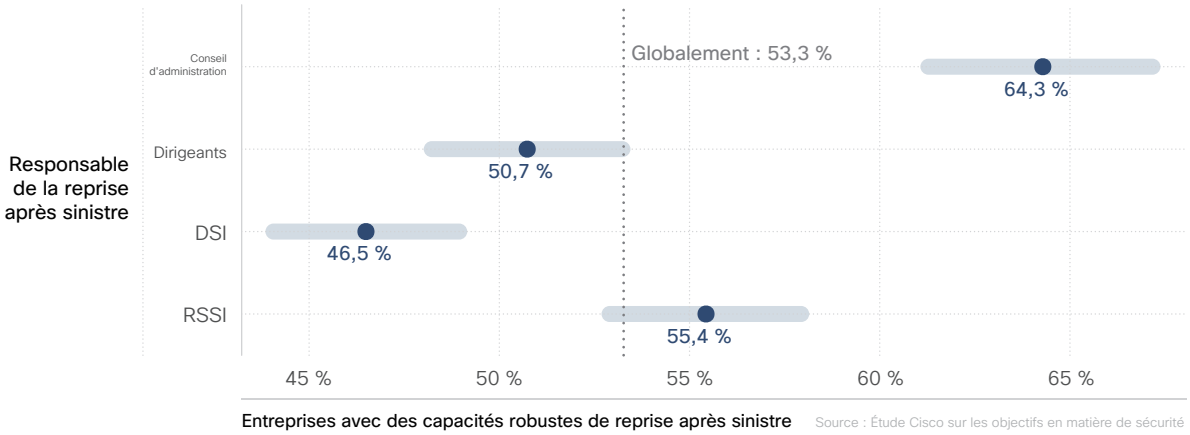


Figure 20 : Effet de la supervision organisationnelle des dirigeants sur les fonctionnalités de reprise après sinistre

Les résultats de la Figure 20 s'expliquent de plusieurs manières. Nous soupçonnons que les entreprises qui rendent des comptes aux CA concernant la reprise après sinistre sont plus préoccupées que les autres par les risques opérationnels et la résilience. Ces préoccupations se traduisent par une supervision plus étroite, une assistance renforcée et des budgets plus importants. Par conséquent, si votre entreprise a des difficultés à améliorer ses fonctionnalités de reprise après sinistre, il peut être judicieux d'opter pour une approche descendante plutôt qu'ascendante.

Qu'en est-il des opérations quotidiennes de reprise après sinistre ?

Outre la responsabilité finale de la supervision, nous avons voulu savoir qui était chargé de gérer les aspects les plus tactiques de la reprise après sinistre. **Les opérations qui relèvent de la cybersécurité ou d'équipes spécialisées dans la continuité de l'activité font souvent état des meilleures performances.** Les programmes gérés par les équipes IT obtiennent généralement des résultats inférieurs. Il est intéressant de noter également que la visibilité du conseil d'administration semble agir comme un levier de performance. Les taux de réussite sont statistiquement égaux quelle que soit la répartition quotidienne des responsabilités, tant que le CA assure la supervision.

La portée de la reprise après sinistre est-elle importante ?

Comme vous le savez, un sinistre n'attend pas que vous soyez préparé pour se produire. Les problèmes de cybersécurité ne font pas exception. C'est pourquoi il est généralement judicieux de se préparer à toutes les éventualités. Or, c'est plus facile à dire qu'à faire.

Moins de trois entreprises sur dix déclarent que leurs fonctions de reprise après sinistre couvrent au moins 80 % des systèmes stratégiques. La moitié d'entre elles couvrent une zone de 50 à 79 % et un peu moins de 20 % admettent des taux de couverture inférieurs. À première vue, cela ne semble pas trop grave. Après tout, la plupart des entreprises couvrent la majorité de leurs systèmes stratégiques. Malheureusement, les sinistres ont tendance à se produire à des endroits inattendus. Selon nos données, cela se produit plus souvent que nous n'aimerions l'admettre.

