Rapport pour les RSSI

Les dernières tendances, menaces et stratégies
que les responsables de la sécurité doivent connaître

splunk>

Résumé

Splunk est au cœur des opérations de sécurité de nombreuses organisations, dont certaines comptent parmi les plus grandes et complexes au monde. Nous passons nos journées à aider les RSSI et leurs équipes à anticiper les menaces émergentes, à réagir rapidement lorsque des incidents surviennent inévitablement et à réussir en tant que catalyseurs de l'entreprise. Mais nous nous sommes posé une question : quel est le point de vue des leaders de la sécurité sur l'IA ? Notre hypothèse selon laquelle les RSSI deviendraient des membres clés de la direction est-elle vraie ? Les conseils d'administration et les RSSI parlent-ils le même langage ?

Dans le Rapport pour les RSSI, nous présentons les résultats de nos recherches originales et des éclairages sur la manière dont les dirigeants peuvent évoluer avec le paysage de la cybersécurité. Voici une sélection des points clés à retenir.

1. Qu'on l'aime ou qu'on la déteste, l'IA est là pour rester

70 % des RSSI pensent que l'IA donne l'avantage aux attaquants sur les défenseurs, mais 35 % l'expérimentent déjà pour la cyberdéfense. Ils l'utilisent notamment pour l'analyse des logiciels malveillants, l'automatisation des workflows et l'évaluation des risques. Mais l'évolution n'a pas attendu l'IA : 93 % des RSSI ont automatisé leurs processus à un degré modéré ou étendu, et l'IA ne fera qu'augmenter ce pourcentage à l'avenir.

2. Les RSSI parlent souvent un langage différent de celui de leur conseil d'administration

Même si les priorités des RSSI et du reste de la direction convergent, un décalage persiste. 84 % des RSSI affirment que leur conseil d'administration ou leur organe directeur se soucie davantage de la conformité réglementaire que des bonnes pratiques de sécurité. Ils sont 31 % à affirmer que des projets ont été retardés en raison d'un manque de financement, et 30 % à dire que l'équipe de sécurité n'a pas été en mesure de soutenir une initiative commerciale.

3. Les RSSI font désormais partie intégrante de la direction

En effet, 47 % des RSSI ont désormais leur PDG comme superviseur direct. Les conseils d'administration jouent un rôle plus actif dans la sécurité. On demande aux RSSI de justifier leurs investissements, mais ce n'est pas une mauvaise chose. C'est le signe que leurs dirigeants sont à l'écoute et qu'ils n'hésitent pas à allouer des budgets supplémentaires pour l'année à venir (même s'ils ne sont toujours pas suffisants).

4. La plupart paient les rançons demandées en cas de ransomware

90 % des RSSI déclarent que leur organisation a subi au moins une attaque majeure au cours de l'année passée. Plus choquant encore, 83 % d'entre eux ont payé à la suite d'une attaque par ransomware, que ce soit directement, via une cyberassurance ou avec un négociateur. Et dans plus de la moitié des cas, la rançon dépassait les 100 000 $.

5. Les directions donnent la priorité au financement de la sécurité

Les RSSI interrogés sont 93 % à prévoir une augmentation de leur budget de cybersécurité au cours de l'année prochaine, mais 83 % d'entre eux observent des réductions dans d'autres secteurs de leur organisation. Les défis économiques ont un impact sur la sécurité, mais pas forcément comme on pourrait l'imaginer : en effet, 90 % déclarent que leur organisation est confrontée à un nombre croissant de menaces qui coïncident avec le déclin de l'économie.

6. Il n'y a pas de résilience sans collaboration

C'est avec les opérations IT que la collaboration est la plus intense en matière de cybersécurité, sans doute parce que ces intégrations sont plus établies. Cette collaboration est qualifiée de bonne par 36 % des personnes interrogées, et 40 % disent qu'elle est bonne, mais peut être améliorée. Les RSSI considèrent également les collaborations avec l'ingénierie logicielle/le développement d'applications (42 %), l'équipe cloud (40 %) et l'architecture d'entreprise (27 %) comme essentielles pour garantir la résilience de toute l'organisation.

À propos des auteurs

Ryan Kovar

Stratège en sécurité et Directeur de l'équipe SURGe

Ryan est Stratège en sécurité et directeur de l'équipe SURGe, la branche de recherche en sécurité de Splunk. Avec plus de 20 ans d'expérience en tant qu'analyste de sécurité, chasseur de menaces, défenseur et plombier Unix, Ryan adore parcourir le monde en quête des plus gros problèmes des clients de Splunk. Avant de rejoindre Splunk, il a travaillé pour la DARPA, l'US Navy, le ministère de l'Intérieur du Royaume-Uni et d'autres organisations en tant que professionnel et décideur en sécurité. Ryan est titulaire d'un MSc en cybersécurité de l'université de Westminster.

Kirsty Paine

Directrice technique et Conseillère stratégique, Technologie et innovation (EMEA)

Kirsty Paine (elle) est Conseillère stratégique auprès des clients Spunk. En tant que technologue expérimentée, stratège et spécialiste de la sécurité, elle s'épanouit face aux problèmes difficiles et dans la recherche de solutions créatives. L'expérience de Kirsty en cybersécurité découle de son parcours en mathématiques et s'est accumulée au fil des ans en travaillant au Centre national de cybersécurité du Royaume-Uni, où elle était spécialisée dans la sécurité, la confidentialité et les technologies Internet.

Les RSSI d'aujourd'hui : en première ligne du changement

Le rôle des responsables de la sécurité des systèmes informatiques (RSSI) d'aujourd'hui est complexe et évolue rapidement. 86 % déclarent que leur rôle a tellement changé depuis qu'ils sont devenus RSSI que c'est quasiment un autre poste. Ils deviennent des stratèges et des leaders et ont davantage voix au chapitre au sein du conseil d'administration. Et ils sont de plus en plus nombreux – 47 % aujourd'hui – à relever directement de leur PDG.

Bien entendu, leurs priorités absolues restent la défense de l'organisation contre un paysage de menaces de plus en plus complexe. Rappelons que 90 % des RSSI ont été confrontés à une attaque majeure au cours de l'année dernière. Et même s'ils s'adaptent pour garder une longueur d'avance sur leurs adversaires, ils ne dorment pas beaucoup la nuit.

L'histoire des RSSI est donc celle d'une lutte constante pour permettre à l'entreprise d'aller vite, toujours sur la corde raide entre des priorités souvent concurrentes : les KPI métier de l'entreprise, scrutés en permanence par le conseil d'administration, et les réalités pratiques de la sécurisation de l'organisation. Pour beaucoup d'entre eux, cela implique de justifier constamment la valeur de leurs équipes auprès de la direction et du conseil d'administration, tout en comblant les lacunes de sécurité causées par le manque de personnel et en trouvant de nouveaux moyens d'atténuer les risques organisationnels. Ce numéro d'équilibriste n'a rien de facile.

L'étude offre une image complète du rôle des RSSI : leurs problèmes, leurs défis et les opportunités auxquels ils sont confrontés au quotidien. Pourtant, malgré un paysage de menaces de plus en plus sophistiqué et des perspectives économiques incertaines, nombreux sont ceux qui restent optimistes. Plus que jamais, ils ont l'occasion de devenir des ambassadeurs capables de transformer la culture de sécurité de leur entreprise. Non seulement les conseils d'administration et les PDG les écoutent, mais ils leur demandent conseil. Les RSSI envisagent un avenir axé sur la collaboration avec les équipes de toute leur organisation dans un objectif commun d'accroître la résilience de l'organisation, afin qu'elle puisse non seulement traverser les tempêtes, mais aussi prospérer dans leurs retombées.

L’IA générative produit de précieuses informations

« Nous essayons de garder une longueur d’avance sur l’IA générative. »

– RSSI, organisation gouvernementale

Nous avons constaté qu'une grande majorité des RSSI (70 %) estime que l'IA générative va introduire sur le champ de bataille une asymétrie qui penchera inévitablement en faveur des cyberadversaires. Nous sommes toutefois plus optimistes. Nous savons que 35 % des RSSI utilisent déjà l'IA pour des applications de sécurité positives, et 61 % comptent l'utiliser au cours des 12 prochains mois.

