Sécurité des données

Prévisions 2023

Résilience, talents, confidentialité et comment faire face aux menaces cybercriminelles

splunk>

La résilience, clé de la survie

Cette année, les conversations de sécurité ne portent plus sur les mêmes sujets. Au niveau de l'entreprise, on parle moins d'une organisation « sécurisée » et plus d'une organisation résiliente face aux perturbations de la chaîne d'approvisionnement, aux pandémies et aux événements climatiques graves, face à l'incertitude économique et, bien sûr, face au nombre apparemment infini de cybercriminels qui sondent chaque centimètre de ce qu'on appelait autrefois votre périmètre.

En mettant l'accent sur la résilience, on modifie le rôle des responsables de la sécurité dans leurs organisations. Ces discussions varient en fonction de nombreux facteurs, notamment le niveau de maturité de l'organisation. Les organisations traditionnelles, établies de longue date, ont plus de mal à adopter de nouvelles approches, qu'il s'agisse de l'automatisation basée sur l'IA, du cadre Zero Trust ou des pratiques DevSecOps, tandis que les jeunes start-ups ont parfois commencé avec elles.

« L'autre jour, un client m'a dit : "Le DevSecOps est notre Graal, mais pour le moment, nous sommes coincés dans la séquence dev-ops-sec", » relate Simon Davies, Vice-président senior et Directeur général de Splunk dans la région Asie-Pacifique.

Dhiraj Goklani, Vice-président de l'observabilité de Splunk dans la région APAC, explique : « Et dans le même temps, des organisations cloud-native ont appliqué le modèle DevOps dès le départ et n'ont presque pas d'autre choix que d'envisager ce niveau d'intégration. »

Ces différentes réalités se retrouvent à travers l'Europe et sur le continent américain. Mais dans les organisations où la supervision des performances et de la sécurité progresse de pair avec une collaboration croissante, la « résilience » est au premier plan.

Gary Steele, qui a rejoint Splunk en tant que PDG en 2022 après près de vingt ans dans le rôle de PDG et fondateur du fournisseur de sécurité Proofpoint ajoute : « La résilience est également un thème qu'on retrouve du côté de l'observabilité. Nous voyons les organisations donner la priorité à la normalisation et à la promotion de la résilience grâce à un ensemble commun d'outils et de données. »

Cette approche a un effet profond sur les méthodes de travail des équipes de sécurité, et c'est là que nous commençons nos prévisions pour 2023.

Prévisions et stratégies de survie pour 2023

Prévision

Avec la convergence des ITOps et des outils et données de sécurité, les RSSI assumeront davantage de responsabilités en matière de cyber-résilience à grande échelle.

La résilience est la nouvelle tendance. Elle est sur toutes les lèvres, y compris les nôtres. Mais on ne sait pas toujours ce que le terme recouvre.

Mark Woods, Conseiller technique en chef de Splunk pour l'Europe et le Moyen-Orient, déclare : « Il existe des poches de résilience fonctionnelle dans toute organisation. Il s'agit de les rassembler pour passer de la résilience fonctionnelle à la résilience commerciale, et c'est tout le problème pour la plupart des organisations. Mais pour le moment, il n'y a pas de définition de ce que cela signifie réellement pour qui que ce soit. »

Ryan Kovar, Stratège en sécurité chez Splunk, remarque : « Je vois souvent le terme de "résilience" employé comme synonyme de cyber-hygiène. La résilience de l'infrastructure IT globale est importante, et la cyber-résilience en est un aspect plus ciblé. »

M. Woods observe : « En Europe, nous voyons des sociétés de services financiers confier des portefeuilles de résilience à des cadres de très haut niveau. Le plus souvent, on les envoie dans l'organisation de la sécurité. C'est naturel : dans la plupart des entreprises, les seules personnes qui savent comment effectuer correctement une supervision robuste sont celles de la sécurité, parce que c'est le nerf de la guerre. Vous ne pouvez pas assurer la sécurité sans une supervision robuste. Tout le reste peut être fait sans supervision, c'est juste que vous le ferez mal. »

C'est logique : les équipes de sécurité ne seront jamais à court de sujets d'inquiétude en matière de résilience.

Mick Baccio, Stratège en sécurité mondiale, explique : « Les ransomwares ne disparaîtront jamais, la cybercriminalité va s'aggraver et les environnements hybrides tentaculaires sont de plus en plus compliqués à sécuriser. C'est là que la résilience organisationnelle entre en jeu. Votre cyber-résilience va donc avoir un impact sur votre résilience organisationnelle. »

Il est indispensable d'avoir une vision holistique de la façon dont certains aspects de la résilience s'additionnent pour former un tout. En effet, au niveau du conseil d'administration ou de la direction, il n'y a pas de risque acceptable, qu'il s'agisse d'un temps d'arrêt affectant le client causé par une interruption de serveur ou un défaut d'observabilité, d'une attaque de ransomware ou du vol de données sensibles.

« Nous parlons de résilience dans toute l'entreprise depuis des décennies, » affirme Patrick Coughlin, Vice-président de la stratégie et de la spécialisation GTM chez Splunk.

M. Coughlin, qui a cofondé la start-up de threat intelligence TruStar, rappelle que par le passé, vous pouviez demander à 10 personnes ce qu'était la cyber-résilience et obtenir 10 réponses différentes.

