Rapport de données de recherche

Tendances en matière de sécurité des réseaux

Comprendre l'état de la sécurité des réseaux aujourd'hui

Par Dan Conde, analyste ESG

Janvier 2017

Ce Rapport de données de recherche d'ESG a été commandé par Gigamon, et est distribué sous licence d'ESG.

Sommaire

Sommaire exécutif

Méthodologie de recherche et objectifs

Au cours de la seconde moitié de l'année 2016, Gigamon a fait réaliser par Enterprise Strategy Group (ESG) une enquête auprès de 300 professionnels en informatique et cybersécurité. L'ensemble des répondants occupaient tous des fonctions incluant des responsabilités et une implication relatives à la planification, la mise en œuvre, et/ou les opérations de politiques, processus et mesures de protection technique en matière de sécurité de leurs entreprises. Les participants disposaient également d'une autorité en matière de décision d'achat ou d'une influence sur les produits et services de sécurité réseau.

Les répondants se situaient en Amérique du Nord et en Europe de l'Ouest. Des entreprises de tailles différentes étaient représentées dans la base de répondants : 25 % des répondants travaillaient dans des entreprises comptant 100 - 499 employés, 34 % dans des entreprises avec 500 - 999 employés, et 41 % dans des entreprises de 1 000 - 4 999 employés. Cette enquête incluait des répondants issus de plusieurs secteurs, incluant fabrication (22 %), commerce de détail / commerce de gros (11 %), services financiers (16 %), services aux entreprises (8 %), santé (5 %), et communications et médias (4 %).

Ce projet de recherche a été entrepris afin d'évaluer les difficultés, changements, meilleures pratiques et les besoins en solution pour les opérations de sécurité réseau et les outils de sécurité réseau. Les répondants ont été interrogés au sujet de caractéristiques organisationnelles, incluant personnel, coordination, et temps d'évaluation de nouvelles technologies. Les répondants ont également été interrogés au sujet de considérations technologiques, telles que l'utilisation de modèles automatisés en comparaison de processus manuels, les types d'outils de visibilité réseau utilisés, l'utilisation des fonctions de surveillance de sécurité, ainsi que le recours actuel et prévu à des services de tiers en matière de sécurité réseau.

Points clés de la recherche

Sur la base des données collectées à partir de l'enquête de recherche, ce rapport parvient à la conclusion que :

- Les opérations de sécurité réseau sont aujourd'hui aussi difficiles ou plus difficiles qu'elles ne l'étaient il y a 24 mois.
- La visibilité à travers l'ensemble des réseaux d'entreprise peut être améliorée, avec pour résultat une posture de sécurité renforcée.
- Les entreprises découvrent qu'elles ne sont pas parvenues à l'état idéal pour lequel des processus automatisés permettent des opérations de sécurité réseau efficaces.
- L'ajout de plus d'outils de sécurité réseau n'est peut-être pas la voie à suivre afin d'améliorer la visibilité et l'atténuation des menaces.
- Une architecture basée sur plateforme en vue d'assurer la visibilité peut permettre aux entreprises d'utiliser plus optimalement les outils de sécurité réseau qu'elles possèdent.