Comme on pouvait s'y attendre, les RSSI pensent que les usages malveillants de l'IA concerneront avant tout l'accélération et l'optimisation des attaques (36 %), les usurpations d'identité (voix et images) à des fins d'ingénierie sociale (36 %) et l'extension de la surface d'attaque de la chaîne d'approvisionnement (31 %).

Bon nombre de ces préoccupations restent théoriques : elles sont essentiellement véhiculées par les médias et les preuves de concept des chercheurs. À l'heure où nous rédigeons ce rapport, nous n'avons pas rencontré d'utilisation majeure de l'IA générative dans des attaques réelles, et ce type d'attaque ne semble pas rencontrer plus de succès que les escroqueries par phishing imaginées par des humains.

« Nous essayons de garder une longueur d'avance sur l'IA générative. Nous savons que cette technologie est utilisée. Au lieu de la bloquer, nous essayons de mettre autant de garde-fous autour d'elle que possible. »

– RSSI, organisation gouvernementale

L'IA générative comble de graves lacunes en matière de cyberdéfense

L'IA va-t-elle remplacer des emplois ? Pas tout à fait. Pour 86 % des RSSI, l'IA générative va réduire les déficits de compétences et de talents au sein de leur équipe de sécurité. Autrement dit, plutôt que de remplacer des emplois, l'IA générative sera plus probablement utilisée pour remplir des fonctions de sécurité chronophages et manuelles que les professionnels de la sécurité, de toute façon, sont réticents à effectuer (rédiger des documents de politiques, par exemple). Ce temps libéré leur permettrait de se consacrer davantage à la stratégie. Il faut voir les choses en face : il n'y a pas assez de professionnels de la cybersécurité pour répondre à la demande. L'IA pourrait donner aux organisations la possibilité d'assister leurs équipes dans de nombreux domaines, de la documentation au tri des tickets.

Face à la crainte que l'IA ne vole l'emploi de qui que ce soit, envisagez-la plutôt comme l'automatisation, qui augmente et soutient les talents plutôt qu'elle ne les remplace. Et en matière d'automatisation, 93 % des RSSI déclarent avoir largement ou modérément intégré l'automatisation à leurs processus, ce qui leur laisse une grande marge de manœuvre pour des scénarios d'utilisation innovants à l'avenir.

« Je ne connais personne dans le monde de la cybersécurité aujourd'hui qui n'ait pas des problèmes de recrutement et de rétention, » affirme le RSSI d'une agence gouvernementale.

D'ailleurs, quand il s'agit d'utiliser l'IA pour la cyberdéfense, les RSSI ont de nombreuses idées. L'IA est un outil de plus pour relever des défis de toute nature, stratégique ou profondément technique. Il n'est pas surprenant que les RSSI souhaitent confier à l'IA une liste toujours plus longue de tâches de routine. Mais nous avons également été ravis de voir les opportunités d'utilisation de l'IA s'étendre à des fonctions stratégiques : assurance qualité des données, enrichissement et hiérarchisation des alertes, gestion de l'analyse de la posture de sécurité et des communications internes. Même quand les problèmes de sécurité ne sont pas nouveaux, l'IA offre de potentielles nouvelles solutions.

Elle donne aussi la possibilité d'améliorer les compétences et le niveau de maîtrise du personnel. 46 % des RSSI interrogés prévoient de former les équipes de sécurité à la rédaction de prompts. On recense également d'autres initiatives, comme la sensibilisation des employés aux menaces posées par l'IA générative (39 %) et l'établissement de protocoles visant à déterminer les types de tâches appropriées aux robots IA (37 %) par opposition à celles qui doivent être effectuées exclusivement par des humains.

« En matière de cybersécurité, nous apprenons après coup. Avec l'IA et l'IAG, nous pouvons adopter une approche plus proactive et peut-être remédier aux pénuries de compétences. »

– RSSI, enseignement supérieur

Comment les entreprises mettent l'IA générative au service de la cybersécurité

35 % Analyse et hiérarchisation dans la gestion de l'hygiène et de la posture de sécurité

27 % Enrichissement des données d'alertes et d'incidents

26 % Communications internes

26 % Analyse des sources de données visant à déterminer celles qui doivent être optimisées ou éliminées

25 % Analyse des malwares

23 % Création de règles de détection

23 % Création de normes de configuration sécurisées

22 % Automatisation des workflows

22 % Recherche des menaces

20 % Notation des risques

20 % Création de politiques

19 % Réponse aux incidents et investigation formelle

Les RSSI et le conseil d'administration établissent clairement leurs priorités

« Le conseil d'administration se penche très sérieusement sur la question du risque, et le cyber est une forme de risque. »

– RSSI, transport, tourisme et transport maritime

Comment les RSSI savent-ils s'ils font du bon travail ? Nous leur avons demandé quels étaient leurs indicateurs de réussite – aussi bien ceux qu'ils observent en priorité que ceux qui intéressent le plus le conseil d'administration. On observe parfois un grand écart entre ces deux réponses, ce qui peut être source d'un manque d'alignement et de frustration sur le terrain.

« Vous pouvez acheter toute la technologie du monde, mais si les utilisateurs ne sont pas bien formés, les choses peuvent mal tourner, » explique le RSSI d'une organisation technologique de plus de 11 000 employés.

Les RSSI soulignent également des différences plus fondamentales en termes de valeurs et de compréhension. Le RSSI d'une entreprise d'externalisation ajoute : « Certains membres du conseil d'administration comprennent l'importance de la sécurité. D'autres, pas du tout. »

Mais dès qu'ils parlent de quantification des risques, de valeur commerciale et de retour sur investissement, les RSSI gagnent peu à peu l'attention du conseil d'administration et de la direction :

- **26 % déclarent communiquer les résultats des tests de sécurité pour signaler aux conseils d'administration les domaines d'intervention prioritaires et faire preuve d'un leadership intelligent et proactif.**
- **27 % partagent en priorité les chiffres du retour sur investissement en matière de sécurité, en précisant les domaines dans lesquels les interventions et les budgets ont déjà été utiles ; ils cherchent ainsi à établir une liaison directe avec la direction financière et à obtenir du soutien pour de futurs investissements.**
- **25 % déclarent que l'acquisition d'une cyberassurance pourrait être le meilleur moyen de montrer aux conseils d'administration à quel point ils sont « en sécurité » et/ou de justifier d'autres investissements.**

« Je pense que l'importance des tests de pénétration et de la cybersécurité est bien mieux comprise aujourd'hui qu'il y a trois ans en raison des récents événements survenus dans l'industrie, » déclare le RSSI d'un organisme de santé.

Cela confirme une autre conclusion surprenante : pour 86 % des RSSI, leur première mission est de veiller à ce que leur organe directeur ou leur conseil d'administration comprenne l'intérêt de financer des investissements dans la sécurité. Comme le dit un RSSI du secteur des transports : « Ce que le conseil d'administration attend avant tout, c'est une quantification des risques. Ils veulent des chiffres précis. »

Pourtant, seuls 20 % des conseils d'administration considèrent la « rentabilité des investissements en sécurité » comme un indicateur de réussite, peut-être parce qu'ils ne comprennent pas bien l'impact du ROI sur le risque, et s'appuient plutôt sur d'autres indicateurs de l'amélioration de la posture de sécurité.

Les exigences en matière de ROI sont indéniablement plus strictes. Près d'un tiers (31 %) des participants déclarent que des projets ont été reportés ou retardés en raison d'un manque de financement, et 30 % ajoutent que leur équipe n'a pas été en mesure de soutenir une initiative commerciale.