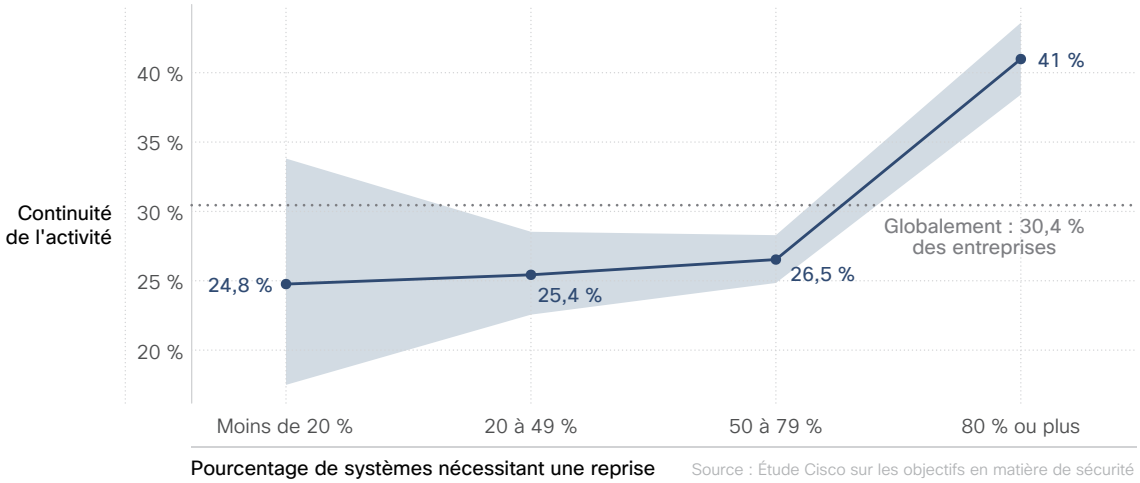


Figure 21 : Effet de la couverture des ressources stratégiques sur les fonctionnalités de reprise après sinistre

La Figure 21 présente un nouvel objectif ajouté à cette étude pour mesurer la capacité de l'entreprise à assurer la continuité de l'activité en cas d'événements perturbateurs. Il s'avère que c'est l'un des trois objectifs les plus difficiles à atteindre selon les participants. Il est donc d'autant plus important de trouver des moyens efficaces d'améliorer vos chances de réussite.

La Figure 21 nous transmet une information importante sur le maintien de la continuité de l'activité. **La probabilité d'atteindre cet objectif ne s'améliore que si les fonctionnalités de continuité de l'activité et de reprise après sinistre couvrent au moins 80 % des systèmes stratégiques.**

Cela s'explique probablement par le fait que les sinistres se produisent presque systématiquement lorsque nous n'y sommes pas préparés. On en déduit donc que les investissements dans la continuité de l'activité et la reprise après sinistre ne se traduisent pas immédiatement par l'atteinte des objectifs. Ce n'est pas réjouissant, mais c'est tout à fait normal, car un sinistre n'est jamais une bonne nouvelle.

L'entraînement permet-il d'atteindre un niveau optimal de reprise après sinistre ?

Pour être direct, malheureusement non. Mais c'est toujours mieux que rien. À quel point ? Voyons cela maintenant.

Il est bien connu dans le secteur militaire qu'aucun plan ne survit au premier contact avec l'ennemi. C'est également vrai en matière de cybersécurité. Il existe plusieurs manières de tester les fonctionnalités de continuité de l'activité et de reprise après sinistre, comme les procédures planifiées, les exercices de simulation, les tests en direct, les tests parallèles et les tests complets de production. Nous avons interrogé les participants sur la fréquence à laquelle leur entreprise mène de tels exercices, et nous avons comparé leurs réponses à leur probabilité de maintenir la continuité de l'activité.

