État de la **cybersécurité en 2023**

Étude mondiale : comment
les organisations leaders mobilisent
l'ensemble de l'organisation
pour renforcer leur résilience

splunk>

La cybersécurité en 2023 : une force de réaction rapide

Les cyberattaques se font toujours plus nombreuses et sophistiquées, tandis que les systèmes des organisations deviennent de plus en plus complexes. Les équipes de sécurité, comme toujours, sont sous pression. Mais notre étude État de la cybersécurité en 2023 présente un résultat surprenant : le nombre de personnes interrogées s'affirmant incapables de suivre le rythme a diminué.

Mais ne criez pas victoire trop vite. Elles sont 53 % à dire qu'il est plus difficile de respecter les exigences de sécurité qu'il y a deux ans, et c'est encore beaucoup. Mais elles étaient 66 % en 2022. Nos propres experts en sécurité, capables de repérer le moindre nuage dans le ciel le plus bleu, rappellent que 2022 n'a pas connu autant d'événements à même de semer le désarroi chez les équipes de sécurité – pas de SolarWinds, pas de Log4J. « Pas d'iceberg pour votre Titanic, » pour les citer directement.

Que ces données représentent une amélioration progressive ou une simple accalmie, tout avantage est bon à prendre. Mais ça ne sera pas facile : la plupart des équipes de sécurité indiquent qu'elles sont encore trop engluées dans une approche réactive pour être réellement proactives.

En approfondissant, nous avons demandé à la petite majorité qui parle d'un travail devenu plus difficile de nous expliquer pourquoi. Les principaux défis de ce groupe sont :

- la sophistication croissante des menaces (selon 38 %, ce qui la place au 1er rang pour la troisième année consécutive) ;
- la complexité de la pile de sécurité (selon 30 %) ;
- les problèmes de supervision et de gestion des risques liés à l'IaaS et au SaaS (29 % et 28 %, respectivement) ;
- la charge de travail, qui englue les équipes dans une approche réactive (28 %).

Ce dernier point trouve écho dans plusieurs réponses minoritaires. Les participants nous disent être dépassés par le nombre d'attaques (24 %) et de faux positifs (25 %). Ils sont encore 25 % à avoir du mal à embaucher ou à retenir suffisamment de personnel qualifié.

Mais ces difficultés varient d'une région à l'autre. Les organisations de la région Asie-Pacifique sont plus nombreuses (5 à 7 points de pourcentage) que la moyenne mondiale à trouver difficile de superviser les applications SaaS et d'analyser efficacement toutes les données de sécurité. Les participants européens sont moins nombreux à s'en plaindre, tandis que les organisations nord-américaines s'alignent sur la moyenne mondiale.

Méthodologie

Les chercheurs ont interrogé 1 520 responsables de la sécurité et de l'IT qui consacrent la moitié de leur temps ou plus aux problèmes de sécurité.

10 pays

Répartis à parts égales entre l'Amérique du Nord, l'Europe de l'Ouest et l'Asie-Pacifique : Australie, Canada, France, Allemagne, Inde, Japon, Nouvelle-Zélande, Singapour, Royaume-Uni, États-Unis

15 secteurs d'activité

Aéronautique et défense, biens de consommation finis, éducation, énergie, services financiers (banque, valeurs, assurance), gouvernement (fédéral/national, étatique et local), santé, sciences de la vie, fabrication, médias, vente au détail/en gros, technologie, télécommunications, transport/logistique, services publics

Nous avons constaté que, tous secteurs et zones géographiques confondus, les responsables de la sécurité et leurs collègues dans l'ensemble de l'organisation collaborent de plus en plus pour améliorer la résilience. La cybersécurité classique concerne la prévention proactive des incidents, tandis que la résilience est réactive : elle décrit ce que vous faites une fois qu'un incident se produit.

Mais lorsque vous préparez votre organisation à se remettre le plus efficacement possible d'une crise, vous êtes dans la proactivité. L'évaluation des risques, la planification de la réponse aux incidents, les investissements clés dans la technologie et la formation… tout cela mérite une réflexion stratégique qui dépasse le strict cadre de la cybersécurité.

Les participants nous disent que les équipes de sécurité réussissent mieux à s'associer à l'ensemble de l'organisation, et sont considérées comme des partenaires précieux. Leurs membres sont vus comme des facilitateurs, et non plus des rabat-joie multipliant les interdits. Comme nous le verrons ci-dessous, 79 % des secteurs d'activité considèrent l'équipe de sécurité comme un partenaire précieux et lui montrent en lui donnant une place à la table de la collaboration – et un meilleur financement.

Quant aux décideurs qui fixent le budget de la sécurité, ils examinent de plus en plus les métriques qui mesurent la résilience, à commencer par le temps moyen de récupération. Le MTTR est même en tête de liste.

Nous observons des défis considérables

Voici un aperçu des chiffres clés que vous lirez dans le rapport de cette année :

- **64 % des équipes SOC ont du mal à passer** d'un outil de sécurité à un autre, et l'intégration insuffisante ne leur facilite pas la tâche.
- **88 % des participants signalent des défis dans le domaine des talents**, qu'il s'agisse de trouver des compétences clés ou simplement d'embaucher suffisamment de personnes.
- Les malfaiteurs finissent toujours par entrer. Et quand ils y parviennent, leur **temps de séjour moyen est de 2,24 mois**, soit neuf longues semaines environ.

Nous observons également des efforts pour relever ces innombrables défis. Quelques points clés :

- **95 % des organisations ont davantage mis l'accent** sur les évaluations des risques liés aux tiers.
- **81 % des organisations font converger** des aspects de la sécurité et des opérations informatiques.
- **95 % des budgets de sécurité augmenteront** au cours des deux prochaines années, et même « de manière significative » pour 56 % d'entre eux.

Dans l'ensemble, qu'ils se disent dépassés ou non, les participants ont identifié un éventail diffus de défis. Aucun type de crise ne dominait, mais on retrouve en première place un problème généralisé : les équipes passent trop de temps à prendre en charge des urgences.

Cette approche réactive perpétuelle a plusieurs causes et, franchement, peu de solutions. Face aux milliers de cyberattaques subies par les entreprises, cette posture réactive est inévitable. Les équipes de sécurité intelligentes font de leur mieux pour devancer les vecteurs d'attaque connus, mais de nouvelles techniques apparaissent sans cesse et vous obligent à agir dans l'urgence.

Et la conformité ne fait que gagner en complexité. La sophistication croissante de la technologie, de l'utilisation des données et des méthodes d'attaque entraîne, à terme, le renforcement des normes réglementaires.

Principaux défis de cybersécurité

Les participants étaient invités à indiquer leurs trois principaux défis internes.

L'état du SOC

Comme l'indiquent les pages précédentes, les équipes de sécurité sont mises à rude épreuve. Le centre des opérations de sécurité d'aujourd'hui a beaucoup à faire, et pas assez de personnel pour s'en occuper.

- **64 % des équipes SOC se plaignent de devoir basculer entre d'innombrables outils de sécurité et consoles de gestion disparates, avec peu (voire pas du tout) d'intégration, ce qui entrave les investigations et empêche d'apporter une réponse complète et rapide.**
- **49 % déclarent manquer de personnel pour trier manuellement les événements de sécurité en augmentation, les analyser et y répondre.**

Le résultat : une augmentation du risque due à la charge de travail. En moyenne, les participants estiment que 41 % des alertes qui mériteraient un examen sont ignorées en raison d'un manque de ressources SOC. Et bien sûr, les alertes que vous n'investiguez pas peuvent inclure un vrai positif, et donc laisser passer une attaque. Tout est compromis : le véritable retour sur investissement des outils coûteux qui génèrent ces alertes, l'efficacité et le moral de votre équipe d'analystes, ainsi que la sécurité et la résilience réelles de votre organisation.

À l'heure où les économies tendent vers la récession, les problèmes de dotation en personnel risquent de devenir encore plus criants.

55 % des participants s'attendent à ce qu'il soit plus difficile de recruter et de fidéliser des employés en période de récession.

32 % pensent que l'embauche et la rétention deviendront au contraire plus faciles.

Impact de la crise des talents

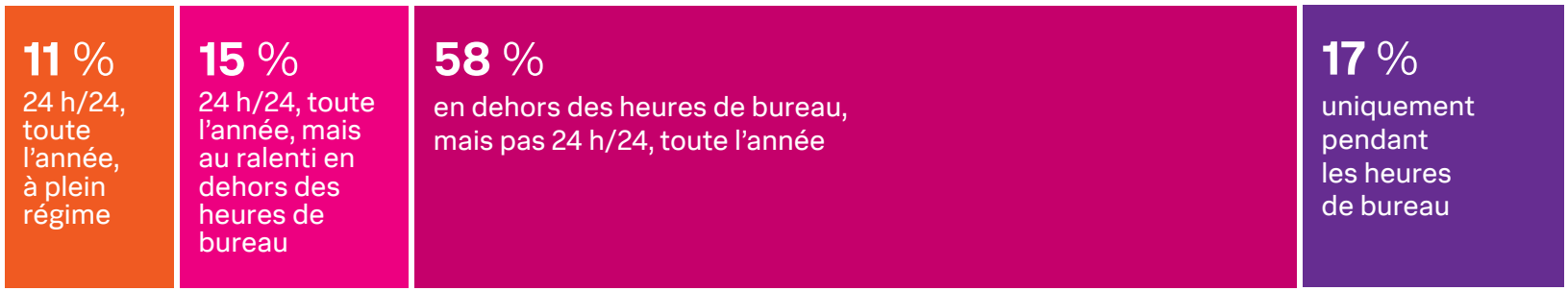
L'éternelle pénurie de main-d'œuvre demeure un grave problème : 88 % des personnes interrogées signalent des difficultés en matière de dotation en personnel et de compétences en cybersécurité ; parmi elles, 53 % déclarent ne pas pouvoir embaucher suffisamment de personnel en général (ce qui correspond aux résultats de l'année dernière) et 59 % (contre 58 %) n'arrivent pas à trouver de talents possédant les bonnes compétences.