En outre, 84 % des RSSI affirment que leur conseil d'administration/organe de direction assimile une sécurité robuste à la conformité réglementaire plutôt qu'aux bonnes pratiques, ce qui pourrait expliquer la légère disparité dans l'importance accordée au « statut et aux résultats des audits de conformité internes et/ou réglementaires ». On ne sera donc pas surpris que 90 % des RSSI déclarent que leur organe directeur/conseil d'administration ne se soucie pas aujourd'hui des mêmes KPI et métriques de sécurité qu'il y a deux ans. Le RSSI d'une entreprise de transport et de logistique déclare : « Mon conseil d'administration adore les chiffres. Mais le problème avec la cybersécurité, c'est qu'il est extrêmement difficile de résumer nos performances à un seul chiffre. »

Les RSSI comme les membres du conseil d'administration doivent actualiser leur approche pour garantir leur alignement.

Les RSSI renforcent leur présence au conseil d'administration et exercent leur influence

Globalement, nos recherches ont montré que les RSSI assument plus formellement leur position : 47 % des RSSI relèvent directement du PDG, et 40 % ont le DSI comme supérieur direct.

Il est intéressant de noter que l'Europe occidentale est en tête de cette tendance : dans cette région, 54 % relèvent directement du PDG tandis qu'ils sont 48 % dans la région APAC et que la région AMER est à la traîne avec 41 %. Cela s'explique sans doute par la législation européenne, déjà en place et à venir, qui rend le PDG personnellement responsable de la sécurité et le pénalise en cas de négligence. Bref, l'ignorance n'est plus une excuse en cas de cyberattaque.

Ce changement au sein des hiérarchies illustre la façon dont les RSSI se réorientent vers les priorités de l'entreprise et formalisent leurs rôles de direction. Ils n'en sont plus à se rapprocher de la direction. Ils en font partie. Cette tendance traduit une nouvelle réalité : aujourd'hui, la sécurité est aussi importante que la finance pour les organisations (les RSSI et les directeurs financiers travaillent côte à côte). Et le risque de sécurité est désormais aussi lourd que le risque financier en termes de coûts, d'implications légales et d'impact sur le cours de l'action.

Le moteur d'un changement de culture

Aujourd'hui, le cyberrisque est un risque commercial. Les organisations intègrent souvent la sécurité à leurs systèmes et processus métier existants. Preuve de son importance au sein de la direction, une large majorité des organisations (78 %) déclarent désormais avoir créé un sous-comité ou un comité d'audit dédié à la cybersécurité, à la confidentialité ou au cyberrisque. Cette démarche peut s'expliquer en partie par la législation européenne, qui rend le PDG personnellement responsable de la sécurité.

Petit à petit, les RSSI deviennent des moteurs de changement pour la culture de sécurité de leur organisation. Ils sensibilisent les employés et intègrent les exigences de sécurité au développement de logiciels et à la prise de décisions commerciales.

Le RSSI d'une entreprise de transport, de tourisme et de construction navale déclare : « Il faut du temps pour faire changer une culture. Cela n'a que très peu à voir avec la technologie elle-même, et c'est la partie la plus difficile du travail. » Soit ils enfoncent des portes ouvertes, soit leurs efforts portent enfin leurs fruits. Mais dans tous les cas, il est clair que leur influence sur la culture s'étend au-delà de leur sphère de contrôle directe : 88 % affirment que leur conseil d'administration ou leur organe directeur déploie des efforts concertés pour s'informer sur la cybersécurité.

Les RSSI et les conseils d'administration classent les facteurs de réussite*

On observe un alignement étroit des facteurs qui indiquent la réussite d'un programme de cybersécurité

RSSI	Conseil	
27 %	20 %	Rentabilité des investissements en sécurité
17 %	23 %	Statut et résultats des audits de conformité internes et/ou réglementaires
26 %	21 %	Résultats des tests de sécurité
23 %	18 %	Taux d'exposition aux risques ou pourcentage de couverture des correctifs et des outils
23 %	19 %	Retours des dirigeants métier, de la direction et du conseil d'administration
22 %	18 %	Pourcentage de systèmes à jour
17 %	21 %	Réalisation des jalons de la feuille de route de sécurité
16 %	19 %	Taux d'inspection des alertes et d'investigation
16 %	18 %	Temps moyen de réponse ou de correction (MTTR)
21 %	23 %	Progrès dans les certifications d'évaluation des modèles de sécurité/maturité
20 %	18 %	Temps moyen nécessaire pour corriger une vulnérabilité
20 %	18 %	Pourcentage de systèmes conformes aux politiques de contrôle de sécurité
19 %	17 %	Nombre d'incidents, de failles et d'autres événements hautement prioritaires à signaler
18 %	20 %	Couverture de l'inventaire des actifs et des logiciels
25 %	23 %	Possibilité de souscrire une cyberassurance
22 %	21 %	Pourcentage d'employés ayant suivi une formation de sensibilisation à la sécurité
17 %	17 %	Nombre de vulnérabilités identifiées
14 %	14 %	Temps moyen de détection (MTTD)

* Facteurs classés par ordre décroissant d'écart

Les RSSI acceptent – mais remettent en question – l'évolution de leur rôle

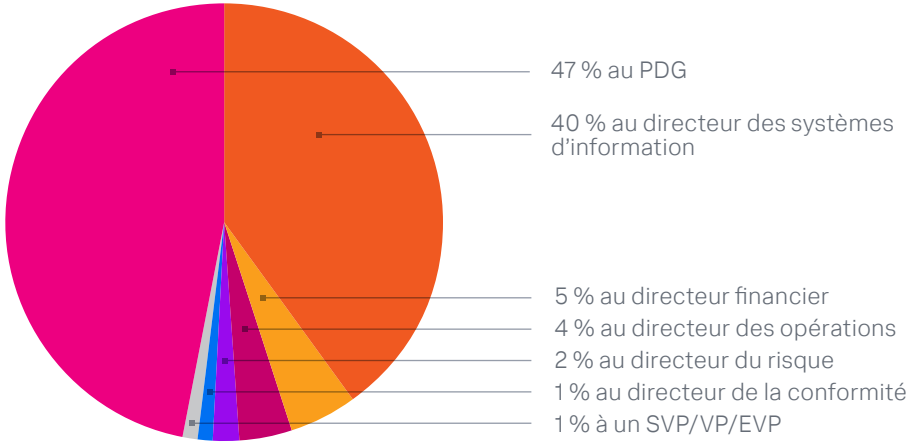
Les lanceurs d'alerte sont toujours là. 82 % des personnes interrogées déclarent que si leur organisation ignorait délibérément les bonnes pratiques de sécurité et leurs obligations de conformité, mettant de ce fait l'entreprise en danger, elles envisageraient de lancer l'alerte. C'est le signe d'un sentiment de responsabilité qui dépasse le cadre de leur emploi, d'un sens moral aigu – et peut-être de leçons apprises après avoir assumé la responsabilité des problèmes de sécurité de leur organisation.

Il n'est pas tout à fait exagéré de dire qu'ils sont des boucs émissaires : 84 % sont d'accord ou tout à fait d'accord pour dire qu'ils s'inquiètent de leur responsabilité personnelle en cas d'incident de cybersécurité. Nos experts vous recommandent de trouver un avocat personnel (et non celui de votre entreprise) auquel vous pourrez faire appel dans de brefs délais en cas de besoin.

En matière de décisions d'achat, vous avez tout intérêt à miser sur les options sûres et éprouvées si vous avez besoin d'impressionner votre conseil d'administration : 90 % déclarent que leur organe directeur/conseil d'administration accorde une grande confiance aux recommandations des analystes du secteur.

De nombreux conseils d'administration et PDG savent que le paysage des risques a évolué, mais ils se sentent impuissants face à cette nouvelle dynamique. C'est l'occasion pour les RSSI de sensibiliser leur conseil d'administration et, à terme, d'améliorer la posture de sécurité de leur organisation. En fin de compte, les RSSI occupent désormais une place plus importante à la table, et leur voix a plus d'impact. La direction et le conseil d'administration sont à l'écoute. Les responsables de la sécurité peuvent utiliser leur nouvelle position pour induire le changement qu'ils souhaitent voir dans l'industrie.

Les RSSI rendent directement compte à la direction



Les RSSI se soumettent aux ransomwares

« Mon but : ne pas être aux commandes en cas de cyberattaque majeure. »

– RSSI, entreprise du secteur bancaire

Selon toute probabilité, les RSSI seront confrontés à une attaque majeure. *Ils sont – et c'est stupéfiant – 90 % à avoir subi au moins une attaque majeure dans leur organisation au cours de l'année écoulée* (une fois pour 43 %, deux fois pour 34 %, plus de deux fois dans 13 % des cas).