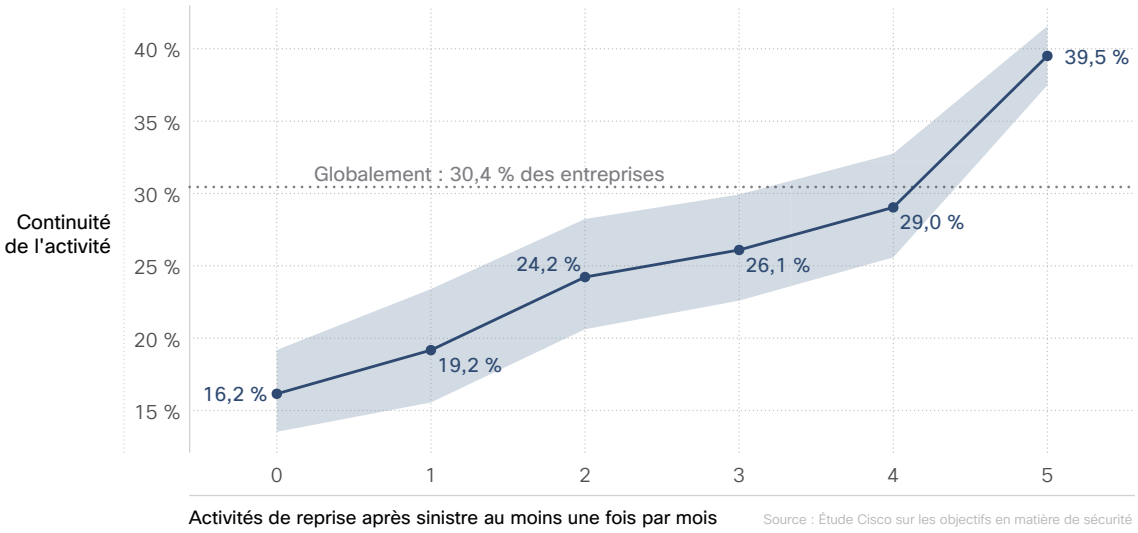


Figure 22 : Effet des tests sur les fonctionnalités de reprise après sinistre

Aucune de ces bonnes pratiques ne se démarque des autres en termes d'efficacité, mais toutes contribuent collectivement à une meilleure résilience. **Les entreprises qui effectuent régulièrement les cinq types de tests de reprise après sinistre sont près de 2,5 fois plus susceptibles de maintenir la continuité de l'activité que celles qui ne le font pas.** Conclusion ? Ne laissez rien au hasard en matière de résilience. Faites régulièrement un test de résistance de vos fonctionnalités de continuité de l'activité et de reprise après sinistre sous différents angles.

Les entreprises qui effectuent régulièrement les cinq types de tests de reprise après sinistre sont **2,5 X** plus susceptibles de maintenir la continuité de l'activité

Faut-il perturber votre réseau intentionnellement ?

Dans un test de résistance du plan de reprise après sinistre, le plus important c'est la « résistance ». L'ingénierie du chaos consiste à perturber régulièrement (et intentionnellement) les systèmes pour tester leur capacité de résistance aux conditions et événements inattendus. Est-ce que perturber vos systèmes IT et de sécurité peut rendre votre entreprise plus résiliente ? Voyons cela.

En interrogeant les participants sur l'utilisation de l'ingénierie du chaos dans leur entreprise, nous avons découvert que cette approche était plus courante que nous le pensions. Notez que nous avons remarqué une relation entre cette bonne pratique et l'intégration des technologies. Comme indiqué dans la Figure 23, plus des 2/3 des entreprises qui utilisent régulièrement l'ingénierie du chaos font état de technologies hautement intégrées prenant en charge leurs fonctionnalités de reprise. Il est difficile de savoir si c'est l'intégration qui favorise le recours à l'ingénierie du chaos ou le contraire. Comme c'est souvent le cas, la réponse est probablement un peu des deux. Gardez un œil sur cette nouvelle discipline, surtout si vous êtes responsable de la continuité de l'activité et de la reprise après sinistre dans un environnement IT complexe et hautement intégré.