Il nuance : « Mais plus récemment, le NIST a fait un excellent travail de définition de la cyber-résilience, en affirmant que nous sommes maintenant à une époque où un incident est un incident, qu'il s'agisse d'une défaillance de la couche d'infrastructure, d'un problème de performances dans une application, d'une interruption de service, d'une menace interne ou d'un malfaiteur externe. Si la résilience de l'entreprise est menacée par des conditions défavorables ou des malveillances, vous devez rapidement trouver le problème, le résoudre, puis ajouter une couche d'automatisation pour ne pas avoir à le refaire. »

Les organisations savent de mieux en mieux exploiter toutes leurs données au lieu de les cantonner à une seule équipe ou un seul outil, ce qui permet aux équipes de sécurité d'adopter une approche plus holistique du risque. Et face à une panne de réseau ou un autre type d'incident, il est logique que la première étape consiste à déterminer s'il s'agit d'une véritable cyberattaque ou de ce que votre équipe opérationnelle pourrait appeler un glitch. Cela change la façon dont les équipes collaborent.

M. Coughlin, qui a dirigé des équipes de cybersécurité dans les secteurs public et privé, déclare : « Nous commençons à voir, dans la dynamique organisationnelle et la définition de la mission, un reflet de la convergence qui se produit au niveau de la couche de données. Les titres et les descriptions de poste évoluent en conséquence, et l'influence du RSSI s'étend à travers l'entreprise pour couvrir cette définition plus large de l'incident. Au final, le RSSI pèse désormais sur les nouvelles décisions dans toute l'organisation. »

Il l'exprime selon les termes de la matrice RACI (Responsible, Accountable, Consulted, Informed) : traditionnellement, les discussions de dirigeants sur les technologies et les processus métier des différentes unités commerciales reléguaient les

RSSI au rang de personnes à *informer* des décisions prises. « Aujourd'hui, les RSSI se déplacent vers la gauche de la matrice RACI. Ils sont systématiquement *consultés* sur les décisions touchant la technologie, les données et les processus de l'ensemble de l'entreprise. Dans certains cas, ils remontent jusqu'au R et au A : Ils deviennent *responsables* dans la définition des processus et des investissements techniques liés à la mission de cyber-résilience. »

On pourrait croire que le RSSI est en train de devenir un « directeur de la résilience », mais ne commandez pas tout de suite les nouvelles cartes de visite. Le titre du RSSI ne changera pas, selon Gary Steele. Mais leurs outils, leurs relations et leur champ d'action, eux, vont évoluer. « De nos jours, les RSSI ont une responsabilité plus large sur les données et se retrouvent donc avec plus de responsabilité en matière de résilience et de performance globale. »

Prévision

Les ransomwares ne vont pas s'envoler, mais l'extorsion directe est également très en vogue.

Les ransomwares s'installent durablement dans le paysage parce qu'ils fonctionnent très bien. Des outils sophistiqués sont échangés sur un marché sophistiqué, et environ la moitié des victimes paient sans se manifester. Les recherches du rapport État de la cybersécurité de Splunk en 2022 ont révélé que, à l'échelle mondiale, 79 % des organisations ont subi des attaques par ransomware, et qu'elles étaient 35 %, soit près de la moitié de la cohorte de victimes, à avoir perdu l'accès à leurs données et leurs systèmes à la suite d'une attaque. Parmi les victimes, 33 % seulement ont pu restaurer une sauvegarde et refuser de payer les attaquants. Les 66 % restants ont déclaré que leur entreprise (dans 39 % des cas) ou leur compagnie d'assurance (27 %) avait payé les escrocs. En moyenne, les personnes interrogées ont déclaré que la rançon la plus élevée payée par leur organisation était d'environ 347 000 USD.

Les ransomwares sont tellement lucratifs que les criminels vont continuer à innover. Il est vrai que le verrouillage de systèmes est une opération très exposée. Mais pourquoi faire une affaire publique de ce qui pourrait être une transaction privée ?

Ryan Kovar avertit : « Les acteurs du ransomware vont sauter l'étape du chiffrement pour passer à l'extorsion directe. Nous avons déjà vu quelques affaires de ce type. Avec les ransomwares classiques, lorsque vous verrouillez le réseau pour tous les utilisateurs, le monde entier sait que vous avez été compromis. Imaginez maintenant que les opérateurs du ransomware entrent et exfiltrent uniquement de l'IP sensible ou des données client. Ils ne suppriment pas les informations : ils entrent simplement en leur possession. Ensuite, ils envoient trois e-mails : au conseil d'administration, au PDG et au RSSI, et c'est tout. Ils prouvent ce qu'ils ont fait et annoncent : "Pour 40 millions de dollars, ce problème disparaît sans faire de bruit." »

C'est une évolution par rapport à la grande tendance de 2021, la « double extorsion » : le groupe derrière le ransomware verrouille vos fichiers et vous menacent à double titre : 1) Payez ou les fichiers restent chiffrés, et 2) Payez ou nous partageons vos données avec le monde entier. Comme l'extorsion directe est moins visible pour le public, on peut raisonnablement penser que ce type d'attaque a déjà lieu. Parce que nous savons déjà qu'au-delà des pratiques habituelles de l'extorsion numérique, les auteurs de ransomwares ont tout intérêt à diversifier leur portefeuille.

« Il n'y a plus une énorme différence entre les techniques d'un groupe d'opérateurs de ransomware et une menace persistante avancée ayant l'appui d'un État-nation, » affirme M. Kovar. La différence réside dans les motivations et les objectifs des criminels purs et durs, qui ne sont pas exactement les mêmes que ceux des acteurs APT soutenus en sous-main par des gouvernements. « Les groupes de ransomware veulent gagner de l'argent, alors que les APT cherchent à perturber les activités ou voler la propriété intellectuelle d'un gouvernement ou d'une entreprise étrangère. Les binaires de ransomware ne sont qu'un outil parmi tout un arsenal pour les malfaiteurs. »

Et il s'agit bien souvent du dernier outil, remarque-t-il. « Une grande partie de nos recherches montre que les malfaiteurs restent sur le réseau pendant des jours. Ils commencent par utiliser des outils traditionnels comme les chevaux de Troie, PowerShell, CobaltStrike, move, del, toutes sortes d'outils normalement utilisés par un cybercriminel ou acteur APT. Mais à la toute fin, les rançonneurs chargent un binaire de ransomware et verrouillent tout. »

Mick Baccio déclare : « Et il ne s'agit plus seulement de ransomware. Les groupes de mercenaires que nous voyons dans le monde entier n'hésitent plus à faire preuve d'audace dans leur offre. Ils ne se contentent plus de chiffrer des fichiers contre de l'argent, ils se livrent à toutes les pratiques pour lesquelles vous voudrez les embaucher. C'est la cybercriminalité en tant que service. »

Ce qui nous amène à notre prochaine prévision.