Dans un tel contexte, on comprend que l'ingénierie sociale, l'OT/IoT et les ransomwares soient des préoccupations majeures pour les RSSI. Ces menaces ne sont pas seulement mises en avant dans les médias, elles sont aussi dévastatrices sur le plan financier. Le RSSI d'un organisme de santé explique : « Vos décisions ont un impact sur le fonctionnement de l'entreprise. Si vous faites de mauvais choix, vous pouvez ruiner son activité. »

ont signalé au moins une attaque majeure

Cybermenaces les plus préoccupantes

40 % Attaques d'ingénierie sociale

37 % Technologie opérationnelle (OT) et Internet des objets (IoT)

33 % Ransomwares

30 % Menaces internes

29 % Risque lié aux tiers

24 % Attaques par déni de service distribué

24 % Logiciel malveillant destructeur

24 % Erreurs et défauts de configurations

24 % Cryptominage

21 % Appropriations de compte

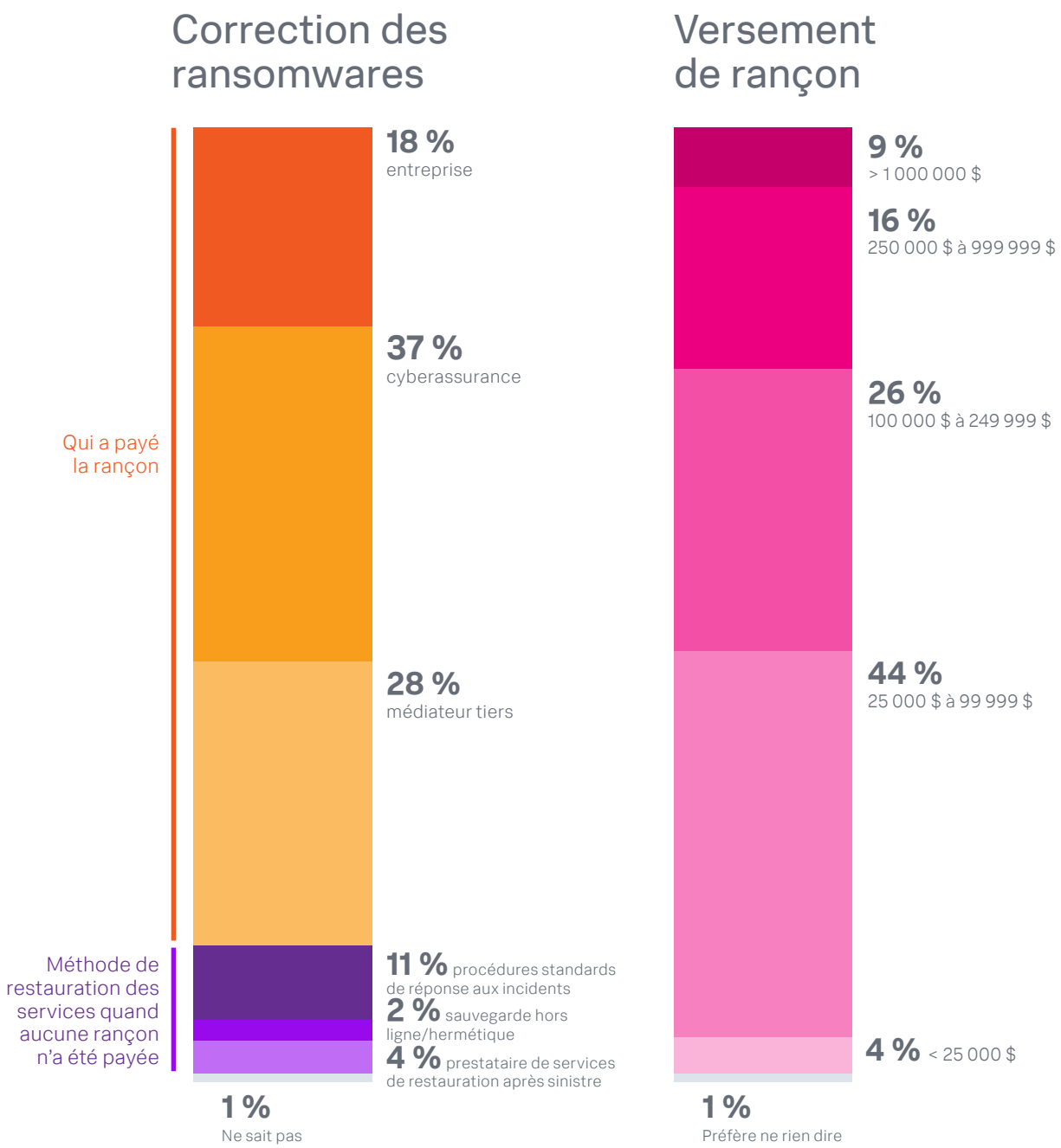
20 % Fraude

Ransomware : les attaquants s'enrichissent

96 % des participants déclarent avoir été victimes d'une attaque par ransomware, et pour 52 % d'entre eux, l'impact sur les systèmes et les opérations d'entreprise a été significatif.

Si le chiffre de 96 % vous impressionne, accrochez-vous : 83 % de ceux qui ont répondu ont déclaré avoir payé la rançon. Et parmi eux, 18 % ont payé la rançon directement, 37 % via une cyberassurance et 28 % en passant par un intermédiaire.

Et les sommes ne sont pas négligeables. Les rançons payées étaient comprises entre 25 000 $ et 99 999 $ dans 44 % des cas, plus de la moitié des participants ont versé des sommes supérieures à 100 000 $, et ils sont même 9 % (soit 1 sur 11) à avoir payé 1 million de dollars ou plus. Le ransomware est une activité hautement lucrative pour les groupes criminels et de nombreuses organisations désespérées jouent avec leur réputation dans l'espoir de déchiffrer leurs données, récupérer leurs systèmes et empêcher la diffusion de contenus sensibles.



La majorité des RSSI (69 %) affirment que le paiement d'une rançon les expose à de potentielles poursuites judiciaires à l'avenir. Même après avoir payé, les organisations parviennent rarement à récupérer pleinement leurs capacités perdues : les brigands n'ont pas le sens de l'honneur. Et la cyberassurance n'est pas la solution miracle ; il est souvent difficile d'en bénéficier, sans même parler d'un remboursement complet.

La véritable conclusion ? Maintenez impérativement des sauvegardes hors ligne séparées, et testez-les régulièrement. Désignez un responsable de la maintenance et procédez à des contrôles réguliers pour vérifier qu'elle est correctement assurée. Pensez également à organiser une simulation au niveau du conseil d'administration pour exercer une pression réelle sur ces systèmes, en toute sécurité.

Et ne pensez pas que le conseil d'administration vous ignore. 73 % des RSSI estiment que leur organe directeur/conseil d'administration s'inquiète trop des ransomwares et de la menace qu'ils représentent pour leur organisation. Et la majorité rapporte que lors d'attaques par ransomware, leur direction a exigé des points d'information réguliers sur la résolution du problème. Ce contrôle étroit ne disparaîtra probablement pas de sitôt, mais c'est une raison de plus de réaliser des exercices avec votre conseil d'administration.