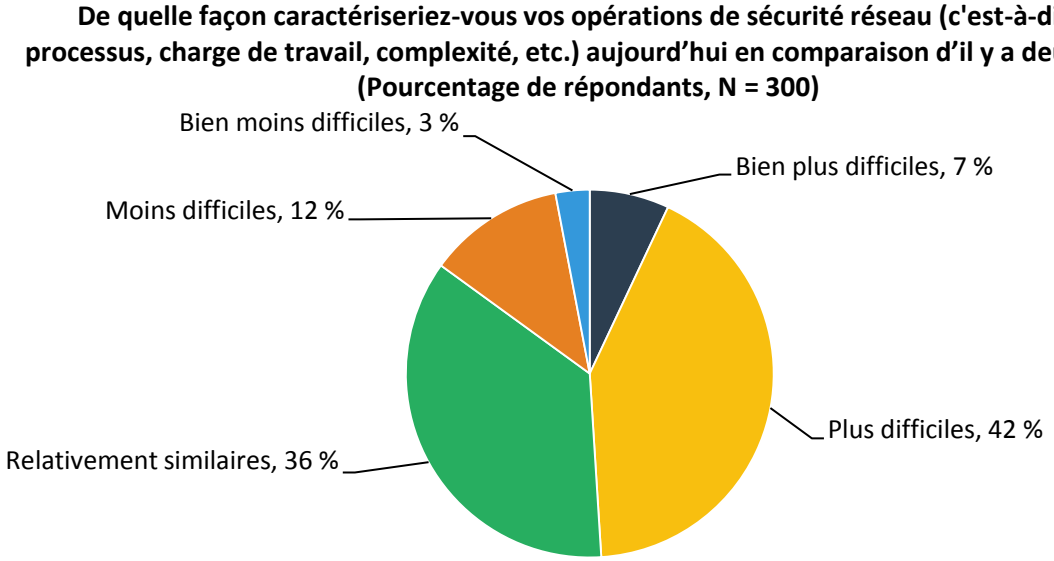
Résultats de la recherche

État actuel des opérations réseau et de sécurité

La recherche ESG indique invariablement que la cybersécurité constitue une priorité majeure[1] et un défi pour les entreprises informatiques, exacerbés par un paysage de menaces à la sophistication croissante, lui-même exacerbé par une lacune chronique en matière de compétences en cybersécurité. De fait, du point de vue de la sécurité réseau, le nombre croissant de périphériques d'utilisateurs finaux, les communications entre périphériques physiques et virtuels, ainsi que le partage de données entre le cloud, les centres de données et les réseaux de campus, posent des défis aux entreprises en matière d'obtention d'une visibilité quant à la façon dont les données sont utilisées et transmises, et quant à la localisation des menaces potentielles.

Lorsqu'il leur est demandé de caractériser leurs opérations de sécurité réseau (c'est-à-dire : processus, charge de travail, complexité, etc.) aujourd'hui en comparaison d'il y a deux ans, 85 % des entreprises rapportent qu'elles s'avèrent aussi difficiles ou plus difficiles qu'elles ne l'étaient il y a 24 mois (voir Figure 1).

Figure 1. Difficulté associée aux opérations de sécurité réseau au cours du temps



Source : Enterprise Strategy Group, 2016

Parmi les répondants indiquant que les opérations de sécurité réseau sont devenues plus ardues au cours des deux dernières années, qu'est-ce qui engendre cette tendance ? Selon la **Figure** 2, les facteurs les plus fréquemment mentionnés incluent un nombre accru de périphériques sur le réseau (61 %), un trafic plus élevé sur le réseau (55 %), des opérations de sécurité englobant plus de types de technologies de sécurité et de mise en réseau (47 %), et de nombreux types de cyber-attaques et vulnérabilités (46 %).

Lorsqu'il leur est demandé si leur entreprise dispose d'une bonne visibilité à travers l'intégralité du réseau / des réseaux afin de procéder efficacement à des analyses de vulnérabilité et de sécurité continues, 75 % des répondants rapportent qu'ils considèrent que la visibilité à travers l'ensemble de leurs réseaux d'entreprise pourrait être améliorée (voir Figure 3). Néanmoins, de nombreuses entreprises réalisent déjà des activités fournissant une visibilité. De fait, lorsqu'ESG a demandé si plusieurs activités clés étaient actuellement réalisées, une majorité a répondu procéder actuellement à une surveillance du trafic réseau aux fins d'analyse des performances, des défaillances et de la disponibilité, à l'analyse des métadonnées