Prévision

L'économie de la cybercriminalité en tant que service va faire augmenter le volume et l'efficacité des cyberattaques.

L'année dernière, nous avions prédit la professionnalisation croissante des groupes de ransomwares. Malheureusement, nous avions raison.

Mick Baccio déclare : « Pour ça, nous avions raison à 100 %. Les ransomwares sont passés du statut de service à celui d'économie. Quand vous regardez l'aspect technique du ransomware, c'est vraiment un peu ennuyeux. Mais comme c'est très facile à lancer, en s'adjoignant d'autres services, c'est devenu un écosystème complet. La pratique a gagné en vitesse et en efficacité. Les opérateurs de ransomware apprennent à conduire des opérations IT à l'échelle de l'entreprise. »

Et leur action ne s'arrête pas aux ransomwares. Elle englobe n'importe quel type de malware ou d'attaque. Besoin d'informations personnelles sur des cibles de grande valeur ? Un botnet pour une attaque DDoS ? Vous avez déjà eu envie que quelqu'un d'autre installe des logiciels malveillants sur un groupe de machines puis vous confie les clés pour que vous puissiez vous occuper de l'extorsion ? Pour cela, il y a le dark web, et le service client ne cesse de s'améliorer.

Robert Pizzari, Vice-président de la sécurité de Splunk dans la région APAC, avertit : « Ces groupes vous vendront des outils avec un retour sur investissement exceptionnel. Et si vous rencontrez des problèmes pour déployer le malware, si des erreurs apparaissent parce que vous avez affaire à un système d'exploitation différent, par exemple, le niveau de service et d'assistance est exceptionnel, d'après les obscurs forums que j'ai parcourus. »

M. Baccio déclare : « Ils ont des programmes de primes aux bugs. Et ils sont souvent bien plus rentables que ceux que bien des entreprises légitimes se sont donné le mal d'établir. »

Le résultat : une triste dilution de l'ancienne élite des pirates informatiques, car à peu près n'importe quel amateur à la morale défaillante peut acheter des outils permettant, par exemple, d'empêcher un hôpital d'accéder à son réseau ou de faire chanter une entreprise du CAC 40 aux contrôles de sécurité laxistes. Avant, il fallait du talent pour être un super méchant.

Et parce que la cybercriminalité devient le fast-food du dark web, le nombre de malfaiteurs va augmenter autant que celui des organisations ciblées.

« Et même si l'automatisation renforce la sécurité, les malfaiteurs savent aussi s'en servir, » avertit Lily Lee. En tant que Responsable senior des solutions de sécurité, elle aide les clients à surmonter les complexités de la sécurisation des environnements hybrides et multicloud. « Non seulement un malfaiteur peu qualifié peut acheter ces outils, mais il peut lancer grâce à eux une attaque de bien plus grande envergure. »

Une raison de plus de faire entrer l'automatisation dans votre SOC, ajoute-t-elle. « C'est la seule façon d'améliorer nos chances face à leur automatisation. »

Ryan Kovar affirme que deux choses restent vraies face à cette explosion de la cybercriminalité industrialisée. Premièrement, les anciennes défenses sont toujours les meilleures. « Beaucoup de techniques qui étaient très distinctes les unes des autres tendent à converger et à se recouper, donc si vous faites bien votre travail, vous allez vous défendre contre 85 % des assauts que vous pourriez subir. Vous devez toujours vous défendre contre les intrusions, les mouvements latéraux, l'exécution de code malveillant sur vos systèmes, et l'exfiltration d'informations. »

La seconde vérité ? « Les gens dans notre métier auront toujours un emploi. »

Prévision

L'usage des cryptomonnaies va reculer dans le paiement des rançons.

Un article d'Axios sur les ransomwares remarquait que le marché des cryptomonnaies avait perdu 1 000 milliards de dollars en valeur entre novembre 2021 et août 2022, et s'interrogeait sur un impact éventuel de la plongée du Bitcoin sur les ransomwares. Si les sources de l'auteur lui ont assuré que les ransomwares ne faibliraient pas, Mick Baccio et Ryan Kovar pensent que les prises d'otage de données et les extorsions vont effectivement abandonner la monnaie numérique.

« Les groupes de ransomwares vont prendre leurs distances par rapport aux cryptomonnaies, pas tant à cause de leur volatilité, même si cela reste un facteur, qu'à cause de sa traçabilité, » déclare M. Kovar.

M. Baccio ajoute : « Les cryptomonnaies ne sont pas aussi anonymes que les gens le pensaient. Elles sont même très traçables. »

Tout ce qui se passe sur la blockchain est visible ; tout est public. Le portefeuille sur lequel les criminels reçoivent leurs cryptomonnaies ne porte pas leur nom, et ils peuvent essayer de brouiller les pistes en répartissant les fonds entre 100 portefeuilles et en panachant les devises avec des outils comme Tornado Cash, mais au final, tout est traçable. Dès que vous essayez d'encaisser la somme, la transaction a besoin d'un nom, et c'est là que les criminels se font prendre.

