

Se protéger aujourd'hui et demain

20 facteurs à prendre en compte pour votre
cybersécurité en 2020



Inclut du
contenu
exclusif sur
la France

Voir page 23

Sommaire

Introduction	3
20 facteurs à prendre en compte pour votre cybersécurité en 2020	4
1. Qui, dans votre entreprise, vous apporte un soutien hiérarchique et une orientation claire ?	4
2. Comment savoir quels indicateurs ont le plus de valeur ?	5
3. Quels sont les principaux facteurs qui influencent les dépenses dans le cadre d'un budget limité ?	6
4. Comment trouver le bon équilibre entre les dépenses pour la vérification de la fiabilité et pour la détection des menaces ?	8
5. Que vous apprend l'analyse de l'impact des failles liées à la sécurité sur l'entreprise ?	9
6. Pourquoi la divulgation volontaire des failles atteint-elle un niveau record ?	11
7. Est-il possible de quantifier les bénéfices de la collaboration entre les équipes responsables du réseau et de la sécurité ?	11
8. Hormis la réduction des coûts, quelles sont les autres raisons qui justifient l'externalisation ?	11
9. La préparation offre-t-elle des résultats concrets ?	13
10. Quelle est l'importance du déploiement de correctifs dans la lutte contre les failles ?	13
11. Quelles sont les causes des interruptions ?	14
12. À quel point est-ce difficile de protéger les collaborateurs mobiles ?	14
13. Comment pourriez-vous étendre la sécurité zero-trust pour protéger les applications ?	14
14. Est-il encore difficile de protéger l'infrastructure de réseau ?	16
15. Est-il possible de mesurer l'impact du regroupement des fournisseurs ?	17
16. Quelles sont les causes de votre épuisement lié à la gestion de la cybersécurité ?	18
17. Quels sont les bénéfices en matière de sécurité liés à l'hébergement de l'infrastructure dans le cloud ?	19
18. Selon vous, quels défis l'avenir nous réserve-t-il ?	20
19. Quelle priorité devez-vous donner à la gestion des incidents ?	21
20. Que pouvez-vous faire aujourd'hui pour renforcer votre sécurité ?	22
En France, des RSSI plus stratégiques qu'opérationnels ?	23-26
Se protéger aujourd'hui et demain.	27
À propos de la série de rapports Cisco sur la cybersécurité	28

Introduction

Outre leurs efforts pour accélérer la croissance et la transformation numérique de l'entreprise, les responsables de la sécurité font face à une multitude de défis. Ce constat provient de vos propres témoignages, que ce soit lors de nos échanges réguliers ou dans le cadre de notre étude comparative annuelle. Certains défis concernent la sécurité, comme la nécessité d'une visibilité ou d'une automatisation renforcées, ou la quête d'une plus grande simplicité pour la gestion et la réponse aux attaques. Certains sont liés à la réussite de votre entreprise, comme l'engagement à soutenir la croissance et la transformation, quel que soit le terminal mobile utilisé ou l'application cloud nécessaire. D'autres consistent à faire aujourd'hui des investissements judicieux qui serviront à votre entreprise demain.

Tout cela s'ajoute à vos missions quotidiennes en tant que RSSI, comme la détection et la neutralisation des menaces avancées. Il est difficile de gérer en même temps des hackers toujours plus ingénieux et une surface d'exposition aux attaques toujours plus vaste. Vous ne devez pas uniquement trouver le moyen de faire plus avec un budget limité. Vous devez également protéger la réputation de votre entreprise, garder la confiance des actionnaires et du conseil d'administration, et recruter les ressources adaptées pour contrer les tactiques, les techniques et les procédures utilisées par les hackers.

Vous devez fournir aux utilisateurs l'accès dont ils ont besoin tout en résolvant ces problématiques de sécurité, de complexité et budgétaires. Vous devez également réduire les frais généraux liés à la technologie, éliminer les principales failles de sécurité, détecter les menaces avant qu'elles infiltrent votre réseau et exfiltrent vos données, dépenser plus intelligemment le budget pour la sécurité et attirer davantage de clients.

Selon le Forum économique mondial, les cyberattaques sont perçues comme le deuxième risque majeur au niveau mondial par les chefs d'entreprise des pays développés, juste derrière les crises financières.¹

En menant notre sixième enquête annuelle auprès de 2 800 décideurs informatiques dans 13 pays, nous avons perpétué notre tradition annuelle de nous plonger dans votre univers pour compiler des statistiques de référence clés.² Nous nous sommes également longuement entretenus avec un groupe de RSSI pour analyser les conclusions de l'enquête et établir une liste de 20 facteurs à prendre en compte en 2020. Ce rapport offre des enseignements précieux que vous pouvez partager avec d'autres membres de l'équipe dirigeante ou du conseil d'administration afin de formuler des recommandations concrètes pour renforcer la sécurité de votre entreprise.

Comme nous savons que l'incertitude règne en maître dans ce secteur, nous avons organisé les sections de ce rapport sous la forme de questions que vous pourriez vous poser au moment de préparer l'année à venir. Si ces questions vous interpellent ou qu'elles vous ouvrent à d'autres questionnements, n'hésitez pas à nous contacter à l'adresse security-reports@cisco.external.com. En attendant, nous espérons que ce rapport vous aidera à relever vos défis liés à la sécurité au cours de cette année.

Pour consulter tous les rapports de notre série sur la cybersécurité, rendez-vous sur : cisco.com/go/securityreports.

¹ « [This is what CEOs around the world see as the biggest risks to business](#) » (article en anglais), Forum économique mondial, 2019

² Étude menée dans les pays suivants : Allemagne, Australie, Brésil, Canada, Chine, Espagne, États-Unis, France, Inde, Italie, Japon, Mexique et Royaume-Uni.

20 facteurs à prendre en compte pour votre cybersécurité en 2020

1. Qui, dans votre entreprise, vous apporte un soutien hiérarchique et une orientation claire ?

Au fil des ans, dans notre enquête, nous avons analysé quatre pratiques clés pour favoriser une relation mutuellement bénéfique entre les membres de l'équipe dirigeante et ceux de l'équipe chargée de la sécurité. Cet exercice mesure la priorité donnée à la sécurité selon le niveau hiérarchique (du haut au bas de la pyramide), où nous avons constaté une légère tendance à la baisse par rapport à l'année dernière. En voici les résultats :

- 89 % des personnes interrogées ont déclaré que leur direction considérait toujours la **sécurité comme une priorité élevée** ; cependant, ce chiffre a baissé de 7 % au cours des quatre dernières années.
- Le pourcentage d'entreprises **ayant clairement identifié les rôles et responsabilités en matière de sécurité au sein de l'équipe dirigeante** a fluctué au cours des dernières années. Il est de 89 % cette année. Compte tenu de la visibilité croissante en matière de cybersécurité et du besoin criant de responsables de la sécurité en haut de l'échelle, il est essentiel de continuer à définir clairement les rôles et responsabilités de chacun.
- L'intégration des évaluations des risques liés à la cybersécurité dans les processus globaux d'évaluation des risques a diminué de 5 % par rapport à l'an dernier, mais elle demeure élevée avec 91 % des personnes interrogées déclarant les utiliser.
- Malgré une baisse de 6 % par rapport à l'an dernier, le pourcentage d'équipes de direction qui établissent des indicateurs clairs pour évaluer l'efficacité des programmes de sécurité est encore relativement élevé à 90 %.

Sur les quatre dernières années, ces chiffres affichent une légère baisse, ce qui peut indiquer : 1) que le niveau de responsabilité en matière de sécurité est en train de changer, 2) que la communication avec l'équipe de direction n'est plus aussi claire qu'avant, 3) que la direction a désormais d'autres priorités, ou 4) que les RSSI et les dirigeants réévaluent leurs paramètres de mesure.

Pourtant, même si ces chiffres sont en baisse, ils restent encore très élevés. Il est possible par exemple que la sécurité, devenue opérationnelle, nécessite désormais d'être mieux représentée dans les hautes sphères de l'entreprise. **Le fait que les chiffres soient encore très élevés indique que les dirigeants et les professionnels de la sécurité continuent d'entretenir des relations solides.**

Les entreprises ont des équipes dirigeantes de composition distincte, et les types de leadership sont nombreux. Le rôle d'un RSSI est de communiquer et de collaborer avec l'ensemble des départements en montrant les bénéfices d'une stratégie de sécurité adaptée pour l'entreprise.

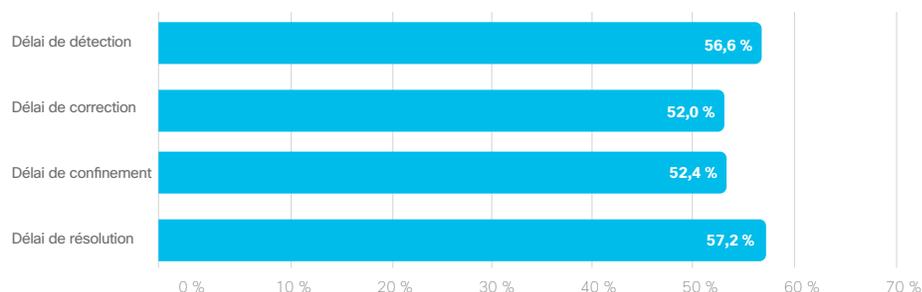
Sir Mick Jenkins, RSSI à l'université Brunel de Londres

2. Comment savoir quels indicateurs ont le plus de valeur ?

Comme nous venons de le voir, 90 % des personnes interrogées ont indiqué que l'équipe dirigeante de leur entreprise avait mis en place des indicateurs clairs pour évaluer l'efficacité de leur programme de sécurité. Cette démarche fait partie intégrante de l'élaboration d'une structure de sécurité, et les équipes de direction et de sécurité peinent souvent à se mettre d'accord sur la manière de mesurer l'amélioration opérationnelle et les performances en matière de sécurité.