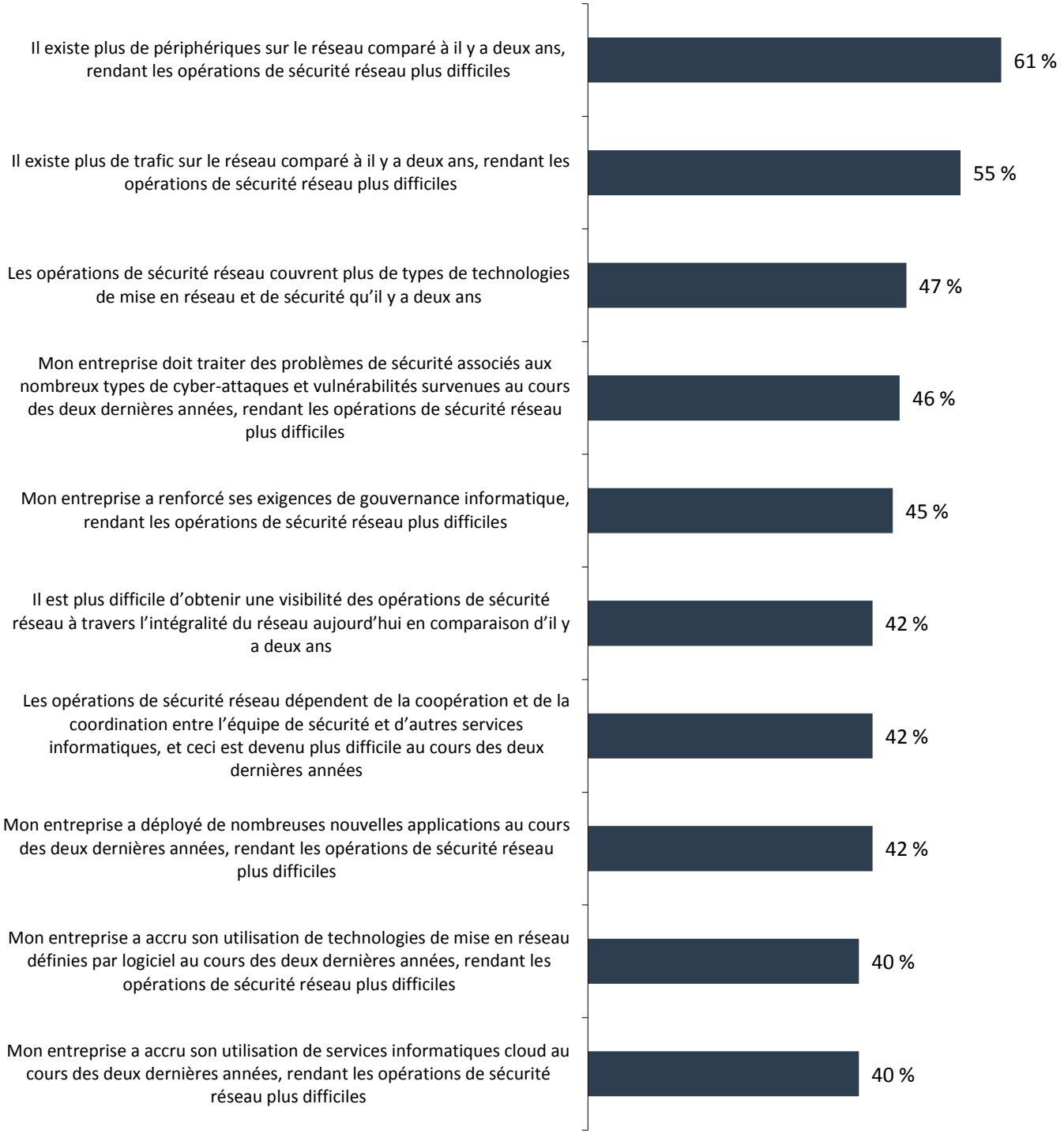
[1] Source : ESG Research Report, *2016 IT Spending Intentions Survey*, Février 2016.

réseau pour la surveillance DNS, à l'analyse des certificats SSL, ou à des analyses de comportement des utilisateurs, et/ou au déchiffrement SSL.

Un paradoxe existe. Bien que ces activités soient couramment réalisées, les entreprises affirment *encore* manquer de la visibilité réseau souhaitée. Lorsqu'il leur est demandé si leur entreprise dispose d'une bonne visibilité à travers l'intégralité du réseau d'entreprise, seuls 25 % répondent disposer d'une excellente visibilité réseau, tandis que 67 % ont déclaré qu'elle pouvait être améliorée, et 8 % ont déclaré disposer d'une visibilité limitée.