M. Kovar confie : « Eh oui, en fin de compte, les cryptomonnaies ne sont pas vraiment anonymes, mais si vous vivez dans un pays qui soutient, parraine ou tolère simplement la cybercriminalité, vous ne serez probablement pas poursuivi, à moins de vraiment contrarier les gens. »

Les plus grands criminels, ajoute-t-il, ne voudront pas leur milliard en Bitcoin. « Ils vous diront : "Nous avons volé vos données, mais personne n'a besoin de le savoir, n'est-ce pas ? Allez simplement voir notre contact en Suisse, vous irez ensemble à la banque et vous réglerez ça de façon civilisée". »

Prévision

Les techniques de la cyberguerre viendront s'ajouter à la cybercriminalité commerciale. Bientôt. Et les infrastructures critiques seront utilisées comme des armes pour perturber le discours politique.

Les cyber-équipes des États-nations sont les laboratoires de R&D de la communauté des cybercriminels dans son ensemble. Au moment où nous rédigeons ce rapport, la guerre de la Russie contre l'Ukraine en est à son neuvième mois, et des cyberattaques compromettent des centres financiers et des installations énergétiques tout en répandant de la désinformation, comme ce deepfake vidéo du président ukrainien Volodymyr Zelensky ordonnant à ses compatriotes de se rendre. Tout cela arrivera bientôt bien plus près de chez vous, et ça ne sera pas nécessairement le fait d'un gouvernement belliqueux.

Patrick Coughlin déclare : « Nous avons vu en Ukraine qu'il est possible de perturber l'infrastructure énergétique et financière au niveau national, et ces techniques seront adoptées par des acteurs menaçants plus commerciaux contre des cibles plus distantes et diversifiées, avec des objectifs beaucoup plus business. »

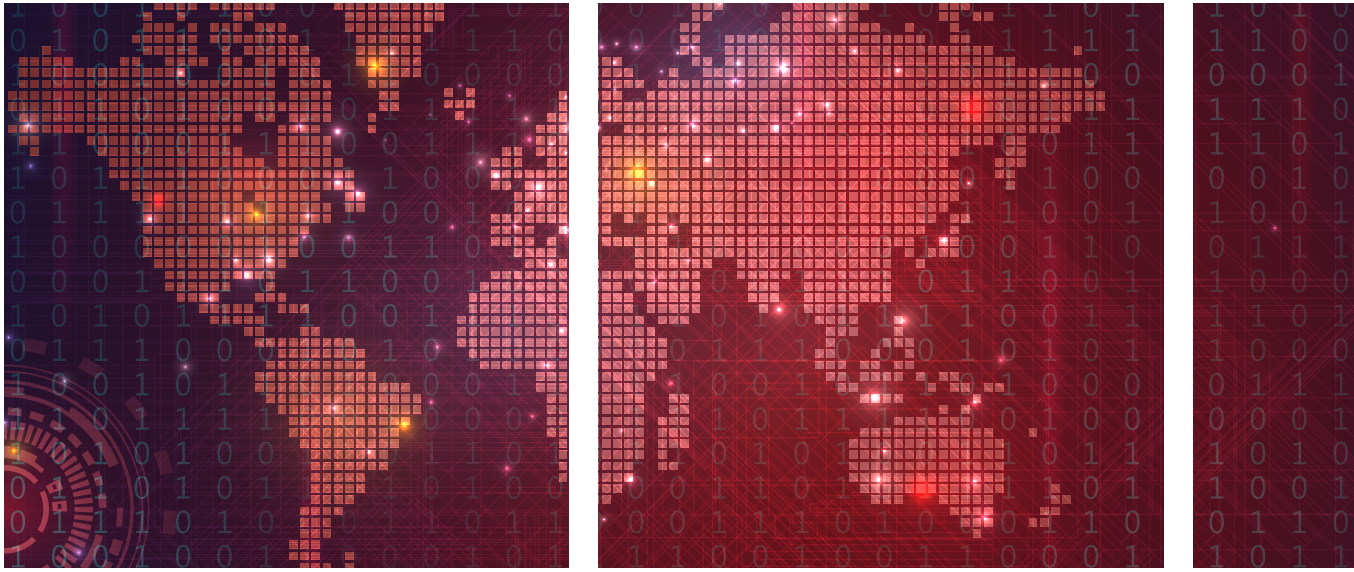
Et étant donné la détermination d'une industrie de la cybercriminalité hautement organisée, il est pratiquement certain que ces techniques de guerre seront bientôt mises au service d'une cupidité apolitique.

M. Coughlin déclare : « Les malfaiteurs recherchent également des débouchés commerciales. Ces évolutions sont inévitables, de la même façon que les entreprises légitimes découvrent comment adapter des drones militaires à des applications et des services de drones commerciaux. »

Ryan Kovar est tout à fait d'accord, mais il va encore plus loin : attendez-vous également à ce que les acteurs des États-nations doublent la mise.