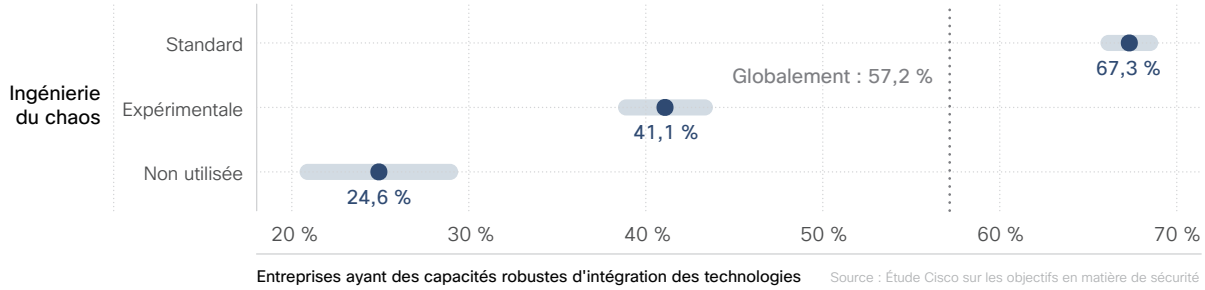


Figure 23 : Relation entre l'ingénierie du chaos et le niveau d'intégration IT

Dans la Figure 24, la comparaison entre le recours régulier à l'ingénierie du chaos et l'objectif de maintien de la résilience de l'entreprise achève de nous convaincre de l'intérêt d'une telle pratique. **Les entreprises qui utilisent régulièrement l'ingénierie du chaos sont deux fois plus susceptibles d'obtenir des résultats très satisfaisants que les entreprises qui ne l'utilisent pas.** Ce résultat vous surprend ? Nous aussi. La bonne nouvelle, c'est qu'en pratiquant vous-même l'ingénierie du chaos, vous pouvez perturber votre réseau avant qu'il ne le soit par surprise.

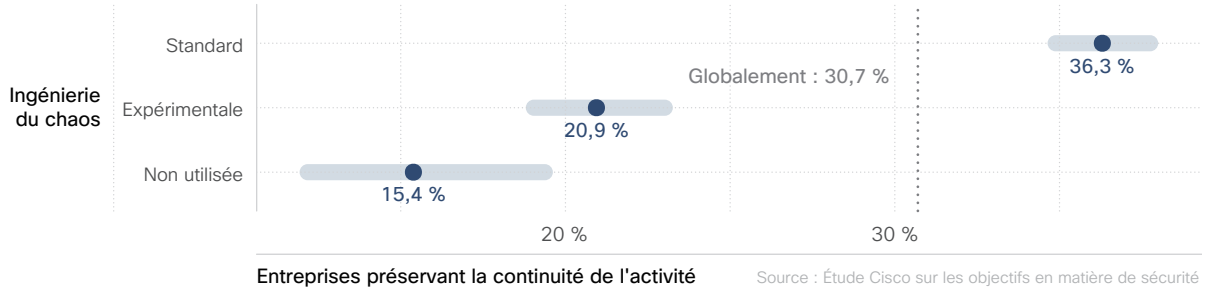


Figure 24 : Effet de l'ingénierie du chaos sur le maintien de la résilience de l'entreprise

Conclusion et recommandations

Nous avons commencé par les bonnes pratiques de sécurité identifiées comme très efficaces dans une étude précédente, puis nous avons recueilli d'autres informations par le biais d'une nouvelle enquête afin de savoir ce qui les rend plus efficaces et de partager ces enseignements avec vous. Nous espérons que ce rapport vous a fourni des conseils pratiques pour améliorer l'efficacité de votre programme de cybersécurité.

Quoi qu'il en soit, il est toujours utile de réfléchir aux conclusions d'une telle étude et de savoir quels enseignements les autres en ont tirés. Nous avons demandé à notre équipe de conseillers RSSI expérimentés d'évaluer chacune des bonnes pratiques que nous avons examinées. Nous avons indiqué leurs principales recommandations ci-dessous. Vous trouverez d'autres informations et points à retenir dans notre série de blogs sur les objectifs en matière de sécurité.

