État de la cybersécurité en 2022

Étude mondiale : les priorités des experts de la cybersécurité pour l'intégrité du cloud, la pénurie de talents et les vecteurs d'attaques les plus urgents.

splunk>

Le sujet est (toujours) brûlant

Le paysage de la cybersécurité en 2022 est toujours frénétique, voire plus encore que d'habitude. Deux ans après le début de la pandémie mondiale qui a pris des millions de vies et perturbé toute l'économie, nous observons non seulement une hausse des attaques, mais aussi une augmentation des violations réussies.

Une nouvelle étude mondiale menée par Splunk et Enterprise Strategy Group auprès de plus de 1 200 responsables de la sécurité a révélé que 49 % des entreprises déclarent avoir subi une violation de données au cours des deux dernières années, contre 39 % dans notre sondage de l'année passée. Et si certains vecteurs d'attaque ont fait les gros titres au cours des deux dernières années, les criminels réussissent toujours en suivant les méthodes traditionnelles :

- 51 % signalent une compromission des e-mails professionnels, contre 42 % il y a un an.
- 39 % des organisations rapportent des attaques internes, contre 27 % il y a un an.
- 79 % des participants déclarent avoir été confrontés à des attaques par ransomware et 35 % admettent qu'une ou plusieurs de ces attaques leur ont fait perdre l'accès aux données et aux systèmes.

De plus, 40 % des participants signalent une infraction à la réglementation (contre 28 % il y a un an). Des attaques de plus en plus sophistiquées, des pénuries aiguës de talents et des défis spécifiques à la pandémie ébranlent les SOC.

État de la cybersécurité en 2022

Il est difficile de dire si ces chiffres ont valeur d'avertissement, indiquant que les malfaiteurs réussissent bien plus aujourd'hui ou si, comme le relève Ryan Kovar, Stratège en sécurité de Splunk, c'est plus une affaire de corrélation que de causalité. Les intrus parviennent-ils plus efficacement à pénétrer nos défenses, ou les équipes de cybersécurité sont-elles plus performantes dans la détection des intrusions ? La réponse est probablement « les deux », l'attaque et la défense améliorant chacune des aspects de leur jeu.

M. Kovar explique : « Et les ransomwares viennent biaiser ces perceptions car ils affirment haut et fort qu'ils ont compromis vos systèmes, tandis que les pirates traditionnels font tout pour circuler sans se faire repérer. »

Quelle que soit la raison pour laquelle les équipes de cybersécurité détectent davantage de failles, elles doivent travailler beaucoup plus dur et ressentent des effets plus importants que jamais.

Au total, 59 % des équipes de cybersécurité déclarent avoir dû consacrer beaucoup de temps et de ressources à la résolution des incidents (contre 42 % il y a un an). 44 % déclarent avoir subi une perturbation des processus métier (contre 35 % il y a un an) et autant affirment avoir perdu des données confidentielles (contre 28 % l'année dernière).

Méthodologie

Les chercheurs ont interrogé 1 227 experts de la cybersécurité et de l'IT qui consacrent plus de la moitié de leur temps aux problèmes de cybersécurité.

11 pays

Australie, Canada, France, Allemagne, Inde, Japon, Pays-Bas, Nouvelle-Zélande, Singapour, Royaume-Uni, États-Unis

15 secteurs d'activité

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

Les coûts de ces incidents ne sont pas théoriques, et leur impact dépasse le budget de cybersécurité. En plus des pertes d'exploitation, des rançons et de la perte de réputation, ces interruptions coûtent extrêmement cher à l'ensemble de l'entreprise. La majorité des participants (54 %) signalent que les applications critiques de l'entreprise subissent au moins une fois par mois des interruptions imprévues en raison d'un incident de cybersécurité, avec une médiane à 12 interruptions par an.

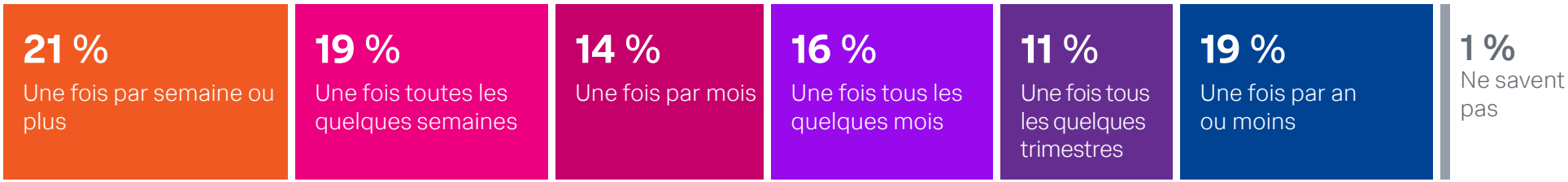
De plus, le temps médian de récupération des workloads critiques touchés par des temps d'arrêt imprévus liés à un incident de cybersécurité est de 14 heures. Nous avons demandé aux participants d'estimer le coût horaire des temps d'arrêt des applications critiques pour l'entreprise, qui, dans l'échantillon de l'étude, s'élevait en moyenne à environ 200 000 $. Cela nous a permis d'établir que le coût annuel moyen des temps d'arrêt liés aux attaques de cybersécurité pour les entreprises est aujourd'hui d'environ 33,6 millions de dollars.

Pour résumer, l'éternelle bataille entre pirates et défenseurs a été aggravée par une complexité croissante. Des environnements multicloud hybrides et complexes hébergent des applications modernes basées sur des microservices cloud-native aux côtés de technologies héritées, et désormais tout le monde doit pouvoir y accéder depuis son coin bureau à la maison.

Les équipes de cybersécurité doivent acquérir une compréhension et une visibilité complètes sur leurs infrastructures cloud pour se concentrer sur l'hygiène du cloud. Elles doivent relever de nouveaux défis en lien avec la sécurité des configurations, les vulnérabilités logicielles et la conformité, tout en conservant une piste d'audit des accès et des activités pour tous ces aspects. Dans le même temps, elles doivent revoir les modèles de menaces spécifiques à l'entreprise à la lumière des nouvelles chaînes d'attaques.

Voyons comment ça se passe.

Les cyberattaques provoquent des interruptions fréquentes



54 % indiquent subir des interruptions au moins une fois par mois

Les équipes de cybersécurité n'arrivent pas à suivre

64 % des personnes interrogées déclarent que le respect des exigences de sécurité est devenu plus difficile ces dernières années, contre 49 % il y a un an. Les principales raisons incluent :

- **le paysage des menaces dangereuses (selon 38 % des participants, contre 48 % l'année dernière. Cela reste au premier rang) ;**
- **une pile de sécurité extrêmement complexe (30 %, contre 25 % et la cinquième place il y a un an) ;**
- **des problèmes de recrutement et de rétention de main-d'œuvre qualifiée (29 % dans les deux cas, en légère hausse par rapport à l'année dernière).**

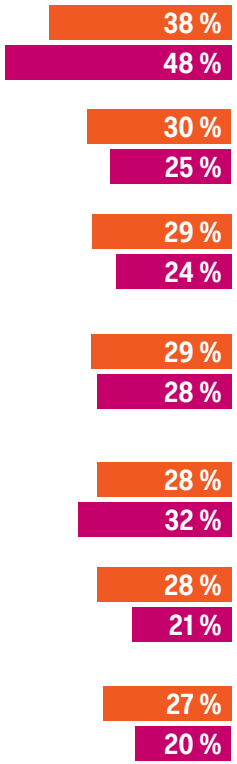
Les principaux défis des équipes de cybersécurité :

- **la nécessité croissante de se concentrer sur la conformité plutôt que sur les bonnes pratiques (29 %, contre 23 % et la quatrième réponse la plus citée l'année dernière) ;**
- **trop de temps consacré à faire face aux urgences (28 %, contre 26 % et la deuxième réponse la plus fréquemment citée il y a un an) ;**
- **difficulté à gérer la complexité des technologies de sécurité (26 %, contre 24 % ; conserve sa position de troisième défi le plus cité) ;**
- **défis du manque de personnel (26 %, contre 22 % il y a un an et le cinquième défi le plus cité).**

Tout compte fait, la conformité qui mobilise une attention croissante, le temps consacré à réagir aux événements et les défis liés à l'excès de complexité et au manque de personnel concordent à empêcher le SOC de se concentrer sur les menaces émergentes.