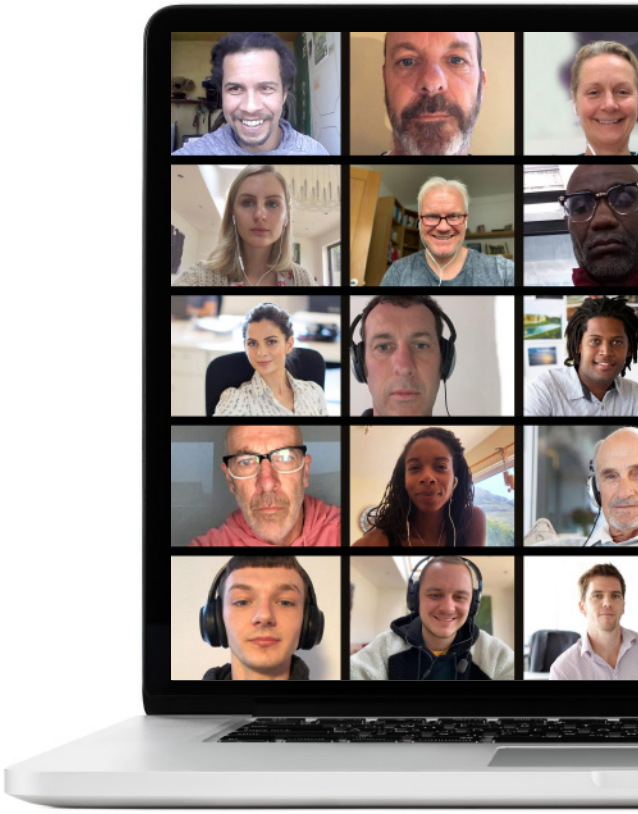
M. Kovar, qui dirige l'équipe de recherche stratégique sur la cybersécurité de Splunk, SURGe, ajoute : « La technologie opérationnelle sera militarisée au cours de l'année à venir, et elle ne ciblera pas seulement la compromission d'infrastructures critiques. L'infrastructure sera utilisée comme une méthode pour changer le discours politique. »

Et comme le souligne M. Kovar, une infrastructure convertie en arme n'a pas à appartenir à un état. De nombreux fournisseurs et autres infrastructures sont privés. « Et de nos jours, de nombreuses technologies, dont les services cloud, sont des infrastructures stratégiques non officielles. »



Prévision

Les attaques de désinformation en entreprise vont devenir un problème vraiment grave.



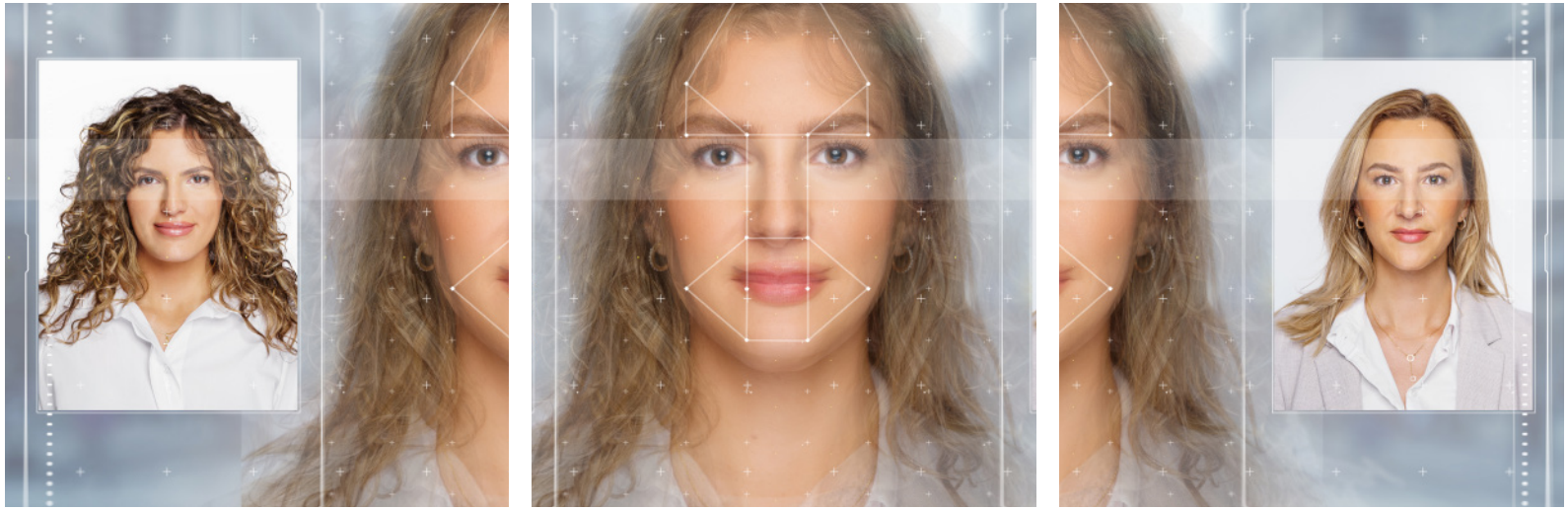
Quand nous commencions à planifier les rapports de prévisions de cette année, l'une de nos collègues a reçu un SMS de notre PDG. Manifestement, le grand chef assistait à un webinaire (c'est ainsi que les PDG passent la majeure partie de leur temps) et avait besoin qu'elle coure chercher des cartes-cadeaux pour faire plaisir à un client (et non, ça ne ressemblait pas du tout à l'exemple du chapitre « pot-de-vin » de notre formation annuelle sur la conformité). Ce message a rapidement été reconnu pour ce qu'il était : une attaque de bas niveau, dont la seule sophistication avait été de rapprocher le numéro de téléphone de notre collègue de son employeur.

Dès le lendemain, deux articles de presse sont apparus sur nos flux : des escrocs avaient créé un « hologramme en IA » sophistiqué d'un cadre supérieur d'une société de cryptographie pour l'utiliser lors d'une réunion avec ses clients, probablement un peu comme l'acteur qui a utilisé la technologie deepfake pour se faire passer pour Tom Cruise (tout en l'admettant dès le départ). Le cadre ciblé n'a pas immédiatement fourni la preuve du deepfake, mais il a déclaré que les dirigeants de quatre entreprises avaient affirmé avoir eu des réunions avec lui, alors qu'il n'y avait jamais assisté.

Nous l'avions vu venir dans nos prévisions de sécurité pour 2020, et c'est aujourd'hui une réalité : une désinformation industrielle, qui s'appuie sur les atouts d'une haute technologie. Les deepfakes vocaux et vidéo vont remplacer (ou soutenir) les SMS et les e-mails maladroits, et les campagnes sur les réseaux sociaux vont saper les organisations légitimes. Comme le deepfake de Volodymyr Zelensky, qui a été diffusé sur Facebook, Telegram et d'autres réseaux sociaux.