Remplacement proactif des technologies

« La question de la dette de sécurité est importante. Pour le RSSI, la solution consiste à élaborer une stratégie de type "acheter, conserver, vendre". Faites un état des lieux, définissez une architecture évolutive, réduisez les risques liés aux dépendances et mettez en œuvre une boucle de vérification pour les futurs cycles d'actualisation. »

Richard Archdeacon, consultant RSSI, Cisco

Technologie bien intégrée

« Nous savons qu'une intégration IT moderne réussie contribue à l'efficacité globale du programme de sécurité. Voici quelques mesures à prendre pour améliorer votre environnement : recherchez des solutions de sécurité cloud, examinez les opportunités d'automatisation et assurez-vous que les exigences d'achat incluent les fonctionnalités d'intégration des technologies. »

Helen Patton, consultante RSSI, Cisco @CisoHelen

Réponse rapide aux incidents

« Disposer de collaborateurs compétents au sein des équipes de réponse aux incidents est un atout indéniable. Mais même si c'est un bon point de départ, cela ne suffit pas. Les entreprises qui combinent des effectifs, des processus et des technologies solides profitent de capacités avancées de détection et de traitement des menaces. »

Dave Lewis, consultant RSSI, Cisco @gattaca

Détection précise des menaces

« Choisissez les collaborateurs les plus compétents pour vos équipes de sécurité, car la qualité prévaut sur la quantité. Si vous ne pouvez pas obtenir le niveau d'expertise dont vous avez besoin, l'automatisation vous aidera à combler le manque d'expérience de vos collaborateurs les moins expérimentés et à obtenir des résultats aussi bons qu'avec des collaborateurs plus chevronnés. »

Wendy Nather, consultant RSSI, Cisco @wendynather

Reprise rapide après sinistre

« Les conclusions de ce rapport mettent l'accent sur l'intérêt des fonctionnalités de continuité de l'activité et de reprise après sinistre. Toutefois, celles-ci ne doivent pas être isolées des autres fonctions de sécurité. La hiérarchisation et le classement des ressources en fonction des risques doivent être partagés avec d'autres fonctions de gestion des risques. De même, il est important d'intégrer la gestion des ressources et des menaces afin de garantir que toutes les équipes travaillent dans la même direction. »

Wolfgang Goerlich, consultant RSSI, Cisco @jwgoerlich

À propos de Cisco Secure

Cisco s'est imposé depuis longtemps comme le leader mondial des technologies web, tout en développant une gamme de solutions ouvertes et intégrées pour la cybersécurité. Nous pensons que les solutions de sécurité doivent fonctionner comme une équipe. Elles doivent apprendre les unes des autres. Elles doivent écouter et réagir en tant qu'entité unique et coordonnée. Lorsque toutes ces conditions sont réunies, la sécurité devient alors systématique et plus efficace. Nos clients nous font confiance depuis des années, car nous sommes à la fois le premier fournisseur mondial de services d'infrastructure IT et de réseau, et le plus grand groupe de cybersécurité au monde.

Cisco Secure repose sur le principe d'une sécurité améliorée, et non augmentée. Il propose une approche rationalisée de la sécurité, centrée sur le client, qui garantit la facilité de déploiement, de gestion et d'utilisation, et de fonctionnement avec tous les autres produits. Les collaborateurs et les clients sont au cœur de nos activités, et c'est ce qui nous motive. Nous comprenons ce que veulent les clients : réduire la complexité et instaurer une sécurité fiable qui tient compte de leurs objectifs. Pour cela, il faut simplifier sans être simpliste. Notre plateforme cloud est un pas de géant vers cet objectif.

Cisco SecureX permet aux professionnels de la sécurité de se protéger en toute confiance contre les menaces actuelles et futures. Nous aidons 100 % des entreprises du Fortune 100 à sécuriser leurs collaborateurs, partout, avec la plateforme la plus vaste et la plus intégrée du marché. Pour savoir comment nous simplifions les expériences, accélérons la réussite et protégeons l'avenir de nos clients, rendez-vous sur cisco.com/go/secure.

Annexe : Données démographiques de l'enquête

Cette annexe présente les données démographiques des 5 123 personnes qualifiées ayant répondu à cette enquête. Nous espérons qu'elles aideront les personnes intéressées à comprendre la représentativité de ces résultats.