Pourquoi la cybersécurité se complexifie encore*

Davantage de menaces, une complexité accrue, des effectifs réduits.



* Top 7 des réponses

Le télétravail reste un défi

L'arrivée de la pandémie de COVID-19 début 2020 a créé des défis sans précédent pour les experts en cybersécurité et, comme nous l'avons noté dans le rapport de l'année dernière, fait apparaître des niveaux inédits de collaboration et de coopération entre les équipes de cybersécurité, informatiques et commerciales. Deux ans plus tard, de nombreux défis restent épineux, parmi lesquels le télétravail n'est pas le moindre.

Les entreprises soutiennent toujours, en moyenne, deux fois plus de télétravailleurs qu'avant la pandémie. Si la moyenne actuelle, 46 % des effectifs, est inférieure de 10 points à celle de 2021, aucun retour aux niveaux pré-pandémie n'est en vue. Les entreprises s'attendent à ce que d'ici à 12 mois, 41 % de leurs employés restent en télétravail. Par conséquent, 90 % d'entre elles estiment qu'il est nécessaire d'ajuster les contrôles et les politiques de sécurité.

Cette augmentation de la part du télétravail a entraîné des défis opérationnels, notamment pour garantir l'accès au réseau de l'entreprise (noté par 29 % des participants), vérifier que les appareils utilisés sont correctement configurés (28 %) et sécuriser l'accès aux actifs du cloud (27 %).

Télétravail : hier, aujourd'hui, demain

Le télétravail a considérablement augmenté et ne devrait pas diminuer.

21 %

des employés étaient en télétravail avant la pandémie

46 %

des employés travaillent à distance **aujourd'hui**

41 %

des employés devraient être en télétravail **dans un an**

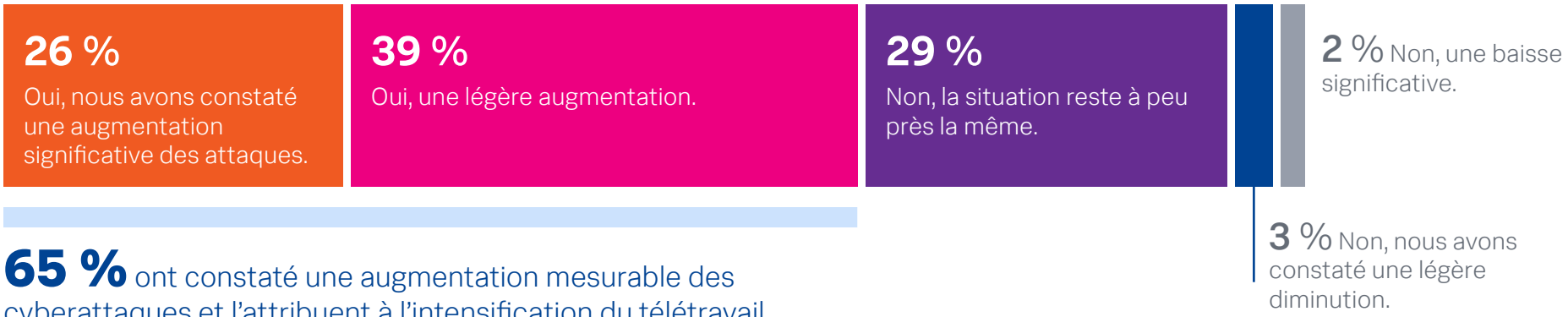
Le travail à distance et les autres mesures sanitaires ont été source de pression pour les organisations informatiques et les unités commerciales, mais les équipes de cybersécurité ont été particulièrement touchées : 80 % déclarent que le SOC doit continuellement créer et mettre en œuvre de nouvelles règles de détection des menaces pour s'adapter aux télétravailleurs.

De plus, 65 % des organisations ont constaté une augmentation mesurable des tentatives de cyberattaques, ce qui est particulièrement problématique puisque 78 % affirment que les télétravailleurs sont plus difficiles à sécuriser.

Comme nous l'avons vu plus haut au sujet des violations réussies, ces nombres en hausse ne sont pas nécessairement causés uniquement par la prolifération des attaques. Il se peut également que les entreprises améliorent leur capacité à détecter les attaques.

Pourtant, les personnes interrogées ont attribué l'augmentation des attaques, au moins en partie, à l'élargissement de la surface d'attaque associée à l'extension du télétravail.

Télétravail, attaques en hausse



65 % ont constaté une augmentation mesurable des cyberattaques et l'attribuent à l'intensification du télétravail.

La chaîne d'approvisionnement est une grande source d'inquiétude

Le concept d'attaques de la chaîne d'approvisionnement a fait couler beaucoup d'encre depuis la découverte, fin 2020, des attaques SolarWinds, suivies de l'attaque Kaseya, Log4Shell et autres. Notre étude sur l'État de la cybersécurité en 2021 a été menée deux mois après la divulgation de SolarWinds ; à ce moment-là, seuls 47 % des RSSI avaient informé les conseils d'administration ou le directoire des risques pesant sur la chaîne d'approvisionnement. Un an plus tard, ce buzz persistant a inspiré des mesures stratégiques.

90 % des organisations (autrement dit, presque toutes) ont déclaré qu'elles se concentraient davantage sur l'évaluation des risques tiers suite à ces attaques très médiatisées. En effet, 61 % des RSSI informent désormais régulièrement leur conseil d'administration et/ou les dirigeants de leur fonction sur les activités dans cet espace (contre 47 % un an plus tôt, deux mois seulement après SolarWinds).

L'intérêt nouveau porté à ce vecteur d'attaque a conduit 97 % des organisations interrogées dans notre étude à prendre des mesures. Le plus souvent (33 %, en hausse de deux points sur un an), les participants ont augmenté leur budget cybersécurité. La capacité du RSSI à impliquer les décideurs commerciaux et le conseil d'administration a également beaucoup de poids. 54 % des personnes interrogées affirment que ces discussions ont accéléré le passage à l'action, et elles sont 38 % de plus à affirmer que ces actions n'auraient pas eu lieu autrement.

M. Kovar déclare : « Tout cela représente un changement considérable. Au cours de mes 20 années de carrière dans la sécurité informatique, je n'ai jamais vu les menaces de la chaîne d'approvisionnement logicielle atteindre ce niveau de visibilité. »

Cette évolution n'est peut-être pas uniquement due au battage médiatique. 40 % des personnes interrogées ont déclaré que leur entreprise avait été affectée par une attaque de la chaîne d'approvisionnement. D'après M. Kovar, les attaques de la chaîne d'approvisionnement vont bientôt transformer l'acquisition et la vente de logiciels.

Il affirme : « Nous verrons probablement les acheteurs exiger un SBOM, une nomenclature logicielle. Celle-ci répertorie les éléments d'un progiciel complexe, de sorte qu'en cas d'attaque de la chaîne d'approvisionnement, vous pouvez rapidement savoir si votre entreprise est vulnérable. »

Principales réponses à la hausse des attaques de la chaîne d'approvisionnement

33 %
Augmentation du budget cybersécurité

29 %
Évaluation des contrôles de sécurité pour déterminer s'ils empêcheraient/détecteraient de telles attaques

27 %
Augmentation de la fréquence des réunions entre RSSI et cadres/conseil d'administration

27 %
Adoption d'une forme de technologie d'authentification forte, comme l'authentification multifacteurs

Ransomware : procédures et versements

S'il existe bien une chose qui suscite plus d'inquiétude en 2022 que les attaques de la chaîne d'approvisionnement, c'est probablement les ransomwares (qui, comme dans les cas Kaseya et Log4Shell, peuvent passer par la chaîne d'approvisionnement). En juin dernier, dans le sillage de son décret sur la cybersécurité, l'administration Biden a publié une note portant spécifiquement sur les ransomwares. Au-delà de l'inquiétude, les organisations agissent : 84 % des organisations interrogées ont développé une procédure formelle compilant les étapes requises pour répondre à une attaque par ransomware. Mais à ce jour, cette approche reste réactive ; parmi les organisations qui ont subi une attaque par ransomware réussie, 71 % n'ont développé leur procédure qu'après avoir subi une attaque.