Les responsables de la sécurité se tournent en grand nombre vers les fournisseurs de services de sécurité gérés (42 % utilisent davantage les MSSP), qui permettent aux équipes à la fois de renforcer la couverture en dehors des heures de travail et de décharger les problèmes de niveau 1 24 h/24. Malgré cela, les difficultés liées aux talents ont entraîné un certain nombre de problèmes au cours des 12 derniers mois :

- **81 % des personnes interrogées affirment que les membres de leur personnel ont été contraints d'assumer des responsabilités pour lesquelles ils ne sont pas prêts, contre 76 % l'année dernière.**
- **81 % déclarent que des membres critiques du personnel ont quitté l'organisation pour un autre emploi en raison d'un burn out.**
- **78 % des participants disent que cette augmentation de leur charge de travail les a incités à envisager un changement de poste, contre 70 % l'année précédente.**
- **77 % rapportent qu'un ou plusieurs projets ou initiatives ont échoué, contre 68 %.**

L'acquisition de talents est toujours en crise dans le secteur de la cybersécurité. Ces chiffres ne sont plus seulement symptomatiques d'une maladie chronique, mais indiquent aussi une maladie de plus en plus aiguë. Et ignorer le problème serait une grave erreur.

Comment les SOC fonctionnent



Atténuer les défis liés aux talents

Les responsables de la sécurité prennent des mesures pour atténuer les défis. Comme indiqué sur la page précédente, les MSSP jouent un rôle plus important : 86 % des organisations se sont appuyées sur des fournisseurs de services pour combler les lacunes en matière de compétences. En effet, 56 % des personnes interrogées affirment que la majorité des opérations de sécurité de leur organisation sont sous-traitées à un fournisseur de services tiers, le plus souvent pour les étendre au-delà des heures habituelles et pour avoir accès aux outils plus avancés des fournisseurs de services. 42 % prévoient d'ailleurs d'augmenter ces engagements.

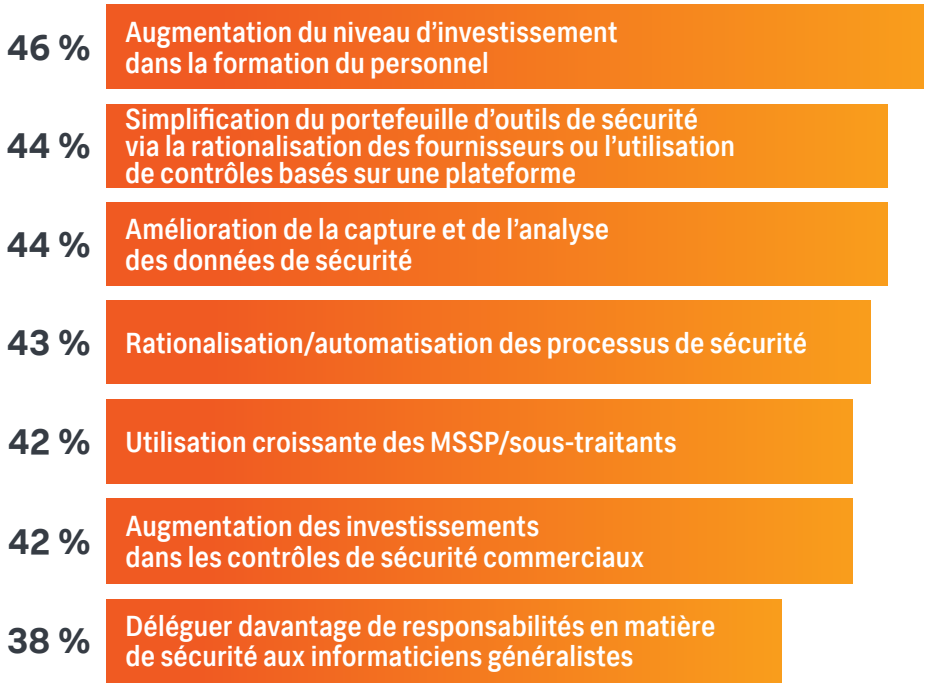
Ils cherchent également davantage d'aide au sein de leur propre organisation : 86 % des entreprises ont commencé à former des personnes extérieures à l'équipe de sécurité pour combler les lacunes, et 38 % prévoient de confier davantage de tâches de sécurité au personnel informatique au cours de l'année à venir.

L'intensification de la formation est le choix numéro 1, avec l'augmentation du recrutement, pour les participants de toutes les régions. Principalement, les équipes de sécurité sont amenées à améliorer leurs compétences au niveau des opérations et de l'architecture cloud (41 %), ainsi que du développement d'applications sécurisées (42 %).

De plus, les équipes de sécurité adoptent l'automatisation et améliorent leurs outils, et elles mettent l'accent sur les données (voir le graphique ci-contre), pour rendre les équipes en sous-effectif bien plus efficaces.

Tactiques prioritaires pour surmonter les défis liés aux talents

(en plus du recrutement)



Le premier choix, toutes régions confondues, était « plus de formation » (45-47 %). Mais dans la région Asie-Pacifique, il arrive ex-æquo avec l'option « plus d'investissements dans les contrôles de sécurité commerciaux », à 47 %.

La résilience est le principal indicateur

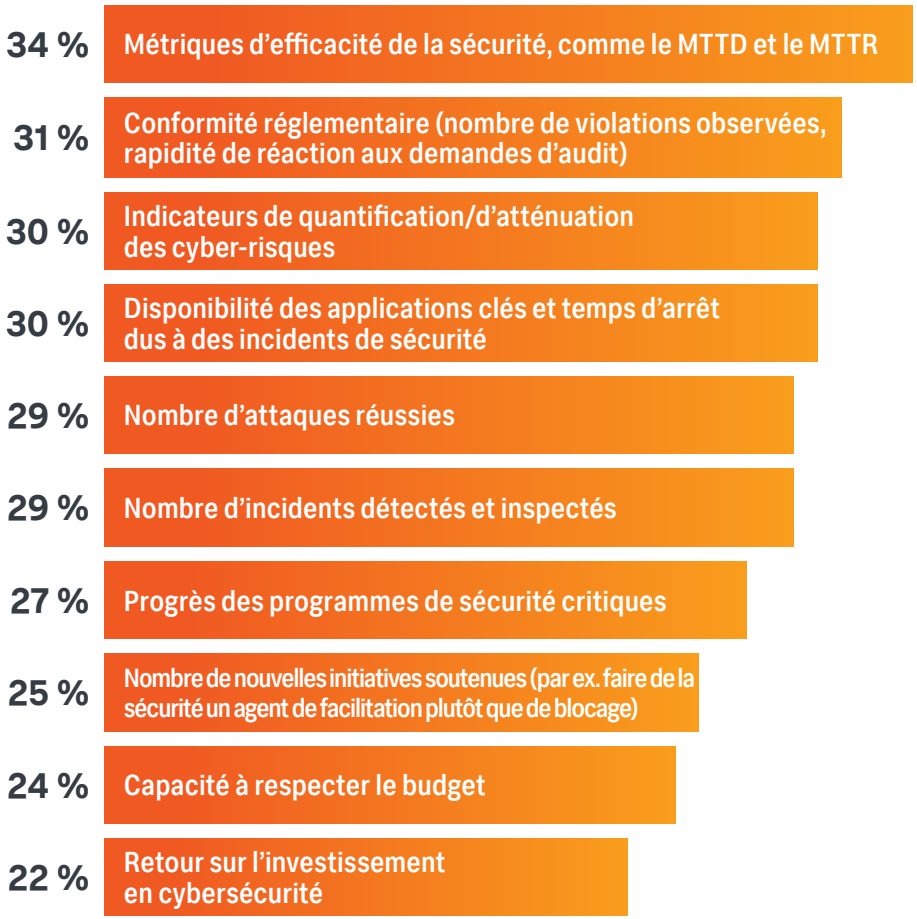
Nous avons demandé aux participants d'indiquer les trois principales métriques de performance utilisées par les décideurs métier pour juger de l'efficacité de la sécurité, et nous voyons émerger un état d'esprit de résilience. Dans le graphique de droite, quatre des six premières réponses (toutes sauf la conformité et l'atténuation des risques) influent directement sur les stratégies de résilience : le temps moyen de détection et de récupération arrive en tête (34 %), et les temps d'arrêt (30 %) devancent le nombre d'attaques et d'incidents.

La quantité et la sophistication des attaques auxquelles vous faites face sont hors de votre contrôle – vous ne savez pas qui vous attaquera demain – mais vous pouvez certainement mesurer votre MTTR. Et si vous acceptez le fait que les interruptions de service sont inévitables, la rapidité et l'efficacité avec lesquelles vous les gérez deviennent cruciales.

Ryan Kovar, éminent stratège en sécurité de Splunk, qui dirige notre équipe SURGe de conseil sur les menaces, souligne : « Le MTTR est plus facile à mesurer et à améliorer. Il n'est pas forcément possible d'améliorer votre MTTD, parce que les menaces sont inconnues. SolarWinds avait un mode opératoire inédit, et son temps de détection a été de deux ans. Mais vous pouvez œuvrer pour améliorer le MTTR. Et c'est là que vous créez de la résilience. »

Comment les décideurs métier mesurent le succès de la sécurité

Principaux indicateurs utilisés par les décideurs métier pour comprendre la cybersécurité



Les équipes de sécurité ont depuis longtemps compris la valeur qu'elles apportent à l'entreprise et savent qu'une bonne sécurité et une résilience forte ne nécessitent pas de dire non à chaque nouvelle initiative. Mais il a fallu du temps aux entreprises pour comprendre cette mentalité et faire de la sécurité un partenaire actif, moteur du succès de l'entreprise. Cette année, notre étude montre que pour la plupart des équipes, les fonctions métier l'ont bien compris.

Les participants nous disent en effet que 79 % des secteurs d'activité considèrent l'équipe de sécurité comme une source d'informations fiable (49 %) ou comme un catalyseur essentiel de la mission de l'organisation (30 %). Une petite minorité considère toujours la sécurité comme un mal nécessaire (12 %) ou un véritable obstacle (8 %).

Ce nouveau rôle de partenaire stratégique et de facilitateur occupé par l'équipe de sécurité a un effet : une collaboration plus large et une focalisation holistique sur la résilience, comme nous allons le voir. Et au niveau de la direction, ce respect et cette inclusion dans les décisions produisent des résultats tangibles. Les personnes interrogées nous disent que cet accès à la direction de l'entreprise aide l'équipe de sécurité à collaborer avec d'autres parties de l'entreprise (46 %) et entraîne une augmentation du financement de l'équipe de sécurité (42 %).

79 % des acteurs de l'entreprise considèrent l'équipe de sécurité comme un partenaire et non comme un obstacle.