Les décideurs informatiques interrogés dans le cadre de notre enquête ont classé le délai de détection en tête des **indicateurs de performance clé (KPI)**. **Toutefois, lorsque vous interrogez l'équipe dirigeante ou le conseil d'administration, le délai de résolution apparaît tout aussi important**, car il représente un ensemble d'indicateurs de l'impact total pouvant inclure : les pannes du système, le nombre d'enregistrements de données affectés, le coût des analyses, la perte de chiffre d'affaires, de clients et d'opportunités commerciales, et les coûts directs (Figure 1). Ce délai peut également servir à mesurer l'efficacité globale de l'équipe IT, car la remédiation peut nécessiter une collaboration de grande envergure entre les départements.

Figure 1 : Indicateurs utilisés pour signaler en interne une faille majeure auprès de l'équipe de direction ou du conseil d'administration (N = 2 800). Les pourcentages sont arrondis.

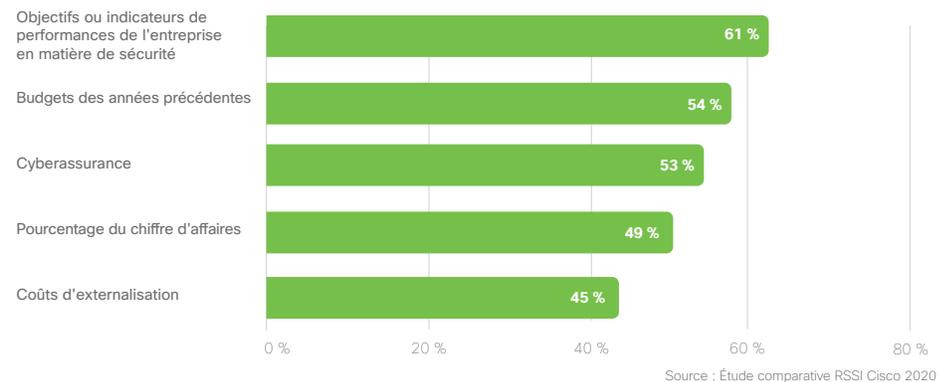


Source : Étude comparative RSSI Cisco 2020

3. Quels sont les principaux facteurs qui influencent les dépenses dans le cadre d'un budget limité ?

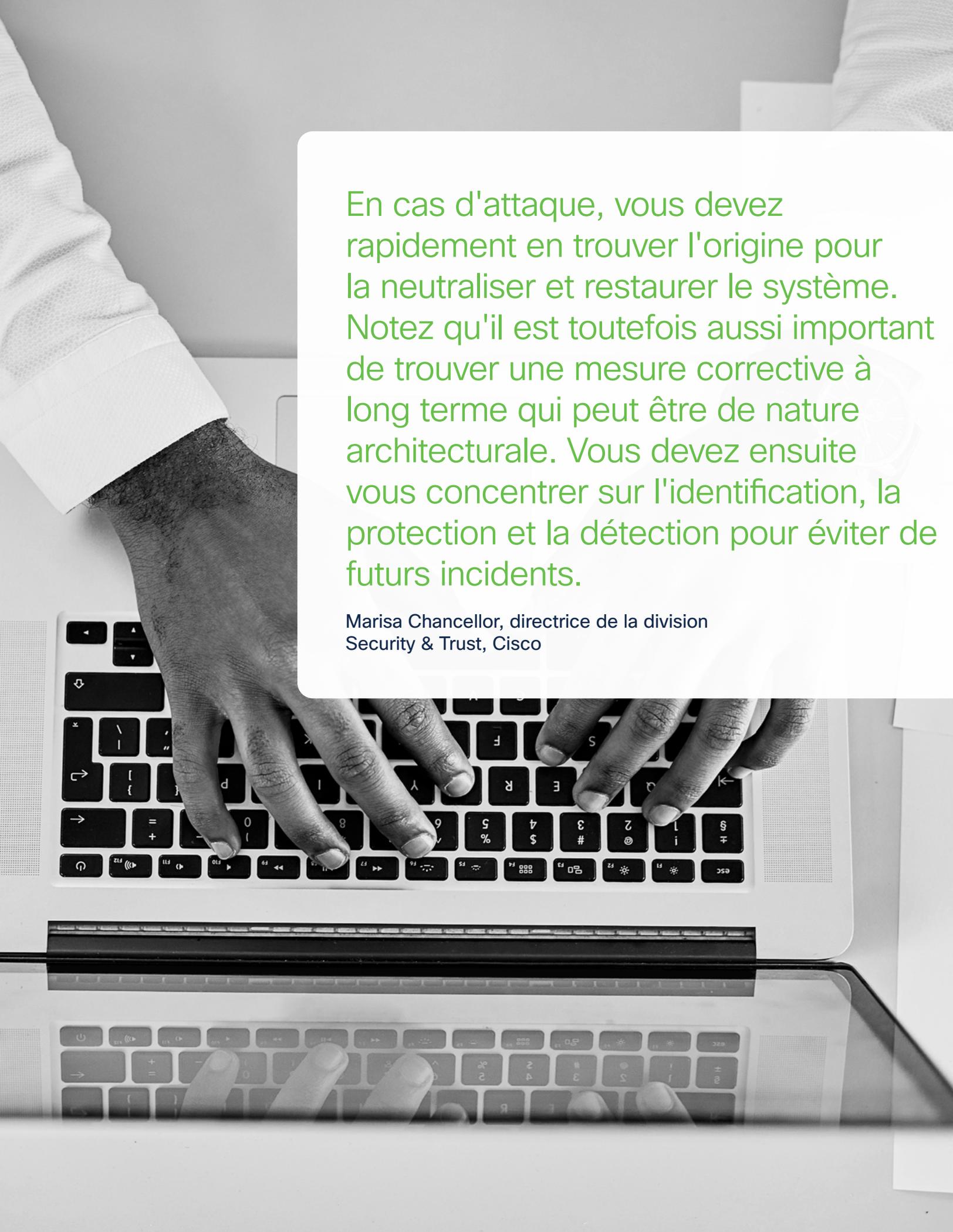
Pour la majorité des personnes interrogées, le budget pour la sécurité est alloué en fonction d'indicateurs et d'objectifs axés sur les résultats. 61 % d'entre elles utilisent cette méthode de planification, soit une augmentation de 10 % par rapport à l'année précédente, une tendance encourageante (Figure 2).

Figure 2 : Qu'utilisent les entreprises pour fixer et/ou contrôler les dépenses en matière de sécurité (N = 2 799). Les pourcentages sont arrondis.



Le « pourcentage de chiffre d'affaires » et les « coûts d'externalisation » sont les facteurs les moins pris en compte pour déterminer les budgets pour la sécurité. 54 % des décideurs établissent le budget en fonction de celui des années précédentes. Même si cette méthode ne permet pas de quantifier les coûts liés à la sécurité avec précision, notamment lorsque l'on sait que le coût moyen d'une violation de données à l'échelle mondiale (3,92 millions de dollars) est rarement pris en compte, si votre budget est stable d'une année sur l'autre ou si vous disposez d'abonnements SaaS prévisibles, il est peu probable que votre budget prévisionnel change beaucoup.³

³ [Rapport 2019 sur l'impact financier d'une faille](#), Ponemon Institute



En cas d'attaque, vous devez rapidement en trouver l'origine pour la neutraliser et restaurer le système. Notez qu'il est toutefois aussi important de trouver une mesure corrective à long terme qui peut être de nature architecturale. Vous devez ensuite vous concentrer sur l'identification, la protection et la détection pour éviter de futurs incidents.

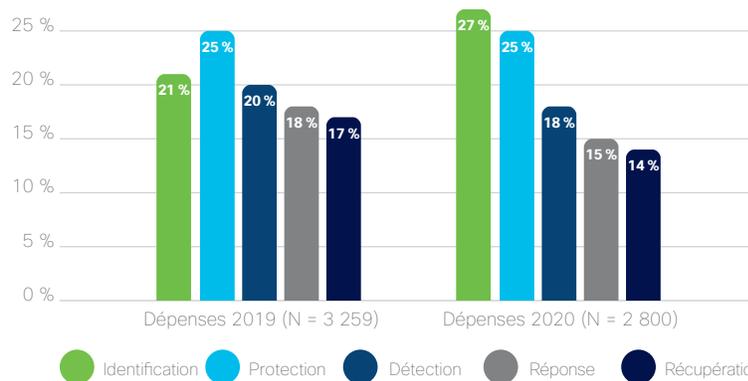
Marisa Chancellor, directrice de la division
Security & Trust, Cisco

4. Comment trouver le bon équilibre entre les dépenses pour la vérification de la fiabilité et pour la détection des menaces ?