La meilleure réponse aux ransomwares : payer. Parmi les personnes interrogées qui ont été victimes d'une attaque par ransomware réussie, elles sont seulement 33 % à avoir évité la rançon en restaurant leurs données à partir d'une sauvegarde. Environ 66 % ont déclaré que les criminels avaient été payés, soit par l'entreprise (dans 39 % des cas), soit par leur compagnie d'assurance (27 %). Interrogés sur le montant de rançon le plus élevé versé aux attaquants, les participants ont répondu en moyenne environ 347 000 dollars.

Il convient de noter que ceux qui n'ont pas été piratés n'hésitent pas à s'en vanter. Parmi les participants qui n'ont pas été victimes d'une attaque, seuls 42 % ont déclaré que leur entreprise était prête à payer les pirates.

M. Kovar suppose : « Elles pèchent peut-être par excès de confiance dans les plans de remédiation. Une fois leur capacité de récupération après sinistre ou de sauvegarde mise à l'épreuve, de nombreuses entreprises risquent de découvrir que ce n'est pas aussi simple qu'elles le pensent. »

Outre une meilleure planification de la réponse, les experts de la cybersécurité misent sur les données : 88 % 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.

La plupart des organisations ont été les cibles de ransomwares

79 % ont repoussé une attaque… ou en ont été victimes

20 % Une partie de nos données et de nos systèmes ont été pris en otage

44 % Nous avons détecté et corrigé des attaques de ransomwares avant de perdre l'accès aux données et aux systèmes

15 % Nous avons été confrontés aux deux situations

21 % Nous n'avons pas été la cible de ransomware

1 % Ne savent pas

Les équipes de cybersécurité sous le choc de la crise des talents

Les talents en sécurité se font toujours rares. Mais cette année, les experts de la cybersécurité font face à une pénurie de main-d'œuvre particulièrement redoutable.

Au moins 87 % des participants signalent des problèmes de compétences ou d'effectifs ; 53 % déclarent ne pas pouvoir embaucher suffisamment de personnel et 58 % se disent incapables de trouver des talents possédant les bonnes compétences. Encore une fois, le problème ne date pas d'hier, mais ces tendances vont dans la mauvaise direction : 85 % déclarent qu'il est devenu plus difficile de recruter et de retenir les talents au cours des 12 derniers mois, qui ont vu le syndrome de la « Grande démission » toucher toutes les industries.

Les défis permanents en matière de talents ont entraîné un certain nombre de problèmes :

- **70 % des participants déclarent que l'augmentation de la charge de travail qui en résulte les a incités à envisager de changer de poste ;**
- **76 % disent que les membres de leur équipe ont été forcés d'assumer des responsabilités pour lesquelles ils ne sont pas prêts ;**
- **68 % déclarent que les pénuries de talents sont la cause directe de l'échec d'un ou plusieurs projets/initiatives ;**
- **73 % disent que des collègues ont démissionné en raison d'un burn out.**

Cette dernière statistique est particulièrement troublante. Si les démissions entraînent d'autres démissions, la crise des talents s'auto-entretient.

Stratégies de sécurité les plus prometteuses (en dehors du recrutement)

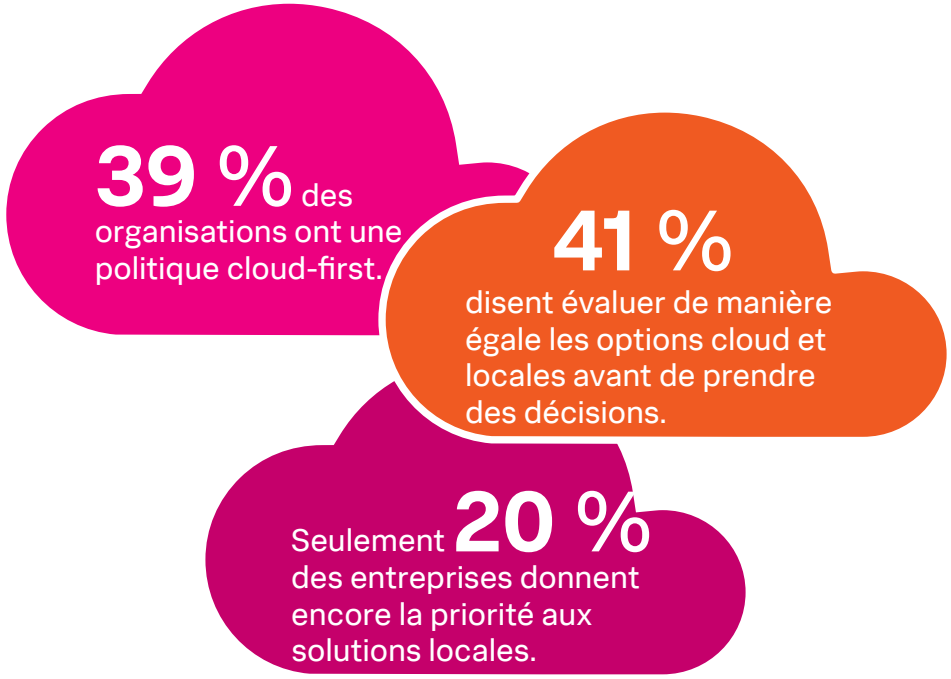
État du cloud : une norme de référence stratégique

Dans l'ensemble, le cloud computing est devenu essentiel pour les organisations, et le rôle qu'il occupe ne cesse de prendre de l'importance. Environ 73 % des participants déclarent utiliser plusieurs clouds publics aujourd'hui. Si l'on compare les données à celles de l'année dernière, nous remarquons que les réalités multicloud ont continué à prendre de l'ampleur : 34 % des participants utilisent au moins trois fournisseurs de services de cloud public (contre 29 % il y a un an). La tendance va se maintenir : 56 % s'attendent à utiliser au moins trois fournisseurs de services de cloud public (IaaS et PaaS) au cours des 24 prochains mois.

Et ces clouds annexes n'ont rien de secondaire. 65 % des utilisateurs multicloud signalent une utilisation significative de tous leurs clouds ; seuls 35 % déclarent que leurs clouds secondaires n'ont qu'une importance mineure ou de niche.

Les applications hébergées dans le cloud exécutent désormais des fonctions stratégiques dans tous les secteurs d'activité ; 66 % des personnes interrogées déclarent que la majorité de leurs applications critiques sont hébergées dans le cloud, contre 41 % il y a un an.

Le cloud a étendu son emprise sur l'infrastructure IT



Le cloud entrave la visibilité de la cybersécurité

Bien que la migration vers le cloud progresse régulièrement depuis quelques années, elle s'est considérablement accélérée avec la pandémie de COVID-19. Les équipes de cybersécurité sont découragées par la complexité qui en résulte. La valeur stratégique croissante du cloud contraint les experts de la cybersécurité à le comprendre en profondeur. Plus des trois quarts des personnes interrogées (79 %) déclarent que leur RSSI est tenu de démontrer une maîtrise accrue du cloud.

Deux défis de sécurité cloud-native continuent de se démarquer :

- **le maintien de la cohérence entre les centres de données et le cloud (45 %, contre 50 % l'année dernière, mais toujours le défi de sécurité cloud numéro un) ;**
- **la multiplication des contrôles de sécurité augmente les coûts et la complexité (37 %, contre 42 % l'année dernière, mais toujours la réponse n° 2).**

Il semble qu'un problème en engendre un autre : la multiplication des outils ponctuels crée de nouveaux silos et angles morts potentiels, ce qui peut inciter à l'adoption d'outils plus ciblés.

En ce qui concerne les domaines de visibilité sur la sécurité cloud qui nécessitent le plus d'être améliorées, les deux principales réponses (voir le tableau ci-dessous) étaient également en tête l'année dernière. On remarquera toutefois que la réponse n° 3, « maintenir une piste d'audit fiable de l'activité des comptes », occupait seulement la 5e place l'année dernière.

Tout comme les pénuries de talents conduisent à la perte d'effectifs, la complexité du cloud a également tendance à s'auto-entretenir : la complexité des éléments d'infrastructure produit un patchwork invraisemblable d'outils ponctuels. Les silos qui en résultent entravent davantage la visibilité et exacerbent les problèmes de coûts opérationnels.