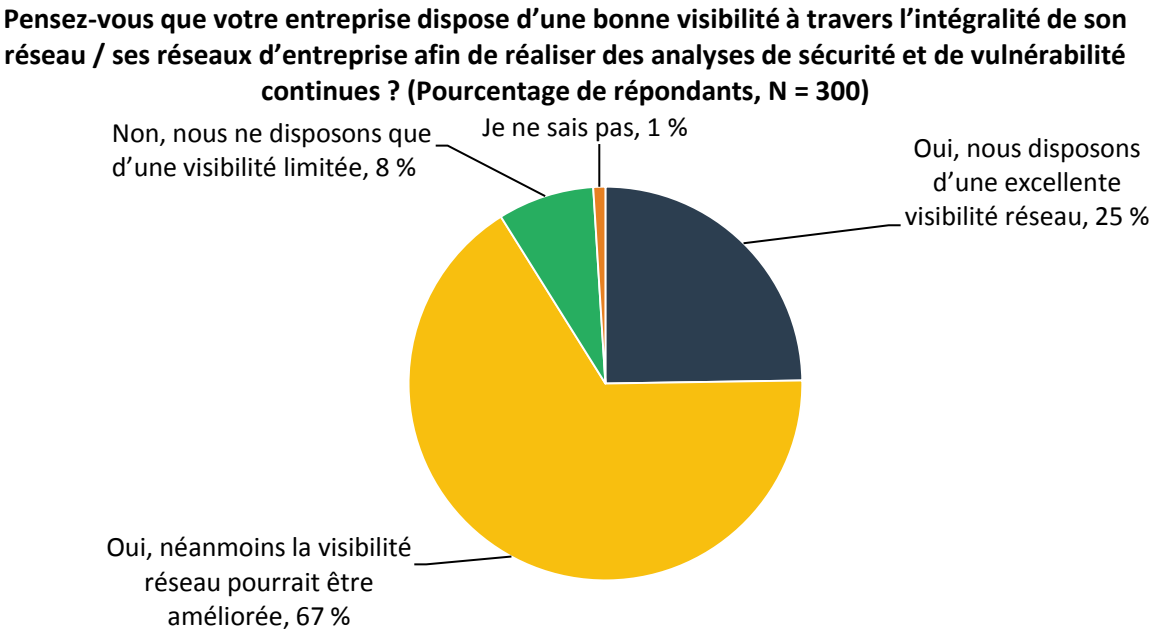
Figure 2. Les dix facteurs principaux engendrant une difficulté accrue concernant les opérations de sécurité réseau

Vous avez indiqué que vos opérations de sécurité réseau étaient devenues plus difficiles au cours des deux dernières années. Lesquels des éléments suivants constituent les facteurs principaux rendant plus difficiles vos opérations de sécurité réseau au sein de votre entreprise ? (Pourcentage de répondants, N = 146)



Source : Enterprise Strategy Group, 2016

Figure 3. Niveau de visibilité réseau



Source : Enterprise Strategy Group, 2016

Défis posés par les opérations réseau et de sécurité

Quatre-vingts pour cent des entreprises utilisent des outils de sécurité en ligne, et une majorité (58 %) de ces dernières effectuent des mises à jour logicielles ou procèdent à des changements de configuration de ces outils au moins une fois par mois (voir Figure 4). Bien qu'il soit important que des correctifs continuent d'être appliqués à ces outils, il est également important de remarquer qu'une des lacunes des outils en ligne est que ces changements et mises à jour perturbent les opérations de sécurité et peuvent véritablement créer des vulnérabilités.

La coordination entre les équipes des opérations réseau et de sécurité peut s'avérer également un autre point faible, avec uniquement 32 % des répondants indiquant que la coordination est facile lorsque ces changements appliqués aux outils en ligne sont effectués. Ce problème est abordé plus en détail dans la prochaine section.

