2024

État de la cybersécurité

La course à l'exploitation de l'IA

splunk>

En tant que professionnel et responsable de la sécurité depuis plus de vingt ans, j'ai vu le secteur évoluer à de nombreuses reprises. Mais cette fois-ci, c'est différent. La cybersécurité fonce vers une nouvelle frontière — la franchir ouvre des opportunités mais s'accompagne aussi de risques avec la montée en puissance de l'IA générative. Dans le rapport État de la cybersécurité en 2024 de Splunk, nous avons constaté que de nombreux RSSI et praticiens se lancent dans cette voie sans même regarder en arrière. Mais ils n'ont aucune certitude sur ce qui les attend, compte tenu des nouvelles réglementations en matière de conformité et de l'incidence de ces dernières sur la responsabilité des RSSI.

Dans le cyberenvironnement actuel, nous nous attendons à ce que les professionnels de la sécurité étudient la façon dont l'IA générative peut renforcer leur parcours de résilience — et avec un pourcentage stupéfiant de 93 % des personnes interrogées affirmant l'avoir adoptée, beaucoup la considèrent déjà comme un point critique d'innovation. Elles utilisent l'IA générative pour construire de meilleures cyberdéfenses, prendre des décisions plus éclairées et combler les lacunes critiques en matière de compétences. Dans le même temps, au moins un tiers des personnes interrogées ne disposent d'aucune politique en matière d'IA générative. Leur plus grande crainte ? Les attaques basées sur l'IA.

Entre-temps, les règles de signalement des incidents plus punitives de la Securities and Exchange Commission (SEC) des États-Unis et de la directive NIS2 de l'Union européenne obligent la communauté des RSSI à rendre davantage de comptes. Mais nous pensons que les professionnels de la sécurité découvriront également de nouvelles opportunités de remodeler leurs rôles et leurs équipes. Pour les RSSI, cela signifie affirmer les priorités dans la salle du conseil, et pour les praticiens de la sécurité, cela nécessite une collaboration plus étroite avec les équipes ITOps, d'ingénierie et de cloud pour étendre la visibilité, minimiser les temps de réponse et augmenter la résilience.

Alors que les professionnels de la sécurité continuent de forger cette nouvelle voie, chez Splunk, nous sommes enthousiasmés par le potentiel de l'IA générative pour les défenseurs et par la rapidité avec laquelle les priorités en matière de sécurité deviennent des priorités métiers.

Jason Lee

Responsable de la sécurité des systèmes d'information, Splunk

L’innovation en mouvement

L’état de la cybersécurité en 2024 est quelque peu contradictoire. Malgré les nombreux obstacles se dressant sur le chemin des professionnels de la sécurité (exigences strictes en matière de conformité, tensions géopolitiques croissantes et menaces de plus en plus sophistiquées), le secteur progresse.

De nombreuses entreprises déclarent que la cybersécurité est de plus en plus facile à gérer par rapport aux années précédentes. Les entreprises collaborent davantage et détectent les menaces plus rapidement, et la plupart d’entre elles disposent de l’autorité et des ressources nécessaires pour résoudre les problèmes auxquels elles sont confrontées.

La victoire totale reste cependant difficile à obtenir, à mesure que les défenseurs tentent de devancer leurs adversaires dans la course à l’exploitation de l’IA générative. Les équipes de sécurité craignent à juste titre que l’IA générative n’intensifie l’impact des attaques qu’elles ont habilement déjouées pendant des années.

Nous pensons que les défenseurs sont à la hauteur de la tâche. L’impact de l’IA générative sur la cybersécurité n’est peut-être pas encore totalement connu, mais une chose est sûre : la course est lancée.

Sommaire

La cybersécurité devient plus facile au fil du temps

Être défenseur signifie que vous voyez rarement les fruits de votre travail. Il est naturel de se demander si tout cela fonctionne. En ce qui concerne le respect des exigences en matière de cybersécurité, les personnes interrogées se répartissent presque équitablement : 41 % déclarent que c'est devenu plus facile, tandis que 46 % trouvent que c'est plus difficile.

Toutefois, les tendances macroéconomiques sont encourageantes. Depuis le rapport État de la cybersécurité en 2022 de Splunk, la gestion de la cybersécurité apparaît de plus en plus facile.

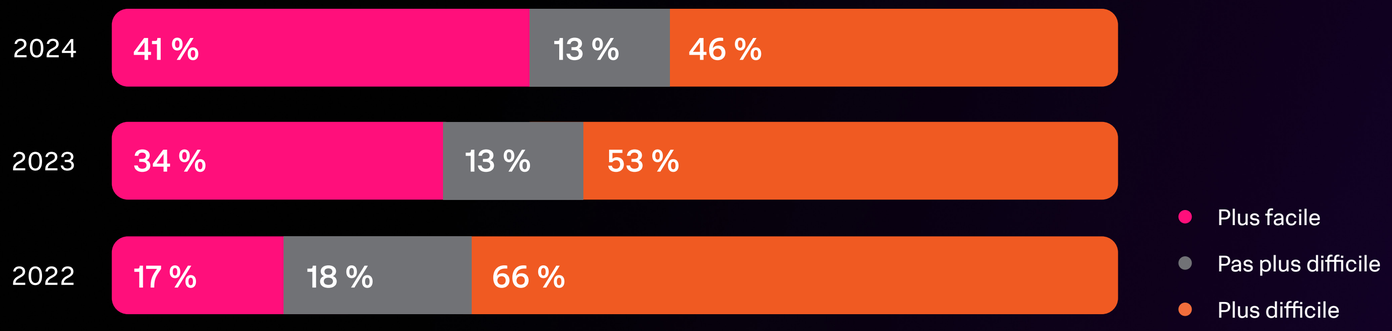
Cette perception peut être surprenante compte tenu de la complexité croissante de l'environnement et de la sophistication des attaques. Mais il est probablement plus facile pour les entreprises dotées de contrôles et de processus de sécurité bien établis de garder une longueur d'avance sur les acteurs de la menace qui s'appuient sur des stratégies d'attaque éprouvées.

La collaboration est peut-être l'une des raisons pour lesquelles la cybersécurité devient plus facile : 87 % des personnes interrogées déclarent travailler plus étroitement avec d'autres équipes qu'il y a un an. Les trois quarts (75 %) des personnes interrogées s'associent davantage aux équipes d'opérations IT cette année.

En outre, 54 % collaborent davantage avec l'ingénierie logicielle, et lorsque la sécurité commence dès les phases de conception et de codage, il devient plus facile de remédier aux vulnérabilités.

Les entreprises détectent également les menaces plus rapidement. 55 % des personnes interrogées estiment que leur temps moyen de détection des incidents à l'origine de perturbations est de 14 jours ou moins. Il s'agit d'une amélioration significative par rapport à l'année dernière, où seulement 28 % des personnes interrogées estimaient que la détection se ferait dans les mêmes délais. Toutefois, ce délai accordé aux attaquants est encore trop long.

Rester au fait des exigences en matière de cybersécurité au cours des deux dernières années



Mais le combat n’est pas terminé

Parmi ceux qui affirment que la cybersécurité devient plus difficile, 38 % citent la sophistication du paysage des menaces pour en expliquer la raison. Les tensions géopolitiques et la cyberguerre s’accroissent. L’IoT, l’IA et les environnements multicloud augmentent les volumes de données de manière exponentielle. En conséquence, les entreprises qui tentent encore de mettre en œuvre des contrôles de cybersécurité de base auront du mal à sécuriser des actifs et des points de terminaison supplémentaires. Elles auront également plus de mal à se protéger contre les simples erreurs humaines, comme les mauvaises configurations, qui constituent le principal vecteur de menace cette année.

Les exigences plus strictes en matière de conformité augmentent également les enjeux, en particulier pour les responsables de la sécurité qui sont désormais personnellement concernés pour les atteintes commises par leur entreprise. 28 % reconnaissent que la conformité réglementaire rend le travail plus difficile. Et les nouveaux décrets gouvernementaux ne feront qu’accentuer la pression.

Comme les années précédentes, 27 % des équipes de sécurité ont du mal à faire face aux urgences et à consacrer suffisamment de temps à l’amélioration de la cybersécurité, ce qui dénote un manque de stratégie et d’investissement à long terme. Il est également difficile de suivre le flot d’alertes de sécurité : 26 % des personnes interrogées reconnaissent que le volume est gênant.

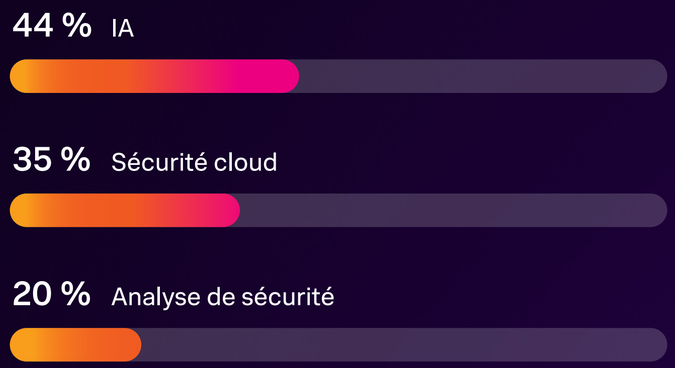
L’IA s’élève au-dessus des nuages

L’une des conclusions les plus remarquables de l’étude de cette année est que le battage médiatique sur l’IA est à la hauteur de la réalité. Près de la moitié (44 %) des personnes interrogées citent l’IA parmi leurs trois principales initiatives en 2024, dépassant la sécurité du cloud.

Si les équipes de sécurité reconnaissent les nombreux avantages de l’IA, il en va de même pour les acteurs de la menace qui ne sont pas entravés par les lois et les politiques. À la question de savoir si l’IA fera pencher la balance en faveur des défenseurs ou des attaquants, les personnes interrogées se répartissent presque équitablement : 45 % prévoient que les attaquants en tireront le plus grand profit, tandis que 43 % estiment que les défenseurs en sortiront gagnants.

L’essor fulgurant de l’IA générative stimule l’imagination de ce qui *pourrait* être, mais soulève également de sérieuses questions sur ce qui *sera*. Quelles seront les conséquences pour le SOC ? Les entreprises introduiront-elles des politiques visant à encourager une utilisation sûre et efficace ? Comment appliqueront-elles ces politiques sans entraver l’innovation ? Les réponses commencent à se dessiner.

Principales initiatives de sécurité en 2024



La ruée vers l’IA

Pendant la ruée vers l’or en Californie, des centaines de milliers de prospecteurs rêvant de faire fortune ont migré vers l’ouest. De même, l’essor actuel de l’IA générative implique la poursuite d’opportunités à une vitesse fulgurante vers une frontière inconnue, où les possibilités semblent infinies et risquées. Tout le monde veut trouver le filon et profiter de l’avantage du premier arrivé. C’est possible, il suffit de creuser un peu.

Les promesses et les possibilités de l'IA générative

L'IA générative s'est généralisée et les entreprises la mettent activement en œuvre pour transformer leurs activités. Qu'il s'agisse de proposer des recommandations personnalisées pour les clients dans le domaine de l'e-commerce ou de cartographier le cerveau humain, ou encore d'imiter les coups de pinceau de Rembrandt, l'IA générative peut s'enorgueillir d'un assortiment de scénarios d'utilisation dans presque tous les secteurs d'activité.