Ryan Kovar nous confie :« Il semble souvent que les équipes de cybersécurité n'en soient encore qu'à évaluer l'étendue de leurs défis cloud. Il y a trois ans, j'entendais : "Comment ça, il faut que je supervise le cloud ?" Maintenant c'est : "Bien sûr que je dois superviser le cloud. Mais comment ?" C'est à cela que je pense quand je parle de renforcer la maîtrise du cloud dans les entreprises. »

Les moyens les plus importants d'améliorer la visibilité sur le cloud

Les problèmes de configuration sont source d'inquiétudes.

39 %
Identification des workloads non conformes ou contraires aux bonnes pratiques

32 %
Identifier les vulnérabilités logicielles

29 %
Conserver une piste d'audit de l'activité des utilisateurs privilégiés et des comptes de service

28 %
Configurer correctement les groupes de sécurité (par exemple, workloads de serveur en contact avec l'extérieur)

25 %
Améliorer l'activité au niveau du système d'exploitation (par exemple, les processus et les modifications du système de fichiers)

23 %
Améliorer la détection des logiciels malveillants

23 %
Améliorer la sécurité des mots de passe, des clés API, etc.

22 %
Maintenir à jour l'inventaire des actifs basés sur le cloud

21 %
Sécuriser les autorisations associées aux comptes de service

19 %
Gérer les API et l'activité des fonctions serverless

15 %
Améliorer la communication des workloads de serveurs et de conteneurs

13 %
Mieux détecter les activités anormales

Répondre à des défis croissants

Après avoir pris la mesure des défis multiples posés par la sécurité informatique moderne, nous tournons notre attention vers les solutions, les technologies et les techniques que les organisations du monde entier utilisent pour rester au niveau, et peut-être dépasser, les malfaiteurs.

Des solutions pour les talents

Invités à choisir des stratégies permettant de surmonter la crise des talents, nos participants ont choisi une combinaison d'outils et de formation.

- **58 % ont choisi « augmenter le financement de la formation » dans une liste d'options.**
- **52 % ont choisi « augmenter l'utilisation des outils de cybersécurité avec IA/ML. »**

D'autres stratégies sont évoquées :

- **l'amélioration de la capture et de l'analyse des données de sécurité : 47 % ;**
- **la simplification du portefeuille d'outils de cybersécurité (rationalisation des fournisseurs ou contrôles basés sur une plateforme) : 45 % ;**
- **l'utilisation croissante des MSSP/fournisseurs d'externalisation : 41 % ;**
- **l'augmentation des investissements dans les contrôles de sécurité commerciaux : 41 %.**

Bien sûr, ces deux stratégies ne sont pas incompatibles et tout le monde ou presque adopte des outils automatisés basés sur l'IA/ML : 80 % conviennent qu'à un moment donné au cours des trois prochaines années, la majorité des activités du centre des opérations de sécurité (notamment la détection des menaces, l'investigation et la réponse) de leur entreprise seront automatisées, avec peu de supervision humaine.

Cela ne veut pas dire que l'automatisation est la panacée face à la pénurie de talents, et de nombreuses organisations essaient de nouvelles approches. Parmi les rôles les plus difficiles à recruter en matière de cybersécurité, il y a les architectes de sécurité cloud et les ingénieurs de sécurité cloud. Dans le diagramme de Venn des compétences en cybersécurité et des connaissances en cloud computing, l'intersection est tout simplement insuffisante. Face à cela, de nombreuses organisations demandent à leurs développeurs de codifier les processus de sécurité afin qu'ils soient réutilisables et reproductibles au sein des équipes de projet.

Ryan Kovar, Stratège en sécurité de Splunk, affirme : « L'automatisation peut aider, si vous veillez à ne pas simplement augmenter le nombre d'outils à superviser. Et sur le front du recrutement, nous devons commencer à envisager des viviers de talents alternatifs car il n'y aura jamais assez de talents en sécurité tels qu'on les définit traditionnellement. »

Pour en savoir plus sur ces deux stratégies, découvrez nos **Recommandations clés** plus bas.

La pénurie de talents, en bref :

- **30 %** des responsables de la sécurité déclarent ne pas pouvoir embaucher suffisamment de personnel pour gérer la charge de travail ;
- **35 %** disent ne pas trouver de personnel possédant les bonnes compétences ;
- **23 %** indiquent souffrir des deux facteurs ;
- et **13 %** de chanceux nous disent ne pas en souffrir ni le vivre comme un défi.

L'analyse et l'automatisation jouent un rôle de plus en plus essentiel

Les capacités d'analyse et d'automatisation permettent aux analystes de sécurité de travailler plus intelligemment et de répondre aux menaces en un clin d'œil. 82 % des personnes interrogées déclarent que leur RSSI est contraint d'augmenter ses capacités d'analyse de données. Au moins 85 % (contre 82 % l'année dernière) déclarent que l'analyse de la sécurité joue aujourd'hui un rôle plus important dans leur stratégie globale de cybersécurité et dans leur prise de décision qu'il y a deux ans.

Le fort investissement des entreprises dans les technologies d'analyse, d'automatisation et SOAR (orchestration, automatisation et réponse de sécurité) se poursuit :

- **67 % des entreprises investissent activement dans des technologies conçues pour l'analyse de la sécurité et pour l'automatisation et l'orchestration des opérations ;**
- **parmi elles, 35 % déclarent que leur organisation utilise ou utilisera des capacités d'automatisation et d'orchestration intégrées à leur système de gestion des informations et des événements de sécurité (SIEM).**

L'adoption des outils d'automatisation et d'analyse est corrélée avec les tendances DevSecOps (voir ci-dessous) ; 35 % des participants déclarent que leur organisation a développé ou va développer des règles de sécurité à l'aide d'outils DevOps pour l'automatisation et l'orchestration (l'approche la plus fréquemment citée).

77 % des organisations ont intégré des solutions d'analyse non liées à la sécurité (gestion de l'entreprise, opérations IT, gestion des risques) à des analyses spécifiques à la cybersécurité pour faciliter la prise de décision.

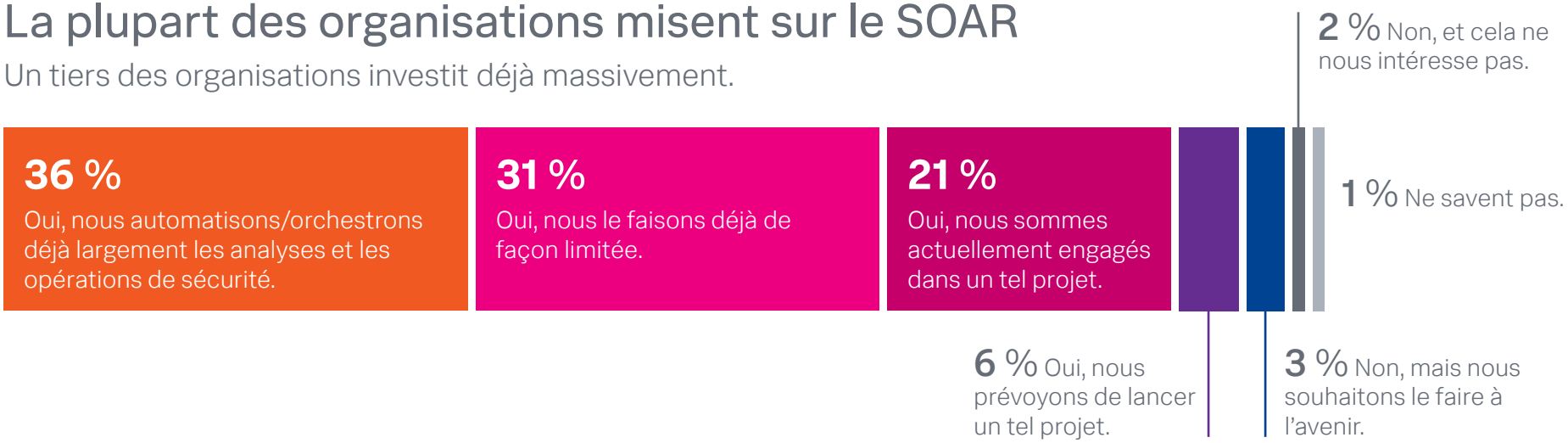
Non seulement les technologies d'analyse et d'automatisation se répandent dans les SOC du monde entier, mais elles sont en outre de plus en plus sophistiquées. Aujourd'hui, 63 % des organisations (contre 54 % il y a un an) ont déployé des technologies de machine learning pour l'analyse de la sécurité. Le plus souvent, les entreprises se tournent vers les technologies basées sur le ML pour améliorer la détection des menaces (37 %), augmenter la productivité des analystes juniors (31 %) et automatiser la correction (30 %).