Dans le cadre de l'analyse de l'utilisation des budgets pour la sécurité, nous avons interrogé les décideurs IT sur leurs dépenses dans cinq catégories (Identification, Protection, Détection, Réponse et Récupération) qui constituent le cycle de vie de la gestion des failles et de la cybersécurité :

- Dans la **catégorie Identification**, la part des dépenses est passée de 21 % à 27 % entre 2019 et 2020
- Dans les **catégories Protection et Détection**, les dépenses sont restées relativement stables, avec une part respective de 25 % et 18 %
- La part des dépenses **dans les catégories Réponse et Récupération** a quelque peu diminué au cours de la même période, représentant respectivement 15 % et 14 % du budget

Figure 3 : Dépenses de sécurité par catégorie du cycle de vie. Les pourcentages sont arrondis.



Source : Étude comparative RSSI Cisco 2020

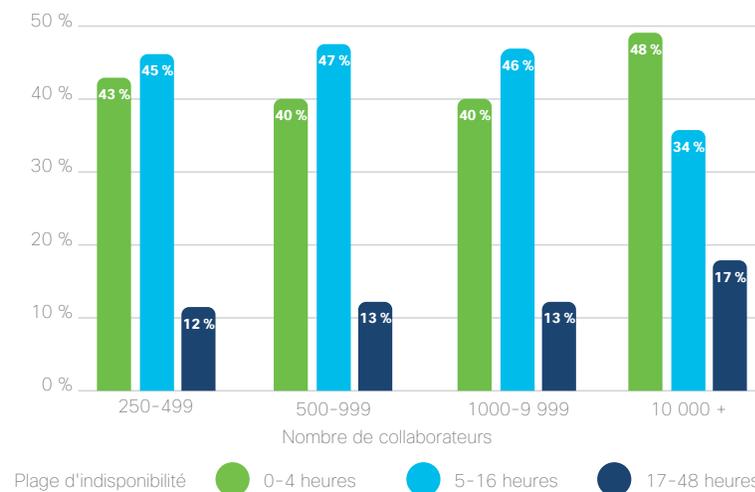
Cette tendance montre qu'en matière de cybersécurité, **les entreprises dépensent davantage pour la prévention que pour la réponse aux attaques**. Les entreprises essaient sans cesse de trouver le bon équilibre entre une attitude proactive et une attitude réactive et résiliente, et chaque année, la tendance s'inverse. L'an passé, les entreprises ont peut-être concentré leurs efforts sur les bases (inventaire des ressources, découverte, etc.). Et théoriquement, si vous dépensez en amont et de manière intelligente dans les catégories Identification, Protection et Détection, vous ne devriez pas avoir à dépenser autant dans les catégories Réponse et Récupération, car les besoins associés sont alors moins importants.

5. Que vous apprend l'analyse de l'impact des failles liées à la sécurité sur l'entreprise ?

Au cours de notre enquête, nous avons interrogé les décideurs IT sur les différents impacts des failles, comme les pannes, les données affectées et l'aspect financier.

Dans quelle mesure les entreprises subissent-elles des pannes en cas de failles majeures ? Nous avons comparé des entreprises de différentes tailles, et les résultats sont dans l'ensemble très similaires. Les grandes entreprises (10 000 employés ou plus) sont moins sujettes aux pannes (entre 0 et 4 heures), car elles ont généralement davantage de ressources disponibles pour neutraliser l'attaque et restaurer le système. Les PME sont les plus nombreuses à afficher un délai de récupération compris entre 5 et 16 heures, et les longues pannes (entre 17 et 48 heures) restent rares dans l'ensemble des entreprises, quelle que soit leur taille (Figure 4).

Figure 4 : Pour la faille de sécurité la plus grave gérée l'année passée, la durée d'indisponibilité des systèmes diminue en fonction de la taille de l'entreprise (N = 2 265). Les pourcentages sont arrondis.

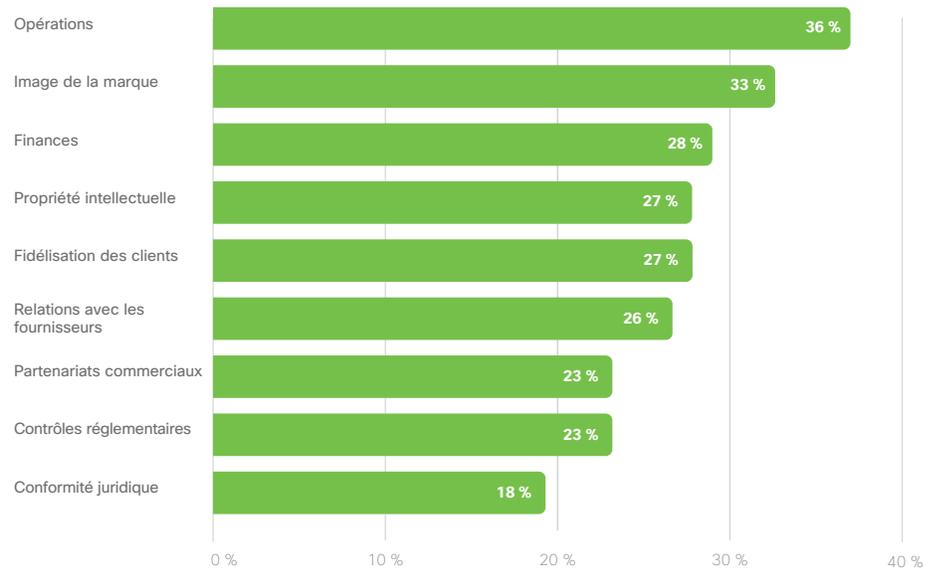


Source : Étude comparative RSSI Cisco 2020

Le pourcentage d'entreprises dont plus de 100 000 enregistrements ont été affectés par la violation de données la plus critique est passé de 15 % l'an dernier à plus de 19 % cette année.

De plus, comme le montre la Figure 5, une faille d'envergure peut avoir un impact sur neuf domaines stratégiques d'une entreprise. **Les domaines les plus touchés sont les opérations et la réputation de la marque**, suivis des finances, de la propriété intellectuelle et de la fidélisation des clients.

Figure 5 : Pourcentage de personnes interrogées citant les domaines d'activité affectés par une faille liée à la sécurité. (N = 2 121). Les pourcentages sont arrondis.



Source : Étude comparative RSSI Cisco 2020

En étudiant l'historique, nous constatons que le nombre de personnes interrogées qui ont constaté un impact sur la réputation de la marque suite à des failles **majeures est passé de 26 % à 33 % en trois ans**. Le pourcentage de compromission des opérations est resté stable (entre 36 % et 38 %). Le pourcentage de personnes ayant signalé un impact sur les finances n'a diminué que d'un point par an au cours des trois dernières années et reste donc également relativement stable. L'impact sur la marque étant de plus en plus important, **il est essentiel de planifier la communication de crise dans le plan global de gestion des incidents**.

6. Pourquoi la divulgation volontaire des failles atteint-elle un niveau record ?

Atteignant aujourd'hui 61 %, le pourcentage de personnes interrogées qui ont déclaré avoir volontairement révélé une faille l'an dernier n'a jamais été aussi élevé au cours des quatre dernières années. Cela montre que, dans l'ensemble, les entreprises signalent les failles de manière proactive, peut-être en raison de la nouvelle législation ou d'une prise de conscience accrue associée à l'envie de conserver la confiance des clients.

Le point positif, c'est que les entreprises victimes d'une attaque qui a duré plus de 17 heures ont été plus de deux fois plus nombreuses à divulguer la faille de leur plein gré, par rapport à celles qui l'ont divulgué involontairement ou en réponse aux exigences de reporting.