Il ne s'agit pas de simples spéculations. Parmi les personnes interrogées, 93 % déclarent que les utilisateurs finaux du secteur d'activité s'appuient sur des outils d'IA générative publics pour les aider à faire leur travail. Cela crée plus de travail pour les équipes de sécurité qui protègent l'entreprise contre les vulnérabilités liées à l'IA générative, telles que les fuites de données.

L'optimisme à l'égard de l'IA générative est suffisamment prononcé pour influencer même les professionnels de la sécurité les plus sceptiques. L'adoption est presque aussi élevée au sein des équipes de sécurité que dans l'ensemble de l'entreprise, avec 91 % des personnes interrogées utilisant l'IA générative publique. De plus, ils encouragent la réussite de l'IA générative, 46 % d'entre eux déclarant que l'IA générative va « changer la donne » pour leurs équipes de sécurité.

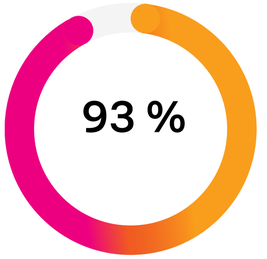
La course à l'exploitation de l'IA générative est si intense que 50 % des personnes interrogées déclarent que leur entreprise est en train d'élaborer un plan formel d'utilisation de l'IA générative pour la cybersécurité, mais que ce plan n'est pas achevé ou n'a pas été convenu.

La sécurité et l'innovation peuvent aller de pair si elles sont menées correctement. Dans le même temps, nous nous demandons si la pression exercée par l'entreprise ou le conseil d'administration (ou tout simplement la bonne vieille peur de passer à côté de quelque chose) est à l'origine de l'adoption de l'IA générative par les équipes de sécurité.

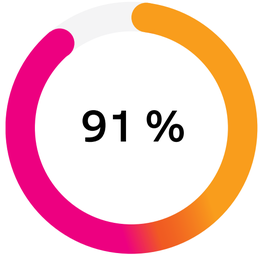
« Il y a seulement deux ans, il aurait été presque absurde de demander aux entreprises combien d'utilisateurs finaux utilisent des outils publics d'IA générative, mais aujourd'hui, l'IA générative dans l'entreprise est un enjeu de taille. »

— Kirsty Paine, Directrice technique et Conseillère stratégique pour la région EMEA, Splunk

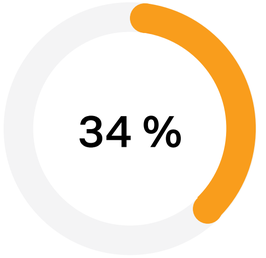
L'adoption de l'IA générative dépasse les politiques



d'adoption au sein de **l'entreprise**



d'adoption au sein des **équipes de sécurité**



ne disposent pas d'une politique complète en matière d'IA

La politique d'IA générative est un territoire inexploré

« Aller vite et tout casser » peut sembler contre-intuitif pour la plupart des praticiens de la sécurité, mais cela pourrait être la bonne philosophie car les entreprises recherchent l'innovation à toute vitesse. Et bien que les équipes de sécurité refusent rarement l'occasion de rédiger une politique, 34 % des entreprises n'ont pas mis en place de politique d'IA générative, malgré son taux d'adoption élevé.

« Les entreprises qui restreignent trop l'utilisation de l'IA générative risquent non seulement de prendre du retard sur leurs concurrents, mais aussi de s'exposer aux malfaiteurs qui n'hésiteront pas à utiliser ces outils », déclare Shannon Davis, Responsable stratégique chargé de la sécurité chez Splunk SURGe.

Si nous avons appris quelque chose de l'adoption du cloud ou de l'IoT, c'est qu'un défaut de processus ou de planification pourrait revenir hanter les équipes de sécurité. La pression exercée par les entreprises pour suivre ces tendances au hasard a eu des conséquences indésirables, telles que des clouds non conformes payés sur des cartes de crédit personnelles, ou des appareils IoT non sécurisés présentant des vulnérabilités au niveau du logiciel. Les équipes de sécurité doivent trouver un équilibre entre la vitesse de l'innovation et des processus réfléchis et durables.

Les politiques robustes dépendent de la compréhension des implications d'une technologie, mais 65 % des personnes interrogées admettent qu'elles manquent de formation sur l'IA générative. Cependant, l'équipe de cybersécurité ne devrait pas être la seule à devoir enseigner l'IA générative au reste de l'entreprise.

« Les entreprises devraient former un conseil de gouvernance interfonctionnel afin de superviser le développement et l'adoption de l'IA avec un cadre complet pour une IA responsable », déclare Hao Yang, Vice-président de l'IA chez Splunk.

L'influence de l'IA générative est vaste, c'est pourquoi il est nécessaire de disposer d'un éventail de perspectives et de spécialisations pour s'y retrouver. Le comité d'IA de Splunk, par exemple, couvre plusieurs unités commerciales, y compris le produit et la technologie, le juridique, la confidentialité, la sécurité, les ressources humaines, la mise sur le marché et le marketing.

Bien sûr, des politiques de sécurité réfléchies ne se traduisent pas nécessairement par une prévention complète, mais elles peuvent grandement contribuer à minimiser les fuites de données et autres nouvelles vulnérabilités.

La loi va s'étendre à l'IA générative

Tout comme la gouvernance interne, la frontière de l'IA générative reste relativement sauvage et non réglementée par des lois exécutoires, du moins pour le moment. Cependant, la conformité de l'IA commence à prendre forme.

Par exemple, la loi sur l'IA de l'Union européenne vise à introduire un cadre réglementaire commun basé sur des catégories de risques. En 2023, le Parlement européen a modifié sa proposition initiale pour inclure l'IA générative, qui doit se conformer à certaines exigences de transparence. Ces exigences comprennent l'enregistrement du modèle de base dans une base de données et l'élaboration et la conservation de la documentation technique.

Aux États-Unis, la Charte des droits de l'IA de l'administration Biden propose que les utilisateurs soient avertis lorsqu'ils communiquent avec un système automatisé, et permet de refuser et d'interagir avec une personne réelle à la place. Ces lignes directrices pourraient préfigurer l'action future des pouvoirs publics.

Ce tsunami imminent de réglementations gouvernementales explique peut-être pourquoi 45 % des personnes interrogées citent un meilleur alignement sur les exigences de conformité comme l'un des principaux axes d'amélioration, juste après les fuites de données. Pour devancer cette tendance, il faut mettre l'accent sur les contrôles de conformité internes.

Les entreprises devraient former un conseil de gouvernance interfonctionnel pour superviser le développement et l'adoption de l'IA avec un cadre complet pour une IA responsable. »

— Hao Yang, Vice-président de l'IA, Splunk

IA générative : amie ou ennemie ?

Qui possède l'avantage de l'IA générative ? Les personnes interrogées sont divisées.

43%

Les défenseurs en profiteront le plus

12%

Ils se neutraliseront mutuellement

45%

Les attaquants en profiteront le plus

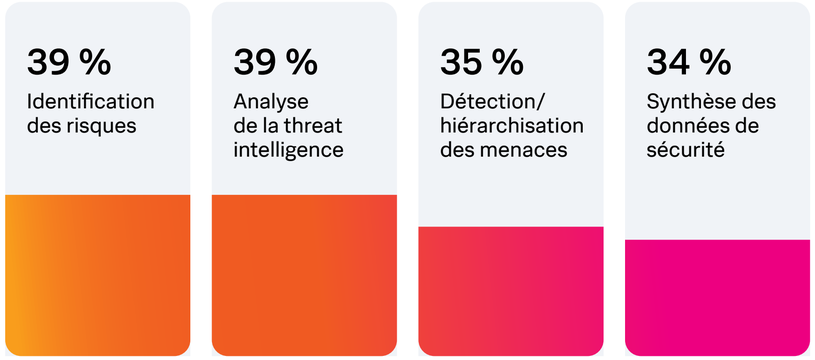
L'IA générative, auxiliaire de sécurité

Les perceptions sur l'IA générative évoluent rapidement. Il y a seulement huit mois, 17 % des personnes interrogées dans le cadre de notre rapport pour les RSSI estimaient que l'IA générative permettrait aux défenseurs d'en tirer un avantage. Aujourd'hui, près de la moitié (43 %) sont du même avis.

De plus en plus de fournisseurs intègrent l'IA générative dans leurs produits, démontrant son utilisation dans les workflows de sécurité, et les défenseurs commencent à en voir les possibilités. Bien que le potentiel de nouvelles attaques génératives basées sur l'IA et l'empoisonnement de l'IA reste une possibilité, elles ne sont pas encore devenues monnaie courante.

Les défenseurs semblent optimistes et reconnaissent que l'IA générative est adaptée à plusieurs scénarios d'utilisation en matière de cybersécurité, citant l'analyse de la threat intelligence et l'identification des risques comme les deux principales applications.

Principaux scénarios d'utilisation de l'IA générative dans le domaine de la cybersécurité



À quoi peuvent ressembler les scénarios d'utilisation de l'IA générative dans la pratique ?

Identifier les risques
L'IA générative peut améliorer les alertes basées sur les risques en agrégeant rapidement divers groupes de données pour fournir aux analystes de la sécurité des alertes riches en contexte. Les grands modèles de langage permettent de fournir ces informations à une vitesse et avec une efficacité qui dépassent de loin les capacités humaines.

Analyse de la threat intelligence
Les grands modèles de langage peuvent déterminer les indicateurs de compromission et les techniques MITRE ATT&CK décrites dans un rapport de threat intelligence. Cela éviterait aux équipes d'informations de nombreuses corvées et leur permettrait d'effectuer plus rapidement des analyses plus approfondies.

Détection et hiérarchisation des menaces
La hiérarchisation et le tri des alertes sont des tâches particulièrement sensibles aux erreurs de classification des analystes, à la fatigue et aux erreurs humaines. L'IA générative peut traiter en parallèle plusieurs menaces tout en améliorant la précision.

Synthèse des données de sécurité
L'IA générative peut faire des résumés rapides, complets et précis pour aider les équipes de sécurité à gagner du temps et à se tenir au courant des nouvelles et des informations, comme le décret de Joe Biden sur l'amélioration de la cybersécurité de la nation.

Résoudre la pénurie de compétences en cybersécurité

Les professionnels qualifiés sont au cœur de tout SOC, et de nombreuses entreprises sont toujours confrontées à des pénuries de talents. L'IA générative pourrait offrir une certaine marge de manœuvre pour répondre à ce besoin très réel.

86 % des entreprises pensent que l'IA générative les aidera à recruter davantage de talents en cybersécurité débutants, et 58 % affirment qu'elle aiderait à intégrer plus rapidement les talents débutants. 90 % des personnes interrogées déclarent que le personnel débutant peut s'appuyer sur l'IA générative pour développer ses compétences dans le SOC une fois qu'il est embauché – ce qui pourrait inclure des tâches fondamentales telles que l'écriture d'un script Python ou la mise en place d'environnements de test.

L'IA générative sera également un atout pour les professionnels de la sécurité chevronnés. Parmi eux, 65 % pensent qu'elle les rendra plus productifs, en permettant aux praticiens expérimentés de synthétiser plus facilement les nouvelles et les informations, et d'accélérer la recherche et l'ingénierie de détection.

Et si la crainte de voir l'IA remplacer des emplois n'est pas totalement infondée (près de la moitié (49 %) affirment que l'IA générative éliminera certaines fonctions de sécurité existantes), il est plus probable qu'elle aide les entreprises à former de nouveaux talents et à prévenir l'épuisement professionnel des employés. Elle pourrait aussi simplement redistribuer les cartes des talents de la cybersécurité en introduisant de nouveaux rôles tels que le prompt engineering.