Incidents, alertes et vecteurs de menace

Malgré de nouvelles stratégies et de meilleurs partenariats au sein de l'organisation, les équipes de sécurité sont confrontées à des défis importants. Et les pirates ne faiblissent pas. À l'échelle mondiale, notre étude a révélé une augmentation du nombre d'incidents, des temps d'attente et des dommages affectant l'entreprise.

Un impact existentiel

Les incidents de sécurité représentent une menace existentielle. En plus du temps et des ressources considérables consacrés à nettoyer les dégâts, un nombre important de participants affirment que les incidents ont nui à la position concurrentielle de leur entreprise, impacté le cours de son action ou dégradé sa réputation. Seuls 4 % des participants déclarent avoir subi des incidents sans conséquence importante.

Concernant les types d'attaques, notez que par « attaques de la chaîne d'approvisionnement » (qui ont touché 46 % des personnes interrogées dans le monde), nous entendons des attaques réelles qui ont abouti en utilisant ce vecteur. Si nous avions soumis aux participants la proposition « vous avez découvert des vulnérabilités inexploitées dans des logiciels tiers et les avez corrigées à temps », ce nombre serait plus élevé. Beaucoup plus élevé.

Quel que soit le chemin, une fois que les malfaiteurs ont infiltré le réseau, ils prennent leurs aises. En moyenne, les participants nous disent qu'il s'écoule 2,24 mois, soit environ neuf semaines, entre le moment où un acteur malveillant pénètre dans leurs systèmes et celui où les acteurs concernés en prennent connaissance. Ce qui laisse beaucoup de temps pour voler ou casser des choses.

Effets des incidents au cours des deux dernières années

Incidents survenus au cours des deux dernières années

Le manque de résilience est une grave menace

Les équipes de sécurité comprennent qu'elles doivent renforcer leur résilience. La plupart des participants (62 %, contre 54 % l'année dernière) signalent que les incidents de cybersécurité interrompent le fonctionnement des applications critiques de l'entreprise au moins une fois par mois. Le nombre moyen de ces interruptions est d'environ 22 par an (contre 19 l'année dernière).

Les équipes de sécurité affirment qu'elles s'efforcent toujours d'améliorer ces indicateurs de résilience. En moyenne, elles disent vouloir réduire le MTTD de 40 % et le MTTR de 53 %. Nous avons constaté une amélioration par rapport aux résultats de l'année dernière : le temps moyen de récupération (MTTR) des workloads critiques touchés par des temps d'arrêt imprévus liés à un incident de cybersécurité est de 15,5 heures (et non plus 21,4 heures). Pourtant, les coûts liés aux interruptions consomment 2,7 % du chiffre d'affaires annuel.

Et le contrôle de ces coûts n'est pas le seul problème. On a demandé aux participants pourquoi ils se concentraient sur la résilience :

- **83 % confient que le risque d'interruption importante de leurs activités est élevé.**
- **79 % pensent qu'une perte de productivité peut leur faire prendre du retard par rapport au rythme de l'innovation.**
- **78 % des personnes interrogées conviennent que l'effet des temps d'arrêt sur l'expérience numérique peut leur coûter des clients.**

Cette problématique a des répercussions au plus haut niveau de direction. Presque tous les participants (91 %) déclarent que leur RSSI collabore plus étroitement avec les responsables métiers (finance, marketing, opérations, etc.) sur les stratégies et les investissements en matière de cyber-résilience. Mais ces RSSI ont fort à faire :

- **Ils ne sont que 31 % à avoir institué une approche formelle de la cyber-résilience à l'échelle de l'organisation, sur l'ensemble des systèmes critiques.**
- **Seuls 38 % ont mis en place une stratégie de résilience dans des domaines spécifiques de l'organisation.**
- **Et 31 % disent qu'ils n'ont pas encore mis en œuvre de stratégies de résilience.**

Alors que **91 % des RSSI** collaborent à l'échelle de l'entreprise sur les questions de résilience, ils sont moins d'un tiers à avoir mis en place une approche de résilience à l'échelle de l'organisation.

Vecteur par vecteur

Lorsque nous avons demandé aux participants d'examiner une longue liste stressante pour choisir les trois vulnérabilités potentielles qui les préoccupent le plus, leurs réponses furent assez uniformément réparties, sans qu'aucune ne se détache. Deux types d'attaques très médiatisées méritent une analyse plus approfondie : les attaques de la chaîne d'approvisionnement logicielle et les ransomwares. L'importance du cloud public comme surface d'attaque des organisations mérite également une attention particulière.

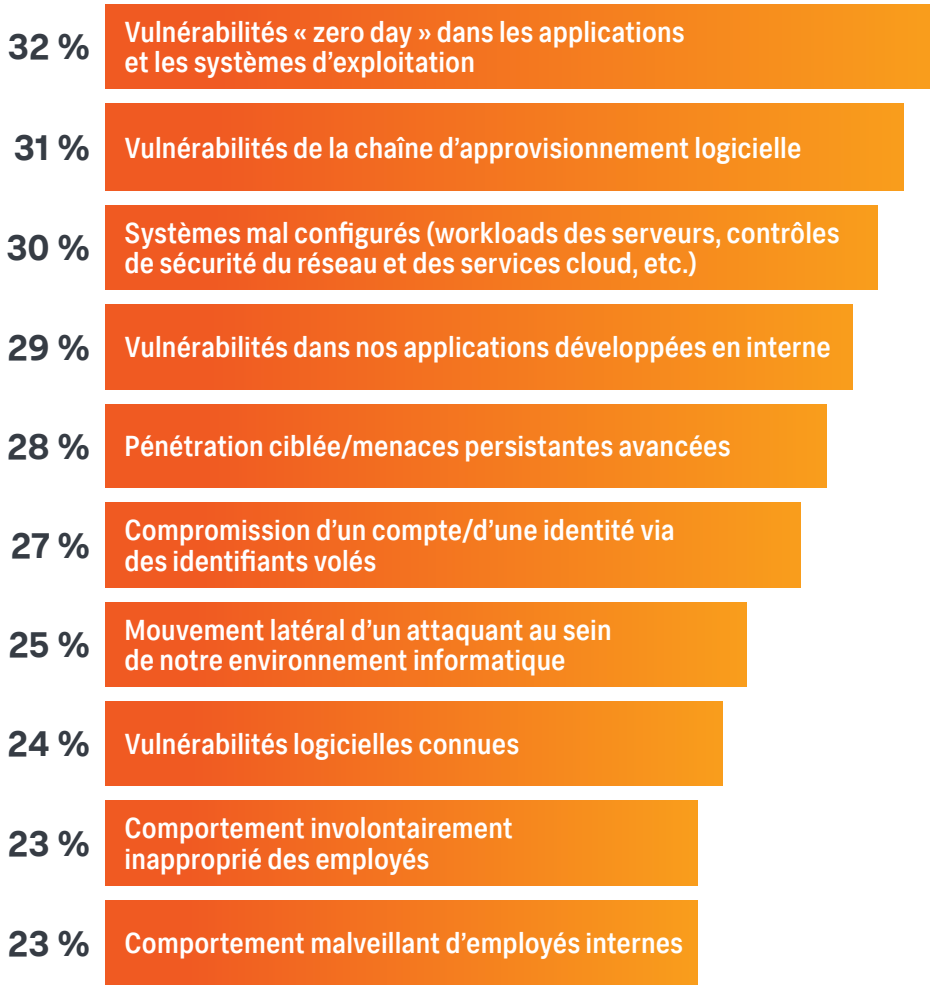
Chaîne d'approvisionnement. Les attaques de la chaîne d'approvisionnement logicielle sont une priorité dans l'ère post-SolarWinds (et Log4j, et Kaseya, etc.). Au moins 95 % des organisations ont davantage mis l'accent sur les évaluations des risques liés aux tiers, contre 90 % – un chiffre déjà remarquable – il y a un an.

L'examen des tactiques impliquées révèle une approche très diffuse de la sécurité de la chaîne d'approvisionnement. Sur une liste de 17 réponses aux menaces de la chaîne d'approvisionnement, les trois premières sont à égalité avec un taux d'adoption de 26 % :

- **évaluer les contrôles de sécurité pour comprendre les capacités de prévention/détection spécifiques aux attaques de la chaîne d'approvisionnement ;**
- **renforcer les systèmes d'authentification ;**
- **augmenter les budgets de sécurité.**

La fragmentation des réponses et l'absence de tactique majoritaire traduisent une approche décousue d'un problème qui n'a été mis au jour que récemment.

Vulnérabilités face aux menaces les plus préoccupantes



Ransomware. Les ransomwares, c'est un peu comme le COVID-19. Vous connaissez peut-être encore des gens qui n'ont pas encore été touchés, mais ils sont de moins en moins nombreux. Depuis l'étude État de la cybersécurité en 2022, le nombre d'organisations affirmant n'avoir jamais subi d'attaque par ransomware est passé de 21 % à seulement 13 %. De même, si 35 % des entreprises en 2022 ont vu leurs données ou leurs systèmes pris en otage, elles sont 43 % cette année.

Et lorsqu'elles sont touchées, elles sont plus susceptibles que jamais de payer. L'année dernière, 66 % des organisations ont déclaré qu'elles (ou leur assureur) avaient tout simplement payé les pirates. Cette année, ce chiffre est de 75 %. Et le montant des rançons continue d'augmenter : l'année dernière, seuls 32 % des participants rapportaient que leur rançon la plus élevée avait été de 250 000 $ ou plus. Cette année, ils sont 50 %. Les participants nous disent en effet que la rançon la plus élevée versée aux attaquants était de 430 978 $ en moyenne, contre 346 897 $ l'année dernière, soit une hausse de 24 %.

(Cela nous a surpris, car d'autres recherches menées au cours de l'année écoulée suggéraient que les rançons étaient en baisse. En vérifiant nos chiffres, nous constatons que les participants occupant des postes à responsabilité, et donc qui devraient être mieux informés, sont encore plus nombreux (79 %) à avoir payé des rançons plus élevées, plus souvent.)

Comme pour les risques liés à la chaîne d'approvisionnement, l'adoption de tactiques de lutte contre les ransomwares est très répandue. On observe cependant davantage de cohérence dans les approches. Deux tactiques sont adoptées ou intensifiées par 33 % des participants : investir dans des solutions SIEM et se concentrer sur la sécurité des e-mails. Quatre autres tactiques affichent un taux d'adoption de 31 % : le SOAR, les analyses avancées, l'authentification multifacteurs et les outils de renforcement de la configuration des terminaux.