Patrick Coughlin prévient : « C'est l'année où nous devrons lutter contre la désinformation à l'échelle industrielle. Nous devons nous attaquer à de nouvelles formes de risque numérique : prises de contrôle de comptes de réseaux sociaux des entreprises, deepfakes de PDG, manipulation du marché des meme stocks et autres activités susceptibles de semer la confusion sur les marchés publics et privés. Nous n'avons même pas effleuré la surface des menaces que nous verrons émerger dans la décennie à venir. »

Alors accrochez-vous. Et dites à vos PDG d'acheter leurs propres cartes-cadeaux.



Prévision

Nous allons voir de nouvelles attaques de la chaîne d'approvisionnement, dont la vulnérabilité principale est le manque de financement et de ressources de l'open source. Les SBOM vont devenir incontournables comme outils de remédiation.

Quand nous nous interrogeons sur l'avenir des attaques de la chaîne logistique, la question n'est pas de savoir si elles vont se poursuivre. SolarWinds, Log4Shell, Kaseya… les assauts vont s'enchaîner, et tout le monde le sait. Dans notre rapport État de la cybersécurité en 2022, 97 % des participants disent avoir augmenté leurs dépenses dans le domaine. En réalité, notre prévision concerne plutôt la réponse que nous allons y apporter : les organisations vont se convertir au SBOM.

Le concept de nomenclature logicielle (SBOM) est simple : une liste des composants d'un package logiciel, incluant les fragments obscurs de code open source dispersés dans un produit commercial donné. Quand un composant devient le vecteur d'une nouvelle attaque, les équipes informatiques et de sécurité peuvent savoir rapidement si l'élément compromis se trouve dans l'un des produits qu'ils utilisent ou vendent.

Lily Lee affirme : « C'est logique. Si vous ne savez pas ce que vous avez, comment savez-vous face à quoi vous êtes vulnérable ? Cela fait autant partie du travail que de connaître vos utilisateurs et vos actifs. »

Ryan Kovar, gourou des menaces au sein de l'équipe SURGe, a écrit sur les SBOM l'été dernier sur Forbes.com. Selon lui, c'est une idée intelligente qui deviendra très rapidement un

standard de l'industrie : « D'ici 2025, vous ne pourrez plus vendre de logiciels au gouvernement fédéral américain sans SBOM. Et une fois que ce sera une norme gouvernementale, le secteur privé l'adoptera rapidement. »

Et encore, il faudra patienter jusqu'en 2025, ajoute M. Kovar. « Deux Noëls de suite, nous avons connu des cyberincidents majeurs qui étaient des attaques de la chaîne d'approvisionnement. Ces attaques vont continuer, et je suis convaincu que la victime du prochain grand coup sera un autre produit open source fondamental. Le monde fonctionne avec l'open source. C'est du très bon matériel, mais le support n'est pas toujours à la hauteur. En effet, les entreprises qui utilisent des composants open source ne contribuent pas toutes au développement et à la maintenance de ces produits. Vous avez donc des outils logiciels majeurs qui fonctionnent en partie sur du code vieux de 15 ans, maintenu par un codeur solitaire en Finlande. »

Quelle que soit la prochaine vulnérabilité de la chaîne d'approvisionnement, tous ceux qui ne disposent pas d'une liste complète des composants logiciels présents dans leur infrastructure ou leur gamme de produits le regretteront certainement.

Prévision

Le prochain grand vecteur de cyberbraquage est la blockchain.

La blockchain a déjà été piratée. L'été dernier, un piratage massif du jeton cryptographique Solana a fait la une des journaux ; il aurait coûté à des milliers d'utilisateurs un total de 4,5 millions de dollars. Au cours du même mois, un reportage de CNBC estimait le montant des vols de cryptomonnaie au premier semestre 2022 à 1,9 milliard de dollars. Mais attendez, la blockchain est impossible à pirater, n'est-ce pas ?

Aucune technologie parfaite n'est inviolable lorsqu'elle est administrée par des humains inévitablement imparfaits. Le piratage de Solana a été attribué à des contrôles de sécurité d'une négligence embarrassante, et non à une faille logicielle profondément enfouie. Pour faire une analogie, c'est comme si des cambrioleurs étaient entrés dans votre maison parce que la clé était sur la porte. L'attaque Nomad aurait exploité une mise à jour défectueuse d'un contrat intelligent. Celle-ci avait compromis un pont blockchain, un dispositif qui permet de réaliser des transferts d'une chaîne de cryptomonnaie à une autre.

Patrick Coughlin, cofondateur et ancien directeur technique de la start-up de threat intelligence TruStar, déclare : « Je pense que les impacts financiers les plus importants en termes de violations du cyberespace toucheront l'espace de la blockchain. Tous ces piratages qui font la une des journaux ne sont que le début. »

Tom Martin, Ingénieur principal des solutions pour la technologie de la blockchain chez Splunk, rappelle : « L'intérêt de la blockchain est d'être décentralisée et traçable. Cela ne signifie pas qu'elle est à l'abri des erreurs de codage. En fait, lorsque vous étudiez ces incidents, les transactions qui ont eu lieu étaient légitimes du point de vue du système en fonction des paramètres qui avaient été programmés. Le système a fonctionné exactement comme prévu et, heureusement pour la suite, il a gardé un enregistrement parfait de tout ce qui s'est passé. »

M. Coughlin confie : « Même avec le crash des cryptomonnaies l'année dernière, beaucoup d'argent circule toujours dans ces réseaux de blockchain. Mais à bien des égards, c'est encore le Far West. Ces incidents nous invitent à réfléchir à ce qui distingue la blockchain en termes de résilience. Comment s'inscrit-elle dans la définition de la cyber-résilience ? Comment pouvons-nous appliquer les enseignements que nous avons acquis ces 20 dernières années sur les personnes, les processus et les technologies pour défendre ces réseaux numériques ? C'est un défi passionnant : nous rencontrerons les difficultés et les embûches des pionniers. Nous devrons apprendre des erreurs du passé et ouvrir de nouvelles voies. »

Quant aux méchants de l'histoire, ils ne manqueront pas de s'enrichir tant que l'industrie n'aura pas rempli sa mission.