51 % des failles ont mis les entreprises sur la défensive et face à la méfiance du public. Toutefois, bien que les exigences gouvernementales en matière de reporting soient devenues plus strictes, le pourcentage d'attaques divulguées de manière involontaire reste relativement stable (27 %). **De plus, 61 % des personnes interrogées constatent aujourd'hui que leur crédibilité augmente lorsqu'elles révèlent volontairement une faille majeure, préservant ainsi la réputation de leur marque.**

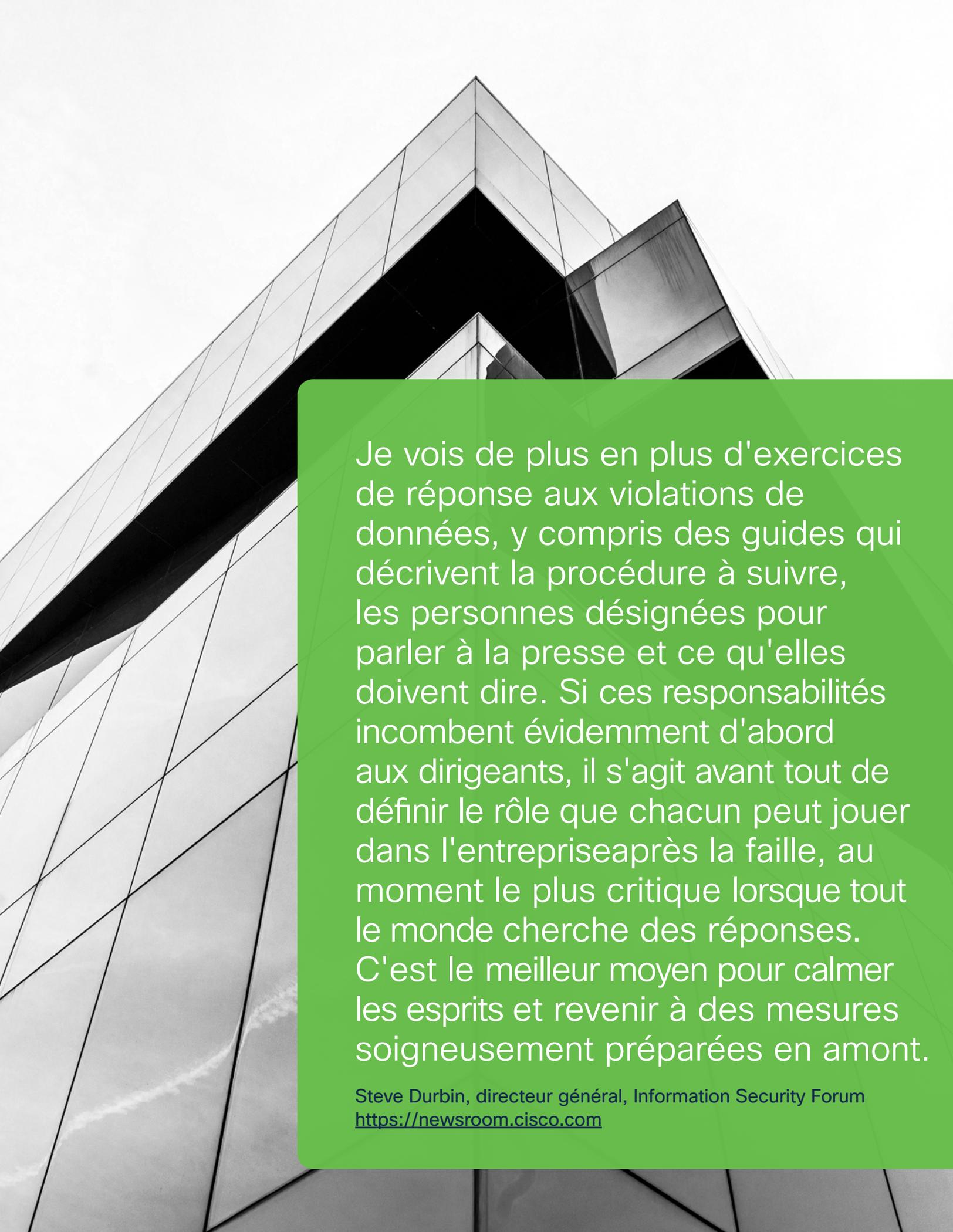
7. Est-il possible de quantifier les bénéfices de la collaboration entre les équipes responsables du réseau et de la sécurité ?

La collaboration entre les équipes **responsables du réseau et de la sécurité demeure élevée**, plus de 91 % des personnes interrogées déclarant cette année entretenir une collaboration très étroite ou extrêmement étroite. La collaboration entre les **équipes chargées de la gestion des terminaux et de la sécurité reste également élevée (87 %)**. Malgré une baisse de quelques points, les entreprises ont globalement tendance à moins travailler en silos.

8. Hormis la réduction des coûts, quelles sont les autres raisons qui justifient l'externalisation ?

Par rapport au rapport de l'an dernier, l'externalisation a progressé de façon significative, marquant peut-être une tendance historique à l'heure où la gestion des fournisseurs devient plus complexe que jamais en interne. Curieusement, les entreprises ont indiqué qu'elles prévoient un déclin de l'externalisation à l'avenir.

Les personnes interrogées dans le cadre de l'enquête font appel à des fournisseurs pour diverses raisons essentielles, et pas uniquement pour des questions d'argent. Si le rapport qualité-prix prend timidement la tête du classement (55 %), il est suivi de près par une plus grande réactivité aux incidents recherchée par les équipes responsables de la sécurité (53 %).



Je vois de plus en plus d'exercices de réponse aux violations de données, y compris des guides qui décrivent la procédure à suivre, les personnes désignées pour parler à la presse et ce qu'elles doivent dire. Si ces responsabilités incombent évidemment d'abord aux dirigeants, il s'agit avant tout de définir le rôle que chacun peut jouer dans l'entreprise après la faille, au moment le plus critique lorsque tout le monde cherche des réponses. C'est le meilleur moyen pour calmer les esprits et revenir à des mesures soigneusement préparées en amont.

Steve Durbin, directeur général, Information Security Forum
<https://newsroom.cisco.com>

9. La préparation offre-t-elle des résultats concrets ?

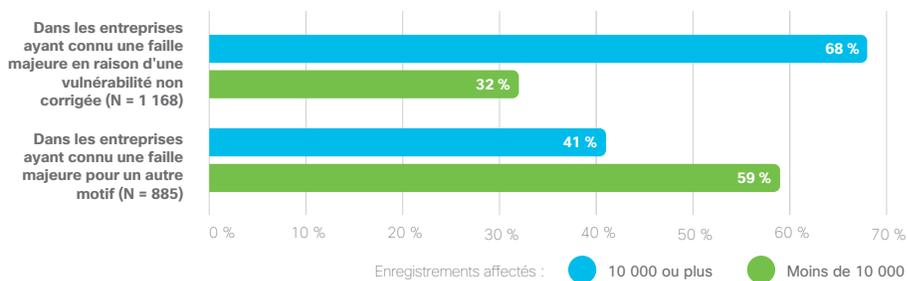
Lorsque nous leur avons demandé quelles pratiques ou politiques de sécurité étaient appliquées dans leur entreprise, nous avons constaté que **les professionnels qui suivent les pratiques listées ci-dessous perdaient souvent moins d'argent en cas de faille majeure**. En d'autres termes, si votre programme de sécurité respecte ces six principes, le coût des attaques dont vous êtes victime aura tendance à ne pas dépasser 100 000 \$.

- Nous révisons et améliorons nos pratiques liées à la sécurité de manière régulière, formelle et stratégique sur le long cours
- Nous vérifions régulièrement les connexions sur le réseau pour nous assurer que les mesures de sécurité fonctionnent comme prévu
- La sécurité est bien intégrée avec les objectifs et les processus de notre entreprise
- Nous recherchons systématiquement l'origine des incidents
- Nos technologies de sécurité sont bien intégrées et fonctionnent efficacement
- Nos dispositifs de détection et de blocage des menaces sont maintenus à jour

10. Quelle est l'importance du déploiement de correctifs dans la lutte contre les failles ?

L'une des principales préoccupations pour 2020 est que 46 % des entreprises (contre 30 % dans le rapport de l'année dernière) ont été victimes d'une attaque liée à une vulnérabilité non corrigée. De plus, **celles qui ont connu l'an dernier une faille majeure en raison d'une vulnérabilité non corrigée ont enregistré des pertes** de données plus conséquentes (Figure 6). Par exemple, 68 % des entreprises victimes d'une attaque liée à une vulnérabilité non corrigée ont perdu l'année dernière au moins 10 000 enregistrements de données. Parmi celles ayant indiqué avoir subi une faille pour d'autres motifs, seuls 41 % ont perdu 10 000 enregistrements ou plus au cours de la même période.

Figure 6 : Nous avons demandé aux sujets de notre enquête s'ils avaient été victimes au cours de l'année passée d'un incident lié à la sécurité résultant d'une vulnérabilité non corrigée ou d'autres causes, ainsi que le nombre d'enregistrements de données perdus (N = 2 053). Les pourcentages sont arrondis.



Source : Étude comparative RSSI Cisco 2020

Nous savons tous que l'application de correctifs peut être complexe et interrompre l'activité. Cependant, ces résultats montrent que la mise en œuvre d'une politique de base minimale pour l'installation des correctifs les plus récents offre un retour sur investissement concret. **Les entreprises doivent tenir à jour l'inventaire des équipements présents dans leur environnement et effectuer une analyse des risques pour les correctifs manquants. Elles doivent ensuite élaborer une procédure de gestion du changement pour assurer le contrôle et la documentation des versions.**

11. Quelles sont les causes des interruptions ?

Comme nous l'avons vu précédemment, les personnes que nous avons interrogées ont signalé plusieurs plages d'indisponibilité. Les malwares et les spams malveillants arrivent respectivement à la première et deuxième place des principales causes d'interruption. Il est intéressant de noter que la troisième cause varie selon la durée de la panne. Pour les incidents liés à la sécurité entraînant une indisponibilité comprise entre 0 et 4 heures, le phishing est la troisième cause la plus fréquente. Pour les interruptions comprises entre 4 et 24 heures, ce sont les logiciels espions. Pour toute interruption de plus de 24 heures, ce sont les [ransomwares](#).