Comment l'IA générative peut-elle combler les déficits de compétences ?

86 % pensent qu'elle peut aider les entreprises à recruter davantage de talents débutants

65 % pensent qu'elle permettra aux professionnels de la sécurité chevronnés d'être plus productifs

L’IA générative, alliée de l’attaquant

Les équipes de sécurité s’inquiètent également à juste titre du fait que l’IA générative est un outil de plus dans l’arsenal des attaquants. 45 % des personnes interrogées pensent que l’IA générative sera un gain net pour les entreprises et 77 % d’entre elles affirment qu’elle élargit la surface d’attaque dans des proportions inquiétantes.

Les temps changent, pas les attaques

Quelles menaces uniques l’IA générative va-t-elle libérer dans le monde ? Il y a fort à parier qu’au lieu d’une manne immédiate de nouvelles attaques, l’IA générative amplifiera les menaces auxquelles les équipes de sécurité sont déjà confrontées.

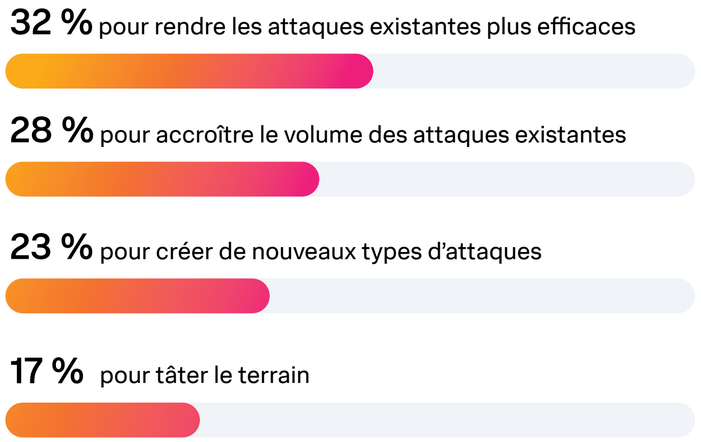
32 % des personnes interrogées craignent surtout que les attaquants utilisent l’IA générative pour optimiser les attaques existantes, par exemple en créant des e-mails de phishing plus réalistes ou en affinant les scripts malveillants. Les pirates moins qualifiés et opportunistes exploiteront l’IA générative pour augmenter de manière significative les attaques d’ingénierie sociale. Enfin, 28 % des personnes interrogées craignent que l’IA générative n’aide les adversaires à augmenter le volume des attaques existantes.

L’ennemi intérieur

Les menaces liées à l’IA ne proviennent pas toutes de sources extérieures : 77 % des personnes interrogées reconnaissent que l’utilisation accrue de l’IA générative s’accompagnera d’une augmentation des fuites de données. Toutefois, seules 49 % de ces personnes accordent une priorité active à la prévention des fuites de données, peut-être parce que les solutions permettant de contrôler le flux de données entrant et sortant des outils d’IA générative ne sont pas encore légion.

Le manque de formation autour de l’IA générative ne fait qu’amplifier ces craintes. Lorsque 65 % des responsables de la sécurité admettent ne pas pleinement appréhender l’IA générative, on peut supposer que la confusion est encore plus grande parmi les rôles non liés à la sécurité. Sans une formation adéquate, les utilisateurs finaux sont condamnés à commettre des erreurs telles que l’introduction de données sensibles de l’entreprise dans un grand modèle de langage, ce qui placera les équipes de sécurité dans le collimateur.

Principales utilisations de l’IA générative par les cybercriminels



« C’est comme la question : “Préférez-vous combattre un canard de la taille d’un cheval ou 100 chevaux de la taille d’un canard ?” Il est certainement plus facile de se concentrer sur une seule menace, mais l’IA générative créera le scénario le moins attrayant, agissant comme un multiplicateur de force pour les attaques existantes. »

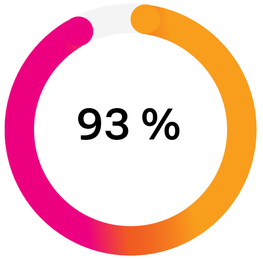
— Kirsty Paine, Directrice technique et Conseillère stratégique pour la région EMEA, Splunk

Cartographier l’avenir de l’IA générative

Quelle sera l’évolution de l’IA générative ? N’est pas Madame Irma qui veut, mais les équipes de sécurité ont adopté des formes traditionnelles d’IA comme le machine learning (ML) depuis un certain temps, et 93 % affirment que ces expériences influenceront leur approche future de l’IA générative.

De nombreuses entreprises ont goûté à l’augmentation de la productivité qu’offrent les outils de ML, 92 % d’entre elles bénéficiant déjà d’avantages substantiels. La technologie n’est toutefois pas parfaite et nécessite une attention particulière : 73 % des personnes interrogées affirment que les outils dotés de capacités traditionnelles d’IA et de ML peuvent générer des faux positifs et 91 % d’entre elles disent qu’ils doivent être ajustés. De même, l’IA générative nécessite une supervision pour repérer et prévenir les hallucinations qui peuvent nuire à sa valeur.

Les pionniers qui ont déjà construit une base solide avec l’IA traditionnelle et le machine learning se retrouveront probablement sur la voie rapide de leur voyage vers l’IA générative.



déclarent que leur expérience du machine learning influencera leur approche future de l’IA générative

Les éléments constitutifs des entreprises leaders

Dans la course pour garder une longueur d'avance sur les menaces, certaines entreprises suivent un modèle de centre d'excellence pour mettre en place des pratiques de cybersécurité matures. En 2024, 47 % des personnes interrogées considèrent que leurs programmes de sécurité sont « extrêmement avancés ». Nous classons ce groupe dans la catégorie des leaders et nous comparerons leurs caractéristiques uniques et leurs réponses à l'étude avec celles de la cohorte qui a qualifié son programme comme étant « en développement ».

Tout d'abord, les leaders sont confiants dans leur capacité à faire face aux menaces. Parmi les leaders, 49 % affirment que la gestion des exigences en matière de cybersécurité devient plus facile, alors que seulement 29 % des personnes interrogées ayant des programmes en cours de développement sont du même avis. Les leaders obtiennent également de meilleurs résultats que les programmes en cours de développement sur plusieurs autres aspects, ce qui donne une image de ce que l'on peut considérer comme des pratiques de référence.

Fournir des ressources et des moyens d'action adéquats

Les entreprises leaders ne naissent pas, elles se construisent. Leur démarche engageante reflète un lien profond avec le conseil d'administration et les parties prenantes de l'entreprise, une collaboration interdépartementale et des investissements réguliers. Les équipes de sécurité les plus performantes disposent du budget nécessaire pour être proactives : 67 % d'entre elles augmenteront considérablement leurs dépenses en cybersécurité au cours des deux prochaines années, contre 28 % pour les personnes interrogées dont les programmes sont en cours de développement.

Un lien étroit avec l'entreprise s'avère également payant pour les entreprises leaders. Un pourcentage impressionnant de 95 % d'entre elles déclarent disposer des ressources et de l'autorité nécessaires pour relever les défis, ce qui reflète les conclusions de notre rapport pour les RSSI, selon lesquelles 47 % d'entre eux sont désormais rattachés au PDG.

Collaborer et reconnaître la résilience

Être connecté à l'entreprise, ce n'est pas seulement avoir l'oreille du PDG, c'est aussi établir des partenariats avec l'ensemble de l'entreprise. Les entreprises leaders collaborent davantage avec ces départements techniques :

Collaboration avec	Entreprises leaders	Entreprises en développement
Ingénierie logicielle	56 %	46 %
Opérations d'ingénierie	51 %	31 %
Opérations informatiques	76 %	67 %

La collaboration s'étend également à la conformité. Parmi les entreprises leaders, 49 % sont tout à fait d'accord pour dire que l'ensemble des membres de l'équipe de sécurité ont intégré la conformité dans leur travail, contre seulement 27 % des entreprises qui développent des programmes de sécurité.

Les entreprises leaders reconnaissent que les enjeux de la résilience numérique sont importants. Elles conviennent largement du fait qu'une plus grande résilience numérique conduit à plus d'innovation (41 %), moins d'interruption d'activité (39 %), et évite les pénalités de conformité (39 %), probablement parce qu'elles sont plus étroitement liées aux résultats de l'entreprise.

« Sans l'adhésion des dirigeants, atteindre la maturité en matière de cybersécurité est peine perdue. »

— Jason Lee, RSSI, Splunk

Innover davantage grâce à l'IA générative

Les entreprises leaders sont également plus susceptibles d'innover avec l'IA, 48 % d'entre elles déclarant qu'il s'agit d'une initiative prioritaire, contre 30 % de leurs homologues moins avancés. L'adoption de l'IA générative au sein de leurs équipes de sécurité est également plus élevée et plus répandue : 75 % des entreprises leaders déclarent que la plupart des membres de l'équipe de sécurité utilisent l'IA générative, alors que seulement 23 % des entreprises en développement disent la même chose.

L'utilisation de l'IA générative dans les entreprises leaders semble être moins expérimentale et plus méthodique que dans les entreprises en développement :

- **82 % des entreprises leaders ont mis en place des politiques de sécurité de l'IA générative, alors que seulement 46 % des entreprises en développement l'ont fait.**
- **55 % des entreprises leaders ont un plan formel pour utiliser l'IA générative dans les scénarios d'utilisation de la cybersécurité, alors que seulement 15 % des entreprises en développement font cette affirmation.**

Détecter les incidents et y répondre plus rapidement

La maturité cybernétique ne se traduit pas par une diminution du nombre de cyberattaques. Cependant, les entreprises leaders détectent et réagissent plus rapidement que leurs homologues, ce qui atténue l'impact d'une attaque et ses conséquences.

En ce qui concerne les incidents ayant entraîné des perturbations, les entreprises leaders citent un temps moyen de détection (MTTD) de 21 jours, tandis que les entreprises en développement passent en moyenne plus d'un mois (34 jours) à détecter une menace au sein de leurs réseaux. Les entreprises leaders passent également beaucoup moins de temps en mode de récupération. Leur temps moyen de récupération (MTTR) des charges de travail critiques est d'un peu plus de 44 heures, alors que le temps moyen de récupération des entreprises en développement est de 5,7 jours.

« La capacité à réduire le temps de détection et de réponse est un indicateur direct de la maturité d'un programme de sécurité. C'est pourquoi le temps moyen de récupération et le temps moyen de détection sont des indicateurs cruciaux pour les conseils d'administration et les dirigeants. Ils veulent voir un succès mesurable sur le long terme », déclare Mick Baccio, Conseiller mondial en sécurité au sein de l'équipe de recherche en sécurité SURGe de Splunk.

La capacité à réduire le temps de détection et de réponse est un indicateur direct de la maturité d'un programme de sécurité. C'est pourquoi le MTTR et le MTTD sont des indicateurs cruciaux pour les conseils d'administration et les dirigeants. Ils veulent voir un succès mesurable à long terme. »

— Mick Baccio, Conseiller en sécurité globale, Splunk

Les éléments constitutifs d'une entreprise leader

Les entreprises qui décrivent leurs programmes de cybersécurité comme extrêmement avancés obtiennent systématiquement de meilleurs résultats que leurs homologues dans quatre critères essentiels.