Prévision

Le machine learning contribue à sécuriser vos systèmes. Mais il va également devenir un nouveau vecteur d'attaque.

L'automatisation apporte de la vitesse et de l'efficacité à la sécurité. Le machine learning rend l'automatisation plus intelligente. Mais comme le Machine Learning imprègne une grande partie de votre environnement, il devient également un vecteur d'attaque.

Subho Majumdar, Chercheur principal en sciences appliquées et membre de l'équipe d'analyse et d'apprentissage des experts de sécurité (SEAL) de Splunk, avertit : « Quand les pipelines ML font partie des systèmes logiciels que vous protégez contre les attaques, vous devez vous préparer à ce que le modèle ML soit attaqué. Par exemple, les malfaiteurs peuvent essayer d'exfiltrer les données de ces modèles ML ou de détourner leurs résultats en injectant des entrées malveillantes. »

M. Majumdar a récemment coécrit un livre sur le ML digne de confiance (Practicing Trustworthy Machine Learning, chez O'Reilly). Selon lui, la transparence est essentielle pour rendre les modèles à la fois éthiques et dignes de confiance. Les modèles de machine learning sont souvent présentés comme des boîtes noires mystérieuses dont le fonctionnement dépasse l'entendement humain. La transparence, la capacité à comprendre ce qui se passe et comment le modèle produit ses résultats, sont indispensables.

« Et la sécurité du ML va revêtir une importance croissante, parce que les modèles vont être mis au service du public à grande échelle, » ajoute-t-il.

Quelle réponse devez-vous y apporter ? Tout d'abord, vous évaluez le niveau de risque. Si le modèle tourne mal, votre service de streaming va-t-il faire des recommandations cocasses de films ou votre banque va-t-elle être poursuivie pour discrimination au crédit involontaire ? Est-ce que cela va dégrader l'efficacité du back-end pendant quelques jours, ou faire fermer toute votre entreprise ?

Ensuite, vous travaillez avec celui qui a construit et entraîné le modèle, qu'il soit interne ou commercial. Insistez sur cette transparence qui renforce la confiance sur laquelle M. Majumdar insiste tant.

Ensuite, vous gardez un œil humain sur vos modèles. Lily Lee explique : « Vous devez valider vos données de référence. Ces idées ont toujours existé : données de référence, empoisonnement des données, manipulation du système. Aujourd'hui, la difficulté réside en partie dans le fait que le ML a l'avantage d'être souvent non supervisé, et donc de pouvoir être laissé sans surveillance, mais c'est aussi ce qui fait sa vulnérabilité. Vous devez prendre le pouls de vos modèles et avoir une idée précise de ce que doit être le succès.

Résumons : données de base, tests, affinage. Toujours.

Prévision

Les entreprises comprennent les exigences des consommateurs en matière de confidentialité et certaines agiront avant la réglementation gouvernementale. Et poursuivront quelqu'un en justice.

La vie privée est un peu le changement climatique de l'industrie technologique : la plupart des gens s'en inquiètent, beaucoup d'entreprises disent le comprendre, mais les gouvernements ne font rien ou pas assez à ce sujet. Au cours des deux prochaines années, les administrations continueront d'hésiter, mais le secteur privé, poussé par les consommateurs, commencera à agir.

« Les citoyens vont obliger les entreprises à prendre davantage de mesures pour le respect de la vie privée et à mieux connaître les données dont elles disposent sur Internet, » déclare Mick Baccio. Cela vaut autant pour la façon dont vos données sont vendues à des fins de profilage marketing invasif, pour mieux vous vendre des choses inutiles ou vous inciter à cliquer sur vos flux de réseaux sociaux, que pour ce que les gouvernements pourraient faire de vos informations.

L'arrêt Dobbs de la Cour suprême américaine, qui a supprimé la protection constitutionnelle de l'avortement, a galvanisé les inquiétudes aux États-Unis. En effet, il est rapidement apparu que les données des applications de suivi menstruel et les données de localisation des téléphones portables pourraient être vendues aux forces de l'ordre (sans mandat) pour qu'elles sachent qui a visité quel genre de cliniques, et pourquoi.

Ryan Kovar observe : « Auparavant, il était assez facile d'écarter les inquiétudes sur la protection de la vie privée en disant : "Si vous n'avez rien à cacher, il n'y a pas lieu de s'inquiéter". Cette parade ne tient plus quand les tribunaux interdisent des choses que la population considérait comme un droit solidement établi. »

Et il ne s'agit pas seulement des développements récents et déstabilisants comme la décision Dobbs ou de la puissance terrifiante (et les failles considérables) des logiciels de reconnaissance faciale, ajoute M. Baccio. Pour lui, l'anecdote la plus probante vient de Signal, une application populaire de messagerie chiffrée.