Notez que les ransomwares ne font pas de distinction. Ils constituent la menace la plus dangereuse pour les PME et les grandes entreprises en matière de temps d'indisponibilité. Les longues périodes d'interruption qui en résultent peuvent s'expliquer par la complexité de l'enquête nécessaire pour évaluer les dommages, tenter de restaurer les sauvegardes et corriger les vecteurs d'entrée.

Pour découvrir comment faire face aux différents types d'attaques, abonnez-vous à notre [blog Talos Threat Intelligence](#).

12. À quel point est-ce difficile de protéger les collaborateurs mobiles ?

Nous avons demandé aux participants d'évaluer la difficulté de protéger certains aspects de leur infrastructure. **52 % nous ont confié que les terminaux mobiles étaient aujourd'hui très difficiles ou extrêmement difficiles à sécuriser.** Ils sont passés devant le comportement des utilisateurs, qui était le plus grand défi du rapport de l'année dernière.

Avec un [modèle zero-trust](#), vous pouvez identifier et contrôler chaque personne et périphérique qui tente d'accéder à votre infrastructure. Le zero-trust est une approche pragmatique et pérenne qui vous aide à protéger efficacement l'ensemble de votre architecture, des collaborateurs aux lieux de travail en passant par les workloads.

Un modèle zero-trust apporte de nombreux bénéfices, dont voici trois exemples :

- L'utilisateur est connu et authentifié
- L'appareil est contrôlé et jugé adéquat
- L'utilisateur a uniquement accès aux zones autorisées de votre environnement

Une approche zero-trust simplifie la protection de votre infrastructure, y compris les terminaux mobiles, face aux menaces potentielles.

13. Comment pourriez-vous étendre la sécurité zero-trust pour protéger les applications ?

Protéger les workloads consiste à sécuriser l'ensemble des connexions des utilisateurs et des équipements sur votre réseau. Une approche zero-trust permet d'identifier les dépendances au sein et à la périphérie des bases de données et des applications pour appliquer une micro-segmentation et limiter les mouvements latéraux.

41 % des entreprises interrogées trouvent les data centers très difficiles ou extrêmement difficiles à protéger, et 39 % déclarent éprouver de grandes difficultés à sécuriser les applications. L'aspect le plus problématique concerne les données stockées dans le cloud public, que 52 % des entreprises trouvent très difficiles ou extrêmement difficiles à protéger.

Un modèle zero-trust vous offre une visibilité sur l'activité de votre réseau et sur les points stratégiques en identifiant et en appliquant les politiques sur l'ensemble du réseau. Il assure également une surveillance continue et réagit aux indicateurs de compromission pour vous avertir en cas de violation d'une politique.



La Threat Intelligence vous aide à comprendre ce que risque votre entreprise en vous informant des menaces réelles qui pèsent sur elle. En mettant l'accent sur ces risques réels basés sur des faits, elle permet aux dirigeants d'entreprise de concentrer leurs ressources limitées sur les problèmes auxquels ils seront réellement confrontés.

Matt Watchinski, vice-président de l'ingénierie, Talos

14. Est-il encore difficile de protéger son infrastructure de réseau ?

L'infrastructure de cloud privé constitue un enjeu de sécurité de premier plan pour les entreprises. (50 % d'entre elles la trouvent très difficile ou extrêmement difficile à protéger.) 41 % des entreprises trouvent que l'infrastructure de réseau est très difficile ou extrêmement difficile à protéger.

Une approche zero-trust s'avère alors particulièrement adaptée. Elle assure un contrôle d'accès sous forme logicielle continu pour l'ensemble des connexions à vos applications et dans un environnement multicloud en tenant compte de l'utilisateur, de l'équipement et de l'application, et non de l'emplacement. Avec ce modèle, vous détectez et neutralisez les risques dans toute l'infrastructure, peu importe les paramètres de distribution ou l'emplacement. Vous trouverez ci-dessous les étapes du déploiement d'un cadre mature de sécurité zero-trust.

Développement d'un modèle mature de sécurité zero-trust

Chez Cisco, nous proposons à nos clients cinq étapes stratégiques pour mettre en œuvre un cadre **zero-trust** dans leur entreprise :

Étape 1 : Disposez-vous d'une stratégie claire de gestion des accès et des identités, alignée avec vos besoins métiers et qui a abouti à la mise en œuvre et à l'intégration complètes d'une solution d'authentification multifacteur basée sur des politiques axées sur les risques ?

Étape 2 : Disposez-vous d'un inventaire des ressources à jour qui distingue les équipements gérés de ceux non gérés avec une fonction intégrée de sécurité qui vérifie l'intégrité de ces équipements ?

Étape 3 : Disposez-vous d'une politique de vérification de la fiabilité pour les équipements qui invite les utilisateurs à mettre à jour leurs périphériques pour les protéger des vulnérabilités connues dans le cadre d'un processus géré, et qui signale les équipements non conformes ?

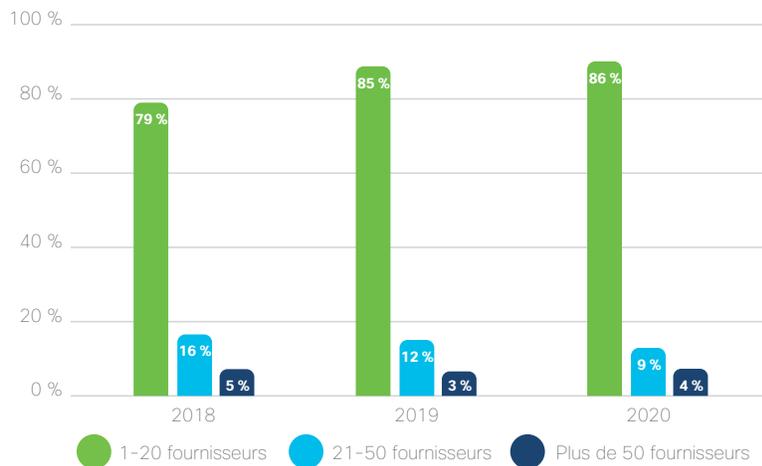
Étape 4 : Contrôlez-vous l'accès des utilisateurs via une politique gérée de manière centralisée qui identifie les exceptions et prend les mesures appropriées ?

Étape 5 : Disposez-vous d'une stratégie zero-trust alignée sur vos besoins métiers et soutenue par une architecture et un ensemble de processus qui permettent aux utilisateurs d'accéder de manière transparente aux applications cloud et sur site ?

15. Est-il possible de mesurer l'impact du regroupement des fournisseurs ?

La tendance à la simplification par le regroupement des fournisseurs se poursuit avec des chiffres stables : **86 % des entreprises utilisent entre 1 et 20 fournisseurs, tandis que seules 13 % en utilisent plus de 20** (Figure 7).

Figure 7 : Nombre de fournisseurs de solutions de sécurité différents (marques, fabricants) présents dans les environnements de sécurité des entreprises interrogées (N = 2 800). Les pourcentages sont arrondis.



Source : Étude comparative RSSI Cisco 2020

Depuis 2017, la manière dont les entreprises appréhendent leur stratégie multifournisseur a changé. **28 % d'entre elles trouvent aujourd'hui qu'il est très difficile de gérer un environnement multifournisseur, soit 8 % de plus qu'en 2017. 53 % trouvent que c'est quelque peu problématique.** Les entreprises sont également moins nombreuses (17 % contre 26 % auparavant) à trouver qu'il est facile de gérer un environnement multifournisseur. 81 % des entreprises estiment aujourd'hui que cette gestion est difficile. Cela peut signifier que vous avez moins de fournisseurs à gérer ou que vous avez commencé à utiliser des outils tels que les moteurs d'analyse pour améliorer les résultats de plusieurs outils disparates.

Nous avons également établi des parallèles entre les alertes reçues dans le cadre d'un environnement multifournisseur et leur impact sur l'épuisement lié à la gestion de la cybersécurité (dont nous allons parler plus en détail dans la rubrique suivante). **42 % des participants à l'étude déclarent souffrir d'un épuisement lié à la gestion de la cybersécurité, qui se traduit par l'arrêt des mesures proactives contre les hackers.**

Nos données montrent que les entreprises qui souffrent de cyberfatigue éprouvent généralement davantage de difficultés à gérer un environnement multifournisseur. Outre le trop grand nombre d'alertes à traiter et la gestion complexe des fournisseurs, nous avons constaté que les failles de sécurité majeures (en termes de nombre d'heures d'indisponibilité) favorisaient également la cyberfatigue. Plus de 96 % des professionnels souffrant d'épuisement affirment qu'il est difficile de gérer un environnement multifournisseur, ce qui **laisse à penser que la complexité est l'une des principales causes de burnout.**

Je ne veux pas passer mon temps à intégrer des produits de sécurité. Je veux juste assurer la sécurité de mon environnement.