- Entreprises avec des programmes extrêmement avancés
- Entreprises avec des programmes en cours de développement

Fournir des ressources et des moyens d'action adéquats

Vont augmenter les dépenses en matière de cybersécurité au cours de l'année ou des deux années à venir :

67 %

28 %

Affirment disposer des ressources et de l'autorité nécessaires pour relever les défis :

95 %

79 %

Collaborer et reconnaître la résilience

Collaboration accrue avec les opérations d'ingénierie au cours de l'année écoulée :

51 %

31 %

Collaboration accrue avec les opérations informatiques au cours de l'année écoulée :

76 %

67 %

Innover davantage grâce à l'IA générative

Disposent d'une politique de sécurité générative en matière d'IA :

82 %

46 %

Affirment que la plupart des membres de l'équipe de sécurité utilisent l'IA générative :

75 %

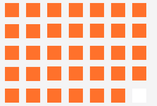
23 %

Détecter les incidents et y répondre plus rapidement

Temps moyen de détection des incidents à l'origine des perturbations :

21 jours

34 jours



Temps moyen de récupération pour les charges de travail critiques :

1,8 jour

5,7 jours

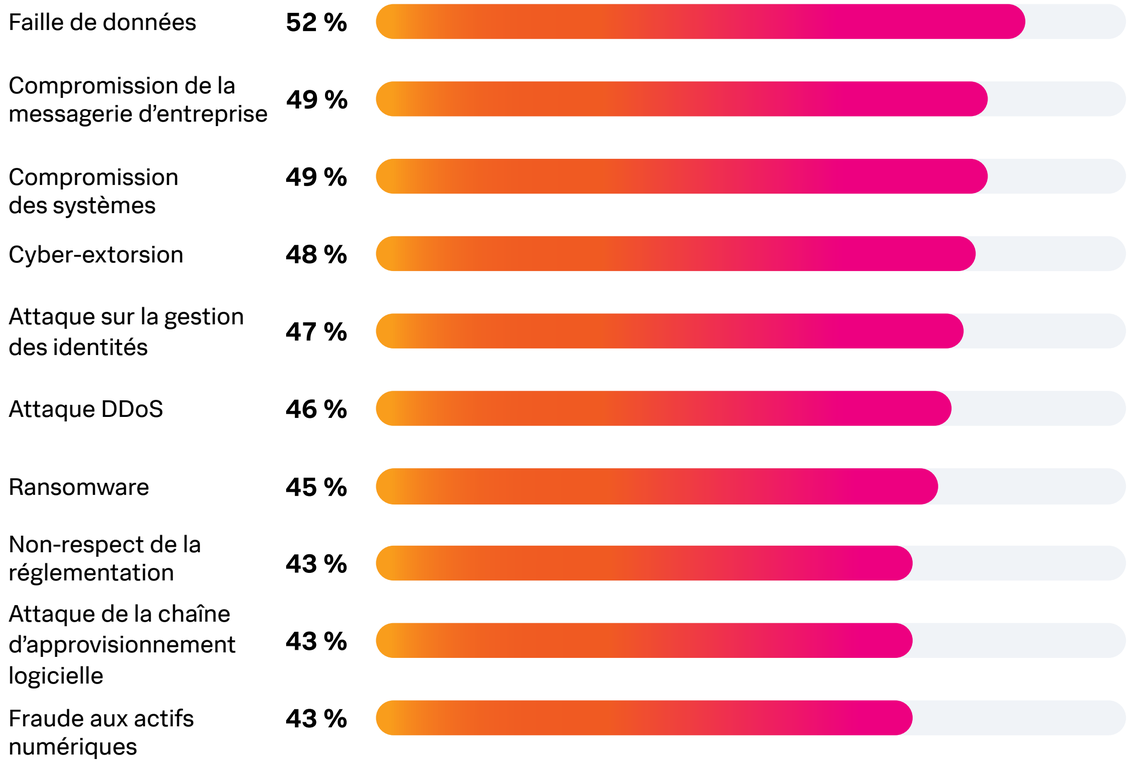
Évaluation du paysage des menaces

Alors que les équipes de sécurité se battent pour la bonne cause, les malfaiteurs trouveront toujours des moyens de contourner les meilleures défenses. Le rapport État de la cybersécurité en 2024 montre que les attaquants ne ralentissent pas, les failles de données et les ransomwares ayant augmenté respectivement de 13 % et 14 % depuis 2021.

En 2024, nous avons vu les attaquants utiliser diverses tactiques, par exemple, la compromission des messageries d'entreprise en capitalisant sur la tromperie humaine ou les attaques DDoS reposant sur la force brute. Malgré la diversité de ces approches, ces menaces ont un objectif commun : provoquer des perturbations.

Les incidents de cybersécurité ont toujours des conséquences considérables en termes de réputation, de droit et de finances, mais les entreprises semblent mieux absorber le choc, même si elles subissent globalement davantage d'attaques. Par exemple, seules 44 % des personnes interrogées déclarent que la correction des incidents a nécessité beaucoup de temps et de personnel cette année, soit une baisse de 13 % par rapport à l'année dernière. En outre, les personnes interrogées ont été moins nombreuses à perdre de la productivité et à subir des failles de données confidentielles cette année, ce qui indique que les initiatives de résilience numérique fonctionnent.

Incidents les plus fréquents survenus au cours des deux dernières années



La cyber-anxiété ne correspond pas toujours à la réalité

Si les rançons payées à coups de millions de dollars, les inculpations de RSSI et les zero-days font les gros titres, elles sont rares. Lorsque l'on interroge les professionnels de la cybersécurité sur les menaces qu'ils considèrent comme les plus préoccupantes par rapport à celles qu'ils rencontrent de manière concrète, leurs craintes sont parfois infondées.

Par exemple, bien que les personnes interrogées déclarent que les attaques par IA sont leur principale préoccupation, elles subissent beaucoup plus souvent des failles de données, des compromissions des messageries professionnelles, des compromissions des systèmes et des attaques basées sur l'identité.

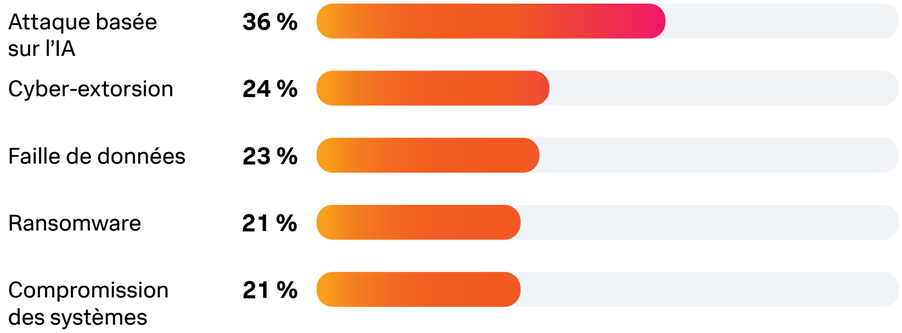
L'inverse est également vrai : les menaces perçues font pâle figure face à l'ampleur de la menace. Seulement 18 % des personnes interrogées considèrent que la compromission des messageries professionnelles est la menace qui les préoccupe le plus, bien qu'elle occupe la deuxième place sur la liste des incidents les plus fréquents en 2024.

Certaines craintes correspondent toutefois à la réalité. Les failles de données, par exemple, sont à la fois une préoccupation majeure et l'attaque la plus souvent subie, 52 % des personnes interrogées ayant signalé au moins une faille de données au cours des deux dernières années.

La peur réside dans l'inconnu. Les entreprises disposent de processus et de procédures de défense contre les attaques connues comme les failles de données, mais elles ignorent encore ce qui, le cas échéant, mettra fin aux attaques basées sur l'IA. »

— Marcus LaFerrera, Directeur de SURGe, Splunk

Quelles sont les cyberattaques les plus préoccupantes ?



Quelles cyberattaques avez-vous subies ?

Dénominateur commun : l'être humain

Comment les malfaiteurs s'infiltrent-ils ? Malgré l'essor de l'automatisation et de l'IA générative, les humains restent le maillon faible. Les personnes interrogées désignent les systèmes mal configurés comme le vecteur de menace le plus courant (38 %) et le plus préoccupant (35 %).

Cette concordance entre les préoccupations et l'expérience suggère que les équipes de sécurité savent que la mauvaise configuration est un problème (bravo à la supervision !) mais ne peuvent pas la gérer efficacement. Des systèmes plus complexes et la pénurie de talents dans la sécurité peuvent exacerber le problème et donner l'impression que l'élimination des mauvaises configurations est un jeu de la taupe.

Principaux vecteurs de menace

38 %

Mauvaise configuration des systèmes

31 %

Vulnérabilités dans les applications développées en interne

30 %

Vulnérabilités zero-day

29 %

Vulnérabilités logicielles connues

28 %

Mouvement latéral

Les attaques à motivation financière persistent

Le trio gagnant des attaques à motivation financière – failles de données, ransomwares et extorsion – fait toujours figure d'épouvantail. Le nombre de personnes interrogées dont les données et les systèmes ont été pris en otage est passé de 35 % en 2022 à 42 % en 2024. La cyber-extorsion, une tactique de ransomware qui consiste à voler et à menacer de rendre publiques les données de l'entreprise, était plus fréquente que le ransomware à proprement parler. Quelque 48 % des personnes interrogées déclarent avoir été victimes de cyber-extorsion, contre 45 % victimes de ransomwares.

La popularité de la cyber-extorsion peut être attribuée au succès de l'incident Colonial Pipeline de 2021 et, plus récemment, aux attaques MOVEit dans lesquelles le groupe de ransomwares Clop, basé en Russie, prévoyait de gagner entre 75 et 100 millions de dollars grâce à l'extorsion.

Alors que les entreprises prennent conscience de l'importance de tester les sauvegardes, les cybercriminels pourraient délaisser le chiffrement au profit de l'exfiltration de données et de l'extorsion, des techniques qui nécessitent moins de travail, rapportent plus et ne reposent pas sur des sauvegardes défectueuses.

La géopolitique enflamme les cyber-malheurs

L'année 2024 est marquée par des troubles mondiaux. Ces tensions géopolitiques croissantes ont des implications cybernétiques qui affectent même les entreprises apparemment apolitiques. L'attaque d'une station d'épuration de Pennsylvanie par des hacktivistes en 2023 montre que personne n'est à l'abri d'un État voyou ou d'un groupe terroriste.

86 % des personnes interrogées déclarent que le climat géopolitique actuel contribue à ce que leur entreprise soit davantage ciblée. Les entreprises technologiques en particulier sont tout à fait d'accord avec ce sentiment (42 %) contre 29 % pour l'ensemble des personnes interrogées. Les atteintes très médiatisées ayant des liens géopolitiques, comme celle de SolarWinds, rappellent aux entreprises technologiques, en particulier aux fournisseurs de services informatiques, qu'elles peuvent servir de passerelle à des acteurs politiquement motivés pour atteindre toute une série de cibles.

Il est intéressant de noter que seules 17 % des personnes interrogées du secteur public sont tout à fait d'accord pour dire que les tensions géopolitiques croissantes font d'elles une cible plus importante, peut-être parce que les entreprises gouvernementales ont été (et seront probablement toujours) la cible d'attaques géopolitiques.