L'automatisation de la réponse aux incidents était motivée par plusieurs priorités :

- **intégrer les outils de sécurité aux systèmes d'exploitation informatique : 29 %,**
- **améliorer la collaboration sécurité/ITOps : 28 %,**
- **donner des moyens aux activités de « chasse » : 28 %,**
- **automatiser les tâches de correction de base : 26 %,**
- **intégrer les informations sur les menaces externes à l'analyse des données de sécurité internes : 26 %,**
- **collecter et centraliser les données de différents outils de sécurité : 24 %.**

La plupart des organisations misent sur le SOAR

Un tiers des organisations investit déjà massivement.



Le virage DevSecOps

Le DevSecOps séduit de plus en plus par sa capacité à soutenir l'évolution de la sécurité parallèlement aux pressions visant à accélérer le développement et le déploiement des applications. 80 % des personnes interrogées affirment que leur RSSI est tenu de développer ses compétences DevSecOps. (Comme l'illustre l'adoption du DevSecOps, les RSSI sont sans cesse contraints d'élargir leurs pratiques.)

Pour nos recherches, nous avons défini le DevSecOps comme « une pratique collaborative d'ingénierie logicielle, d'opérations et de cybersécurité consistant à intégrer les mesures et contrôles de cybersécurité à chaque phase du processus CI/CD [intégration continue et livraison/déploiement] ». Ce n'était pas un scoop : 75 % des organisations déclarent utiliser le DevSecOps aujourd'hui.

Les trois cinquièmes des participants environ déclarent que le DevSecOps implique l'automatisation de différents workflows de sécurité :

- **identification et correction des vulnérabilités logicielles avant la production (62 %) ;**
- **identification et correction des logiciels malveillants avant la production (64 %) ;**
- **application des contrôles de sécurité à l'API d'exécution (61 %).**
- **Suivi des modifications de code pour l'audit (59 %)**

Si le principe général du DevSecOps consistant à intégrer la sécurité dès le début du processus de développement, plutôt que d'en faire un critère de vérification à un stade plus tardif, est généralement bien compris, nous avons demandé aux participants pourquoi ils avaient adopté cette approche. Les grands moteurs :

1. **permettre à la cybersécurité de suivre le rythme très soutenu des équipes de développement (46 %) ;**
2. **établir une posture de sécurité plus proactive (43 %) ;**
3. **accroître l'efficacité opérationnelle grâce à l'automatisation (41 %) ;**
4. **mieux sécuriser les données hébergées dans le cloud (41 %) ;**
5. **favoriser la collaboration entre les équipes de cybersécurité, de développement et d'exploitation (39%).**

Mais est-ce que ça marche ? Oui. 70 % des utilisateurs du DevSecOps signalent une amélioration de la capacité de l'équipe de cybersécurité à suivre le rythme des équipes de développement, 70 % rapportent une posture plus proactive, et 69 % indiquent une amélioration de leur capacité à sécuriser les données hébergées dans le cloud.

Le DevSecOps s'est banalisé

75 % des organisations utilisent le DevSecOps aujourd'hui.

La voie à suivre

Les défis ne font que s’intensifier, mais nos recherches montrent que les organisations prennent des mesures intelligentes pour rester à la hauteur, et même prendre de l’avance, sur un environnement de menaces en constante évolution.

La pression est un thème clé qui ressort de cette recherche de 2022. Les groupes criminels et les États-nations maintiennent la pression par des attaques de plus en plus nombreuses, variées et sophistiquées. Et à mesure que les décideurs métier prennent conscience de l'intensité du paysage de la cybersécurité et de ses enjeux existentiels, ils exigent davantage des responsables de la sécurité. Heureusement, ils sont également prêts à payer pour cela.

Toutes les organisations que nous avons interrogées ou presque (93 %) s'attendent à augmenter les budgets cybersécurité au cours des 12 à 24 prochains mois (le chiffre était déjà impressionnant il y a un an avec 88 %). L'augmentation de la formation du personnel de cybersécurité et des opérations IT reste le principal domaine d'intérêt (cité par 26 % des participants).

Priorités de sécurité immédiates*

Les actions prioritaires des organisations pour les deux prochaines années.

26 %	Fournir une formation sur les opérations de sécurité au personnel de cybersécurité et des opérations IT.
22 %	Acquérir des outils d'opérations de sécurité conçus pour faciliter l'automatisation et l'orchestration des processus des opérations de sécurité.
21 %	Développer et construire activement une architecture logicielle intégrée pour les outils d'analyse et d'exploitation de la sécurité.
21 %	Rechercher, tester et/ou déployer des technologies d'analyse et d'opérations de sécurité basées dans le cloud en plus de nos outils existants.
20 %	Embaucher davantage de personnel d'opérations de sécurité.
20 %	Déplacer les technologies d'analyse et des opérations de sécurité sur site vers le cloud.
19 %	Travailler avec des organisations de services professionnels pour développer des processus formels d'opérations de sécurité.
18 %	Consommer et analyser davantage d'informations sur les menaces externes (open source et commerciales).
18 %	Tester plus souvent nos processus d'opérations de sécurité.

* Top 9 des réponses

Recommandations clés

Si on accorde davantage d'attention aux problèmes de sécurité, du conseil d'administration jusqu'au terrain, on exerce aussi davantage de pression sur les équipes de cybersécurité. Dans de nombreuses organisations, on augmente les budgets, mais est-ce vraiment suffisant ?

Dans un monde sous la menace croissante des ransomwares, des attaques de la chaîne d'approvisionnement et du burn out, sans parler des attaques internes et de l'ingénierie sociale (le tsunami habituel, si vous voulez), voici les conseils qui ressortent de cette étude mondiale.

1. Recherchez des talents, enseignez des compétences.

Les organisations nous disent déjà qu'elles donnent la priorité au recrutement, à la formation et à la rétention des talents. Tous les efforts traditionnels dans ce domaine sont importants et recommandés. Mais ils ne suffisent pas. Le domaine des analystes en sécurité est tout simplement trop petit pour répondre à la demande : c'est pourquoi Ryan Kovar se concentre sur le « talent » dans son sens d'origine, et pas seulement comme un euphémisme pour « salarié ».

Il prévient : « Vous n'allez jamais combler les lacunes avec la main-d'œuvre de sécurité traditionnelle. Nous devons envisager des viviers de candidats alternatifs. »

On pensera bien sûr aux personnes qui ont de l'expérience dans des rôles informatiques sans lien avec la sécurité, mais M. Kovar nous dit qu'il regarde encore plus loin : « Nous avons besoin de talents bruts, pas de compétences formées. J'ai eu beaucoup de chance en recrutant des personnes issues du journalisme, des ressources humaines et de la création. J'ai simplement besoin de personnes qui possèdent une curiosité innée et un talent pour synthétiser et comprendre les données. »

Les personnes qui sont diplômées en sciences humaines, a-t-il découvert, peuvent exceller dans ce domaine, et souvent s'avérer meilleures que celles qui possèdent un diplôme en informatique traditionnel.

« Je peux enseigner le rôle d'analyste de sécurité à une personne capable de synthétiser des données et de les communiquer plus facilement que je ne peux l'enseigner à quelqu'un qui sait juste coder en C++. »

2. Connaissez votre cloud.

Près de huit participants sur 10 nous ont dit que les RSSI sont tenus de renforcer leur maîtrise du cloud. Ils sont également nombreux à faire part de leur confusion quant à la répartition des responsabilités de sécurité entre leurs équipes et leurs fournisseurs de cloud. Tout le monde, de la direction de la sécurité aux analystes de niveau 1, doit comprendre son environnement hybride et multicloud.

Les organisations doivent prendre du temps et se former pour comprendre l'interaction complexe de leurs solutions publiques, privées et SaaS. Elles ont besoin des outils et de la formation nécessaires pour configurer en toute sécurité divers environnements, gérer l'accès et l'authentification, et minimiser les MTTD et MTTR (temps moyens de détection et de récupération).

De nombreuses organisations sont encore dans un état de confusion à propos du cloud, et c'est un risque qui doit être éliminé au moyen d'une approche globale des compétences, des outils, de la collaboration inter-équipes et de l'éducation.