Pour moi, trois principes de base doivent être appliqués à chaque nouveau produit :

- Vérifier son bon fonctionnement
- Vérifier qu'il offre une visibilité totale S'assurer de l'absence d'angle mort
- Vérifier qu'il est intégré avec le reste de notre écosystème de sécurité

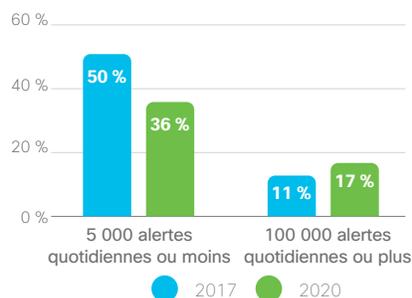
Steve Martino, vice-président, RSSI, Cisco

16. Quelles sont les causes de votre épuisement lié à la gestion de la cybersécurité ?

Dans la section précédente, nous avons commencé à établir un parallèle entre les environnements multifournisseurs et une cyberfatigue grandissante. Intéressons-nous maintenant au volume moyen d'alertes de sécurité que reçoit chaque jour une entreprise.

Le nombre total d'alertes que vous devez traiter au quotidien a augmenté par rapport aux années précédentes. En 2017, 50 % des entreprises recevaient au maximum 5 000 alertes quotidiennes ; aujourd'hui, elles ne sont que 36 % dans cette catégorie. De plus, le pourcentage d'entreprises recevant au moins 100 000 alertes par jour est passé de 11 % en 2017 à 17 % en 2020 (Figure 8).

Figure 8 : Nombre d'alertes reçues (N = 2 800). Les pourcentages sont arrondis.



Source : Étude comparative RSSI Cisco 2020

Il est possible que cette hausse du volume d'alertes et des ressources de traitement nécessaires explique pourquoi l'analyse des alertes est à son plus bas niveau depuis quatre ans (juste en dessous de 48 %). (Ce chiffre était de 56 % en 2017 et n'a cessé de diminuer depuis.) Le taux d'incidents légitimes (26 %) reste stable d'une année sur l'autre, ce qui laisse à penser que les analyses renvoient souvent de faux positifs.

Sur une note plus positive, le pourcentage de menaces légitimes neutralisées a augmenté depuis le rapport de l'année dernière pour revenir aux niveaux de 2017 (50 %). Cependant, cela signifie toujours que la moitié des incidents réels échappent à votre contrôle.

Le nombre impressionnant d'alertes a sans conteste un impact réel sur l'épuisement lié à la gestion de la cybersécurité. **Parmi les professionnels qui indiquent souffrir de cyberfatigue, 93 % reçoivent plus de 5 000 alertes par jour.**

Pour faire face à l'augmentation des faux positifs et du volume d'alertes, nous préconisons une approche basée sur l'automatisation. L'automatisation permet d'appliquer les politiques de manière plus cohérente, plus rapide et plus efficace. Lorsqu'un équipement est identifié comme infecté ou vulnérable, il est automatiquement mis en quarantaine ou interdit d'accès sans aucune intervention de l'administrateur.

17. Quels sont les bénéfices en matière de sécurité liés à l'hébergement de l'infrastructure dans le cloud ?

Dans le cadre de nos recherches, nous avons constaté que le gain d'efficacité et de visibilité était l'une des principales raisons pour lesquelles les entreprises choisissaient de migrer leur sécurité (88 %) et leur infrastructure (89 %) vers le cloud. De plus, sans surprise, **86 % d'entre elles indiquent que la sécurité cloud** leur offre une meilleure visibilité sur leurs réseaux. En 2020, plus de 83 % des entreprises gèrent plus de 20 % de leur infrastructure informatique dans le cloud (que ce soit en interne ou en externe).

Les clients font de plus en plus appel à des fournisseurs pour bénéficier d'une analyse plus poussée des incidents, et obtenir des données d'analyse avancées et des rapports d'investigation détaillés. Les fournisseurs de services de gestion des incidents doivent proposer des combinaisons de produits et de processus hautement spécialisés afin de réduire le délai moyen de confinement et le délai moyen de résolution d'un incident actif.

Guide du marché des services d'investigation numérique et de gestion des incidents, Gartner, décembre 2019⁴

⁴ Brian Reed, Toby Bussa, Guide du marché des services d'investigation numérique et de gestion des incidents, Gartner, 11 décembre 2019

18. Selon vous, quels défis l'avenir nous réserve-t-il ?

Malgré la multitude de changements d'infrastructure qu'elle implique et qui peuvent être difficiles à mettre en œuvre, la transformation numérique reste une opportunité concrète pour les responsables IT et de la sécurité d'innover et de renforcer leur compétitivité.

Les professionnels de la sécurité adoptent des technologies et des approches de pointe, de l'intelligence artificielle à l'apprentissage automatique, en passant par la mise en œuvre sécurisée de processus DevOps et la micro-segmentation. De plus, comme nous le savons tous, la popularité des environnements multicloud ne faiblit pas.

Face au dynamisme de ces environnements, les professionnels de la sécurité doivent non seulement maîtriser les bases de la sécurité, mais aussi se tenir au courant des dernières technologies disponibles. Certaines de ces nouvelles technologies devraient sans doute devenir des composants essentiels de votre écosystème de sécurité, même si elles n'en font actuellement pas partie.

Nous constatons par exemple qu'à l'ère de l'ubiquité numérique, **seules 27 % des entreprises utilisent à ce jour l'authentification multifacteur**. Ce pourcentage est faible pour une technologie zero-trust aussi efficace. Les taux d'adoption les plus élevés de l'authentification multifacteur ont été enregistrés dans les pays suivants, dans cet ordre précis : États-Unis, Chine, Italie, Inde, Allemagne et Royaume-Uni. Les secteurs d'activité affichant les taux d'adoption les plus élevés sont (dans cet ordre) le développement logiciel, les services financiers, l'administration publique, le commerce de détail, la fabrication et les télécommunications.

En matière de transformation numérique, l'automatisation remporte un très franc succès aux côtés de l'adoption des technologies du cloud. De nombreux professionnels de la sécurité découvrent les bénéfices de l'automatisation, notamment pour faire face à la pénurie de compétences, en adoptant des solutions qui offrent des fonctions avancées [d'apprentissage automatique et d'intelligence](#) artificielle.

Comme le montre la Figure 9, **77 % des participants à l'enquête prévoient de développer l'automatisation afin de simplifier et d'accélérer la gestion des incidents dans leurs écosystèmes de sécurité**. Au moment de planifier les processus d'automatisation, vous devez identifier de manière stratégique à quel poste l'automatisation sera la plus efficace et fournira le meilleur retour sur investissement pour votre entreprise.

Figure 9 : Personnes prévoyant de développer l'automatisation au sein de l'écosystème de sécurité de leur entreprise dans l'année à venir (N = 2 800). Les pourcentages sont arrondis.



Source : Étude comparative RSSI Cisco 2020

19. Quelle priorité devez-vous donner à la gestion des incidents ?

Le paysage des menaces a évolué et représente aujourd'hui un défi de taille pour les entreprises du monde entier. En raison d'une pénurie de talents et de l'augmentation du nombre d'incidents, la plupart des entreprises affichent un faible niveau de sécurité. En restant passives dans l'attente d'une alerte, les entreprises s'exposent à de lourdes amendes, à une surveillance accrue, à des pertes de propriété intellectuelle, à des soucis de [confidentialité des données et à une baisse d'activité](#). Pour protéger votre infrastructure, il est désormais essentiel d'adopter une attitude proactive en étendant votre visibilité, en partant à la chasse aux menaces et en déployant un cadre zero-trust.

Dans l'enquête que nous avons menée auprès de décideurs IT, **76 % ont indiqué être très à l'aise avec la gestion des incidents, et 23 % ont indiqué être plutôt à l'aise, ce qui représente au total 99 % des participants**. Le constat est rassurant. Mais comme notre enquête le révèle, la complexité de la sécurité provoque un épuisement lié à la gestion de la cybersécurité, ce qui peut mettre à rude épreuve vos ressources si précieuses. L'externalisation a ici un rôle important à jouer.

Figure 10 : Pourcentage de participants qui sont très à l'aise ou plutôt à l'aise avec la gestion des incidents (99 % au total). N = 2 800. Les pourcentages sont arrondis.



Selon les résultats de l'étude, 34 % des professionnels de la sécurité externalisent les services de gestion des incidents, et 36 % utilisent des services externes ou tiers pour analyser les systèmes compromis, un chiffre en hausse par rapport à l'année dernière. Faire appel à un service de gestion des incidents s'avère aujourd'hui efficace pour protéger ses ressources, réduire les risques et assurer la conformité. Un tel service peut aider votre entreprise à se protéger des menaces inconnues grâce à une planification proactive et au savoir-faire d'experts pour coordonner et apporter une réponse en cas d'attaque.

[Vous souhaitez savoir comment développer vos compétences en cybersécurité ou celles de votre équipe ?](#)

[Accédez à la page : Certifications de sécurité Cisco.](#)

20. Que pouvez-vous faire aujourd'hui pour renforcer votre sécurité ?

Vous êtes face à des hackers virulents qui ont beaucoup de moyens et une patience à toute épreuve. Vous devez également relever des défis récurrents, comme tenir à jour un inventaire précis des utilisateurs, des applications et des équipements. Vous jonglez entre les risques métiers et les risques liés à la sécurité tout en donnant aux équipes les moyens d'agir rapidement. Pourtant, l'entreprise continue de prendre des décisions sans tenir compte de la sécurité. Et lorsque vous ajoutez les nouvelles réglementations, les exigences du conseil d'administration, les budgets serrés, la gestion des risques et le chassé-croisé des experts en sécurité, la situation devient vite ingérable.