Prochaines étapes

Pour quelle raison ces processus et outils n'offrent-ils pas les résultats souhaités ? Les entreprises doivent se poser plusieurs questions pouvant contribuer à combler les lacunes en visibilité :

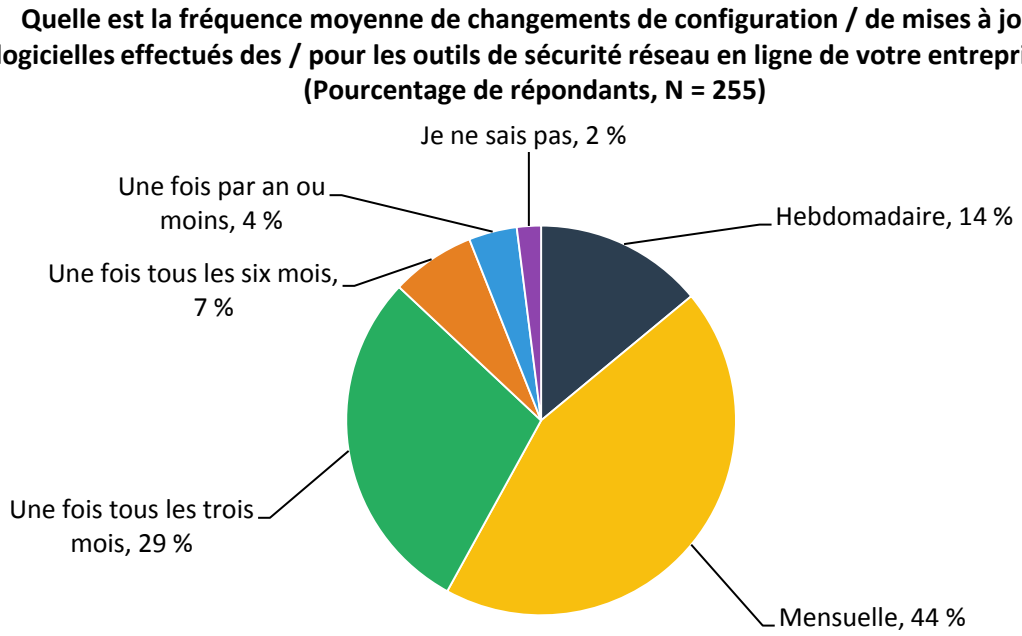
Est-ce que disposer de plus d'outils pourrait aider ?

Les données de l'enquête n'indiquent pas que disposer de plus d'outils serait utile. De fait, les données d'ESG révèlent que le nombre habituel d'outils que les entreprises utilisent par site est de cinq à sept (ainsi que rapporté par 64 % des répondants). Même des entreprises plus importantes avec des effectifs supérieurs n'optent pas pour le recours à un plus grand nombre d'outils. Ceci indique que ces entreprises ne considèrent pas l'ajout de plus d'outils dans leur environnement comme une solution efficace, même si elles ne sont pas limitées par le nombre d'individus pouvant utiliser ces outils.

Est-ce que des changements organisationnels peuvent aider ?

Des améliorations organisationnelles peuvent permettre aux entreprises d'utiliser de manière plus optimale leurs outils existants. Les données de la recherche d'ESG indiquent que trois entreprises sur dix (30 %) aujourd'hui ne disposent pas d'un personnel dédié pour les opérations réseau et de sécurité. Au sein des entreprises disposant d'un personnel dédié avec groupes de sécurité et réseau, 93 % ont rapporté que quatre ou moins de personnes étaient employées à ces fins. En outre, les groupes de sécurité ont rapporté un accent mis dans une large mesure sur la réponse aux incidents. Lorsqu'il est demandé combien de personnes sont affectées à la réponse aux incidents, une majorité relative a répondu que deux personnes étaient affectées à cette fonction. Aussi, il est très courant que la moitié ou plus du personnel des opérations de sécurité soit affectée à la réalisation d'activités réactives de réponse aux incidents.