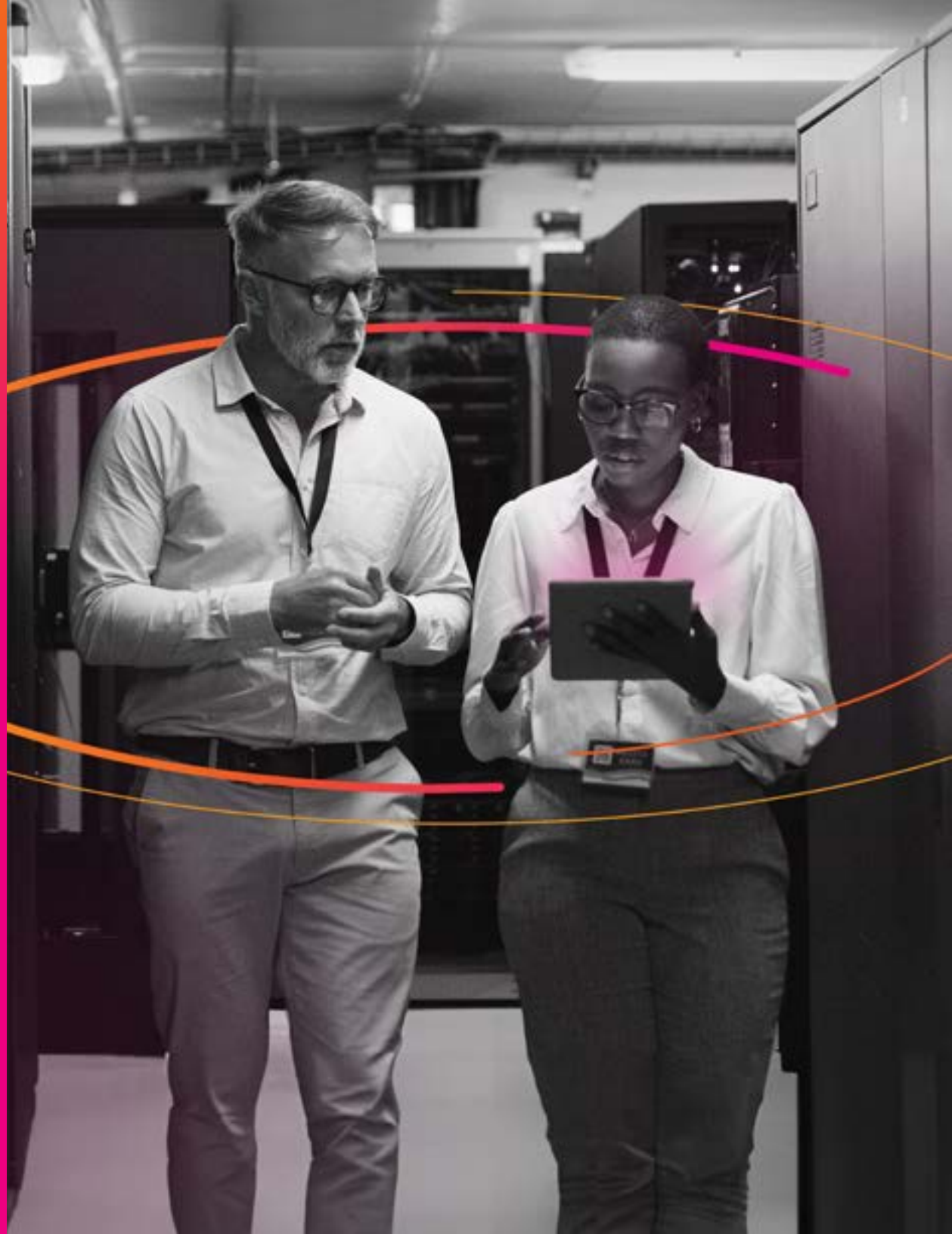
« Le processus de cyberassurance a changé au cours des dernières années. Nous en arrivons au point où nous nous demandons si cela vaut la peine d'y consacrer notre temps. »

– RSSI, société financière

Les investissements de sécurité en hausse

« Les ressources sont mon seul véritable point faible : le défi est d'avoir suffisamment d'heures dans la journée et suffisamment de personnes pour assumer toutes les responsabilités. »

– RSSI, société de services financiers



93 % des organisations s'attendent à augmenter leurs dépenses de cybersécurité, de manière significative ou modérée, au cours de l'année à venir. C'est une excellente nouvelle pour les équipes de sécurité, puisque 85 % des RSSI déclarent qu'une réduction des dépenses nuirait à leur capacité à répondre aux menaces. Ils sont également 80 % à souligner que leur organisation est confrontée à un nombre croissant de menaces, qui coïncident avec le déclin de l'économie.

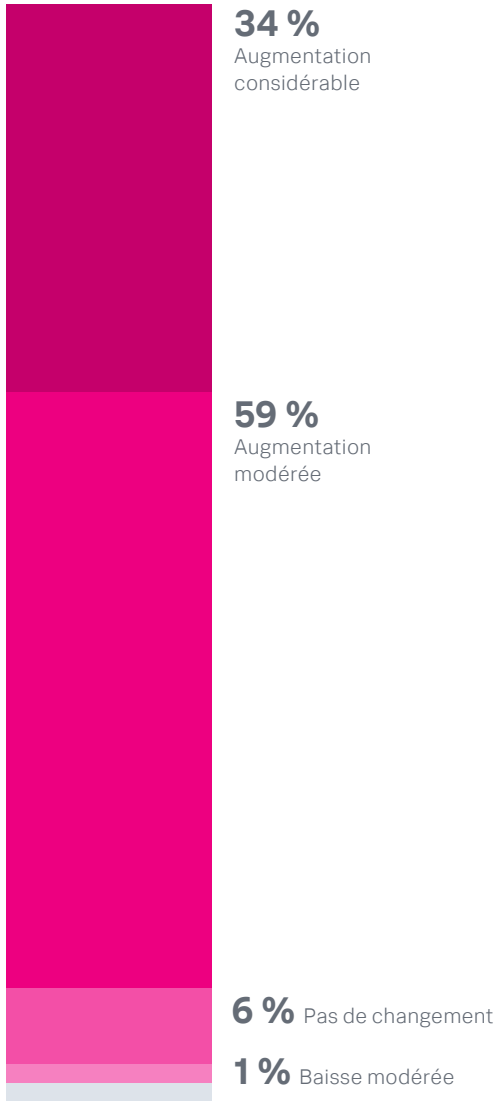
Pourtant, 83 % des RSSI observent des baisses de budget dans d'autres secteurs de leur organisation, et 85 % se disent inquiets de l'incertitude macroéconomique et de son impact potentiel sur leur équipe.

Près d'un tiers (31 %) déclarent que des projets ont été retardés ou abandonnés en raison d'un manque de financement. S'ils sont 87 % à dire qu'ils sont parvenus à justifier une augmentation du budget d'une année à l'autre, seuls 35 % déclarent que leur conseil d'administration alloue des budgets adéquats à la cybersécurité.

L'augmentation prévue des budgets de sécurité donne des raisons d'être optimiste. Cependant, malgré l'augmentation des investissements, ce financement supplémentaire n'est toujours pas suffisant pour de nombreux RSSI aux prises avec une lourde dette technique.

Nous avons constaté que les RSSI justifient auprès du conseil d'administration le ROI de la sécurité, et certains d'entre eux ciblent particulièrement la prolifération des outils. La grande majorité (88 %) dit qu'il est nécessaire de reprendre le contrôle sur les outils d'analyse et d'opérations de sécurité en misant sur des solutions telles que le SOAR, le SIEM et la threat intelligence, afin de résoudre les problèmes de prolifération et de complexité des outils. Ils ne sont que 2 % à ne pas ressentir le besoin de consolider leurs outils. C'est un message qui séduit toujours la direction financière – et contribue à démontrer le retour sur investissement.

Dépenses en cybersécurité en 2024



des RSSI s'attendent à une augmentation des dépenses en matière de cybersécurité

« Mon directeur financier m'a affirmé que mon budget serait toujours suffisant… tant que je peux justifier un financement, je l'obtiendrai. »

– RSSI, secteur bancaire

La collaboration est essentielle pour renforcer la résilience

« Un bon programme de résilience se remet sans cesse en question et essaie de s'améliorer. Il ne faut jamais rester immobile, et toujours interroger et repousser les limites du programme. »

– RSSI, entreprise de télécommunications

Lors de nos échanges avec les RSSI du Forbes Global 2000 et au-delà, nous avons plaidé en faveur d'une culture de collaboration interfonctionnelle faisant converger les équipes de sécurité, l'IT et l'ingénierie. En effet, nous avons constaté à maintes reprises que les organisations qui misent sur la collaboration des équipes ont plus de chances d'éviter que les problèmes ne se transforment en catastrophes majeures, de remédier plus rapidement aux incidents et, en fin de compte, de mieux s'adapter à l'évolution de l'environnement. On comprend donc que 27 % des RSSI considèrent la collaboration entre les équipes des opérations informatiques, des opérations de sécurité et de l'ingénierie ou du développement logiciel comme un moyen clé de renforcer, étendre et maintenir la résilience de leur organisation.