D'autre part, le pourcentage plus faible d'investissement dans des capacités de sauvegarde et de restauration étanches (21 % des participants) suggère que les entreprises donnent la priorité à la détection et à la réponse plutôt qu'au rétablissement.

La réponse est dans les données : 91 % pensent en effet que l'amélioration de la capture et de l'analyse des données de détection est l'un des outils les plus efficaces pour empêcher les attaques par ransomware de réussir.

Sécurité cloud. C'est dans le cloud que se déroule l'action. 50 % des personnes interrogées affirment que la majorité du temps de leur équipe SOC est consacrée à la résolution de problèmes dans le cloud public, tandis qu'elles ne sont que 13 % à consacrer l'essentiel de leur temps à des problèmes sur site.

Et c'est logique, car une grande partie de nos environnements informatiques se trouve dans le cloud. 53 % des personnes interrogées déclarent que la majorité de leurs applications et workloads critiques s'exécutent dans le cloud. Fait intéressant : ce chiffre est en baisse par rapport à l'année dernière (66 %), mais cela reste significatif. Et dans le cloud public, le risque n'est pas tant qu'une attaque déjoue les défenses de votre fournisseur de cloud. Il est plus probable qu'il vienne d'une mauvaise configuration de votre côté. Les malfaiteurs ne cherchent pas à enfoncer les portes ; ils savent que vous en laisserez une ouverte.

Les participants nous ont donné leurs trois principaux défis en matière de sécurité dans le cloud :

1. **maintenir la cohérence de la sécurité dans leurs centres de données et leurs environnements de cloud public (défi n° 1 pour la troisième année consécutive, mais avec un pourcentage qui passe de 45 % l'année dernière à 33 % en 2023) ;**
2. **garantir l'exactitude des systèmes de gestion des identités et des accès (IAM) et les tenir à jour (32 %, et une place de gagnée par rapport à l'année dernière) ;**
3. **l'augmentation des coûts et de la complexité liée à la multiplication des contrôles de cybersécurité (28 %, en recul d'une place au classement).**

Nous leur avons ensuite demandé ce qu'ils faisaient à ce sujet. Encore une fois, l'éventail des tactiques était large, sans véritable leader, mais quelques approches courantes se dégagent :

1. **identifier les configurations de workload qui ne sont pas conformes et/ou qui ne respectent pas les bonnes pratiques du secteur (n° 1 pour la troisième année consécutive, bien que le pourcentage soit passé de 39 % en 2022 à 30 % cette année) ;**
2. **configurer les groupes de sécurité (notamment les workloads des serveurs en contact avec l'extérieur) (25 %, et remonte d'une place au classement) ;**
3. **améliorer la compréhension des pistes d'audit parmi les comptes privilégiés et de service (24 %, conserve sa troisième place).**

Les architectures cloud et hybrides sont nouvelles et complexes, et elles évoluent sans cesse. Elles continueront à représenter un défi de taille.

Il faut connaître le cloud : lorsque nous avons posé des questions sur les différents domaines dans lesquels les équipes de sécurité sentent qu'elles doivent améliorer leurs compétences, les opérations et l'architecture du cloud étaient en tête, citées par 41 % des personnes interrogées.

Objectifs et stratégies

La poursuite de la cyber-résilience et de la résilience globale de l'entreprise oriente les stratégies de sécurité à plusieurs égards : augmentation du financement et de la collaboration, priorités axées sur le cloud, l'analyse, l'automatisation et plus encore.

Converger vers la résilience

Pour relever les défis nouveaux ou persistants, les organisations misent sur la résilience et l'agilité. Pour les 12 prochains mois, 51 % des personnes interrogées prévoient des solutions ou des investissements qui combinent des efforts de cyber-résilience aux initiatives traditionnelles de continuité des activités et de préparation à la reprise après sinistre. De plus, 48 % comptent investir pour accélérer la reprise des services aux utilisateurs, et 47 % prévoient des investissements pour accélérer la réponse des équipes de sécurité.

La résilience est un sport d'équipe, et la plupart des participants voient une promesse dans la convergence des opérations de sécurité avec d'autres fonctions (par exemple, collaborer plus étroitement, créer des rôles hybrides qui superposent les fonctions, etc.) :

- **81 % des organisations font converger des aspects de la sécurité et des opérations informatiques.**
- **69 % font converger des aspects des opérations de sécurité et de l'expérience numérique.**
- **69 % font converger des aspects des opérations de sécurité et du développement d'applications.**
- **61 % font converger des aspects des opérations de sécurité et de l'observabilité.**

Pourquoi ? Les participants pensent le plus souvent que la convergence contribuera à la visibilité globale des risques dans leur environnement (58 %) et qu'ils bénéficieront d'une meilleure coopération dans les processus d'identification et de réponse aux menaces (55 %).

Principales initiatives de sécurité

Invités à nommer leurs trois principales priorités, les participants citent le plus souvent celles-ci :

Les budgets augmentent, les priorités changent

Les équipes de sécurité dépensent plus et collaborent plus largement. Au moins 95 % des personnes interrogées s'attendent à ce que leurs dépenses de sécurité augmentent au cours des deux prochaines années, et 56 % déclarent que les dépenses augmenteront de manière significative (contre 51 % l'année précédente).

Là où le financement ira aux outils et à la technologie, les approches sont réparties uniformément : 50 % prévoient d'opter essentiellement pour des outils basés sur une plateforme avec une intégration prête à l'emploi. L'autre moitié va plutôt mettre l'accent sur des solutions de pointe individuelles, en les intégrant à l'aide d'API au besoin.

Les orientations stratégiques ont changé depuis l'année dernière, comme en témoignent ces quatre priorités principales :

- **développement et construction d'une architecture logicielle intégrée pour les outils d'analyse et d'opérations de sécurité (38 % contre 21 % il y a un an – cette stratégie, précédemment ex æquo à la 3e place, est aujourd'hui n° 1) ;**
- **acquérir des outils d'opérations de sécurité conçus pour faciliter l'automatisation et l'orchestration des processus (35 % contre 22 % il y a un an) ;**
- **réunir les outils et le personnel au sein d'un SOC d'entreprise (35 %, contre 15 % en 2022, ce qui fait entrer cette approche dans le top 10) ;**
- **développer des processus d'opérations de sécurité documentés plus formels (33 %, contre 17 %, ce qui lui donne la 10e place).**

Prises dans leur ensemble, ces quatre stratégies principales traduisent le besoin de créer un SOC plus efficace, plus rapide et plus professionnalisé.

95 % des budgets de sécurité augmenteront au cours des deux prochaines années, et même « de manière significative » pour 56 % d'entre eux.

Analyse et automatisation

Le déploiement de technologies conçues pour l'analyse de la sécurité et pour l'automatisation et l'orchestration des opérations est resté remarquablement stable cette année. 67 % des personnes interrogées déclarent déployer de telles technologies, dont 37 % de manière intensive. Ces résultats sont sensiblement identiques à ceux de l'année dernière, qui donnaient 67 % d'adoption, dont 36 % d'adoption intensive.

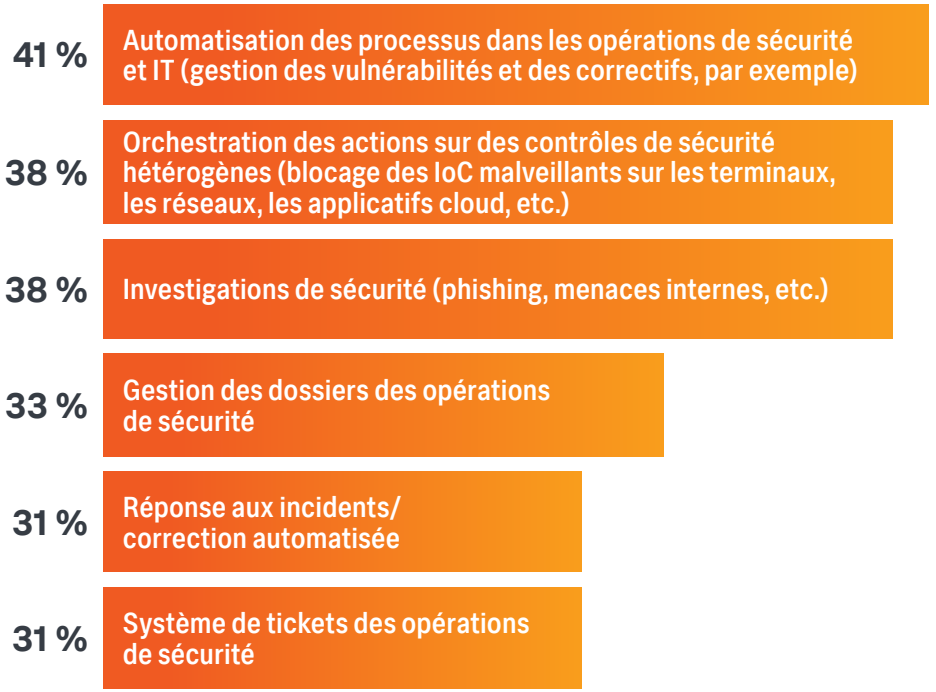
Les personnes interrogées déclarent utiliser l'analyse tout au long du cycle de vie des attaques, pour améliorer la détection des menaces (37 %), pour identifier les cyber-risques (36 %), pour accélérer les investigations (33 %) et pour automatiser les mesures de correction (35 %).

Elle est également employée pour automatiser les processus de sécurité basés sur des données en temps réel (33 %) et pour faciliter la hiérarchisation des investigations (également 33 %).

L'automatisation est mise au service de plusieurs tâches clés :

- **29 % choisissent d'intégrer les outils de sécurité aux systèmes d'exploitation informatique.**
- **27 % donnent la priorité à l'intégration de threat intelligence externe aux données de sécurité internes.**
- **27 % privilégient l'automatisation des tâches de correction de base (comme la mise à jour des contrôles de sécurité des terminaux) avec leurs initiatives d'automatisation et d'orchestration.**

Principales priorités pour l'automatisation des processus



Tout ne progresse pas au même rythme. Les efforts visant à enrichir les analyses de sécurité par d'autres analyses – opérations IT, fonctions métier et gestion des risques – semblent plafonner. Il y a un an, 43 % des organisations faisaient état d'un niveau significatif d'intégration entre ces sources ; aujourd'hui, ce chiffre est tombé à 39 %. (Et 35 % encore, dans le monde, signalent une intégration marginale.) On observe une nette différence d'une région à l'autre : 45 % des participants nord-américains font état d'une intégration significative, alors qu'ils ne sont que 35 % et 36 %, respectivement, en Europe et en Asie-Pacifique.