Figure 4. Fréquence moyenne de changements de configuration d'outil de sécurité réseau en ligne



Source : Enterprise Strategy Group, 2016

Lorsqu'ESG a demandé aux entreprises allouant du personnel dédié aux équipes réseau et de sécurité, et utilisant des outils de sécurité en ligne, dans quelle mesure la coordination des efforts entre les équipes concernées était difficile lors de l'application de changement aux outils de sécurité en ligne, moins d'un tiers ont répondu que cela était facile.

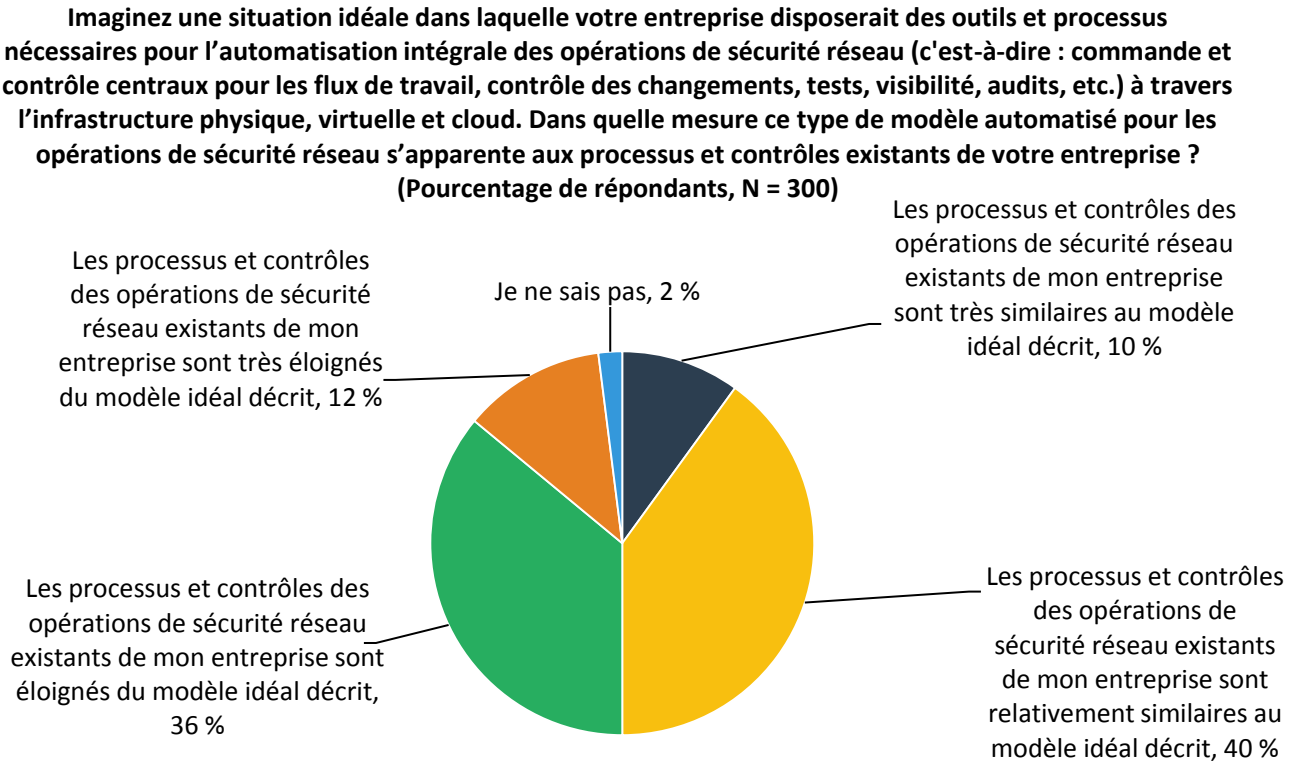
La situation d'ensemble révélée par ces données ne s'avère pas positive. De nombreuses entreprises n'allouent pas actuellement de personnel dédié aux rôles de sécurité, et celles le faisant sont toujours susceptibles de se voir limitées en ressources, soit du point de vue des effectifs, soit du point de vue des compétences requises. De plus, les difficultés en termes de collaboration entre l'équipe de sécurité et les autres disciplines informatiques sont plutôt fréquentes.