3. Développez une nomenclature logicielle, une SBOM.

Je le redis, vous devez *vraiment* connaître votre cloud. Et tous vos logiciels. Chaque organisation logicielle doit maintenir (entendez, tenir à jour sans relâche) une nomenclature logicielle répertoriant tous les composants logiciels exécutés en production via une analyse de composition logicielle (SCA).

M. Kovar souligne : « Beaucoup d'organisations ne le font pas encore. Grâce à l'attention portée aux attaques de la chaîne d'approvisionnement, les clients vont commencer à exiger des SBOM de leurs fournisseurs, et cela va rapidement devenir la norme. »

4. Utilisez l'automatisation pour soutenir les analystes humains.

Si nous n'avons jamais assez d'humains dans l'équipe, la solution est de tout automatiser, n'est-ce pas ? M. Kovar prévient que l'automatisation peut créer autant de maux de tête qu'elle en résout.

Il explique : « La surcharge, puis l'épuisement des analystes est un problème grave, mais dans un sens, l'automatisation peut l'aggraver. Plus vous donnez d'outils disparates à quelqu'un, plus il a de choses à faire et à suivre. Ce n'est pas comme ça que l'on lutte contre le burn out. »

Alors automatisez dans le but de libérer vos analystes humains pour qu'ils puissent mieux faire leur travail. Il faudra peut-être réduire le nombre d'outils plutôt que l'augmenter. Il faudra peut-être aussi adopter une approche de plateforme qui permet aux analystes non seulement de suivre leurs outils, mais aussi d'agir sur des événements importants, pendant que les soucis de base sont corrigés en un clin d'œil. On doit chercher à réduire le sentiment de surcharge et d'épuisement.

M. Kovar poursuit : « Les spécialistes de la sécurité font ce métier pour résoudre des problèmes, et non pour remplir des feuilles de calcul. »

5. Faites progresser le DevSecOps.

Aux 23 % de participants qui n'ont pas encore découvert le DevSecOps, nous disons : « Ne tardez pas ». Aux 2 % qui n'y pensent même pas, nous vous encourageons vivement à faire un peu de lecture sur le sujet. Pour la grande majorité qui progresse déjà : continuez.

Nos recherches ont révélé que 75 % des organisations utilisent le DevSecOps pour identifier et corriger les vulnérabilités, corriger les logiciels malveillants avant le déploiement, mais aussi pour consigner les modifications de code à des fins d'audit et d'application des contrôles de sécurité de l'API d'exécution. En fin de compte, le DevSecOps aide les organisations à résoudre les problèmes de visibilité (et à empêcher les logiciels malveillants de passer en production). Les avantages classiques du DevSecOps.

La prochaine étape, selon M. Kovar, consiste à appliquer le DevSecOps spécifiquement pour se défendre contre les ransomwares et les menaces persistantes avancées. Il confie : « Une approche DevSecOps vous aide à consolider les défenses de votre réseau pour éliminer les pertes d'efficacité. C'est une étape importante, car les malfaiteurs combinent de plus en plus les techniques d'attaque de manière à mieux exploiter les lacunes et les défaillances de notre couverture. »

Et assurez-vous que votre approche DevSecOps couvre tout le développement logiciel, pas seulement le travail de l'équipe officielle d'ingénierie. Il rappelle : « De nos jours, tout le monde développe des logiciels. Les gens ne réalisent pas nécessairement qu'un employé d'une entreprise du Fortune 50 utilisant Microsoft VBA [Visual Basic for Applications] dans Excel pourrait générer plus de revenus à lui seul que des entreprises entières au bas du Fortune 1000. »

6. Consolidez les ensembles d'outils tentaculaires.

Il faut avoir le bon outil pour la bonne tâche, tout le monde est d'accord avec ça. Mais un logiciel n'est pas seulement un outil rangé dans une boîte. C'est une application active qui a besoin de suivi pour être efficace, et de vigilance pour produire des retours d'expérience. En ce sens, elle s'apparente plus à un animal de compagnie, et vous ne pouvez pas héberger 30 millions d'amis dans votre maison sans être cerné par le chaos. Et les crottes.

La consolidation consiste à disposer des bons outils pour les tâches à accomplir, tout en veillant à ce que votre équipe puisse en assumer les soins. Comme une automatisation aléatoire, une consolidation négligente des outils peut accroître la frustration et l'épuisement des collègues. En vous concentrant sur l'arsenal indispensable, en particulier avec une approche de plateforme capable de réunir plusieurs entrées sur un seul tableau de bord, vous doterez vos analystes de puissantes informations plutôt que de leur donner des millions de résultats à consulter. À long terme, les organisations économisent sur les coûts de maintenance, de formation et de licence, et peuvent réinvestir judicieusement ces économies. Dans le même temps, un ensemble d'outils bien pensé améliore la visibilité sur l'infrastructure, les performances des applications et la sécurité.

Points clés par secteur

Les données remarquables d'une sélection de sept industries dans le monde.

Communication et médias

Les sociétés de communication et les médias souffrent d'interruptions plus fréquentes que dans les autres industries : 33 % des personnes interrogées déclarent que leur entreprise souffre d'interruptions hebdomadaires des applications critiques liées à des actions d'acteurs malveillants, contre une moyenne de 22 % dans les autres secteurs.

Près de la moitié (46 %) des entreprises de communication et de médias attribuent l'échec de projets ou d'initiatives au cours des 12 derniers mois à des lacunes ou à des manques de compétences, contre une moyenne intersectorielle de 34 %.

Les RSSI ont un impact démesuré sur l'orientation de la chaîne d'approvisionnement dans les entreprises de communication. Parmi les organisations qui ont pris des mesures (nouvelles politiques ou investissements) dans ce domaine à la suite d'attaques, 55 % ont déclaré que ces actions n'auraient pas eu lieu sans le rôle moteur du RSSI (contre 37 % des participants dans d'autres secteurs) .

Sur le front du cloud, les entreprises de communication et de médias ont tendance à être plus diversifiées que les autres secteurs. Seules 18 % travaillent avec un seul fournisseur d'infrastructure de cloud public aujourd'hui (contre une moyenne de 28 % dans d'autres secteurs) et 41 % travaillent avec trois partenaires ou plus (contre 32 %).

Services financiers

Les organisations de services financiers interrogées ont tendance à avoir des SOC plus vastes que leurs pairs : 27 % déclarent que leur SOC compte plus de 50 équivalents temps plein (contre 16 %, en moyenne, sur les autres industries).

Un lien possible : les organisations de services financiers étaient nettement moins nombreuses à déclarer que les attaques quotidiennes les empêchent d'affiner les outils et les processus (19 % contre 29 % en moyenne pour les autres secteurs) ou d'évoquer la difficulté à trouver suffisamment de talents pour gérer la charge de travail comme leur principal défi (21 % contre 30 %).

Les organisations de services financiers se laissent majoritairement séduire par le cloud lorsqu'il s'agit de déployer de nouvelles applications ; 50 % déclarent avoir une politique « cloud-first » en ce qui concerne les nouvelles applications, contre 38 % des organisations dans d'autres secteurs.

Les organisations financières sont également en avance sur leurs pairs dans l'adoption des pratiques DevSecOps, et sont en effet 84 % à indiquer que ces approches sont en place dans une plus ou moins grande mesure (contre 73 % des participants d'autres secteurs).

Santé et sciences de la vie

Les organismes de santé dépendent davantage du cloud : 81 % déclarent exécuter la plupart de leurs applications importantes dans une infrastructure cloud, contre 64 % des personnes interrogées dans d'autres secteurs.

Les organisations de soins de santé sont plus nombreuses (46 % contre une moyenne de 25 % dans les autres secteurs) à dire qu'il est beaucoup plus difficile aujourd'hui qu'il y a deux ans de se tenir au courant des exigences de cybersécurité (déploiement/ajustement des contrôles, supervision du comportement du réseau, suivi de la threat intelligence, etc.).

Les défis du cloud : 37 % des organisations de soins de santé (contre 26 % dans d'autres secteurs) indiquent que la migration des workloads vers le cloud public a rendu plus difficile la supervision de la surface d'attaque ; 33 % (contre seulement 18 % dans les autres secteurs) déclarent que leurs outils de sécurité ne prennent pas efficacement en charge le passage au cloud.