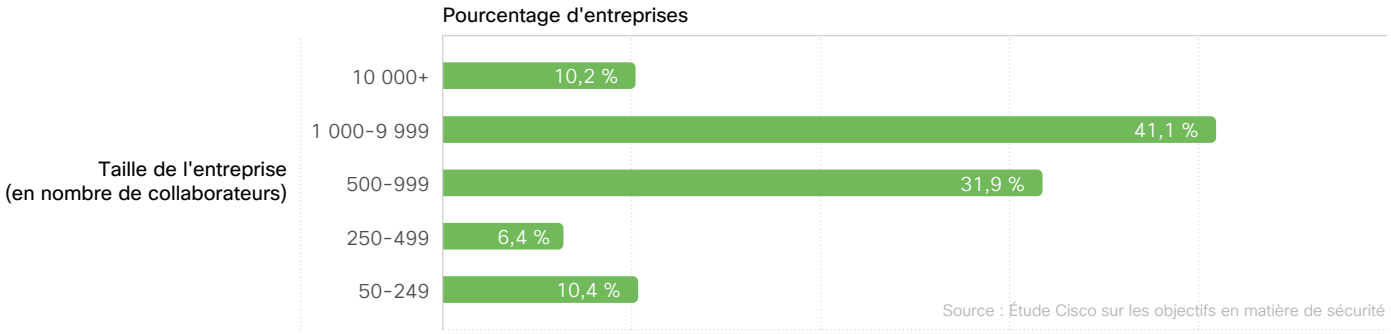


Figure A1 : Nombre d'employés des entreprises participantes

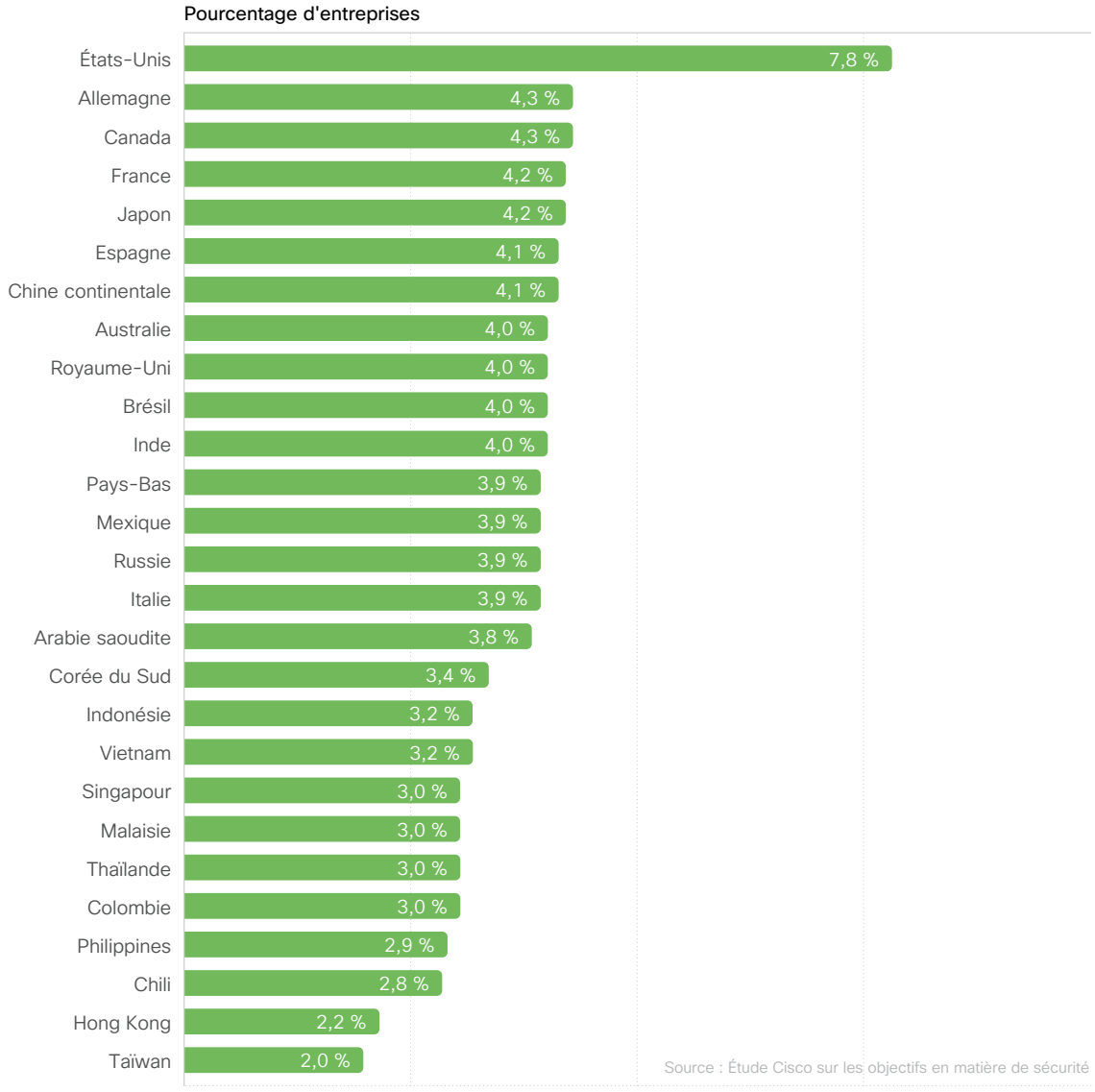


Figure A2 : Pays accueillant le siège social des entreprises participantes