La collaboration ouvre les portes et fait tomber les murs

Bien qu'on parle d'un changement de culture progressif, nous avons constaté que les différentes équipes des organisations collaborent de plus en plus étroitement. C'est avec les opérations IT que la collaboration est la plus intense en matière de cybersécurité, sans doute parce que ces intégrations sont plus établies. Cette collaboration est qualifiée de bonne par 36 % des personnes interrogées, et 40 % disent qu'elle est bonne, mais peut être améliorée. Les RSSI considèrent également les collaborations avec l'ingénierie logicielle/le développement d'applications (42 %), l'équipe cloud (40 %) et l'architecture d'entreprise (27 %) comme essentielles pour garantir la résilience de toute l'organisation.

Avantages de la collaboration

44 %
Meilleure intégration entre les outils et les processus de la sécurité et des opérations IT

42 %
Réduction du délai nécessaire pour comprendre, quantifier et hiérarchiser les risques associés aux nouvelles initiatives commerciales

40 %
Meilleur transfert de connaissances entre les groupes

37 %
Collaboration accrue sur le déploiement des achats et l'exploitation des technologies de sécurité

37 %
Meilleure visibilité sur la surface d'attaque

33 %
Réduction du délai d'atténuation des risques

31 %
Davantage d'opportunités de carrière permettant d'entrer ou de sortir du service de sécurité

29 %
Moins de conflits sur les responsabilités des différentes équipes

D'autres domaines propices à une intégration solide de la cybersécurité émergent encore :

- **le développement d'applications,**
- **l'observabilité,**
- **l'expérience client/expérience numérique.**

Dans ces trois domaines, entre 73 % et 76 % des personnes interrogées affirment que le niveau de collaboration est satisfaisant. Parmi elles, certaines manifestent un désir de l'améliorer encore, d'autres non. Cependant, dans la pratique, la collaboration dans l'exécution des fonctions est souvent différente de la théorie. Le RSSI d'une société financière décrit la relation entre l'informatique et la sécurité comme respectueuse, mais conflictuelle : « Ils ne contestent jamais ce que nous voulons faire, mais on les entend marmonner des obscénités dans leur barbe dès qu'on a le dos tourné. »

Même si elle demande du temps et des efforts, la collaboration ne présente que des avantages. Les RSSI vantent ses nombreux bénéfices. En premier lieu, l'intégration générale des outils et processus des opérations de sécurité et IT (44 %), qui contribue également à réduire le budget et à justifier le ROI.

Renforcer la résilience pour l'avenir

Un nombre important de RSSI annoncent également qu'ils vont continuer à perfectionner les compétences de l'organisation en lien avec la résilience, notamment en développant davantage de plans complets de réponse aux incidents décrivant clairement les mesures à prendre en cas d'incident de sécurité. Dans le cadre de cet effort, ils comptent également définir et automatiser des processus de réponse aux incidents englobant différentes équipes et individus (25 %).

Ces pratiques ne sont pas nouvelles pour les RSSI, qui considèrent souvent la résilience comme une extension de leurs pratiques de sécurité ; et comme les PDG associent la résilience au risque et la réponse aux attaques, elle relève souvent de la compétence des RSSI. Toutefois, les changements requis par de nombreuses réponses de sécurité reposent sur l'informatique, ce qui incite certains RSSI à utiliser la résilience comme moyen de travailler plus étroitement avec l'informatique. Le résultat : une meilleure réponse numérique.

Créer et développer une culture de résilience est une entreprise monumentale. Les RSSI estiment que la collaboration en matière de résilience numérique doit être à la base de tout, depuis la planification et la modernisation des produits jusqu'à la stratégie commerciale. À cette fin, 55 % d'entre eux affirment avoir la possibilité d'intégrer la sécurité dans tous les aspects du cycle de vie du développement logiciel, et 50 % déclarent que la sécurité devrait faire partie intégrante du processus de modernisation. Les RSSI soutiennent également que les efforts de collaboration en matière de résilience permettront de mieux comprendre les comportements inhabituels ou anormaux du système ou du réseau (48 %) et d'améliorer la réponse d'une organisation à la dégradation des applications critiques (44 %). Autant d'arguments en faveur d'une meilleure intégration des fonctions de sécurité et d'observabilité.

Activités collaboratives de résilience

55 %
Intégrer la sécurité dans l'intégralité du cycle de vie du développement logiciel

50 %
Projets de modernisation

48 %
Analyse du comportement inhabituel ou anormal d'un système ou d'un réseau

44 %
Observabilité et réponse de l'organisation à une dégradation des applications ou des services stratégiques

38 %
Processus et protocoles de gestion de crise

Une nouvelle ère de résilience

Le temps où les RSSI travaillaient dans des bulles et des silos est révolu. Ils prennent conscience – et le reste de la direction les imite – qu'il faut « tout un village » pour créer des organisations plus fortes, plus sûres et, à terme, plus résilientes. La collaboration stratégique entre l'ingénierie et l'informatique est essentielle à cette mission.

Les données de ce rapport le montrent clairement : les RSSI ont plus de contacts et plus d'influence que jamais sur le PDG et la direction. Et même s'ils doivent sans cesse justifier les investissements technologiques, leurs dirigeants les écoutent mieux et leur allouent davantage de budget. Petit à petit, les RSSI et le reste du directoire apprennent à parler le même langage.

Parallèlement à cela, nous ne pouvons ignorer les nouveaux défis et les pressions sans précédent auxquels les RSSI sont confrontés. Des réglementations de sécurité strictes, à commencer par les nouvelles règles de la Security and Exchange Commission publiées en juillet 2023, accentuent le risque pour les RSSI en les rendant potentiellement responsables en cas de cyberincident. L'IA ouvre la porte à de nouvelles opportunités, mais peut tout aussi bien être exploitée par des pirates informatiques pour élaborer des contrefaçons, de la désinformation et des programmes d'ingénierie sociale plus élaborés. Quant aux ransomwares, ils continuent de poser des dilemmes complexes : faut-il contenir le malware ou payer discrètement les pirates dans l'espoir que la menace disparaisse ?

Les RSSI feront face à ces aléas de diverses manières, mais une chose est sûre : ils ne peuvent pas faire cavalier seul. L'intégration de la sécurité et des opérations informatiques n'est pas entièrement nouvelle, mais certains signes indiquent que ce type de collaboration est en expansion. Les fonctions de sécurité travaillent plus étroitement avec le développement d'applications, l'observabilité et l'expérience client. Dans l'ensemble de l'organisation, ces rapprochements offrent de nouvelles opportunités d'apprendre et de gagner en efficacité.

Certes, cela ne se fera pas du jour au lendemain. Mais les équipes de l'organisation vont communiquer, collaborer et s'intégrer davantage pour accroître la visibilité et l'efficacité globale, et se donner ainsi les moyens de réussir encore mieux. Dans un contexte où les dirigeants envisagent de plus en plus le cyberrisque comme le risque commercial qu'il est réellement, le RSSI défend un paradigme axé sur la sécurité qui inaugure une nouvelle ère de résilience.