La meilleure explication de cette régression réside sans doute dans la complexité des données et la difficulté à intégrer des outils disparates.

Ryan Kovar, à la tête de l'équipe SURGe, note : « Il y a beaucoup de complexité dans le développement de bonnes analyses. La pandémie a entraîné de nombreux changements et une explosion de nouvelles sources de données. Alors que les organisations viennent tout juste de maîtriser ce type d'intégration analytique, elles se retrouvent avec toutes ces nouvelles données et doivent tout refactoriser. »

Cela dit, les fournisseurs (y compris Splunk) cherchent toujours à créer des moyens plus simples et immédiats de réduire la complexité pour aider les entreprises à surmonter ces écueils. Pour se remettre sur les rails, il faut reprendre les processus depuis le début : définir des objectifs d'intégration ; normaliser les données, utiliser des détections prédéfinies souvent fournies avec les solutions et, si possible, les outils d'analyse de sécurité ; et continuer à cultiver la collaboration et la confiance entre les équipes et les silos.

Intégration de l'analyse de sécurité aux autres données d'analyse

par ex. : ITOps, fonctions métier, gestion et autres analyses

Du quasi-zéro au héros de la résilience

Nous avons constaté que les équipes de sécurité sont de plus en plus perçues comme des partenaires précieux plutôt que des obligations ou des obstacles à surmonter. Le résultat (ou la cause) en est une collaboration plus profonde à tous les niveaux.

Pour prendre un exemple au niveau le plus bas, le DevSecOps est pratiquement omniprésent. Seuls 3 % des participants indiquent que leur organisation n'exploite pas les pratiques DevSecOps, contre 25 % en 2022.

Côté leadership, nous avons noté que 91 % des RSSI collaborent avec d'autres dirigeants sur la résilience. Ils sont en effet 68 % à rencontrer le conseil d'administration chaque semaine (29 %) ou chaque mois (39 %). Seuls 8 % se réunissent moins d'une fois par trimestre. Et ces réunions produisent des résultats très intéressants :

- **meilleure capacité à collaborer entre les unités commerciales (46 %) ;**
- **meilleure perception de la sécurité par les autres parties de l'organisation (44 %) ;**
- **meilleure place accordée aux dépenses de sécurité (43 %) ;**
- **augmentation du financement de la sécurité (42 %) ;**
- **diffusion des initiatives de cybersécurité dans une culture plus large (42 %).**

Dans tous les domaines, les pratiques collaboratives aident les équipes de sécurité à tenir la ligne de front face à des attaquants de plus en plus sophistiqués.

63 % des participants ont évoqué chacun des avantages suivants du DevSecOps : efficacité opérationnelle ; meilleure sécurité du cloud ; logiciels plus sûrs et plus fiables ; posture de sécurité renforcée et plus proactive.

59 % font part d'une baisse du nombre d'incidents de sécurité grâce aux pratiques DevSecOps.

Notez que les participants en Europe étaient plus nombreux à rapporter des résultats positifs, dépassant à chaque fois la moyenne mondiale de 4 à 9 points de pourcentage.

Recommandations

Les équipes de sécurité doivent travailler avec l'ensemble de l'organisation pour réussir. Nous allons voir, en huit pratiques, la façon dont les équipes les plus axées sur le partenariat construisent des organisations plus résilientes.

La véritable résilience des entreprises ne repose pas seulement sur les efforts cruciaux de l'équipe de sécurité pour améliorer la détection des menaces et la réponse aux incidents : elle s'appuie aussi sur une collaboration globale. Dans les organisations avec lesquelles nous avons travaillé, la résilience atteignait son plus haut niveau lorsqu'une approche collaborative dans laquelle toutes les problématiques – du développement logiciel à la supervision de l'infrastructure en passant par la planification de la continuité des activités – rassemblent les responsables de la sécurité et les responsables informatiques et commerciaux autour de la table pour protéger l'organisation.

Le thème du partenariat a traversé les conclusions dans notre étude de cette année. Et quand nous examinons comment ces organisations qui jouissent de la confiance de leurs collègues poursuivent leur mission, certaines recommandations émergent. Les quatre premières sont directement liées à la valeur du partenariat inter-organisationnel.

1. Utilisez les données et l'analyse pour optimiser la détection et la réponse aux menaces.

Les équipes de sécurité considérées comme des facilitatrices exploitent plus souvent l'analyse pour identifier les cyber-risques (38 % contre 26 %), améliorer la détection des menaces (40 % contre 25 %), accélérer les investigations (35 % contre 27 %) et automatiser les mesures de correction (38 % contre 22 %). Ces équipes œuvrent à renforcer l'efficacité de la détection, de l'investigation et de la réponse en s'appuyant sur les données. Et tout en améliorant les résultats des opérations de sécurité, ces efforts contribuent également à élever le statut de l'équipe de sécurité au sein de l'entreprise.

2. Planifiez la résilience.

Les « business enablers » sont beaucoup plus enclins à affirmer travailler au sein d'organisations qui ont une approche formelle de la cyber-résilience, instituée à l'échelle de l'entreprise (32 % contre 19 % de ces équipes considérées comme des obstacles). Et c'est essentiel. Être un facilitateur n'est pas seulement une question de collégialité. Il existe une corrélation directe avec l'amélioration réelle de la posture de votre entreprise en matière de résilience.

3. Investissez dans la résilience.

Les équipes de sécurité considérées comme des facilitatrices ont des plans d'investissement rigoureux ciblant des solutions qui visent à :

- accroître la visibilité sur l'ensemble de l'environnement technologique (48 % contre 38 % des équipes « obstacles ») ;
- accélérer la prise en charge et la résolution des incidents (53 % contre 39 %) ;
- accélérer la reprise des services clients et utilisateurs (50 % contre 40 %) ;
- combiner les efforts de cyber-résilience avec la préparation traditionnelle de la continuité des activités/de la reprise après sinistre (54 % contre 39 %).

4. Adoptez la convergence fonctionnelle.

Les équipes d'opérations de sécurité considérées comme des facilitatrices sont 2,5 fois plus nombreuses (32 % contre 13 % de la cohorte des « obstacles ») à dire qu'elles collaborent avec « tous » les domaines fonctionnels adjacents inclus dans l'étude : ITOps, développement d'applications, observabilité et expérience numérique.

Du point de vue de la sécurité, la résilience émerge d'une approche holistique du cycle de vie des menaces. Les outils de données et d'analyse vous aident à détecter les anomalies, tandis que des playbooks solides, automatisés avec efficacité, vous aident à réagir plus rapidement. Ensuite, une approche unifiée des opérations de sécurité évite aux équipes de devoir basculer d'un outil ponctuel à un autre. (Nous sommes toujours prêts à vous aider à ce niveau, d'ailleurs.)

Les prochaines recommandations sont encore des mesures que l'on retrouve plus souvent chez les équipes facilitatrices, bien qu'il n'y ait pas nécessairement une corrélation directe entre ces actions et une collaboration efficace. Nous les consignons à titre de bonnes pratiques supplémentaires, appliquées par les organisations qui s'appuient sur un partenariat inter-équipes pour améliorer leur posture de sécurité, instaurer une résilience plus large et augmenter leurs budgets.

5. Concentrez-vous sur les fondamentaux.

Quand les équipes de sécurité sont considérées comme des partenaires, elles maîtrisent les fondamentaux. Les équipes vues comme des obstacles sont plus nombreuses à dire qu'un manque d'hygiène de base sur les actifs informatiques les empêche de prévenir correctement les incidents de sécurité (28 % contre 19 % des équipes « facilitatrices »). C'est intéressant, car on pourrait penser que les équipes « obstacles » seraient plus strictes quant à l'application des protocoles de base. Il apparaît pourtant que les équipes les plus collaboratives maîtrisent également mieux les bases.

6. La sécurité du cloud est essentielle.

Les équipes « facilitatrices » sont plus nombreuses que les équipes « obstacles » (31 % contre 20 %) à accorder de l'importance à l'identification des workloads cloud mal configurés, des défauts d'alignement avec les cadres de bonnes pratiques comme CIS, etc. Selon nous, un renforcement plus rigoureux des workloads cloud place ces équipes de sécurité dans une meilleure position pour dire « oui » aux projets de transformation cloud de l'organisation, ce qui explique en partie pourquoi elles sont tenues en plus haute estime. Ryan Kovar, de l'équipe SURGe, observe : « Il est toujours préférable d'être une équipe qui peut dire oui qu'une équipe qui dit non. »

7. Investissez contre le risque de ransomware.

Les facilitateurs sont beaucoup plus susceptibles de signaler une augmentation des investissements visant explicitement à atténuer le risque de ransomware. Non seulement la protection contre les ransomwares est importante en soi, mais les mesures proactives prises par les facilitateurs pour se protéger contre cette menace très médiatisée marquent également des points auprès des décideurs métier et favorisent une relation plus efficace. Pour y parvenir, les équipes « facilitatrices » utilisent plusieurs angles :

- analyse avancée pour la détection des anomalies (35 % contre 18 %) ;
- solutions SOAR (35 % contre 21 %) ;
- détection et réponse au niveau des points de terminaison (34 % contre 17 %) ;
- supervision des comptes privilégiés (30 % contre 20 %).

8. Adoptez une attitude proactive face aux menaces ciblant la chaîne d'approvisionnement.

Comme pour les ransomwares, les équipes facilitatrices sont visiblement plus proactives face aux risques visant la chaîne d'approvisionnement. Encore une fois, les avantages sont doubles : amélioration de la sécurité et de la résilience, et établissement d'une crédibilité et d'un partenariat qui font de la sécurité une force plus efficace dans l'organisation. Plus précisément, les équipes facilitatrices privilégient les mesures suivantes pour faire face au spectre des attaques de la chaîne d'approvisionnement :

- rencontres plus fréquentes entre le RSSI et les autres dirigeants et/ou le conseil d'administration (26 % contre 15 %) ;
- activités de réponse aux incidents – recherche des menaces et/ou investigations (25 % contre 13 %) ;
- évaluation de la capacité des contrôles de sécurité actuels à empêcher/détecter les attaques sur la chaîne d'approvisionnement (30 % contre 15 %) ;
- augmentation de l'inspection des logs (26 % contre 16 %).

Nous savons tous qu'aucun protocole, action, groupe d'actions ou rituel surnaturel mystérieux ne mettra complètement nos organisations à l'abri des attaques. Mais les stratégies et les tactiques des équipes qui ont le plus réussi à devenir des partenaires stratégiques au sein de leur entreprise sont autant d'excellents moyens de commencer à atténuer les risques tout en renforçant la résilience pour résister à toute tempête.