Les défis que vous devez surmonter pour protéger votre entreprise prennent toujours plus d'ampleur, et ce n'est pas prêt de s'arrêter. Il est temps de travailler plus intelligemment, de rationaliser votre stratégie de défense et de vous concentrer sur la prévention, ainsi que sur la détection et la neutralisation des menaces. Dans ce rapport, nous avons répondu à 20 questions pour vous aider à mieux protéger votre entreprise. Nous vous avons fourni un certain nombre de recommandations, dont voici un résumé :

- Mettez en place plusieurs couches de défense incluant l'authentification multifacteur, la segmentation du réseau et la protection des terminaux.
- Étendez au maximum votre visibilité pour renforcer la gouvernance des données, réduire les risques et accroître la conformité.
- Renforcez vos systèmes de défense, mettez à jour les équipements, appliquez les correctifs nécessaires et concentrez-vous sur l'intégrité informatique en développant vos compétences et en suivant des formations.
- Améliorez la maturité de votre infrastructure de sécurité en établissant un cadre zero-trust (Figure 13).

Figure 11 : Une stratégie zero-trust protège les collaborateurs, les workloads et les lieux de travail.



Chez Cisco, nous pensons qu'il est temps que le secteur de la sécurité évolue. Les solutions de sécurité doivent fonctionner comme une équipe. Les membres d'une équipe communiquent en temps réel, apprennent les uns des autres et réagissent comme une entité unique et coordonnée. Vos outils de sécurité des terminaux doivent collaborer avec vos outils de sécurité du réseau et du cloud. Vous avez également besoin d'une solution d'authentification multifacteur pour gérer les identités et les accès. **Nous avons la conviction que la meilleure façon de protéger une entreprise est d'adopter une plate-forme de sécurité capable de palier toutes les vulnérabilités.**

En France, des RSSI plus stratégiques qu'opérationnels ?

Les RSSI de France sont toujours à la manœuvre quant aux initiatives en matière de cyber sécurité. 74% d'entre eux affirment que leur périmètre d'action, et leurs connaissances des politiques et des pratiques de sécurité couvrent l'ensemble des organisations de l'entreprise. C'est 4 points de plus que la moyenne EMEA (70%), et 3 points de plus que la moyenne mondiale (71%).

Paradoxalement, moins de la moitié (45%) pense avoir l'autorité finale quant au choix des pratiques et des politiques de sécurité et seuls 63% se déclarent impliqués dans l'approbation des budgets, soit 4 points de moins que la moyenne EMEA (67%). 28% des déclarants français restent plutôt convaincus de diriger ces réflexions et d'influer plus que quiconque sur les pratiques et politiques de sécurité de l'entreprise - soit près de 10 points de plus que la moyenne européenne.

Leur connaissance de l'écosystème et des solutions n'est pas en cause puisque 74% de nos RSSI déclarent participer aux recommandations en matière de choix de solutions et de vendeurs. Et si seulement un peu plus de la moitié (52%) déclare avoir autorité quant au choix des solutions et services de sécurité, près d'un RSSI sur trois (30%) pense directement influencer sur ces décisions d'achats - soit 8 points de plus que la moyenne européenne.

Nos RSSI seraient-ils devenus plus influenceurs que décisionnaires ? Et cela pourrait-il s'expliquer par une nouvelle démographie des RSSI ? A en croire notre dernière enquête, plus d'un tiers des répondants français ont moins de 35 ans (39%), soit 3 points de plus que la moyenne déclarée sur la zone EMEA. Mais le raccourci resterait sans fondement puisque les RSSI d'Allemagne, dont 42% ont entre 25 et 34 ans, déclarent eux être impliqués dans l'approbation des budgets (77%) et avoir autorité tant le choix des politiques de sécurité (55%) que sur le choix des vendeurs, et des solutions et services (62%).

RSSI en France : plus d'innovations, moins d'opérations ?

Bien que toujours à la manœuvre, les RSSI de France sont impliqués sur des sujets vastes, parfois transverses appelant à plus de réflexion et d'innovation. Près de la moitié des RSSI de l'hexagone (48%) déclarent avoir consacré au maximum 60% de leur temps à des tâches ou problèmes liés à la sécurité au cours des 12 derniers mois. Soit 6 points de plus que la moyenne sur la zone EMEA, qui, elle, voit 36% de ses RSSI consacrer jusqu'à 80% de leur temps à des tâches de sécurité, quand la France en affiche 7% de moins (29%).

Quand on leur demande les domaines technologiques dont ils sont responsables au sein de leur organisation, « seuls » 87% mentionnent la sécurité informatique, la sécurité de l'information, la sécurité du cloud ou la cyber sécurité. C'est 4 points de moins que la moyenne EMEA (91%), et 5 points de moins que la moyenne mondiale (92%). A l'inverse, 70% des répondants français mentionnent l'infrastructure réseau telle que routeurs ou commutateurs, soit 2 points de plus que la moyenne EMEA.

Cela s'analyse surtout à l'aune des pratiques d'autres sujets technologiques, qui mobilisent les RSSI français plus qu'ailleurs en Europe, tels que le Machine Learning ou l'intelligence artificielle. Une intelligence artificielle appelée comme recours afin de faciliter les opérations de sécurité et de réduire le niveau d'effort des équipes : 55% des répondants de France indiquent que plus de la moitié de leurs processus de sécurité est assistée par une forme d'intelligence artificielle. C'est 6 points de plus que la moyenne mondiale (49%), et 10 points de plus que la moyenne sur la zone EMEA (45%). Quant au Machine Learning, il permet l'identification des équipements par étude de leur modèle comportemental pour 62% des répondants français, conférant à la France 5 points d'avance par rapport à la moyenne EMEA.

Les environnements industriels ne sont pas en reste puisque 61% des RSSI français déclarent être responsables de la sécurité des environnements OT, plaçant la France bien au-dessus de la moyenne EMEA (53%) et de la moyenne mondiale (51%). Cela se faisant au détriment des Services de Sécurité externalisés qui assurent globalement la gestion des environnements OT en Europe (18% sur la zone EMEA, contre 10% seulement en France). Des services managés loin d'être boudés par nos RSSI puisque 59% d'entre eux déclarent se reposer un tiers pour gérer intégralement de 20 à 60% de leur sécurité. C'est 6 points de plus que la moyenne de la zone EMEA (53%).

Prévenir plutôt que guérir ?

Sans doute faut-il aussi rapprocher ces comportements des éléments sur lesquels les RSSI de France reposent pour déterminer et/ou contrôler leurs dépenses : la cyberassurance à 60% (soit 6 points de plus que la zone EMEA, et 10 points de plus qu'en Amériques) ou l'analyse des objectifs ou des mesures de leurs résultats (61%). Des dépenses qui restent stratégiques et non liées au chiffre d'affaires, puisque seuls 42% des répondants déclarent intégrer cet élément dans la détermination des budgets, soit 7 points de moins que la moyenne mondiale.

En matière d'objectifs, les RSSI répondants portent un intérêt renforcé au délai de détection et au délai de correction et ce faisant se rapprochent plus de leurs collègues américains qu'euro-péens. 62% de nos RSSI placent le délai de détection

comme indicateur clé, et 56% d'entre eux le délai de correction, soit respectivement +4 points et +6 points que la moyenne sur la zone EMEA qui reste inférieure à la moyenne mondiale sur ces deux indicateurs. Les délais de correction (60%) et de résolution (61%) étant les deux indicateurs les plus utilisés pour signaler et mesurer l'impact d'une violation significative aux instances dirigeantes ou conseils d'administration. C'est 11 points de plus que la moyenne sur la zone EMEA pour le simple délai de correction.

Cyber assurance, délais de détection et de correction ... Les RSSI de France répondants semblent plus enclins à vouloir prendre les devants et se positionner en amont des menaces. Si la majorité des participants à l'enquête déclare réaliser un test une fois tous les 6 mois, nos RSSI de France confirment cette tendance avec 4 points de plus que la moyenne sur la zone EMEA (51% contre 47%) et réussissent même à se hisser 2 points au-dessus de la moyenne mondiale (49%). Des RSSI français également plus pédagogues puisque 68% d'entre eux estiment cultiver une sensibilisation à la cyber sécurité auprès des plus hautes instances de l'entreprise. Soit 9 points de plus que la moyenne européenne, et 6 points de plus que la moyenne mondiale.

Cela a une conséquence directe sur les dépenses d'outsourcing ou l'appel à des tiers pour la gestion des services de sécurité. Plus en amont sur la compréhension et la recherche des menaces, les RSSI français répondants déclarent faire appel à l'outsourcing plus pour des services de surveillance (42%) ou de résolution (39%) - soit respectivement +4 points et +8 points par rapport à la moyenne sur la zone EMEA - que, par exemple, la Threat Intelligence (34%, -3 points par rapport à la zone EMEA). Et l'appel à ces services externalisés ou à l'outsourcing ne repose pas tant sur la recherche de résultats rapides que sur le manque de ressources et d'expertise interne : respectivement 37% et 35%, soit +4% et +5% par rapport à la moyenne EMEA. L'automatisation devient donc une piste particulièrement intéressante dont la progression devra être suivie l'année prochaine.