Néanmoins, si le personnel des opérations de sécurité peut devenir plus efficace et coordonner de meilleure façon ses tâches avec le personnel des opérations réseau, les résultats en matière de sécurité seront améliorés. L'automatisation peut également aider dans ce domaine. Si les processus réseau et de sécurité peuvent être automatisés, le besoin de coordination manuelle sera moindre. L'automatisation peut également réduire le temps consacré à la réponse aux incidents et libérer plus de temps à allouer aux activités proactives et préventives.

Est-ce qu'une approche architecturale différente peut aider ?

Comprendre la situation actuelle des entreprises et la comparer à une situation idéale peut clarifier davantage la perception que les organisations informatiques ont d'elles-mêmes et où des possibilités d'améliorations existent. ESG a demandé aux entreprises d'imaginer une situation idéale dans laquelle les outils et processus nécessaires pour l'automatisation intégrale des opérations de sécurité réseau (telles que commande et contrôle centraux pour les flux de travail, contrôle des changements, tests, visibilité et audits) étaient en place, et de comparer cela à leurs processus et contrôles d'entreprise existants. Uniquement 10 % des entreprises ont considéré que les processus et contrôles de sécurité réseau existants de leur entreprise étaient très similaires à ce modèle idéal (voir Figure 5). Ce déficit important accrédite l'idée que cette lacune peut être comblée par une approche architecturale complètement différente de la sécurité réseau fournissant commande et contrôle centraux pour les tâches opérationnelles.

Figure 5. Comparaison d'un modèle automatisé idéal avec les processus existants



Source : Enterprise Strategy Group, 2016

Ce type d'approche architecturale basée sur plateforme et centralisée doit permettre à des outils disparates d'être gérés plus efficacement en leur permettant d'être vus, administrés, et surveillés depuis une console unique. L'association de la consolidation des outils et de l'automatisation des tâches manuelles doit permettre aux outils de fonctionner plus efficacement, et aux processus d'être rationalisés.

L'idée d'utiliser l'automatisation afin d'aider à la sécurité réseau a été évoquée dans une autre enquête ESG, qui indiquait que le domaine ayant la relation la plus forte avec l'automatisation des réseaux était la sécurité réseau.[2] Ceci renforce le résultat révélant que l'automatisation permet une utilisation des ressources (ressources informatiques et humaines) plus efficace.

[2]Source : ESG Research Report, *Network Automation: Enabler of IT Process Goals*, Juillet 2016.

La vérité principale

Ainsi que clairement démontré par les données de recherche d'ESG, la plupart des entreprises peuvent améliorer leur visibilité réseau et réduire leurs vulnérabilités en matière de sécurité. Néanmoins, elles doivent procéder à des investissements intelligents. L'ajout d'outils ponctuels supplémentaires à un environnement de sécurité et de surveillance déjà fragmenté ne fera qu'aggraver la situation plutôt que de produire des résultats meilleurs. Au contraire, il est plus probable que l'entreprise typique puisse obtenir de meilleurs résultats en matière de sécurité en investissant dans du personnel (probablement trop dispersé aujourd'hui) ou en consolidant les outils par le biais d'une approche, basée sur une plateforme, de la visibilité, dans laquelle les données, analyses et rapports issus de divers outils peuvent être agrégés et consommés via un panneau de contrôle unique.

Cette méthodologie architecturale pour l'approche à adopter concernant ces défis est une solution particulièrement intéressante, car elle permet aux entreprises de préserver leurs investissements dans les outils existants, en les rendant plus performants, tout en donnant le contrôle aux personnes les utilisant. Améliorer l'utilisation des ressources informatiques et humaines existantes au sein de l'organisation est une façon prudente de répondre à ces défis.

Enterprise Strategy Group est une société de stratégie, de validation, de recherche et d'analyse informatique, fournissant des informations et renseignements exploitables à la communauté informatique mondiale.