Points clés d'une année à l'autre

Évolutions notables des moyennes mondiales

2022 a été une année difficile pour les personnes chargées de satisfaire les exigences de sécurité. En 2021, ils étaient 49 % à dire qu'il était un peu ou beaucoup plus difficile de suivre leur évolution. Ce chiffre a bondi pour atteindre 66 % en 2022, avant de se stabiliser à 53 % cette année.

Rester au fait des exigences en matière de cybersécurité au cours des deux dernières années, c'est :

	2021	2022	2023
Beaucoup plus difficile :	13 %	28 %	23 %
Un peu plus difficile :	36 %	38 %	30 %
Pas plus difficile :	20 %	18 %	13 %
Un peu plus facile :	22 %	10 %	22 %
Beaucoup plus facile aujourd'hui :	9 %	7 %	12 %

Le changement le plus important selon les participants qui ont eu du mal à suivre le rythme des exigences de sécurité concernait « le paysage des menaces plus sophistiquées ». En 2021, 48 % évoquaient ce problème, mais ils étaient seulement 38 % en 2022 et 2023. (Nous avons mené notre étude de 2021 un peu moins d'un an après le début de la pandémie de COVID-19.)

Nous avons demandé aux participants quel type d'attaques ils avaient subi au cours des deux années précédentes. Dans tous les cas, on observe un grand saut entre 2021 et 2022, et une légère augmentation ou une stagnation entre 2022 et 2023. Exemples :

- **Fuite de données :** 39 % en 2021, 49 % en 2022, 52 % en 2023
- **Ransomware :** 31 % en 2021, 45 % en 2022, 49 % en 2023
- **Compromission de l'e-mail d'entreprise :** 42 % en 2021, 51 % en 2022, 51 % en 2023
- **Attaques internes :** 27 % en 2021, 39 % en 2022, 40 % en 2023

Les temps d'arrêt sont en hausse. En comparant les chiffres de 2022 à 2023, des perturbations liées à la sécurité se sont produites :

- **Une fois par semaine ou plus :** 21 % en 2022, en hausse à 24 % en 2023
- **Toutes les quelques semaines :** 19 % en 2022, en hausse à 22 % en 2023
- **Une fois par mois :** 14 % en 2022, en hausse à 16 % en 2023
- **Tous les quelques mois :** 16 % en 2022, en baisse à 15 % en 2023
- **Tous les quelques trimestres :** 11 % en 2022, en baisse à 10 % en 2023
- **Une fois par an ou moins :** 19 % en 2022, en net recul à 12 % en 2023

Le temps moyen de récupération s'est amélioré depuis 2022.

- **Quelques minutes :** 10 % en 2022, 17 % en 2023
- **Quelques heures :** 31 % en 2022, 29 % en 2023
- **Plusieurs heures :** 32 % en 2022, 34 % en 2023
- **Plusieurs jours :** 16 % en 2022, 15 % en 2023
- **Une semaine ou plus :** 10 % en 2022, 6 % en 2023

Au fil du temps, les priorités stratégiques ont changé. Les quatre stratégies suivantes occupent une place beaucoup plus importante en 2023 :

- **Développer et construire activement une architecture logicielle intégrée pour les outils d'analyse et d'opérations de sécurité :** 38 %, contre 21 % en 2022 et 18 % en 2021
- **Rassembler les outils et le personnel au sein d'un SOC d'entreprise :** 35 %, contre 15 % en 2022 et 14 % en 2021
- **Acheter des outils pour automatiser et orchestrer les processus des opérations de sécurité :** 35 %, contre 22 % au cours des deux années précédentes
- **Développer des processus d'opérations de sécurité plus documentés et formels :** 33 %, contre 17 % en 2022 et 15 % en 2021

Points clés par pays

Aperçus de l'état mondial de la sécurité

Australie et Nouvelle-Zélande

Les ransomwares ne sont pas vraiment une priorité en Australie et en Nouvelle-Zélande (ANZ) : seuls 19 % les considèrent comme tels pour l'année prochaine, contre 29 % des personnes interrogées dans le reste de la région Asie-Pacifique. Un début de piste : les organisations d'ANZ semblent s'appuyer davantage que leurs homologues sur la cyber-assurance pour faire face aux ransomwares. Les blocages du système ne sont peut-être pour elles qu'un coût d'exploitation supplémentaire. Nous avons également vu que l'ANZ s'intéressait plus aux approches Zero Trust et moins aux ransomwares. Elles comptent davantage sur leur assurance.

Parmi les organisations victimes d'attaques réussies de ransomwares, elles sont 38 % dans la région ANZ à avoir le plus souvent fait payer leur compagnie d'assurance (contre 21 % de leurs pairs dans le reste du monde). Peut-être que le coût des assurances est plus faible en ANZ, dans la mesure où les rançons dans ces deux pays ont tendance à être plus faibles que dans le reste du monde. Pour le moment…

Autres découvertes notables :

- Les RSSI ont tendance à rencontrer moins souvent leurs pairs des fonctions métier : seuls 14 % déclarent que leur RSSI donne des briefings hebdomadaires sur la posture de sécurité ; c'est deux fois moins que dans le reste du monde (30 %).
- Bien que les organisations ANZ soient légèrement plus nombreuses à faire du DevSecOps un domaine d'intérêt important, elles affichent moins de succès à ce niveau. Seuls 49 % déclarent que le DevSecOps a entraîné une réduction des incidents (contre 60 % dans le reste du monde), et seulement 48 % déclarent qu'il a contribué à la conformité (contre 63 %).

Canada

Les participants du Canada sont généralement plus anxieux face à l'augmentation des menaces et des exigences de sécurité ; 76 % affirment que le respect des exigences de sécurité est devenu plus difficile au cours des deux dernières années, contre 51 % dans le reste du monde.

Leur pessimisme est peut-être justifié. Les organisations canadiennes sont plus nombreuses à déplorer des incidents de sécurité ces derniers temps, qui concernent des compromissions de systèmes par des acteurs malveillants (62 % contre 51 % dans le reste du monde) et des violations (65 % contre 51 % dans le reste du monde). Les participants canadiens signalent également de plus grandes difficultés concernant la disponibilité et les temps d'arrêt des workloads critiques : 33 % déclarent avoir observé des interruptions de service hebdomadaires ou plus fréquentes dans les applications critiques de l'entreprise à la suite d'incidents de sécurité, contre 19 % de leurs homologues américains.

Mais les organisations canadiennes affichent des performances supérieures à la moyenne concernant le MTTD et le MTTR.

- MTTD : 39 % des Canadiens affirment que leur délai moyen de détection est de deux semaines ou moins, contre 26 % aux États-Unis.
- MTTR : les Canadiens sont également plus nombreux que les participants américains à afficher un temps de récupération mesurable en minutes (24 % contre 14 %).

Autrement dit, si les organisations canadiennes sont aux prises avec davantage d'incidents et des temps d'arrêt plus fréquents, elles font preuve d'une agilité relativement élevée dans la gestion des problèmes.

Les participants canadiens sont également plus susceptibles que leurs homologues américains de dire que les pratiques DevSecOps renforcent la collaboration entre les équipes de sécurité et de développement (73 % contre 63 %) et améliorent la conformité (71 % contre 59 %).

Les Canadiens expriment également une plus grande confiance dans la capacité de l'IA à renforcer le SOC : 61 % affirment que les technologies d'IA surpassent les analystes humains dans l'identification des actions frauduleuses, contre 40 % aux États-Unis.

France

Les participants français ont vraiment l'impression de maîtriser la situation. Seuls 14 % déclarent qu'il est devenu beaucoup plus difficile de garder une longueur d'avance sur l'évolution du paysage des menaces, contre 29 % de leurs pairs ailleurs en Europe et 24 % dans le reste du monde. Deux raisons potentielles :

1. Les Français interrogés sont moins nombreux à avoir des difficultés à trouver de la main-d'œuvre qualifiée (10 %, contre 23 % dans le reste de l'Europe et 26 % dans le reste du monde).
2. Seuls 12 % des participants français déclarent être inondés de faux positifs et/ou d'alertes sans contexte, soit la moitié du taux de leurs homologues à l'échelle de l'Europe (25 %) ou du monde (26 %).

Comme dans d'autres pays où les inquiétudes sont moindres (voir l'Allemagne sur la page suivante), les incidents sont également moins nombreux :

- 29 % des organisations françaises signalent des violations au cours des deux dernières années, contre 61 % dans le reste de l'Europe.
- 23 % rapportent des violations de conformité, contre 54 % ailleurs en Europe.
- 26 % ont été victimes d'attaques internes, contre 53 % ailleurs en Europe.
- 27 % ont subi des attaques d'appropriation de compte, contre 52 % ailleurs en Europe.

Les Français constatent également moins d'interruptions critiques liées à la sécurité : 6 % en souffrent chaque semaine, contre 40 % dans le reste de l'Europe ; et 22 % déclarent que des interruptions surviennent au plus une fois par an, contre 6 % en Europe.

Les participants français font état de progrès comparables en matière de résilience, mais il y a une nuance : 61 % déclarent que leurs investissements dans la résilience pour l'année prochaine se concentreront sur l'accélération de la prise en charge et de la résolution des incidents (contre 40 % dans le reste de l'Europe), tandis que leurs homologues européens se focalisent davantage sur leur capacité à récupérer une copie fiable des données (42 % ailleurs en Europe, 31 % en France).

À noter également : les participants français ont davantage de difficultés avec la complexité des outils.

- Lorsque l'on aborde les défis de sécurité généraux, 29 % ont des difficultés à gérer un grand nombre d'outils de sécurité ponctuels et déconnectés, contre 19 % dans le reste de la région.
- Concernant les défis spécifiques au cloud, 37 % déclarent que la multiplication des contrôles de cybersécurité augmente les coûts et la complexité (contre 24 % dans le reste de la région).

Ces deux chiffres indiquent que les équipes françaises ont tout intérêt à chercher à simplifier et rationaliser les outils ponctuels – sans sacrifier l'efficacité de la sécurité, bien sûr.

Allemagne

Seuls 38 % des participants allemands déclarent qu'il est devenu plus difficile de suivre le rythme des menaces et des exigences de sécurité au cours des deux dernières années, alors qu'ils sont 61 % dans les autres pays européens et 54 % dans le reste du monde.