Audra Streetman, Stratège en sécurité chez Splunk SURGe, déclare : « L'hacktivisme n'est pas toujours sophistiqué. Les attaquants à motivation politique utilisent souvent des vulnérabilités plus anciennes, des mots de passe par défaut et d'autres moyens simples pour cibler les entreprises, c'est pourquoi il est plus important que jamais de s'engager en faveur de l'hygiène informatique. »

« Les tensions géopolitiques croissantes vont continuer à accroître les risques, même pour les entreprises apparemment apolitiques. Un sous-produit de notre chaîne d'approvisionnement mondiale est le risque hérité de chaque lien numérique. »

— Mick Baccio, Conseiller en sécurité globale, Splunk

La pression croissante de la conformité

Pour les professionnels de la sécurité, la conformité réglementaire est au même niveau que la mort et les impôts : inévitable. En fait, 62 % d'entre eux affirment avoir déjà été touchés par l'évolution des décrets de conformité qui exigent la divulgation des failles majeures.

Les professionnels de la sécurité sont parfaitement conscients que l'environnement réglementaire entraînera des changements dans leur travail, de manière intentionnelle ou peut-être involontaire. Par exemple, 87 % d'entre eux reconnaissent que dans un an, ils traiteront la conformité de manière très différente. Et bien que la conformité et la cybersécurité ne soient en aucun cas contradictoires, les conséquences involontaires pourraient être le sacrifice d'un programme au profit d'un autre. 86 % affirment qu'ils modifieront leurs budgets pour donner la priorité aux réglementations de conformité plutôt qu'aux meilleures pratiques de sécurité.

Ces réponses font écho à notre rapport pour les RSSI d'octobre 2023, dans lequel 84 % des RSSI interrogés s'inquiètent de la responsabilité personnelle en cas d'incidents liés à la cybersécurité. Dans la même étude, 84 % des RSSI ont déclaré que leurs conseils d'administration ou organes de gouvernance assimilaient une sécurité forte à la conformité réglementaire et non aux mesures traditionnelles de réussite en matière de sécurité.

Cela se comprend aisément. Aux États-Unis, de nouvelles règles imposent aux entreprises réglementées par la Securities and Exchange Commission (SEC) de divulguer et de décrire tous les incidents de cybersécurité « majeurs » et de partager chaque année des informations sur leurs programmes de gestion des risques. Le non-respect de cette directive peut entraîner de lourdes sanctions financières, des poursuites judiciaires, voire des peines d'emprisonnement pour les dirigeants. Dans l'Union européenne, la directive NIS2 exige que les entreprises mettent en place des équipes appropriées pour répondre aux incidents et des systèmes d'information pour échanger des informations. Les dirigeants peuvent être tenus personnellement responsables en cas d'infraction.

Les professionnels de la sécurité sont pris entre le marteau et l'enclume. S'ils sous-estiment les dégâts, ils risquent d'être accusés de fraude et de voir des poursuites judiciaires engagées. S'ils les surestiment, leurs hypothèses peuvent faire chuter le cours des actions et susciter la méfiance générale du conseil d'administration.

La réglementation est désormais un pilier indéniable de la stratégie de sécurité. Les exercices de simulation tels que les « tabletops » peuvent aider les entreprises à découvrir les lacunes, tout en prouvant aux autorités de réglementation qu'elles s'investissent dans l'amélioration continue, avant qu'elles ne fassent l'objet du prochain gros titre.

Les conséquences de la nouvelle réglementation relative à la divulgation des failles majeures

63 %

s'attendent à ce que les entreprises surdéclarent les infractions pour éviter des sanctions.

61 %

prévoient que les évaluations des entreprises cotées en bourse diminueront à la suite du signalement des failles majeures.

26 %

pensent que les deux phénomènes se produiront.

Les équipes chargées de la sécurité, du droit et de la conformité unissent leurs forces

Il fut un temps où la conformité était essentiellement une fonction transactionnelle. Les équipes chargées de la conformité travaillaient en vase clos, souvent sans communiquer avec les équipes chargées de la sécurité ou sans même comprendre pleinement leur rôle, et vice versa.

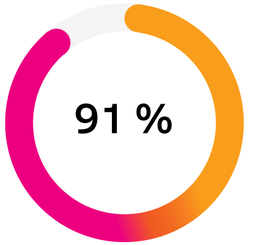
Cette époque est maintenant révolue car le non-respect des règles a des conséquences plus graves. En octobre 2023, la SEC a inculpé l'ancien RSSI de SolarWinds pour fraude et manquements aux contrôles internes qui ont conduit à la cyberattaque dévastatrice de 2020, alléguant qu'il avait trompé les actionnaires sur les pratiques de cybersécurité de l'entreprise. La communication entre le conseil d'administration, l'équipe juridique, l'équipe de conformité et l'équipe de sécurité n'est pas négociable.

Les entreprises et leurs conseils d'administration devront réfléchir longuement à la question de savoir qui est le plus responsable en cas de faille. Il s'agit probablement du RSSI. Mais il pourrait également s'agir du CTO, du DSI ou même du cyber-expert au sein du conseil d'administration, qui pourrait faire l'objet d'une action en justice dérivée ou d'un examen plus approfondi.

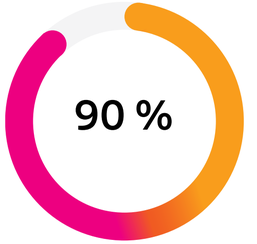
Les professionnels de la sécurité n'échappent pas à cette évolution, la majorité des personnes interrogées renforçant les pratiques de sécurité et facilitant l'alignement des équipes juridiques et de conformité.

Mettre tout le monde sur la même longueur d'onde portera ses fruits. L'alignement des priorités, des rôles et des responsabilités rend votre dispositif de sécurité plus efficace, tout en permettant aux équipes juridiques et de conformité de devenir plus autonomes.

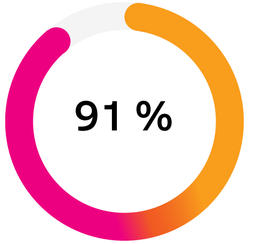
Comment les équipes chargées de la sécurité et de la conformité collaborent-elles ?



intensifient la formation à la **sécurité** pour les équipes juridiques et de conformité



renforcent la formation des équipes de sécurité en matière de **droit et de conformité**



déclarent que tous les membres de leur équipe de sécurité ont intégré la conformité dans leur travail

La conformité devient personnelle

L'inculpation de SolarWinds a marqué un tournant : c'était la première fois que la SEC inculpait un RSSI dans le cadre d'un incident de cybersécurité. Cette action sans précédent a marqué un tournant dans la façon dont le monde perçoit la cybersécurité et aura des conséquences durables pour les responsables de la sécurité et leurs équipes. Le risque cybernétique est désormais sans équivoque synonyme de risque métier.

La SEC demande aux dirigeants et aux autres parties prenantes de rendre des comptes, et ils n'hésitent pas à le faire. En plus d'une série de nouveaux décrets mondiaux pleinement appliqués, les équipes de sécurité doivent également signaler les incidents plus rapidement. La directive NIS2 de l'Union européenne prévoit un délai de 24 à 72 heures, tandis que la SEC offre un peu plus de marge de manœuvre, avec un délai de quatre jours ouvrables. Il n'en reste pas moins que la fenêtre se rétrécit : une évolution qui constituera probablement un appel aux armes pour les professionnels les plus chevronnés.

Une plus grande responsabilité en cas d'incident peut conduire à de meilleures pratiques en matière de sécurité, mais elle peut aussi avoir un effet dissuasif sur la profession. Combien de personnes seraient prêtes à risquer l'engagement de procédures judiciaires pour avoir commis une erreur dans le cadre de leur travail ?

La crainte est probablement exagérée, mais ces aberrations ont un effet dissuasif réel. À l'heure où les équipes cyber sont confrontées à une pénurie de talents, la crainte de sanctions liées à la conformité est une raison supplémentaire d'envisager une autre carrière.

La pression de la conformité crée des doutes sur la carrière

76 % s'accordent à dire que le risque de responsabilité personnelle rend la cybersécurité moins attrayante.

70 % déclarent avoir envisagé de quitter le secteur en raison du stress professionnel.

36 % déclarent avoir envisagé de quitter le secteur à plusieurs reprises.

Aller de l’avant

En 2024, la cybersécurité sera guidée par un ensemble de dynamiques mondiales, notamment de nouvelles exigences en matière de conformité et des tensions géopolitiques, mais il y a aussi des raisons d’espérer. L’audace et l’optimisme en matière d’IA seront de bon augure pour les défenseurs, surtout si les entreprises peuvent atténuer les risques et garder le contrôle sur la façon dont leurs employés utilisent les outils d’IA.

Une autre raison d’être optimiste est que les entreprises investissent davantage dans la cybersécurité. Presque toutes les entreprises interrogées (96 %) déclarent qu’elles augmenteront leurs dépenses en matière de cybersécurité au cours de l’année ou des deux années à venir.

Quelques conseils

Avec tous ces changements et l'évolution de ces technologies, les entreprises peuvent avoir du mal à déterminer où concentrer leurs efforts. Les experts de Splunk dispensent leurs conseils en tenant compte des données de cette année.

Adopter l'IA générative dans toute l'entreprise.

L'adoption généralisée est déjà en cours dans l'ensemble des entreprises (93 %) et au sein des équipes de sécurité (91 %). Les entreprises qui résistent à l'IA générative risquent d'être distancées. Tenter de l'interdire complètement fermera la porte à l'innovation tout en ouvrant la porte à l'IA clandestine.

Élaborer des politiques d'IA générative avisées sans sacrifier l'innovation.

Se précipiter pour adopter l'IA générative sans tenir compte des risques et des implications est une erreur. Créez une politique autour de l'IA générative et élaborez un plan pour les scénarios d'utilisation métiers et de sécurité afin de devancer les 34 % d'entreprises dénuées de politique codifiée. Déterminez quels risques liés à l'IA générative sont les plus préoccupants (pour 49 % des personnes interrogées, il s'agit de la fuite de données) et élaborez des politiques qui les abordent de manière spécifique.

Mettre l'accent sur la collaboration entre les équipes et la consolidation des outils.

Les entreprises résilientes sur le plan numérique suppriment les cloisonnements dans les domaines de l'ingénierie logicielle, des opérations d'ingénierie et, surtout, des technologies de l'information. 76 % des grandes entreprises ont renforcé leur collaboration avec les services informatiques cette année afin d'améliorer la résilience numérique. Un autre moyen de réduire les frictions est la consolidation des outils, qui peut éviter la surcharge des tableaux de bord et aider les équipes à se concentrer sur les menaces significatives. 43 % des personnes interrogées déclarent qu'elles alternent entre un trop grand nombre d'outils de sécurité et de consoles de gestion disparates.

Se mettre au diapason des équipes juridiques et de conformité.

Cette année marque le début d'une nouvelle ère de conformité pour les responsables de la sécurité, qui doivent travailler en étroite collaboration avec les équipes juridiques et de conformité pour une harmonisation maximale. 91 % d'entre eux affirment que les équipes de sécurité ont déjà intégré la conformité dans leur travail. Les entreprises peuvent s'appuyer sur des exercices de simulation tels que les « tabletops » permettant de découvrir les lacunes en matière de sécurité et de conformité, tout en prouvant aux autorités de réglementation qu'elles s'investissent dans l'amélioration continue.