En France, des RSSI trop sévères avec eux-mêmes ?

Hormis la protection des installations informatiques considérées comme bien protégées à 58%, soit +8 points par rapport à la moyenne de la zone EMEA, tous les indicateurs qualitatifs permettant aux équipes de sécurité d'apprécier leur travail sont en dessous de la moyenne européenne. Qu'il s'agisse de la bonne gestion des contrôles de sécurité des systèmes et réseaux : moins de la moitié des répondants pense pouvoir l'appliquer à leur entreprise - 48%, - 6 points par rapport à la moyenne sur la zone EMEA. Pareil pour la pertinence des droits d'accès aux réseaux, systèmes et applications (46%, -6 points) ou simplement affirmer faire du bon travail dans l'intégration des problématiques de sécurité aux systèmes et applications (46%, - 6 points).

Pourtant les résultats de nos RSSI sont très positifs qu'ils soient qualitatifs ou quantitatifs.

En matière d'incidents, au cours des 12 derniers mois, les RSSI de France auraient eu à gérer moins d'attaques de type Phishing (29%), Ransomware (21%) ou d'attaques DDos (16%), soit respectivement - 7 points, - 2 points et - 8 points par rapport à la moyenne sur la zone EMEA ; mais plus de failles liées à l'utilisateur comme un partage de fichier impropre (24%) ou des identifiants volés (23%). Peu étonnant donc que les RSSI français répondants placent la prolifération du BYOD et des smart devices dans le top 3 des menaces (30%, 7 points de plus que la moyenne européenne), au même niveau que le Ransomware. Selon notre enquête,

les RSSI de France s'attendent à une exposition plus sévère de leur entreprise à un partage impropre de fichier (25%, 6 points de plus que la moyenne sur la zone EMEA) quand les menaces liées au Phishing (30%) et Ransomware (23%) restent, elles, en dessous de la moyenne européenne (respectivement -5% et -4%).

Il existe, entre autres, trois moyens de valider quantitativement la gravité des violations de sécurité : les temps d'arrêts des systèmes, le nombre de données/d'archives impactées, et l'impact financier. Sur ces trois éléments, les RSSI de France montrent un certain succès.

- A la question « combien de temps les systèmes ont-ils été arrêtés en raison d'une violation de sécurité », les RSSI français répondants déclarent des périodes de pannes plus courtes : 63% entre 1 heure et 8 heures contre 53% pour la moyenne sur la zone EMEA, et 24% au-delà de 8 heures (6 points de moins que la zone EMEA à 30%).

- Le nombre d'archives impactées par l'attaque la plus significative des 12 derniers mois reste en dessous de 1000 pour 24% des RSSI répondants en France, +8 points par rapport à la moyenne sur la zone EMEA (16%).

- Enfin, l'impact financier lié à la faille de sécurité la plus significative au cours des 12 derniers mois se chiffre à moins de 100 000 dollars pour 39% des répondants en France, soit 10 points de plus que la moyenne EMEA (29%) pour cette première tranche.

Paradoxalement, avec des RSSI à la manœuvre sur les problèmes de sécurité étendus, la consolidation du nombre de vendeurs est moins flagrante en France qu'ailleurs en Europe et sur la zone MEA. Seuls 33% des RSSI répondants en France déclarent travailler avec 2/5 vendeurs (5 points de moins qu'en Europe), alors que 54% déclarent travailler avec entre 6 et 20 vendeurs (10 points de plus que la moyenne européenne). Ramenés au nombre de solutions : seuls 15% déclarent travailler avec moins de 6 produits (soit 5 points de moins que la moyenne sur la zone EMEA), quand 22% des répondants déclarent travailler avec entre 26 et 50 produits - 5 points de plus que la moyenne EMEA. Ceci expliquant sans doute pourquoi le nombre d'alerte constatées semble supérieur avec une fourchette de 100 001 à 500 000 alertes déclarées par jour pour 13% des répondants, soit 7 points de plus que la moyenne européenne. La simplification et l'intégration de l'ensemble des solutions de sécurité deviennent donc un enjeu clé pour les RSSI de France cette année. Et le récent lancement de Cisco SecureX est justement là pour y répondre.

Se protéger aujourd'hui et demain

Notre but est de protéger nos clients contre les menaces actuelles et futures afin qu'ils puissent se concentrer sur leur cœur de métier en nous confiant leur sécurité.

Nous vous proposons aujourd'hui la plate-forme de sécurité Cisco [SecureX](#) qui a été développée par les meilleurs experts en sécurité au monde et qui vous apporte une protection adaptée aux besoins spécifiques de votre entreprise.

- Nous fournissons en premier lieu des **solutions de pointe** pour sécuriser le réseau, les terminaux, les applications et le cloud.
- Nous utilisons ensuite la **vérification de la fiabilité** pour garantir que seules les personnes autorisées ont accès à votre réseau.
- Chaque produit intègre les services de [Threat Intelligence de l'équipe Talos](#) pour bloquer davantage de menaces et mieux protéger votre entreprise.
- Nous proposons **des réponses automatisées aux menaces avancées** et **simplifions les opérations grâce à une gestion intégrée des menaces et de la sécurité** sur l'ensemble de notre gamme.
- **Nous concevons nos produits de manière à ce qu'ils s'intègrent avec les différentes technologies que vous utilisez, même autres que Cisco**, afin de mettre en place une sécurité intégrée.

SecureX renforce la visibilité, l'automatisation et la sécurité. Des applications cloud sur mesure ont également été intégrées à la **plate-forme SecureX** pour simplifier la sécurité. Nous regroupons les solutions de sécurité intégrée de Cisco et les produits tiers de l'environnement client au sein d'une interface cohérente. De plus, grâce aux innovations de Cisco en matière de plate-forme, vous bénéficiez des fonctions d'analyse les plus intégrées au monde. Tout fonctionne de concert :

- [SecureX](#) regroupe les équipes en charge des opérations IT, du réseau et de la sécurité autour de workflows collaboratifs pour améliorer la productivité.
- [Cisco Threat Response](#) simplifie l'analyse et la remédiation des menaces pour accroître l'efficacité des équipes chargées de la sécurité.
- [Les analyses](#) simplifient la détection des menaces inconnues afin d'optimiser les décisions en matière de politique, de réduire les délais de réponse et d'éliminer plus efficacement les menaces.

Grâce à sa gamme de solutions intégrées et à sa Threat Intelligence de pointe, Cisco offre le champ d'application, l'évolutivité et les fonctionnalités pour s'adapter à la complexité et au volume des menaces. En donnant la priorité à la sécurité, vous pouvez innover tout en préservant vos ressources. Chez Cisco, la sécurité prime dans toutes nos activités et nous sommes les seuls à vous offrir une sécurité réseau performante capable de faire face aux menaces de demain. Pour en savoir plus sur notre approche basée sur une plate-forme, rendez-vous sur cisco.com/go/security.

À propos de la série de rapports Cisco sur la cybersécurité

Au cours des 10 dernières années, Cisco a publié de très nombreuses informations concrètes sur les menaces et la sécurité à l'attention des professionnels intéressés par l'état de la cybersécurité au niveau mondial. Ces rapports complets présentent en détail le paysage des menaces et leurs implications pour les entreprises, ainsi que les bonnes pratiques pour se protéger contre les répercussions négatives des violations de données.

Cisco Security publie aujourd'hui une série d'articles basés sur des données et des recherches : les rapports Cisco sur la cybersécurité. Nous avons étendu le nombre de titres pour inclure différents rapports destinés aux professionnels de la sécurité ayant des intérêts variés. Cette série annuelle de rapports s'appuie sur l'expertise de chercheurs et d'innovateurs du secteur de la sécurité. Elle comprend une étude comparative de la confidentialité des données, un rapport sur les menaces et une étude comparative des RSSI. D'autres suivront tout au long de l'année.

Pour plus d'informations et pour accéder à tous les rapports et copies archivées, rendez-vous sur www.cisco.com/go/securityreports.



Confidentialité des données 2019



Rapport 2019 sur les menaces



Étude comparative sur les RSSI 2019



E-mail : attention avant de cliquer



Le seuil de sécurité



La recherche des menaces



Enquête sur la confidentialité des données des consommateurs



Les menaces de l'année 2019



Confidentialité des données 2020



Étude comparative sur les RSSI 2020

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

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

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

Cisco compte plus de 200 agences à travers le monde. Les adresses, numéros de téléphone et numéros de fax sont répertoriés sur le site web de Cisco, à l'adresse www.cisco.com/go/offices.

Publié en février 2020

CISO_02_0220

© 2020 Cisco et/ou ses filiales. Tous droits réservés.

Cisco et le logo Cisco sont des marques commerciales ou déposées de Cisco et/ou de ses filiales aux États-Unis et dans d'autres pays. Pour voir la liste des marques commerciales de Cisco, rendez-vous sur : www.cisco.com/go/trademarks. Les autres marques commerciales mentionnées dans ce document sont la propriété de leurs détenteurs respectifs. L'utilisation du terme « partenaire » n'implique pas de relation de partenariat entre Cisco et toute autre entreprise. (1876404)

 **Secure**