Il se peut que la confiance des Allemands vienne de leurs progrès en termes de résilience : 27 % déclarent avoir une approche formelle de la cyber-résilience à l'échelle de l'entreprise, contre seulement 18 % des autres participants de la région (en cela, les Allemands sont au niveau de la norme mondiale, et non en avance).

Il se peut également que les organisations allemandes aient connu moins d'incidents. Seuls 40 % des participants déclarent avoir été piratés au cours des deux dernières années, contre 57 % sur les autres marchés européens étudiés et 53 % dans le reste du monde. Les participants allemands rapportent également moins de violations de conformité (25 % contre 52 % dans les autres pays européens interrogés), d'attaques internes (32 % contre 50 %) et de compromissions des e-mails d'entreprise (36 % contre 63 %).

En revanche, lorsque ces incidents se produisent, la réponse allemande est plus lente. Les analyses post-incident montrent qu'en Allemagne, les acteurs malveillants ont accès aux systèmes pendant près de trois mois avant que l'organisation n'en ait connaissance, alors que ce délai est inférieur à deux mois parmi les autres participants européens. Le MTTR est également plus long, dans des proportions similaires.

D'autres différences : les participants allemands déclarent plus souvent qu'il leur est devenu plus difficile de trouver du personnel de sécurité qualifié (33 % contre 18 % parmi les autres en Europe). De plus, les participants allemands montrent une plus grande hésitation vis-à-vis de l'IA. Seuls 30 % déclarent que l'IA est capable de surpasser les analystes en matière de détection d'anomalies (contre 53 % des participants dans le reste de la région). Ils ont également fait moins de progrès en matière d'automatisation et d'orchestration des opérations de sécurité : seuls 29 % rapportent des progrès considérables dans le domaine, contre 40 % de leurs pairs dans la région. La rareté des compétences, combinée à des investissements moindres dans l'IA et dans l'automatisation, peut amener les organisations allemandes dans une situation où les équipes de sécurité auront finalement plus de mal à suivre.

Inde

Les données de l'Inde présentent un tableau décourageant. D'une part, les équipes indiennes sont très bien équipées : 66 % des participants comptent plus de 25 ressources ETP dans leur SOC contre 36 %, en moyenne, dans le reste du monde. D'un autre côté, elles ont énormément de difficultés à suivre le rythme :

- 42 % des organisations indiennes déclarent être dépassées par le nombre d'attaques (contre 23 % dans le reste du monde).
- 44 % se disent inondées de faux positifs (contre 24 % ailleurs).

Une partie du problème semble être lié à la complexité de leurs

écosystèmes d'outils : 48 % se plaignent que leur pile de sécurité est trop complexe, contre 28 % dans le reste du monde.

Le résultat, sans surprise, est que les personnes interrogées en Inde sont plus nombreuses à avoir été victimes d'une violation de sécurité au cours des deux dernières années (59 % contre 45 % des personnes interrogées ailleurs dans la grande région Asie-Pacifique), et que les incidents ont plus fréquemment des conséquences négatives sur les résultats commerciaux, ce qui inclut une baisse de la valorisation de l'entreprise (42 % contre 25 % dans le reste de la région).

La bonne nouvelle est que les RSSI relèvent le défi : 33 % déclarent informer chaque semaine les chefs de secteur d'activité de la position de sécurité de l'organisation (contre 16 % dans le reste de l'Asie-Pacifique). Les efforts portent leurs fruits : 57 % des personnes interrogées affirment que cela a directement conduit à donner davantage de priorité à l'investissement dans la sécurité (contre 42 % dans le reste de la région).

Autre point positif, les organisations indiennes semblent plus souvent faire converger les aspects de leurs opérations de sécurité avec des fonctions complémentaires que leurs homologues : 42 % déclarent faire converger les opérations de sécurité avec tous les domaines mentionnés dans l'étude (observabilité, expérience numérique, ITOps et développement d'applications) contre 25 % dans le reste de la région. Ce chiffre doit être mis au crédit de l'enthousiasme pour les avantages potentiels : 74 % cherchent à améliorer la visibilité sur les risques (contre 53 % dans le reste de la région) ; 64 % visent à identifier les problèmes plus tôt (contre 51 %), et 70 % font converger les aspects de la sécurité et d'autres fonctions pour améliorer la collaboration interfonctionnelle (contre 53 %).

Japon

Les Japonais sont plus focalisés sur les ransomwares : 35 % des personnes interrogées les classent parmi les trois principales initiatives pour l'année prochaine, contre 23 % dans le reste de la région Asie-Pacifique. Et il semble que cette focalisation porte ses fruits : seulement 40 % des organisations japonaises déclarent avoir subi une attaque par ransomware au cours des deux dernières années, contre 50 % dans le reste du monde.

Dans d'autres domaines, en revanche, le Japon est en retard :

- Les organisations japonaises sont moins nombreuses à avoir mis en œuvre une approche formelle de la cyber-résilience à l'échelle des systèmes critiques de l'organisation (23 % contre 34 % dans le reste de la région).
- Elles sont également moins nombreuses à prévoir des investissements dans les technologies de résilience pour gagner en visibilité (37 % contre 46 % dans le reste de la région) ou pour mieux comprendre les impacts en aval des incidents (40 % contre 50 %).

Les entreprises du Japon semblent également plus complaisantes vis-à-vis des attaques de la chaîne d'approvisionnement logicielle. Seulement 15 % d'entre elles déclarent que des incidents récents ont conduit à augmenter le nombre de réunions entre le RSSI et les autres dirigeants (15 % contre 29 % des participants dans le reste de la région) ou à des modifications de leurs politiques de gestion des risques fournisseurs (16 % contre 26 %).

Singapour

Les préoccupations des participants singapouriens sont souvent très différentes de celles du reste du monde.

Commençons par la chaîne d'approvisionnement : les organisations singapouriennes sont moins nombreuses à faire de la sécurité de la chaîne d'approvisionnement logicielle un domaine prioritaire pour l'année à venir (23 % contre 33 % dans le reste du monde). En effet, elles sont seulement 38 % à avoir considérablement accru leur attention en la matière à la suite des récentes attaques de la chaîne d'approvisionnement logicielle (contre 70 % des participants dans le reste du monde). Et elles ont moins souvent pris des mesures visant spécifiquement à atténuer ces risques, telles que :

- faire appel à des prestataires de services indépendants pour effectuer une évaluation des risques (15 % contre 26 % dans le reste du monde) ;
- adopter des politiques de sécurité plus rigoureuses concernant la chaîne d'approvisionnement logicielle (15 % contre 23 %) ;
- effectuer des tests d'intrusion ou des exercices de type « red team » (15 % contre 25 %).

Deuxième exemple : les ransomwares. Les participants singapouriens sont moins nombreux à déclarer que leur organisation a mis en place ou investi davantage dans des contrôles clés pour lutter contre les ransomwares, notamment :

- détection et réponse des points de terminaison (17 % contre 30 % dans le reste du monde) ;
- solutions de mise en place de règles de détection des ransomwares (17 % contre 26 %) ;
- analyses avancées pour la détection des anomalies (22 % contre 32 %).

Enfin, les personnes interrogées à Singapour augmentent leurs investissements dans la sécurité à un rythme inférieur à celui de leurs pairs : seuls 27 % déclarent que leur organisation augmentera considérablement ses dépenses au cours des 12 à 24 prochains mois (contre 59 % dans le reste du monde).

Bien que les équipes de sécurité de Singapour ne signalent pas à ce jour une incidence plus élevée de ransomwares ou d'attaques de la chaîne d'approvisionnement, ce déficit d'attention et de financement peut augmenter les risques futurs.

Royaume-Uni

Le tableau de la sécurité au Royaume-Uni est sombre. Les participants britanniques sont deux fois plus nombreux à avoir été victimes d'une violation récente que leurs homologues d'Europe occidentale (68 % contre 34 %), et ils ont aussi plus souvent enfreint la réglementation (64 % contre 24 %). De plus, les participants britanniques sont plus susceptibles de dire que ces incidents ont eu des conséquences concrètes, comme une baisse de la valorisation de leur entreprise (37 % contre 25 %).

Il n'est donc pas surprenant que les participants britanniques affichent des niveaux plus élevés d'anxiété quant au respect des exigences de sécurité et des menaces (35 % déclarent que c'est devenu beaucoup plus difficile au cours des deux dernières années contre 12 % des participants dans le reste de l'Europe occidentale).

Deux facteurs clés : 26 % des personnes interrogées se disent submergées par les faux positifs et les alertes sans contexte (contre 15 % dans le reste de l'Europe occidentale) et 30 % déclarent que leur position de cybersécurité repose sur des exigences réglementaires plutôt que sur les bonnes pratiques de sécurité (contre 20 % dans le reste de la région).

La résilience est également à la traîne : 25 % des participants britanniques affirment que leurs équipes de sécurité n'ont pas

encore développé de stratégie formelle de résilience – un chiffre cinq fois supérieur à la moyenne du reste du monde. Et seulement 16 % ont institué une approche formelle de la cyber-résilience à l'échelle de l'organisation (contre 35 % des organisations dans le reste du monde).

Les participants britanniques savent qu'ils ont du pain sur la planche :

- Ils visent des réductions plus importantes à la fois du MTTD (48 % contre 41 % sur les autres marchés européens) et du MTTR (67 % contre 48 %).
- Ils comprennent la valeur de la résilience et sont tout à fait d'accord sur le fait qu'une négligence dans ce domaine les expose au risque de perdre des clients (59 % contre 35 % sur les autres marchés européens) et d'être dépassés par l'innovation de leurs concurrents, en raison des perturbations et des pertes de productivité (57 % contre 28 %).
- Ils accordent également une importance croissante aux activités d'évaluation indépendante des risques à la suite des récentes attaques de la chaîne d'approvisionnement logicielle, et ce, bien plus souvent que leurs pairs (79 % contre 64 %).