Annexe

Points clés par région

Les participants à notre étude se répartissent géographiquement comme suit : Amérique du Nord (41 %), Asie-Pacifique/Japon (30 %) et Europe occidentale (29 %). Ils ont donné les réponses suivantes dans les différents thèmes abordés :

Le rôle du RSSI

- C'est en Europe occidentale que le plus grand nombre de RSSI relèvent directement de leur PDG (54 %), suivie par l'Asie-Pacifique/Japon (48 %) et l'Amérique du Nord (41 %), avec une moyenne de 47 % du total des participants.
- Les RSSI d'Amérique du Nord sont les plus nombreux à dire que le rôle de RSSI a tellement changé qu'il s'agit presque d'un travail différent : 90 % sont « d'accord » ou « tout à fait d'accord » avec cette proposition, suivis par les RSSI de la région APAC avec 89 % et ceux d'Europe occidentale avec 76 %.
- On retrouve dans la région APAC le pourcentage le plus élevé de participants dont les priorités sont passées des contrôles et de la mise en œuvre à la stratégie (94 %). Vient ensuite l'Amérique du Nord, avec 90 %, et l'Europe occidentale avec 88 %.
- Les indicateurs de réussite des RSSI varient considérablement selon les régions. Il est intéressant de noter que c'est en Amérique du Nord que l'on recense le pourcentage le plus élevé de participants (25 %) qui considèrent le nombre de failles, d'incidents et d'événements hautement prioritaires comme un indicateur de réussite. En revanche, un grand nombre de personnes interrogées en Europe occidentale considèrent les retours des décideurs métier, des directeurs et du conseil d'administration comme le meilleur indicateur de réussite (29 %).

Comité de direction

- Dans le monde entier, le manque d'alignement entre les priorités du conseil d'administration et celles des RSSI est source de frustration, mais on observe des variations d'une région à l'autre. 43 % des personnes interrogées en Amérique du Nord déclarent que l'équipe de sécurité s'est trouvée dans l'incapacité de soutenir une initiative commerciale, contre seulement 15 % des personnes interrogées en Europe occidentale. La raison en est probablement la réglementation, plus stricte en Europe qu'aux États-Unis. En Asie-Pacifique, 33 % des participants ont déclaré avoir dû réduire leurs effectifs de cybersécurité en raison d'un mauvais alignement des priorités, contre seulement 18 % des RSSI d'Europe occidentale interrogés.
- Le manque de coordination entre les indicateurs de réussite du conseil d'administration et des RSSI est, lui aussi, inégal d'une région à l'autre. 30 % des RSSI nord-américains déclarent que les progrès accomplis dans le modèle de maturité en matière de sécurité restent le principal indicateur du succès de leur conseil d'administration, contre seulement 16 % des personnes interrogées en Europe occidentale. Parallèlement, 28 % des participants de la région APAC affirment que leur direction est attentive au pourcentage de systèmes conformes aux politiques de contrôle de sécurité (MFA, WAF, chiffrement, etc.), contre seulement 11 % de ceux d'Europe occidentale. C'est en Europe occidentale que le plus grand nombre de RSSI (27 %) a cité le statut et/ou les résultats des audits internes de conformité réglementaire comme l'indicateur de réussite prioritaire de leur conseil d'administration.

Résilience numérique

- Les participants nord-américains accordent une plus grande importance que leurs homologues des autres régions à la formation en cybersécurité dans leur stratégie de résilience numérique : 30 % des personnes interrogées en Amérique du Nord affirment que former le personnel de cybersécurité aux bonnes pratiques et miser sur la formation continue est le facteur le plus important pour garantir la résilience numérique, contre 19 % respectivement en Asie-Pacifique comme en Europe occidentale.

L'essor de l'IA générative

Dans toutes les régions, les premiers avis sur les applications de l'IA générative en matière de sécurité sont généralement optimistes.

- 84 % sont d'accord ou tout à fait d'accord pour dire qu'ils vont développer leurs propres modèles de langage ou d'autres solutions basées sur l'IA à des fins de cybersécurité.
- 89 % envisagent avec plus ou moins de fermeté d'adopter l'IA générative pour la cybersécurité en faisant appel à des produits ou fonctionnalités élaborés par des fournisseurs.
- 86 % des participants estiment que l'IA générative va réduire les déficits de compétences au sein de leur équipe de sécurité.
- 82 % pensent que les robots d'IA générative vont prendre en charge des tâches et des activités effectuées actuellement par les humains.
- La région APAC est celle qui exprime le plus grand espoir que l'IA soit utilisée comme outil défensif : 24 % des participants de cette région estiment qu'elle leur donnera un avantage modéré ou significatif sur les cybercriminels, contre 12 % des personnes interrogées en Amérique du Nord et 17 % en Europe occidentale. Cela dit, dans toutes les régions, les RSSI estiment que l'IA générative donnerait aussi un avantage modéré ou significatif aux cybercriminels.
- Il est donc logique que les participants de l'APAC (23 %) soient aujourd'hui les plus enclins à utiliser l'IA générative pour la cybersécurité, contre seulement 11 % de leurs homologues en Amérique du Nord ou en Europe de l'Ouest.
- Ce sont les RSSI européens qui expriment le plus d'intérêt pour l'utilisation de l'IA générative dans le domaine de la cybersécurité au cours des 12 prochains mois (57 %), contre 39 % des personnes interrogées en Amérique du Nord et 35 % en Asie-Pacifique.

Le paysage des menaces

- L'Asie-Pacifique et l'Europe occidentale observent le plus grand écart en matière de sécurité dans l'infrastructure cloud, avec respectivement 57 % et 51 %, contre 40 % seulement des participants nord-américains.
- Les RSSI de la région APAC craignent également davantage les attaques ciblant les technologies opérationnelles (OT) et l'IoT (46 %) que les Européens (25 %).
- Même si toutes les régions sont touchées par les ransomwares, les personnes interrogées en Asie-Pacifique (64 %) et en Amérique du Nord (53 %) étaient plus nombreuses à avoir subi une attaque affectant considérablement leurs systèmes et leurs opérations commerciales, par rapport aux participants d'Europe occidentale (38 %).
- Des rançons sont payées dans toutes les régions de la même manière, que ce soit directement, via une cyberassurance ou par le biais d'un tiers. Les personnes interrogées en Amérique du Nord ont été plus nombreuses (39 %) à verser des rançons comprises entre 100 000 $ et 249 999 $ qu'en Europe occidentale (20 %) ou en APAC (14 %). C'est toutefois dans la région APAC que des rançons supérieures à 1 million de dollars ont été le plus fréquemment consenties (17 %), bien plus qu'en Amérique du Nord (3 %) ou en Europe occidentale (7 %).

Points clés par secteur

Participants par secteur

30 % Services financiers

22 % Fabrication

9 % Communication et médias

8 % Technologie

7 % Santé

7 % Détail/ Vente en gros

6 % Services profes-sionnels

10 % Autre

1 % Gouvernement

Le rôle du RSSI

Les RSSI de nombreux secteurs relèvent désormais directement du PDG, notamment :

- 84 % dans le secteur de la santé,
- 63 % dans les communications et les médias,
- 44 % dans la fabrication,
- 34 % dans les services financiers.

1. La conformité réglementaire est la priorité absolue pour les RSSI du secteur de la vente au détail (56 %), mais aussi de la technologie (29 %). Dans les secteurs de la communication et des médias (59 %) et de la technologie (50 %), c'est la confidentialité des données qui préoccupe en premier lieu les RSSI.
2. Pour près de la moitié des RSSI (48 %) du secteur de la vente au détail, le nombre d'incidents hautement prioritaires représente l'indicateur de réussite le plus révélateur. Une part importante (34 %) des RSSI du secteur des communications et des médias évaluent avant tout leur progression dans le modèle de maturité de la sécurité pour mesurer leur réussite. Pour les RSSI du secteur de la technologie (39 %), le succès est associé à la possibilité d'acquérir une assurance de cybersécurité.
3. Dans tous les secteurs, les RSSI ont le sentiment que leur rôle a si profondément changé qu'il est aujourd'hui presque un tout autre poste. Les secteurs les plus concernés par ce constat sont :
   - Communication et médias : 93 %
   - Services financiers : 92 %
   - Technologie : 89 %
   - Détail/Vente en gros : 85 %
   - Santé : 84 %

4. Les RSSI sont particulièrement préoccupés par leur responsabilité personnelle en matière de cybersécurité dans les secteurs suivants :
   - Services financiers : 94 %
   - Technologie : 93 %
   - Services professionnels : 86 %
   - Santé : 84 %
5. Dans tous les secteurs ou presque, les RSSI affirment (ils sont d'accord ou tout à fait d'accord) que leur rôle, qui consistait auparavant à mettre en œuvre et administrer des contrôles, est désormais celui d'un stratège en matière de sécurité :
   - Gouvernements : 100 %
   - Détail/Vente en gros : 97 %
   - Services financiers : 95 %
   - Services professionnels : 91 %
   - Fabrication : 89 %
   - Communication et médias : 87 %
   - Santé : 84 %
6. Lorsqu'ils évoquent les compétences les plus demandées, c'est la sécurité du cloud qui est la plus évoquée par les RSSI des communications et des médias (47 %). Dans le commerce de détail, les RSSI ont besoin de recruter davantage de personnes à des postes seniors de cybersécurité (41 %).