Priorités absolues en matière de cybersécurité au cours des deux prochaines années

1. Fournir une formation sur les opérations de sécurité au personnel de cybersécurité et des opérations informatiques

2. Acheter des outils d'opérations de sécurité conçus pour aider à automatiser/orchestrer les processus SecOps

3. Développer et construire activement une architecture logicielle intégrée pour les outils d'analyse et d'opérations de sécurité

4. Rechercher, tester et/ou déployer des technologies d'analyse et d'opérations de sécurité basées dans le cloud en plus des outils existants

5. Accroître le recours à l'externalisation pour les opérations de sécurité (par exemple, des fournisseurs de services de sécurité gérés par des tiers)

Apprendre à plaider efficacement en faveur des ressources.

La maturité en matière de cybersécurité vient d'en haut : 95 % des entreprises leaders déclarent disposer des ressources et de l'autorité nécessaires pour résoudre les problèmes. Les RSSI, en particulier, doivent pouvoir discuter et traduire le risque de sécurité d'un point de vue commercial afin de gagner une place à la table des dirigeants. Communiquer avec le conseil d'administration de manière à mettre en évidence la valeur commerciale des investissements dans la cybersécurité. Il s'agit notamment de rendre compte de l'impact des incidents de cybersécurité sur l'entreprise, ou de formuler des exigences de conformité ayant de graves conséquences juridiques ou financières.

Sortir des sentiers battus pour combler les lacunes en matière de talents.

Les données montrent que les entreprises leaders s'appuient sur des méthodes d'embauche et de formation moins traditionnelles. 53 % des dirigeants utilisent l'IA et le machine learning pour combler les lacunes en matière de recrutement, contre seulement 28 % des entreprises en développement. Ces stratégies créatives de recrutement et de formation, comme les programmes qui permettent à des personnes n'exerçant pas de fonctions dans le domaine de la sécurité de faire de l'observation au sein du SOC, peuvent contribuer à combler le déficit de compétences et à insuffler la diversité dont l'équipe de sécurité a tant besoin.

Ne pas oublier les principes de base.

Alors que les menaces de cybersécurité deviennent de plus en plus sophistiquées, les adversaires s'appuient toujours sur des techniques éprouvées et les systèmes mal configurés restent un des principaux vecteurs en 2024. C'est en mettant en place des contrôles de base que les entreprises peuvent obtenir le meilleur retour sur investissement, ce qui leur permet de répondre plus facilement aux exigences à long terme. Bien que 76 % des entreprises déclarent que la réalisation d'un inventaire des actifs informatiques prend trop de temps, ce temps est utilisé fort à propos. Une vue actualisée de vos actifs et de leurs dépendances permet d'éviter les angles morts dangereux.

Se mettre au diapason des dynamiques mondiales qui affectent le paysage de la cybersécurité.

La cybersécurité n'existe pas en vase clos. La politique, les conflits mondiaux et le renforcement des décrets de conformité ont des répercussions directes et indirectes sur le paysage des menaces. 86 % des personnes interrogées déclarent que le climat géopolitique actuel fait d'elles une cible d'attaque plus importante, et 62 % disent qu'elles ont été affectées par l'évolution des décrets de conformité. Lorsque les entreprises sont conscientes de cette dynamique changeante, elles peuvent plus facilement surmonter les obstacles qui y sont associés.

Découvrez comment catalyser votre résilience numérique avec Splunk

Les Résilients : le podcast des super-héros du numérique

Notre podcast met en scène des super-héros du numérique qui œuvrent au quotidien pour protéger leurs organisations. RSSI, DSI ou CTO, ils savent se protéger des cyberattaques. Leur valeur commune ? La résilience d'entreprise.

En savoir plus

Bâtir la résilience numérique

Les équipes de sécurité d'aujourd'hui sont soumises à la pression constante des cybermenaces, des réglementations en constante évolution et des tensions géopolitiques croissantes. Découvrez comment votre entreprise ne se contente pas de se rétablir, mais prospère au milieu des perturbations.

Se lancer

Points clés par secteur

Nous avons identifié des informations clés dans six secteurs d'activité dans le monde entier.

Fabrication

Les fabricants se concentrent davantage sur la sécurité de l'informatique dématérialisée que les autres secteurs, 40 % d'entre eux la citant comme une initiative prioritaire. Les vulnérabilités de type zero-day sont également au centre des préoccupations des fabricants, 39 % d'entre eux les citant comme une préoccupation majeure, peut-être en raison de la difficulté inhérente à la mise en place de correctifs pour les infrastructures critiques.

Les personnes interrogées dans le secteur de la fabrication ont également du mal à suivre l'évolution du paysage des menaces :

- **51 % des professionnels de la sécurité dans le secteur de la fabrication déclarent que les exigences en matière de sécurité sont devenues plus strictes au cours des 12 derniers mois.**
- **Les personnes interrogées dans le secteur de la fabrication sont plus enclines à dire que la sophistication croissante des menaces les décourage (50 % contre 38 % pour l'ensemble des secteurs d'activité).**

Ces revers pourraient indiquer un manque d'investissement de la part de l'entreprise, car les fabricants sont beaucoup moins susceptibles (36 %) de s'attendre à une augmentation significative des dépenses en matière de cybersécurité, contre 48 % pour l'ensemble des secteurs d'activité.

Toutefois, les personnes interrogées du secteur de la fabrication semblent avoir un avantage sur les autres secteurs lorsqu'il s'agit d'embaucher des personnes compétentes en matière de sécurité :

- **27 % déclarent que le stress au travail les a amenés, eux ou d'autres, à envisager de quitter la cybersécurité à plusieurs reprises, ce qui est bien inférieur aux 36 % enregistrés dans l'ensemble des secteurs d'activité.**
- **27 % déclarent qu'un projet critique a été retardé à plusieurs reprises en raison du manque de compétences, contre 37 % pour l'ensemble des secteurs d'activité.**

Les entreprises de fabrication ayant du mal à obtenir un budget supplémentaire pour la cybersécurité, les responsables de la sécurité doivent démontrer l'impact financier des incidents et se concentrer sur les principaux risques afin d'obtenir l'adhésion de la suite et du conseil d'administration.

Services financiers

Par rapport à d'autres secteurs, les personnes interrogées du secteur des services financiers sont plus optimistes quant à leur capacité à répondre aux exigences en matière de cybersécurité. 50 % d'entre elles déclarent qu'il a été plus facile de suivre le rythme cette année, contre 41 % pour l'ensemble des secteurs d'activité.

Une collaboration accrue entre l'informatique et l'ingénierie pourrait être à l'origine de cet optimisme. Les équipes de sécurité des institutions financières se disent prêtes à travailler plus étroitement avec les opérations d'ingénierie sur les initiatives de résilience numérique (64 % contre 46 % pour l'ensemble des secteurs d'activité).

Les personnes interrogées du secteur des services financiers sont également plus optimistes quant au rôle de l'IA générative dans l'atténuation de la pénurie de talents. Elles conviennent que l'IA générative serait utile pour :

- **pour les entreprises pour la recherche et l'intégration plus rapide de talents (63 % contre 58 % pour l'ensemble des secteurs d'activité),**
- **pour permettre aux professionnels de la sécurité chevronnés d'être plus productifs (71 % contre 65 % pour l'ensemble des secteurs d'activité).**

Cependant, elles reconnaissent également le risque de l'IA générative. 76 % des personnes interrogées du secteur des services financiers déclarent ne pas être suffisamment formées pour comprendre pleinement les implications de l'IA générative, contre 65 % pour l'ensemble des secteurs d'activité. Par conséquent, 39 % d'entre elles considèrent les attaques par l'IA comme une préoccupation majeure.

Sans surprise, les professionnels de la sécurité des entreprises de services financiers déclarent que la conformité est devenue une tâche si importante qu'elle nécessite une équipe distincte (43 % contre 39 % dans les autres secteurs). La cyber-extorsion est également plus fréquente dans les institutions financières (54 % contre 48 % dans les autres secteurs).

Méthodologie

Les chercheurs ont interrogé 1 650 responsables de la sécurité en décembre 2023 et en janvier 2024. Les personnes interrogées se trouvaient en Allemagne, en Australie, aux États-Unis, en France, en Inde, au Japon, en Nouvelle-Zélande, au Royaume-Uni et à Singapour. Elles représentaient également 16 secteurs d'activité : aérospatiale et défense, services aux entreprises, biens de consommation finis, éducation, services financiers (banque, valeurs, assurance), gouvernement (fédéral/national, étatique et local), santé, technologie, sciences de la vie, fabrication, médias, pétrole/gaz, vente au détail/en gros, télécommunications, transport/logistique et services publics.

Communication et médias

Les personnes interrogées du secteur des communications et des médias sont les plus nombreuses (57 %) à qualifier leurs programmes de cybersécurité comme étant « extrêmement avancés » (contre 47 % pour l'ensemble des secteurs d'activité). Ce secteur est toutefois également le plus susceptible de déclarer qu'il ne dispose pas des ressources ou de l'autorité nécessaires pour relever les défis (16 % contre 8 % pour l'ensemble des secteurs d'activité).

Le secteur des communications et des médias est celui qui a le plus de difficultés si l'on tient compte de ce qui suit :

- **82 % déclarent qu'il est difficile d'assurer l'hygiène de sécurité et une bonne posture en raison des changements fréquents et de l'augmentation de la surface d'attaque, contre 71 % pour l'ensemble des secteurs d'activité.**
- **62 % déclarent que leur SOC jongle entre de trop nombreux outils de sécurité et consoles de gestion disparates, contre 43 % pour l'ensemble des secteurs d'activité.**
- **47 % déclarent qu'eux-mêmes ou d'autres ont envisagé de quitter la cybersécurité à plusieurs reprises en raison de l'impossibilité d'embaucher ou de conserver du personnel possédant les compétences adéquates, contre 36 % pour l'ensemble des secteurs d'activité.**
- **74 % des entreprises se disent touchées par l'évolution des obligations de conformité, contre 62 % pour l'ensemble des secteurs d'activité.**

Ces difficultés peuvent avoir conduit les entreprises du secteur des communications et des médias à rencontrer plus fréquemment plusieurs types d'incidents, notamment des attaques d'initiés (55 % contre 42 % pour l'ensemble des secteurs), des fraudes sur les actifs numériques (59 % contre 43 % pour l'ensemble des secteurs), des attaques de la chaîne d'approvisionnement en logiciels (57 % contre 43 % pour l'ensemble des secteurs) et des attaques ciblées (54 % contre 44 % pour l'ensemble des secteurs) que leurs homologues des autres secteurs d'activité. Les systèmes mal configurés sont plus problématiques pour le secteur des communications et des médias, 44 % des personnes interrogées l'ayant cité comme cause première au cours des deux dernières années.

Les entreprises de communication et des médias devraient s'efforcer d'obtenir l'adhésion de la direction afin d'accroître encore la maturité de leurs programmes de cybersécurité. Lorsque les équipes de cybersécurité disposent des ressources et de l'autorité nécessaires pour résoudre les problèmes, elles sont susceptibles d'obtenir de meilleurs résultats en matière de prévention des menaces.

Technologie

Les personnes interrogées dans les entreprises technologiques ont indiqué avoir du mal à gérer les environnements complexes. Par conséquent :

- **Les entreprises technologiques sont plus susceptibles de citer la complexité de la pile de sécurité comme raison pour laquelle il leur est difficile de se conformer aux exigences en matière de cybersécurité (36 % des entreprises technologiques, contre 26 % pour l'ensemble des secteurs d'activité).**
- **Les entreprises technologiques sont plus enclines à dire qu'elles ont trop d'outils de sécurité fragmentés et qu'elles manquent de ressources humaines pour effectuer le travail manuel (37 % des entreprises technologiques, contre 26 % pour l'ensemble des secteurs d'activité).**
- **Les vulnérabilités connues des logiciels (34 %) et les vulnérabilités des applications internes (34 %) sont plus souvent à l'origine des incidents dans le secteur technologique.**

L'évolution de l'environnement réglementaire est un autre obstacle : 41 % des personnes interrogées dans les entreprises technologiques déclarent que cela contribue à leurs difficultés à rester dans la course, contre 28 % dans l'ensemble des secteurs d'activité.