C'est dans les entreprises de soins de santé que les violations de données sont les plus courantes : 58 % ont indiqué que leur organisation avait rencontré une ou plusieurs violations récentes, contre 37 % des participants d'autres secteurs.

Fabrication

Les entreprises manufacturières interrogées ont tendance à avoir des SOC plus réduits que leurs pairs : 8 % déclarent que leur SOC compte plus de 50 équivalents temps plein (contre une moyenne de 20 % dans les autres industries).

Les fabricants ont enregistré moins d'incidents et d'attaques dans leurs environnements récemment ; ils sont notamment moins nombreux à avoir souffert d'une violation de données (39 % contre 51 % dans d'autres secteurs), d'une attaque interne (32 % contre 41 %) et d'attaques DDoS (36 % contre 46 %).

Les fabricants semblent adopter une approche plus réactive face aux attaques de la chaîne d'approvisionnement logicielle. Seuls 20 % signalent une hausse de la fréquence des réunions entre le RSSI et les dirigeants métier à la suite de ces attaques (contre 29 % dans d'autres secteurs) et 19 % signalent une augmentation de l'activité de recherche des menaces (contre 26 %).

Dans le même ordre d'idées, les fabricants sont aussi moins nombreux à demander des évaluations des risques externes, par exemple en auditant leurs partenaires, en demandant aux fournisseurs de remplir des questionnaires de sécurité ou en examinant les résultats des tests d'intrusion.

Secteur public (éducation et institutions gouvernementales)

Seulement 33 % des organismes du secteur public prévoient une augmentation significative de leurs investissements dans la cybersécurité au cours des 12 à 24 prochains mois (contre 52 % dans les autres secteurs).

L'analyse progresse plus lentement : 26 % seulement des organisations du secteur public affirment que l'analyse de la sécurité joue un rôle beaucoup plus important dans leur stratégie globale de cybersécurité qu'il y a deux ans (contre 44 % des personnes interrogées dans d'autres secteurs). Cependant, 24 % déclarent que l'embauche d'une ou plusieurs personnes possédant des compétences en science des données est une priorité absolue au cours des prochaines années (c'est beaucoup plus que les autres industries qui affichent une moyenne de 15 %).

Les approches DevSecOps ont une dynamique plus faible dans le secteur public avec seulement 24 % à annoncer un décalage significatif de la cybersécurité vers l'amont (contre 39 % dans d'autres secteurs).

Les organisations du secteur public affichent également une plus grande réticence vis-à-vis du cloud que leurs pairs : 45 % déclarent que la majorité des applications critiques s'exécutent actuellement dans le cloud public, un chiffre nettement inférieur à la moyenne des autres industries (68 %).

Commerce de détail

Les détaillants adoptent massivement le cloud : 50 % ont une politique « cloud-first » pour les nouvelles applications, contre 38 % des organisations des autres secteurs.

Autre signe d'aisance avec le cloud : 31 % des détaillants déclarent avoir une compréhension complète du modèle de responsabilité en matière de sécurité dans tous les types de cloud, un chiffre bien au-dessus de la moyenne de 21 % dans les autres secteurs.

Les détaillants sont apparemment plus susceptibles de payer les auteurs d'attaques par ransomware. Parmi ceux qui ont subi une telle attaque, 51 % ont directement payé la rançon (contre 37 % de leurs pairs).

Les détaillants interrogés ont tendance à avoir des SOC plus réduits que leurs pairs : 8 % déclarent que leur SOC compte plus de 50 équivalents temps plein (contre 20 % dans les autres industries). De plus, 33 % considèrent comme un défi majeur le faible effectif de l'équipe de cybersécurité par rapport à la taille de leur organisation (contre 25 % dans d'autres secteurs).

Technologie

Les entreprises technologiques avaient tendance à avoir des SOC plus grands que leurs pairs : 28 % déclarent que leur SOC compte plus de 50 ETP (contre 15 % des SOC, en moyenne, dans les autres secteurs).

Les entreprises technologiques sont à la pointe de l'adoption du multicloud : 42 % sont aujourd'hui associées à trois fournisseurs d'infrastructure de cloud public ou plus (contre une moyenne intersectorielle de 29 %), et 67 % prévoient de le faire dans les 24 mois (contre 52 % de leurs homologues des autres secteurs).

Les entreprises technologiques ont vu plus d'activités malveillantes que leurs pairs : 57 % rapportent des attaques d'hameçonnage réussies (contre 45 % dans les autres secteurs) ; 44 % ont été témoins d'attaques par appropriation de compte (contre 35 %) et 49 % ont découvert des sites web frauduleux se faisant passer pour leur marque (contre 38 %).

En ce qui concerne les lacunes de compétences, les entreprises technologiques sont plus susceptibles de voir dans la promesse des données un moyen de franchir le gouffre : 54 % affirment que l'amélioration de la capture et de l'analyse des données de sécurité est l'un des moyens les plus prometteurs de surmonter les problèmes de dotation à court terme.

Points clés par pays

Les données remarquables de 10 pays du monde.

Australie et Nouvelle-Zélande

Les personnes interrogées en Australie et en Nouvelle-Zélande ont signalé moins d'attaques au cours des 24 derniers mois que dans d'autres pays, en particulier en termes de violation de données (35 % contre 49 % des organisations des autres pays), de compromission de la messagerie professionnelle (33 % contre 52 %) et d'attaque par hameçonnage réussie (33 % contre 48 %).

Les organisations en Australie et en Nouvelle-Zélande connaissent des temps d'arrêt plus longs suite aux incidents de sécurité. Seuls 57 % déclarent que leur MTTR typique se compte en heures ou moins, contre 75 % des participants des autres pays.

Seuls 72 % des participants d'Australie et de Nouvelle-Zélande signalent une augmentation des difficultés contre 86 % de leurs pairs dans le monde. Ce niveau de stress plus faible peut expliquer pourquoi ils sont seulement 22 % à déclarer avoir envisagé de quitter leur emploi en raison de la pression exercée par le manque de personnel ou de compétences, contre 38 % des participants des autres pays.

L'Australie et la Nouvelle-Zélande sont moins optimistes quant à la promesse de l'IA et du ML pour l'automatisation de la sécurité. Seulement 15 %, contre 36 % dans les autres pays, sont tout à fait d'accord pour dire que les activités du centre des opérations de sécurité (détection des menaces, investigation et réponse) de leur organisation vont être automatisées, avec peu ou pas d'intervention de l'administrateur humain, au cours des trois prochaines années.

Canada

Les participants canadiens indiquent que leur entreprise augmente son budget cybersécurité à un rythme plus lent que leurs homologues à l'échelle mondiale. Alors que 37 % des participants déclarent que leur organisation augmentera considérablement ses investissements au cours des 12 à 24 prochains mois, ils sont 52 % à dire de même dans les autres pays.

Au Canada, seulement 26 % des participants affirment que leur RSSI subit une pression extrême concernant le développement de sa capacité à utiliser les données pour identifier des modèles et optimiser les opérations de sécurité, contre 40 % des participants dans d'autres pays.

Les entreprises canadiennes ne sont pas aussi avancées en matière d'analyse de la sécurité. Alors que 38 % des participants en dehors du Canada ont largement déployé des technologies conçues pour l'analyse de sécurité et pour l'automatisation et l'orchestration des opérations, seulement 18 % des entreprises du pays l'ont fait.

Les participants du Canada déclarent qu'en moyenne 56 % des employés de leur entreprise travaillent actuellement à distance, contre 46 % en moyenne dans le reste du monde.

France

Les entreprises françaises sont moins dépendantes de l'infrastructure cloud actuellement ; 41 % déclarent que leur organisation exécute la plupart de ses applications importantes sur une infrastructure cloud, contre 68 % des personnes interrogées dans d'autres pays.

En ce qui concerne les temps d'arrêt, les participants français affirment que leur organisation est plus résiliente. Seuls 3 % rapportent des interruptions d'applications liées à des incidents de sécurité sur une base hebdomadaire, contre 23 % de leurs pairs dans le monde.

Les participants français étaient également beaucoup moins nombreux que leurs pairs à avoir subi diverses perturbations suites à de récents incidents de sécurité, notamment en ce qui concerne la perturbation des processus métier (29 % contre 45 %) et l'affectation d'une quantité importante de temps du personnel informatique/de sécurité à la résolution des incidents (38 % contre 60 %).