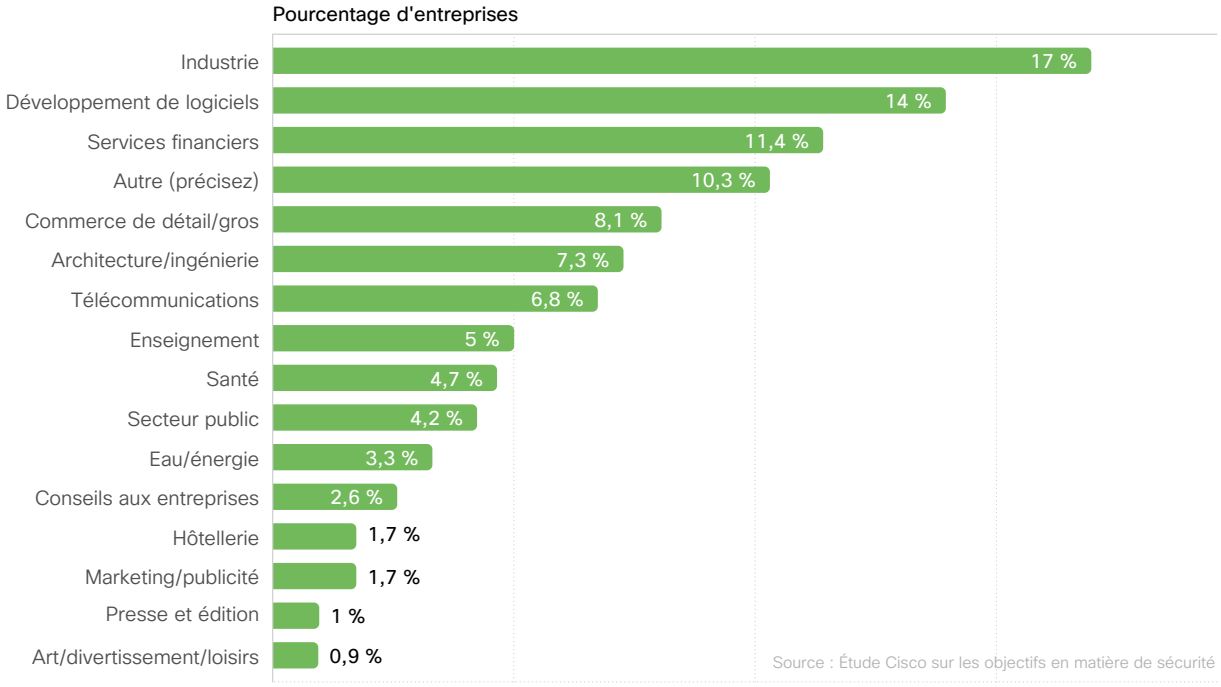


Figure A3 : Secteurs représentés par les entreprises participantes

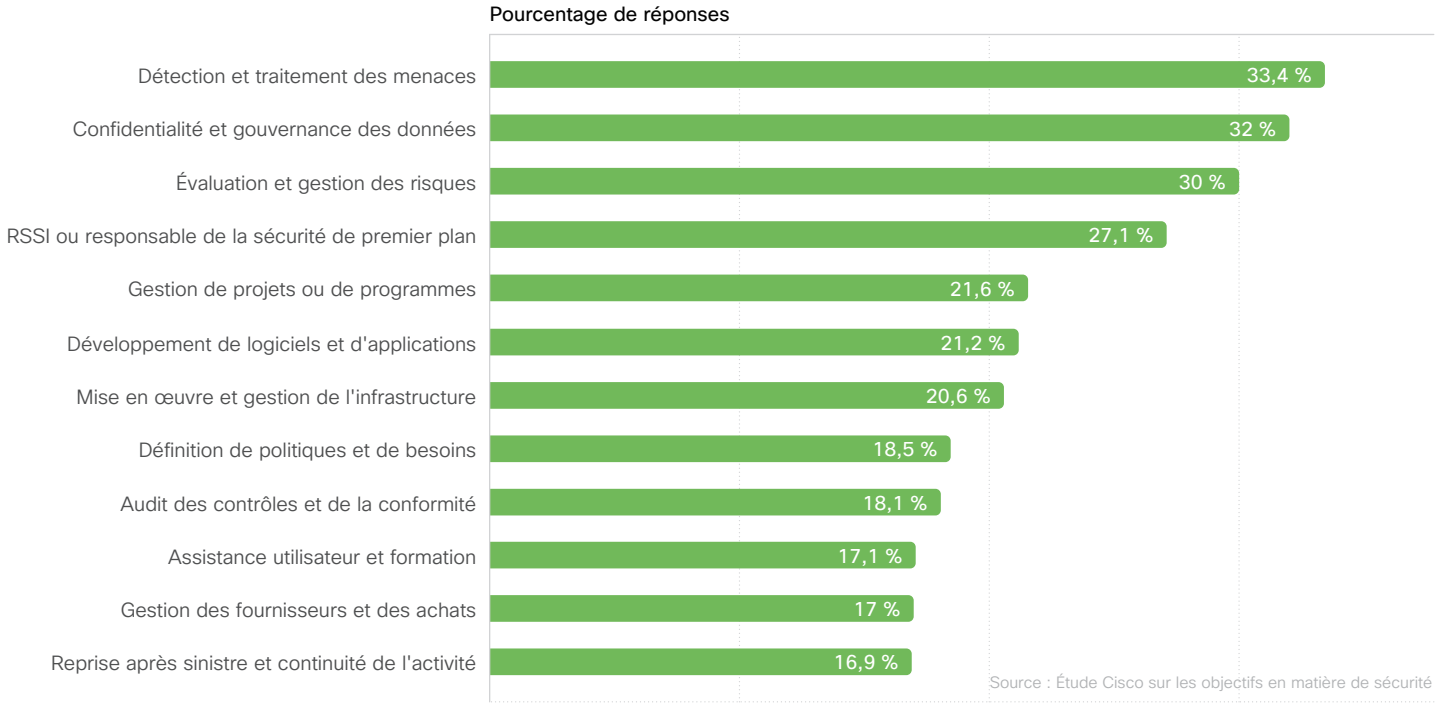


Figure A4 : Principales responsabilités professionnelles des participants

CISCO
SECURE

Siège social en Amérique
Cisco Systems, Inc.
San José, Californie

Siège social en Asie/Pacifique
Cisco Systems (États-Unis) Pte. Ltd.
Singapour

Siège social en Europe
Cisco Systems International BV
Amsterdam, Pays-Bas

Publié en décembre 2021