Les conflits géopolitiques affectent également les entreprises technologiques de manière plus prononcée. Elles sont tout à fait d'accord (42 %) pour dire que les conflits internationaux contribuent à ce que leur entreprise soit davantage ciblée par des adversaires, contre 29 % pour l'ensemble des secteurs d'activité.

Sur une note plus positive, les entreprises technologiques sont beaucoup plus susceptibles (63 %) de faire état d'une augmentation significative des dépenses de sécurité prévues, contre 48 % pour l'ensemble des secteurs d'activité.

Pour les entreprises technologiques qui luttent contre la complexité, le mot d'ordre devrait être la simplification. La consolidation des outils pourrait être une initiative importante pour ce secteur qui semble souffrir du syndrome de l'objet brillant.

Santé

Les organismes de santé ont les temps moyens de détection les plus problématiques de tous les secteurs, 31 % d'entre eux déclarant mesurer les temps moyens de détection en mois, contre seulement 19 % des organisations de tous les secteurs d'activité. Ils sont également davantage confrontés aux attaques de ransomwares que les autres secteurs, 56 % d'entre eux ayant signalé une attaque de ransomware au cours des deux dernières années, contre 45 % pour l'ensemble des secteurs d'activité. Le secteur de la santé est également plus enclin que les autres secteurs à citer les comptes trop permissifs (33 %) comme la cause première la plus fréquente des incidents.

Les personnes interrogées du secteur de la santé signalent davantage de problèmes liés à l'embauche que les autres secteurs d'activité :

- **44 % déclarent que des membres de leur équipe ont été invités à diriger des projets sans avoir l'expérience requise, contre 39 % pour l'ensemble des secteurs d'activité.**
- **44 % déclarent que des projets ou des initiatives critiques ont été retardés en raison de problèmes de recrutement, contre 37 % pour l'ensemble des secteurs d'activité.**

La plupart des personnes interrogées dans le secteur de la santé déclarent avoir été affectées par l'évolution des obligations de conformité (67 %). Elles sont également plus nombreuses à être tout à fait d'accord (44 %, le taux le plus élevé de tous les secteurs d'activité) pour dire que ces changements obligent un plus grand nombre de cadres supérieurs à être disponibles 24 heures sur 24 et 7 jours sur 7, contre 35 % dans l'ensemble des secteurs d'activité.

Les personnes interrogées dans le secteur de la santé sont les moins optimistes en ce qui concerne l'IA générative. 52 % d'entre elles déclarent s'attendre à ce que les malfaiteurs en profitent davantage, contre 45 % pour l'ensemble des secteurs d'activité. Elles manifestent également moins d'intérêt pour utiliser l'IA afin de lutter contre l'avantage concurrentiel que leurs concurrents pourraient en tirer : seulement 37 % des organismes de santé considèrent l'IA comme une priorité, contre 44 % pour l'ensemble des secteurs d'activité.

Compte tenu des difficultés rencontrées par le secteur de la santé en matière de détection des menaces, de prévention des ransomwares et d'embauche, le retour aux fondamentaux de l'hygiène en matière de cybersécurité pourrait être une solution efficace pour permettre à ces entreprises d'en faire davantage avec moins.

Secteur public

Les données du secteur public mettent en évidence une quête de connaissances. Les personnes interrogées du secteur public mettent davantage l'accent sur la formation à la sensibilisation à la sécurité (24 % contre 17 % pour l'ensemble des secteurs d'activité). En conséquence, elles considèrent que leur principal défi est le manque de connaissances et d'engagement des dirigeants en matière de cybersécurité (28 % contre 20 % pour l'ensemble des secteurs d'activité).

Alors que les personnes du secteur public interrogées l'année dernière hésitaient quant à la capacité de l'IA traditionnelle à alléger la charge de travail de l'équipe de sécurité, cette année, le secteur public se montre optimiste à l'égard de l'IA générative :

- **Les personnes interrogées du secteur public sont les plus susceptibles de voir des opportunités pour l'IA générative d'avoir un impact « qui change la donne » pour l'entreprise (55 % contre 47 % pour l'ensemble des industries) et anticipent le plus d'avantages pour l'équipe de sécurité (55 % contre 46 % pour l'ensemble des secteurs d'activité).**
- **Les équipes de sécurité du secteur public sont en tête pour l'adoption de politiques d'utilisation acceptable de l'IA (77 % contre 66 % pour l'ensemble des secteurs d'activité).**
- **Les personnes interrogées du secteur public sont également plus susceptibles d'envisager des scénarios d'utilisation de l'IA générative dans le domaine de la sécurité, notamment la détection des menaces (46 % contre 35 % pour l'ensemble des secteurs), les tests de pénétration (42 % contre 29 % pour l'ensemble des secteurs) et la formation des équipes de sécurité (44 % contre 34 % pour l'ensemble des secteurs d'activité).**

Les entreprises du secteur public semblent également avoir de plus grandes aspirations d'automatisation SecOps que leurs homologues, y compris l'automatisation de la gestion des certificats SSL (43 % contre 31 % dans l'ensemble des industries), l'orchestration des actions à travers les contrôles de sécurité (53 % contre 38 %) et l'enrichissement des alertes (47 % contre 32 %).

En ce qui concerne les principes de base de la cybersécurité, le secteur public cite plus fréquemment les mauvaises configurations comme le principal vecteur de menaces, 42 % d'entre eux déclarant qu'elles en sont le plus souvent la cause première. Les personnes interrogées du secteur public sont également plus enclines à s'inquiéter des mouvements latéraux, 39 % d'entre elles les citant comme leur principale préoccupation.

Le manque de connaissances et l'enthousiasme pour l'IA peuvent être une combinaison dangereuse, de sorte que les entreprises du secteur public devraient adopter une approche mesurée de l'adoption de l'IA et se former aux risques avant de sauter dans le train de l'IA générative.

Points clés par pays

Des aperçus de la situation de huit pays aux quatre coins de la planète.

Australie

Les données fournies par les entreprises australiennes dressent un tableau alarmant du paysage de la cybersécurité dans le pays. Les entreprises australiennes sont plus susceptibles d'être tout à fait d'accord pour dire que les tensions géopolitiques exacerbent les cyberattaques (44 % contre 29 % à l'échelle mondiale). 56 % des personnes interrogées en Australie ont subi des attaques d'États voyous, contre 39 % à l'échelle mondiale.

En fait, les personnes interrogées en Australie connaissent un taux plus élevé que la moyenne pour chaque type d'attaque, y compris, mais sans s'y limiter, les atteintes aux données (63 % contre 52 % à l'échelle mondiale), les atteintes à la conformité réglementaire (53 % contre 43 % à l'échelle mondiale), les attaques d'initiés (55 % contre 42 % à l'échelle mondiale) et la compromission de l'e-mail professionnel (59 % contre 49 % à l'échelle mondiale).

La fréquence plus élevée des cyberattaques peut éventuellement être attribuée aux problèmes de visibilité des personnes interrogées en Australie. 72 % d'entre elles déclarent trop avoir à jongler entre les différents outils de sécurité (contre 43 % à l'échelle mondiale), et 35 % citent des problèmes de visibilité sur la surface d'attaque (contre 20 % à l'échelle mondiale). Il n'est donc pas surprenant que l'Australie indique également des problèmes de détection, 50 % des personnes interrogées déclarant que le temps moyen de détection typique prend des mois, contre 19 % à l'échelle mondiale.

Les personnes interrogées en Australie sont également plus confrontées aux défis liés au personnel que les autres pays :

- **52 % déclarent que des membres de leur équipe ont été invités à diriger plusieurs fois des projets sans avoir l'expérience requise, contre 39 % à l'échelle mondiale.**
- **50 % déclarent que le stress au travail les a amenées, elles-mêmes ou d'autres, à envisager de quitter la cybersécurité à plusieurs reprises, contre 36 % à l'échelle mondiale.**
- **52 % déclarent que des projets ou des initiatives critiques en matière de sécurité ont été retardés à plusieurs reprises, contre 37 % à l'échelle mondiale.**

L'Australie est un leader à la fois dans l'adoption de l'IA générative et dans la création de politiques, avec 69 % déclarant que les employés utilisent des outils d'IA générative publics pour faire leur travail, contre 54 % à l'échelle mondiale, et 73 % déclarant avoir établi des politiques de sécurité pour l'utilisation de l'IA générative, contre 66 % à l'échelle mondiale.

France

Les personnes interrogées en France sont plus enclines à dire qu'elles ont eu du mal à se conformer aux exigences en matière de cybersécurité au cours de l'année écoulée (56 % contre 46 % à l'échelle mondiale). Il n'est pas surprenant de constater que la maturité des entreprises en matière de cybersécurité est plus faible, puisque seulement 37 % d'entre elles qualifient leurs programmes d'« extrêmement avancés », contre 47 % dans le monde.

Lorsqu'on leur demande pourquoi il est plus difficile de répondre aux exigences en matière de cybersécurité, 33 % des personnes interrogées en France déclarent que le nombre d'outils et de fournisseurs dans leur pile de sécurité est devenu trop important, contre 26 % dans le monde. Une pile technologique complexe entraîne souvent des erreurs de configuration et 40 % des personnes interrogées en France citent ce problème.

La France est derrière les autres pays en ce qui concerne l'adoption massive d'outils de cybersécurité dotés de capacités d'IA et de machine learning (27 % contre 37 % dans le monde). Et si les entreprises françaises sont plus enclines à dire qu'elles se concentrent sur l'IA (56 % en France, contre 44 % dans le monde), elles sont également moins susceptibles d'avoir établi des politiques de sécurité pour l'utilisation de l'IA générative à 52 %, contre 66 % dans le monde.

D'un autre côté, les personnes interrogées en France déclarent avoir subi moins d'incidents que la moyenne mondiale pour les types d'attaques suivants au cours des deux dernières années :

- **44 % ont subi une faille de données,**
- **37 % ont enfreint la conformité réglementaire,**
- **37 % ont subi une attaque DDoS,**
- **40 % ont été victimes d'une attaque par ransomware.**

Allemagne

Les données des personnes interrogées en Allemagne indiquent une prise de conscience plus poussée des risques de l'IA générative par rapport à leurs homologues :

- **41 % des personnes interrogées en Allemagne sont tout à fait d'accord pour dire que l'IA générative élargit leur surface d'attaque de manière préoccupante, contre 31 % dans le monde.**
- **38 % des personnes interrogées en Allemagne sont tout à fait d'accord pour dire que l'IA générative rend leur surface d'attaque existante plus vulnérable, contre 29 % dans le monde.**

Les entreprises allemandes semblent avoir du mal à recruter du personnel. 33 % d'entre elles citent l'incapacité à recruter suffisamment de personnel de sécurité qualifié comme la raison pour laquelle les exigences en matière de cybersécurité ont été plus difficiles à satisfaire au cours de l'année écoulée, contre 25 % dans le monde.