Les participants en France s'attendent à un ralentissement de l'adoption du multicloud. Seuls 12 % prévoient que leur organisation ait recours à quatre fournisseurs de cloud public ou plus d'ici à deux ans, soit moins de la moitié de la moyenne des autres pays (25 %).

Allemagne

Une étrange juxtaposition : les Allemands sont plus nombreux que la moyenne (48 % contre 38 % dans le reste du monde) à indiquer que leur organisation a une politique « cloud-first » pour les nouvelles applications. Pourtant, l'Allemagne se distingue également par le nombre d'entreprises appliquant une politique donnant la priorité au local (27 % contre 19 % dans les autres pays).

Interrogés sur leurs plus grands défis en matière de sécurité du cloud public, 35 % des participants allemands ont déclaré que « le respect des bonnes pratiques prescrites pour la configuration des workloads et des services cloud » figurait en haut de leur liste, contre 26 % de leurs collègues dans le reste du monde.

La difficulté des organisations allemandes à recruter et à retenir les talents en sécurité était comparable à celle d'autres pays, mais elles indiquaient plus souvent que ces difficultés avaient causé plusieurs retards de projet au cours des 12 derniers mois (53 % contre 43 % dans les autres pays).

Les Allemands misent sur l'automatisation pour résoudre la crise des talents. Ils sont plus enclins que leurs homologues d'autres pays (63 % contre 50 %) à dire que l'automatisation est l'approche la plus prometteuse au cours des 12 à 24 prochains mois. Et ils sont moins susceptibles de considérer l'externalisation vers des fournisseurs de services de sécurité gérés comme séduisante (32 % contre 43 % dans le reste du monde).

Inde

Les participants indiens indiquent que seuls 33 % des employés de leur entreprise travaillent actuellement à distance, ce qui est nettement inférieur à la moyenne du reste du monde (49 %).

Parmi les organisations indiennes qui ont augmenté le nombre de télétravailleurs depuis la période précédant la pandémie, 70 % déclarent avoir constaté une augmentation significative des tentatives d'attaques ciblant ces employés (contre 21 % dans le monde) et 35 % signalent des difficultés à sécuriser les outils achetés pour faciliter la transition vers le télétravail (contre 21 % dans le monde).

Les entreprises indiennes intègrent de manière agressive des analyses extérieures à la sécurité (opérations IT, analyses commerciales et gestion des risques) à des analyses de sécurité pour améliorer la prise de décision : 77 % annoncent une intégration importante contre 37 % dans les autres pays.

De même, les organisations indiennes sont à la pointe lorsqu'il s'agit d'adopter des contrôles de sécurité possédant des capacités de machine learning : 72 % déclarent en effet une adoption étendue de ces techniques contre 28 % de leurs pairs dans le reste du monde.

90 % des personnes interrogées en Inde déclarent que leur entreprise va augmenter considérablement ses investissements au cours des 12 à 24 prochains mois, contre seulement 45 % de leurs collègues dans le monde.

Japon

Les organisations japonaises dépendent moins de l'infrastructure cloud que le reste du monde ; 53 % déclarent que leur organisation exécute la plupart de ses applications importantes sur une infrastructure cloud, contre 67 % des personnes interrogées dans les autres pays.

Lorsqu'ils parlent de manière générale des principaux problèmes de sécurité de leur organisation, les participants japonais signalent plus souvent des problèmes liés au suivi des nouveaux appareils et de nouveaux types de dispositifs qui s'intègrent à leurs environnements (43 % contre 25 % dans le reste du monde) et au manque de contexte fourni avec les alertes, qui rend les investigations difficiles et chronophages (38 % contre 23 %).

Les participants japonais étaient nettement moins nombreux que leurs homologues du monde entier à déclarer avoir subi, au cours des 24 mois précédents, différents types d'incidents de sécurité, tels qu'une violation de données (20 % contre 51 % des organisations en dehors du Japon), une infraction à la réglementation (23 % contre 41 %) ou une attaque interne (18 % contre 41 %).

Les entreprises japonaises ont été plus modérées dans leur adoption des pratiques DevSecOps : 22 % des personnes interrogées dans le pays signalent une large adoption par leur entreprise, contre 39 % dans le monde.

Singapour

Les entreprises de Singapour sont plus hésitantes dans leur approche du cloud. Alors que 40 % de leurs pairs dans le monde ont une politique « cloud-first », c'est le cas de 22 % seulement des participants à Singapour.

Les entreprises de Singapour étaient moins nombreuses à signaler avoir récemment été confrontées à différents incidents de cybersécurité : attaques DDoS (22 % contre 45 % dans le reste du monde), sites web frauduleux (24 % contre 41 %) et attaque de la chaîne d'approvisionnement logicielle (16 % contre 41 %).

En ce qui concerne les temps d'arrêt, les participants de Singapour affirment que leur organisation est plus résiliente. Seuls 2 % rapportent des interruptions d'applications liées à des incidents de sécurité sur une base hebdomadaire, contre 22 % de leurs pairs dans le monde. Les participants basés à Singapour rapportent plus souvent une fréquence des temps d'arrêt d'une fois par an ou moins (33 % contre 18 % ailleurs).

Les pénuries de compétences en cybersécurité semblent être particulièrement difficiles à Singapour, où 44 % des participants se plaignent des problèmes liés à la fois à l'embauche et à la rétention des talents (contre 22 % de leurs collègues dans le reste du monde).

Royaume-Uni

Si le marché du travail de la cybersécurité au Royaume-Uni ne semble pas moins difficile, les personnes interrogées dans ce pays sont moins nombreuses à déclarer que la perturbation qui en résulte a entraîné l'échec de plusieurs projets (26 % contre 36 % dans le reste du monde) ou les a retardés (34 % contre 45 %) au cours des 12 derniers mois.

Les attaques ciblant la chaîne d'approvisionnement logicielle n'ont pas autant impressionné les entreprises britanniques. Alors que 45 % des personnes interrogées au Royaume-Uni affirment que leur organisation accorde beaucoup plus d'importance à ce type d'attaques aujourd'hui, le pourcentage dans le reste du monde est nettement plus élevé (59 %).

Les entreprises britanniques sont nettement moins susceptibles d'indiquer que la majorité de leurs applications importantes s'exécutent sur une infrastructure cloud (57 % contre 67 % de leurs homologues dans le monde), et elles sont aussi beaucoup plus nombreuses à évaluer les emplacements locaux et cloud de la même manière pour le déploiement de nouvelles applications (53 % contre 39 %).

Cela dit, les participants basés au Royaume-Uni étaient moins susceptibles de déclarer que leurs contrôles de sécurité existants ne couvrent pas les environnements cloud (9 % contre 18 % de leurs pairs dans le monde).

États-Unis

63 % des entreprises américaines prévoient d'utiliser au moins trois fournisseurs d'infrastructure de cloud public d'ici à 24 mois (contre 52 % dans le monde), et 70 % déclarent que la majorité de leurs applications critiques s'exécutent aujourd'hui dans le cloud (contre 64 % dans le monde).

Elles semblent avoir des contrôles de sécurité plus sophistiqués : elles sont seulement 16 % à déclarer que leurs contrôles ne prennent pas en charge le cloud efficacement (contre 23 % à l'échelle internationale), 22 % à se plaindre de devoir constamment éteindre des feux (contre 31 %), et 15 % à dire que leurs contrôles ne peuvent pas les protéger des menaces modernes (contre 21 %).

Les organisations américaines semblent souffrir davantage des déluges d'alertes que leurs homologues : 30 % d'entre elles affirment en effet que le suivi des alertes fait partie de leurs principaux défis (contre 21 %).

Elles voient plus de promesses dans les solutions d'analyse de sécurité basées sur le machine learning pour améliorer l'identification des cyber-risques (34 % contre 28 % à l'échelle internationale) et la détection des menaces (41 % contre 35 %).

Découvrez comment Slack, REI, Aflac, Nasdaq et d'autres utilisent la plateforme d'opérations de sécurité centrée sur les données de Splunk pour détecter les menaces avec précision, mener des investigations et automatiser la réponse sur les environnements cloud, locaux et hybrides.

En savoir plus

22-22513-Splunk-State of Security-EB-107

splunk>