Le conseil d'administration

1. Les services financiers (92 %) et les soins de santé (92 %) sont les secteurs les plus susceptibles de mettre en place un comité dédié à la cybersécurité au niveau du conseil d'administration, suivis du commerce de détail et de la vente en gros (85 %) et de la fabrication (84 %).
2. C'est également dans le secteur de la vente au détail et en gros que les conseils d'administration sont les plus enclins à allouer des budgets adéquats pour garantir la mise en place de mesures de cybersécurité (59 %), ce qui peut s'expliquer par l'assujettissement de ce secteur à la norme PCI et à d'autres réglementations sur la confidentialité des données des clients. Les services professionnels (62 %) et les services financiers (51 %) sont les plus susceptibles d'être dotés d'exigences de gouvernance mises en place par le conseil d'administration pour garantir le signalement des incidents de cybersécurité. 100 % des RSSI travaillant dans des administrations déclarent avoir une plus grande responsabilité : faire en sorte que leur direction voie la valeur de leurs investissements dans la sécurité.
3. Dans tous les secteurs, de nombreux RSSI participent régulièrement aux réunions du conseil d'administration, notamment :
   - Technologie : 100 %
   - Gouvernements : 100 %
   - Communication et médias : 94 %
   - Santé : 88 %
   - Fabrication : 86 %
4. Les RSSI sont également nombreux à affirmer que leurs conseils d'administration assimilent la sécurité à la conformité réglementaire, ce qui représente une source de frustration pour eux.
   - Services financiers : 89 %
   - Communication et médias : 87 %
   - Fabrication : 87 %
   - Santé : 84 %
   - Services professionnels : 81 %
5. Pour renforcer leur valeur auprès de leur direction, la majorité des RSSI du commerce de détail et de la vente en gros (59 %) déclarent qu'ils fournissent des mesures de cyberrisque et lui demandent de prendre des décisions basées sur les risques. La majorité des RSSI des services professionnels (52 %) déclarent positionner la sécurité comme un catalyseur commercial.

Résilience numérique

- Les RSSI de nombreux secteurs emploient des stratégies de résilience qui impliquent des équipes de toute l'organisation. Tous les RSSI travaillant pour une administration et 59 % des RSSI du secteur du commerce de détail affirment que les opérations de sécurité (SecOps) vont favoriser la résilience numérique. À 79 % dans le secteur des technologies et à 56 % dans la fabrication, les RSSI déclarent que les opérations informatiques ont des responsabilités importantes en matière de résilience numérique.
- Les RSSI des services professionnels (76 %) et des communications et médias (63 %) considèrent l'intégration de la sécurité dans le cycle complet du développement logiciel comme une stratégie de résilience majeure. Pour 59 % des RSSI des communications et des médias, l'observabilité et la prise en charge d'une dégradation des applications sont des activités qui renforcent la résilience.

L'essor de l'IA générative

Les secteurs qui expriment le plus la crainte que l'IA générative ne donne un avantage modéré ou significatif aux cyberadversaires sont la santé (88 %), la fabrication (76 %) et les services financiers (72 %). Dans les services financiers, 51 % des RSSI prévoient de mettre en œuvre des contrôles de cybersécurité spécifiques pour atténuer les risques de sécurité de l'IA.

Les secteurs les plus intéressés par l'adoption de l'IA générative au cours des 12 prochains mois sont le commerce de détail (59 %), la santé (56 %) et la fabrication (51 %).

Dans la plupart des secteurs, la majorité des RSSI affirment que l'IA va remplacer des postes de professionnels de la cybersécurité. Mais les RSSI du secteur des services financiers (91 %), des services professionnels (85 %) et de la fabrication (80 %) sont convaincus qu'elle va atténuer la pénurie de compétences en cybersécurité.

Le paysage des menaces

Ce sont les applications et infrastructures cloud qui inquiètent le plus les RSSI lorsqu'on les interroge sur les lacunes dans la couverture de sécurité, tous secteurs confondus. Les RSSI des services professionnels (71 %), de la santé (64 %) et de la technologie (64 %) mentionnent les applications cloud, tandis que les RSSI du secteur de la fabrication (64 %) observent les failles de sécurité les plus importantes dans la sécurité du cloud. Les services financiers (57 %) craignent davantage les lacunes de sécurité qu'ils observent chez les tiers et dans la chaîne d'approvisionnement.

96 % des organisations du secteur de la santé et 90 % des entreprises manufacturières déclarent avoir été victimes d'au moins une attaque perturbatrice au cours de l'année écoulée.

Dans le secteur des communications et des médias, une part importante des RSSI (44 %) souligne que les processus de réponse aux incidents ou des problèmes de communication ont facilité la tâche des adversaires. Un pourcentage important des RSSI du secteur des technologies (42 %) évoquent la présence de vulnérabilités inconnues ou mal gérées dans les systèmes, ainsi que des défauts de configuration.

De nombreux secteurs ont été victimes d'attaques par ransomware qui ont eu un impact significatif sur leurs systèmes et leurs opérations commerciales ; en tête, les services financiers (59 %), la vente au détail (59 %) et la santé (52 %).

Contrairement à la croyance populaire, le secteur le plus susceptible de verser la rançon demandée par des pirates est celui du commerce de détail, où ils sont 95 % à avoir payé directement, via une cyberassurance ou par le biais d'un tiers.

C'est également ce secteur qui a le plus souvent versé une rançon comprise entre 25 000 $ et 99 999 $. La majorité des organisations du secteur de la communication et des médias attaquées par un ransomware (56 %) ont payé entre 100 000 $ et 249 999 $.

Méthodologie

Une société de recherche indépendante a mené deux études distinctes : l'une quantitative, l'autre qualitative. L'étude quantitative a ciblé 350 RSSI, DSI et autres dirigeants qualifiés équivalents en matière de sécurité. L'étude qualitative a ciblé 20 RSSI, DSI et responsables de la sécurité lors d'entretiens téléphoniques approfondis d'une heure.

Régions géographiques

L'étude quantitative a été répartie entre l'Amérique du Nord (États-Unis, Canada), la région EMEA (Royaume-Uni, Allemagne, France) et la région APAC (Australie, Nouvelle-Zélande, Japon, Singapour, Inde). Des études qualitatives ont été menées aux États-Unis, au Canada et au Royaume-Uni.

Secteurs d'activité

Les participants aux études qualitatives et quantitatives représentaient 17 secteurs, dont les services financiers (banque, valeurs mobilières, assurance), la fabrication, les médias et communications, la technologie, la santé, la vente au détail et en gros, les services professionnels, l'administration et le secteur public, l'enseignement (primaire, secondaire, supérieur/université), l'agriculture et la foresterie, le bâtiment et le génie, les biens de consommation, les sciences de la vie, l'exploitation minière, pétrolière et gazière, les télécommunications, les transports et les services publics.

Perspectives by Splunk : les leaders parlent aux leaders.

Découvrez les éclairages de décideurs sur la sécurité, l'informatique et l'ingénierie dans notre publication en ligne, Perspectives by Splunk. Vous pourrez écouter les dirigeants et les experts de Splunk, ainsi que des invités du secteur. Notre objectif est d'offrir les points de vue intéressants, provocateurs et inspirants de personnes qui font le même travail que vous dans de grandes entreprises du monde entier.

Visitez Perspectives by Splunk

Poursuivez la conversation avec Splunk :

splunk>

23-295950-Splunk-The CISO Report-EB-122_FR