Dans le SOC, 53 % des personnes interrogées en Allemagne déclarent qu'il y a trop d'alternance entre des outils de sécurité disparates (contre 43 % dans le monde). Il est possible qu'un grand nombre de ces outils disparates soient basés sur le cloud, car l'Allemagne cite les attaques contre l'infrastructure du cloud comme l'un des types d'incidents les plus préoccupants (23 %).

Ces contraintes en matière de recrutement et d'outillage peuvent avoir contribué à allonger légèrement les temps moyens de détection par rapport à leurs homologues ; 40 % des personnes interrogées en Allemagne mesurent leur temps moyen de détection en semaines, contre 35 % dans le monde.

Malgré ces revers, l'Allemagne se distingue des autres pays par sa capacité à récupérer les données et les systèmes lors d'une attaque de ransomware. 58 % d'entre eux y sont parvenus au cours des deux dernières années (le pourcentage le plus élevé de tous les pays étudiés), contre 44 % dans le monde.

Les personnes interrogées en Allemagne sont également plus susceptibles d'admettre (94 %) que le climat géopolitique actuel contribue à ce que les entreprises soient davantage ciblées par des attaquants, contre 86 % dans le monde.

Inde

Par rapport aux autres pays, l'Inde a le pourcentage le plus élevé d'entreprises (66 %) qui considèrent leurs programmes de sécurité comme « extrêmement avancés », contre 47 % à l'échelle mondiale. Elles affichent également des taux plus élevés de collaboration entre les équipes internes : 58 % avec l'ingénierie des logiciels, 52 % avec les opérations d'ingénierie et 78 % avec l'informatique.

Les personnes interrogées en Inde sont également particulièrement attentives à la sécurité cloud, 48 % d'entre elles la citant comme une initiative majeure, contre 35 % dans le monde. Sans surprise, l'Inde est le pays le plus enclin à citer les attaques contre les infrastructures cloud comme une préoccupation majeure (25 %) par rapport aux autres pays. Toutefois, c'est la cyber-extorsion qui est la plus préoccupante pour l'Inde, avec 37 % des personnes interrogées, contre 24 % dans le monde.

Les décrets de conformité exigeant la divulgation des failles majeures semblent avoir un impact important sur l'Inde, puisque 81 % des personnes interrogées en Inde déclarent avoir été touchées par ces changements, contre 62 % dans le monde. En conséquence, 54 % des personnes interrogées en Inde sont convaincues que tous les membres de l'équipe de sécurité devraient faire de la conformité une partie de leur travail, contre 42 % dans le monde.

Les personnes interrogées en Inde sont les plus optimistes quant à la manière dont l'IA générative fera pencher la balance : 51 % s'attendent à ce que les défenseurs en bénéficient davantage, contre 43 % dans le monde. Elles reconnaissent également des scénarios d'utilisation potentiels de l'IA générative plus fréquents, notamment :

- **la détection et la hiérarchisation des menaces (52 % contre 35 % dans le monde),**
- **les scénarios d'utilisation de la formation (50 % contre 34 % dans le monde),**
- **l'analyse de la threat intelligence (55 % contre 39 % dans le monde),**
- **la création de règles de détection (44 % contre 30 % dans le monde),**
- **la synthèse des données de sécurité (54 % contre 34 % dans du monde).**

De même, les personnes interrogées en Inde semblent avoir une longueur d'avance dans la mise en place de politiques relatives à l'IA générative. 82 % ont établi des politiques de sécurité de l'IA générative pour les utilisateurs finaux, contre 66 % dans le monde.

Japon

Par rapport à leurs homologues, les Japonais sont plus enclins à dire que les exigences en matière de cybersécurité sont de plus en plus difficiles à respecter (54 % contre 46 % dans le monde). Seulement 27 % des personnes interrogées au Japon déclarent que la sécurité devient plus facile, contre 41 % dans le monde. Parmi ces personnes interrogées, seulement 5 % affirment que la sécurité devient beaucoup plus facile, alors que la moyenne mondiale est de 17 %.

Pourquoi les entreprises japonaises ont-elles du mal à suivre ? Elles citent plus souvent que leurs homologues les écueils suivants :

- **36 % déclarent que leurs piles de sécurité sont devenues trop alambiquées, contre 26 % dans le monde.**
- **29 % ne sont pas en mesure d'analyser efficacement toutes les données relatives à la sécurité, contre 21 % dans le monde.**
- **27 % ont une visibilité limitée de leur surface d'attaque, contre 20 % dans le reste du monde.**

Une autre possibilité pourrait être le manque de budget. Le Japon est moins susceptible (38 %) de faire état d'une augmentation significative des dépenses prévues en matière de cybersécurité.

Les personnes interrogées au Japon sont moins optimistes quant aux avantages de l'IA générative pour les praticiens du SOC, puisque seuls 37 % d'entre eux sont tout à fait d'accord pour dire qu'elle les aiderait à développer leurs compétences, contre 43 % dans le monde.

Parmi les pays étudiés, c'est le Japon qui se concentre le plus sur la protection contre les ransomwares, avec 21 % des personnes interrogées qui en font une initiative prioritaire. Cette attention accrue pourrait porter ses fruits sous la forme d'un temps moyen de détection plus rapide : 43 % des personnes interrogées au Japon font état d'un temps moyen de détection mesuré en jours, alors que la moyenne mondiale est de 33 %.

Singapour

Les données fournies par les Singapouriens indiquent que les programmes de cybersécurité de leurs entreprises sont moins avancés que ceux des autres pays.

- **C'est à Singapour que l'on trouve le pourcentage le plus élevé de personnes interrogées qui considèrent que leurs programmes de cybersécurité sont « en développement » (14 % contre 7 % dans le monde).**
- **Elles sont moins susceptibles de dire qu'elles ont l'autorité et les ressources nécessaires pour s'attaquer aux défis de cybersécurité (77 % seulement, contre 91 % dans l'ensemble).**
- **Elles sont les moins nombreuses (28 %) à signaler une hausse significative des prévisions de dépenses en matière de cybersécurité.**
- **26 % des personnes interrogées à Singapour ne connaissent pas leur temps moyen de récupération, et 25 % n'ont pas effectué d'analyse post-incident pour calculer le temps moyen de détection.**

Ainsi, les personnes interrogées à Singapour sont moins susceptibles de reconnaître l'impact métier de la résilience numérique. Seulement 23 % d'entre elles sont tout à fait d'accord pour dire que la résilience numérique pourrait améliorer la fidélisation de la clientèle, contre 33 % dans le monde. 25 % sont tout à fait d'accord pour dire que la résilience numérique pourrait empêcher des perturbations importantes des opérations, contre 35 % dans le monde.

Les entreprises de Singapour semblent accorder moins d'importance à la collaboration entre les équipes chargées de la conformité, de la sécurité et des questions juridiques. Seulement 29 % d'entre elles sont tout à fait d'accord avec l'idée d'intensifier la formation de leur équipe de conformité en matière de sécurité, contre 42 % dans le monde. Seulement 29 % sont tout à fait d'accord avec le concept d'intégration de la conformité dans le workflow de l'équipe de sécurité, contre 42 % dans le monde.

Nos données indiquent une corrélation entre la maturité des programmes et la priorité accordée à l'IA. Il n'est donc pas surprenant que seulement 36 % des personnes interrogées à Singapour se concentrent sur l'IA contre 44 % dans le monde. Elles sont également moins nombreuses (48 %) à avoir mis en place des politiques en matière d'IA générative. Par rapport à d'autres pays, Singapour est également le pays le moins inquiet des attaques par l'IA, avec seulement 23 % de réponses l'indiquant comme préoccupation majeure.

Royaume-Uni

Les données du Royaume-Uni dressent un tableau généralement positif par rapport à leurs homologues mondiaux.

Les entreprises britanniques collaborent de plus en plus pour atteindre la résilience plus souvent :

- **66 % déclarent que leurs équipes de sécurité et de développement de logiciels collaborent davantage (contre 54 % dans le monde).**
- **56 % déclarent que leurs équipes chargées de la sécurité et des opérations d'ingénierie collaborent davantage (contre 46 % dans le monde).**

Les personnes interrogées au Royaume-Uni sont également en avance sur les autres pays en ce qui concerne leurs capacités d'automatisation. En particulier, elles ont des taux d'automatisation élevés en ce qui concerne l'automatisation des processus généraux (40 %) et la gestion de la vulnérabilité (35 %).

Les pénuries de compétences n'affectent pas les entreprises britanniques autant que les autres pays. 30 % des personnes interrogées au Royaume-Uni déclarent que des membres de leur équipe ont été invités à diriger plusieurs fois des projets sans avoir l'expérience requise, contre 39 % dans le monde. Seulement 23 % des personnes interrogées déclarent que des projets de sécurité critiques ont échoué à plusieurs reprises en raison de pénuries de compétences, contre 33 % dans le monde.

Ces succès expliquent peut-être pourquoi les entreprises britanniques connaissent des taux inférieurs à la moyenne pour les types d'attaques suivants par rapport à leurs homologues :

- **Infractions à la réglementation (35 % contre 43 % dans le monde)**
- **Attaques internes (37 % contre 42 % dans le monde)**
- **Compromission de la messagerie électronique professionnelle (38 % contre 49 % dans le monde)**
- **Attaque DDoS (38 % contre 46 % dans le monde)**
- **Attaque par prise de contrôle de compte (34 % contre 42 % dans le reste du monde)**
- **Attaque par ransomware (37 % contre 45 % dans le monde)**
- **Attaque de la chaîne d'approvisionnement en logiciels (35 % contre 43 % dans le monde)**

États-Unis

Les données des personnes interrogées aux États-Unis s'écartent rarement des moyennes mondiales. Cependant, un domaine dans lequel les personnes interrogées aux États-Unis sont en avance sur la moyenne est la politique d'utilisation de l'IA générative : 72 % en ont établi une, contre 66 % dans le monde. À l'inverse, les personnes interrogées aux États-Unis sont le groupe le moins concerné par l'utilisation abusive de l'IA en tant que cause première, avec seulement 18 %.

Les personnes interrogées aux États-Unis sont également confrontées à des temps moyens de détection plus longs. 40 % mesurent leurs temps moyens de détection en semaines, contre 35 % dans le monde, et 22 % déclarent qu'un temps moyen de détection typique est de plusieurs mois, contre 19 % dans le monde. Mais le processus semble être sur la bonne voie, puisque 30 % des personnes interrogées indiquent avoir amélioré leur temps moyen de détection grâce à l'automatisation des processus, contre 25 % dans le monde.

En ce qui concerne les priorités futures, les personnes interrogées aux États-Unis sont légèrement plus enclines à s'attaquer à la pénurie de talents dans le domaine de la cybersécurité. 21 % d'entre elles déclarent vouloir recruter davantage de personnel pour les opérations de sécurité (contre 18 % dans le monde) et 25 % prévoient de dispenser une formation aux opérations de sécurité (contre 23 % dans le monde).

À propos de Splunk

Splunk aide les organisations à renforcer leur résilience numérique. Les grandes entreprises utilisent notre plateforme unifiée de sécurité et d'observabilité pour assurer la sécurité et la fiabilité de leurs systèmes numériques. Les entreprises font confiance à Splunk pour empêcher les incidents d'infrastructure, d'application et de sécurité de devenir des problèmes majeurs, pour se remettre plus rapidement des chocs subis par les systèmes numériques et pour s'adapter rapidement aux nouvelles opportunités.

Poursuivez la conversation avec Splunk.

splunk>

24-492903-Splunk-State-of-Security-113-FR