États-Unis

Les participants américains sont généralement moins soucieux de suivre les évolutions des exigences de sécurité et du paysage des menaces que leurs pairs : 44 % disent que c'est devenu plus difficile au cours des deux dernières années, contre 76 % dans le reste de l'Amérique du Nord (hors Etats-Unis) et 56 % dans le reste du monde. Plusieurs facteurs contribuent à réduire le niveau de stress des organisations américaines. Deux se distinguent particulièrement :

1. la dotation en personnel semble moins pénible. Seuls 20 % des participants américains se plaignent que leur équipe de sécurité est en sous-effectif, contre 30 % parmi les autres participants en Amérique du Nord et 23 % dans le reste du monde. Les participants américains sont également plus nombreux à renforcer leurs équipes internes avec des services gérés : 54 % affirment que la majorité de la charge de travail de leur SOC est gérée par des partenaires contre 41 % de leurs homologues dans la région (et 56 % dans le reste du monde).
2. Les organisations américaines ont mis davantage l'accent sur la résilience en tant que principe de sécurité. Elles sont 45 % à avoir institué une approche formelle de la cyber-résilience à l'échelle des systèmes critiques de l'organisation, contre seulement 25 % dans le reste du monde.

Ces différenciateurs aident les organisations américaines à mieux faire face aux incidents de sécurité. Au niveau régional, les participants américains sont moins susceptibles de déclarer avoir subi, au cours des deux dernières années, une violation de données (51 % contre 65 % dans le reste de l'Amérique du Nord), une compromission des adresses e-mail d'entreprise (42 % contre 58 %), des attaques DDoS (39 % contre 53 %) et des compromissions du système (46 % contre 62 %). Cela se traduit par des temps d'arrêt moins fréquents au niveau des workloads critiques (moyenne annuelle : 19 contre 25).

Stratégiquement, les participants américains sont plus enclins à mettre l'accent sur le DevSecOps (37 % contre 28 % dans le reste du monde) et l'automatisation de la sécurité (41 % contre 35 %) au cours de l'année à venir, mais ils pourraient être confrontés à des niveaux d'exposition plus élevés aux ransomwares. Ils sont seulement 19 % à affirmer qu'il s'agit d'une initiative de sécurité de premier plan (contre 30 % dans le reste du monde).

Points clés par secteur

Données remarquables d'une sélection de quatre secteurs dans le monde

Communication et médias

Les données du secteurs des communications et des médias présentent deux tendances notables :

1. La complexité des outils de sécurité apparaît comme un problème plus sérieux. Interrogés sur leurs opérations SOC, les participants du côté des communications et des médias sont plus nombreux à se plaindre que leurs analystes perdent du temps à basculer entre d'innombrables outils de sécurité et des consoles de gestion disparates, avec peu ou pas d'intégration, ce qui les empêche d'apporter une réponse complète et rapide (47 % contre 37 % chez les représentants des autres secteurs).

   Les données révèlent plusieurs facteurs contributifs possibles :

   - Les personnes issues du secteur des communications déclarent plus souvent que leurs outils de sécurité existants ne prennent pas en charge les environnements cloud (27 % contre 19 % dans les autres secteurs) ; elles ont donc peut-être ressenti le besoin d'adopter des solutions distinctes pour leur environnement cloud.
   - Les représentants du secteur des communications sont également moins nombreux à faire converger des aspects des opérations informatiques avec la sécurité (75 % contre 82 %).
   - Des niveaux plus élevés de fragmentation (entre les équipes et les environnements) peuvent contribuer à la complexité, bien que les participants de ce secteur soient plus susceptibles de dire que leur organisation prévoit d'opter pour une approche de plateforme pour la sécurité (57 % contre 49 %).

2. Les RSSI de ce secteur échangent moins avec les décideurs métier. Seuls 17 % des participants de ce secteur déclarent en effet que leur RSSI a des discussions hebdomadaires avec les autres dirigeants sur la posture de sécurité globale et les indicateurs clés (contre 30 % des participants de tous les autres secteurs).

   L'un des principaux résultats de ce type de discussions, et de leur fréquence, est l'augmentation du financement de l'équipe de sécurité. Comme les RSSI des entreprises de communication ont des points de contact moins fréquents avec les décideurs métier, on ne sera pas surpris que les participants qui en sont issus anticipent moins souvent une augmentation significative des dépenses de sécurité au cours des 24 prochains mois (45 % contre 57 % parmi les autres industries).

Services financiers

Les participants du secteur des services financiers se démarquent de leurs pairs des autres secteurs de trois façons :

1. Ils ont mieux réussi à atténuer les risques associés aux ransomwares. En effet, ils sont 32 % à avoir subi une prise d'otage de leurs données et de leurs systèmes, contre 45 % dans les autres secteurs. Les sociétés financières sont également plus susceptibles d'avoir réalisé ou augmenté des investissements dans quatre domaines dans l'intention délibérée d'appuyer la détection, la prévention et la prise en charge des ransomwares :
   - renforcement de la sécurité des e-mails (41 % contre 31 % dans l'ensemble) ;
   - création/mise en place de règles spécifiques de détection des ransomwares (32 % contre 24 %) ;
   - solution d'analyse avancée pour la détection des anomalies (36 % contre 30 %) ;
   - solution de gestion des informations et des événements de sécurité (SIEM) (39 % contre 32 %).

2. Ils ont aussi rencontré plus de succès dans la prévention des attaques de la chaîne d'approvisionnement. 44 % des entreprises financières déclarent avoir subi une attaque de la chaîne d'approvisionnement, contre 48 % dans les autres secteurs. Plus spécifiquement, on retrouve plus souvent chez les sociétés financières :
   - une réévaluation ou une modification des politiques de gestion des risques liés aux fournisseurs (27 % contre 21 % dans les autres secteurs) ;
   - une évaluation des contrôles de sécurité actuels pour déterminer s'ils préviendraient ou détecteraient les attaques de la chaîne d'approvisionnement (31 % contre 25 %) ;
   - une augmentation des questionnaires et des audits de leurs fournisseurs de logiciels (30 % contre 22 %).

3. Ces entreprises ont, en revanche, eu moins de succès dans la mise en place d'initiatives DevSecOps. Les personnes interrogées dans le domaine de la finance sont nettement moins nombreuses à dire que leurs initiatives DevSecOps ont porté leurs fruits dans des domaines tels que :
   - la répétabilité entre les projets de développement logiciel (56 %, derrière les autres secteurs qui affichent une moyenne de 63 %) ;
   - l'approche proactive de la cybersécurité (57 % contre 65 % dans les autres secteurs d'activité) ;
   - la collaboration entre les équipes de cybersécurité, de développement et d'opérations (67 % contre 59 %) ;
   - la capacité à répondre aux audits (55 % contre 62 %) ;
   - la sécurité des données sensibles hébergées dans le cloud (65 % contre 55 %).

Compte tenu de ces résultats plus mitigés, il n'est pas surprenant que les participants des services financiers soient plus susceptibles de considérer le DevSecOps comme un domaine prioritaire pour l'année à venir (40 % contre 28 %).

Industrie Manufacturière

Les participants du secteur de l'industrie manufacturière signalent de graves problèmes de pénurie de personnel et de compétences. Par exemple, 56 % d'entre eux déclarent qu'ils n'ont pas assez de personnel pour gérer le volume croissant d'événements de sécurité (contre 47 % dans les autres secteurs). De même, les fabricants se plaignent plus souvent d'avoir du mal à embaucher suffisamment de personnel, possédant les bonnes compétences, pour gérer la charge de travail (31 % contre 22 %).

Il n'est donc pas surprenant qu'ils soient plus nombreux à dire qu'au cours des 12 derniers mois, les problèmes de personnel ont contribué à faire émerger les situations suivantes :

- Des collaborateurs envisagent de chercher un nouvel emploi en raison de leur charge de travail actuelle (51 % contre 39 % dans les autres secteurs).
- On demande aux membres de l'équipe de mener des projets sans l'expérience requise (60 % contre 40 % ailleurs).
- Un projet échoue (52% contre 36%).

De plus, les fabricants sont moins nombreux à avoir un SOC opérationnel 24 heures sur 24, 365 jours par an : 17 % contre 27 % dans les autres secteurs d'activité. Les fabricants exploitent plus souvent leur SOC uniquement pendant les heures ouvrables : 30 % contre 13 % dans les autres secteurs d'activité.

Les fabricants semblent essayer de combler leurs lacunes en matière de compétences grâce à l'automatisation et à l'IA. Ils s'appuient plus fréquemment sur les technologies de machine learning pour l'analyse de la sécurité (43 % contre 32 %) et ont largement déployé des technologies d'automatisation et d'orchestration de la sécurité et des opérations (44 % contre 35 %). Par contre, ils sont plus nombreux à souffrir d'interruptions hebdomadaires affectant des systèmes stratégiques à cause d'un problème de sécurité (44 % contre 19 %), ce qui suggère que ces approches n'ont pas complètement compensé leurs problèmes de dotation en personnel.

Secteur public

Nos participants du secteur public ont un point commun : ils ont du mal à suivre le rythme du paysage des risques. Plus des deux-tiers (68 %) affirment explicitement qu'il est beaucoup plus difficile aujourd'hui qu'il y a deux ans de respecter les exigences de cybersécurité (déploiement/ajustement des contrôles, supervision du comportement du réseau, suivi de la threat intelligence, etc.), contre 52 % dans les autres secteurs.

Les volumes d'alertes, en particulier, semblent être un problème : 34 % des participants du secteur public affirment que le suivi des alertes de sécurité fait partie de leurs principaux défis en matière de sécurité (contre 23 % dans les autres secteurs).

Deux causes sont en jeu : la complexité des outils et le manque de personnel. Les participants du secteur public sont plus nombreux que leurs homologues du secteur privé à déclarer que leur organisation souffre des deux problèmes (37 % contre 26 % dans les autres secteurs).

Ils sont aussi systématiquement plus pessimistes quant à la capacité de l'IA à alléger la charge de l'équipe de sécurité. Ils sont moins nombreux à penser que l'IA peut dès aujourd'hui surpasser les analystes humains dans des domaines tels que :

- la recherche des menaces (24 % contre 46 % dans les autres domaines) ;
- le tri et la hiérarchisation des événements (43 % contre 28 %) ;
- l'identification des comportements anormaux des utilisateurs (30 % contre 47 %).

En tant que secteur, ces organisations auraient tout intérêt à étudier la manière dont une automatisation judicieuse peut aider leur équipe, et ainsi combler l'écart de temps de récupération observé dans l'industrie (un MTTR de 22,3 heures, contre 15,1 heures dans les autres secteurs).

Rendez votre organisation plus résiliente grâce à une plateforme unifiée de sécurité et d'observabilité. Passez d'une visibilité globale à une action efficace, rapide et à grande échelle. Découvrez comment Splunk peut vous aider à préserver les opérations de votre organisation en toute sécurité, quelles que soient les perturbations numériques qui se manifestent.

En savoir plus

23-119356-Splunk-State of Security-EB-110-FR

splunk>