M. Baccio déclare : « J'ai vu un nombre ridicule de personnes se convertir à Signal au cours de la dernière année. Pendant cinq ans, il n'y avait eu que moi, Ryan, et une bande de vétérans. Des gens qui ont vécu toute leur vie en ligne sans jamais penser à la vie privée se disent : "Finalement, je veux m'assurer que ce que je dis n'est pas enregistré par Facebook", et c'est un changement radical d'état d'esprit par rapport à la situation d'il y a 10 ans. »

M. Baccio dit : « Je pense que cela nous ramène à la question plus large de savoir quand publier ses données sur Internet, où elles vont et qui a quels droits dessus. Il n'y a pas d'équivalent américain au RGPD, pas de norme mondiale de confidentialité, et la législation en vigueur au Congrès en ce moment pourrait finir par être assez édulcorée. »

C'est donc à l'entreprise privée d'arrêter de monétiser chacun de nos clics pour protéger ce qui reste de notre confidentialité numérique.

Patrick Coughlin déclare : « Nous commençons à voir la confidentialité dans l'entreprise devenir une priorité : les entreprises s'affirment et établissent des politiques de confidentialité des données avec leurs partenaires et fournisseurs ; au final, elles protègent bien mieux la confidentialité de leurs clients. Je ne pense pas que les régimes supranationaux de confidentialité seront la réponse qu'ils promettent. Je démarrais une entreprise lorsque le RGPD est entré en vigueur, et je me souviens à quel point les entreprises et les investisseurs étaient terrifiés par les amendes astronomiques annoncées. Les régimes réglementaires ne sont pas autant une force motrice que le sentiment des consommateurs vis-à-vis de la confidentialité. »

Si les gouvernements ne sont pas là pour punir les violations de la vie privée, qui va brandir le bâton quand la carotte des consommateurs satisfaits ne suffira pas ? Pour M. Coughlin, des entreprises vont poursuivre d'autres entreprises en justice.

Il affirme : « Dans les trois à cinq prochaines années, nous verrons une forme ou une autre de recours collectif. Des entreprises vont s'unir pour poursuivre, par exemple, un fournisseur de logiciels pour violation des clauses de confidentialité. »

On pense souvent, dit-il, que la technologie évolue trop rapidement et fait preuve de négligence sur les questions de confidentialité, et que les gouvernements avancent beaucoup trop lentement. Il incombera aux entreprises axées sur le client de veiller au respect de la vie privée, pour le bien de leurs clients et de leur propre image.

Prévision

Deux solutions à la crise des talents : automatisation et diversité des parcours via une focalisation sur le talent (plutôt que sur les compétences techniques). Les deux arrivent à grands pas.

Une première solution à la crise des talents est l'automatisation, qui doit compenser la pénurie de talents humains. Si l'automatisation est là, la pénurie de talents, elle, n'a pas disparu. L'automatisation va prendre de l'ampleur, et tout outil capable d'aider les analystes à travailler plus intelligemment et plus rapidement, ou même de gérer les problèmes de base sans intervention humaine, améliorera la situation. Mais l'automatisation ne sera jamais une réponse suffisante à la crise des talents.

Mick Baccio déclare : « Nous allons encore avoir besoin de personnel. Et nous allons devoir arrêter de chercher les profils habituels dans les endroits habituels. »

Pour M. Baccio, la clé consiste à mobiliser une gamme plus diversifiée de talents. On parle de diversité du point de vue du genre et de l'ethnicité, mais aussi de diversité en termes de parcours.

Patrick Coughlin ajoute : « Chaque année, toute l'industrie se plaint parce que nous avons trop de postes vacants. Nous nous arrachons les cheveux, mais rien ne change. Nous devons nous demander s'il y a réellement un manque de compétences en cybersécurité, ou si c'est nous qui ne vendons pas bien la mission. La mission elle-même est séduisante : vous allez occuper une fonction critique dans la pile de sécurité de chaque organisation que vous approcherez au cours de votre vie professionnelle. Une telle mission devrait être un avantage concurrentiel pour attirer les talents. »

Petra Jenner, Vice-présidente senior et Directrice générale de Splunk pour l'EMEA, renchérit : « C'est tout à fait vrai. Les jeunes travailleurs, notamment, veulent rejoindre des organisations qui affichent un objectif et une vision clairs, et cela a un impact

réel sur la compétition pour les talents dans les domaines de la technologie et de la sécurité. »

M. Coughlin ajoute : « Mais quand il s'agit de sécurité, nous avons tendance à rejeter l'essentiel des profils en nous considérant comme les grands prêtres de la complexité, tout simplement parce que nous avons travaillé dans des environnements classés secret défense ou dans des agences à trois lettres. C'est ridicule. »

Lily Lee confie : « Nous nous entêtons à trouver des personnes qui connaissent une technologie spécifique, et c'est là qu'est vraiment l'écueil. Nous disons : "J'ai besoin de quelqu'un qui connaît cet outil spécial pour les terminaux." Et si je vous présente quelqu'un qui comprend l'idée de la sécurité des terminaux et qui peut apprendre l'outil ? Si vous avez des connaissances fondamentales, vous pouvez être efficace n'importe où. »

Ryan Kovar, qui dirige l'équipe de chercheurs en sécurité SURGe de Splunk, le confirme. Il sélectionne les candidats pour leur curiosité et leurs compétences en résolution de problèmes bien plus que pour leur expérience de codage ou leur connaissance des outils ou de plateformes spécifiques.

Il affirme : « Je peux vous apprendre à utiliser un SIEM. Je ne peux pas vous apprendre à être motivé ou à aimer résoudre les mystères. J'ai donc eu au moins autant de bonnes surprises en embauchant des personnes ayant une formation de journaliste ou de marketing qu'en recrutant des codeurs. »

Lily Lee ajoute : « Si vous êtes sans cesse à la recherche de personnes capables de sortir des sentiers battus, il suffit parfois de sortir des sentiers battus pour les trouver. »

M. Coughlin déclare : « Si nous élargissons le champ des recherches, il ne devrait pas être difficile d'attirer des personnes exceptionnelles. La mission de sécurité est séduisante, et c'est un avantage concurrentiel pour acquérir des talents. »

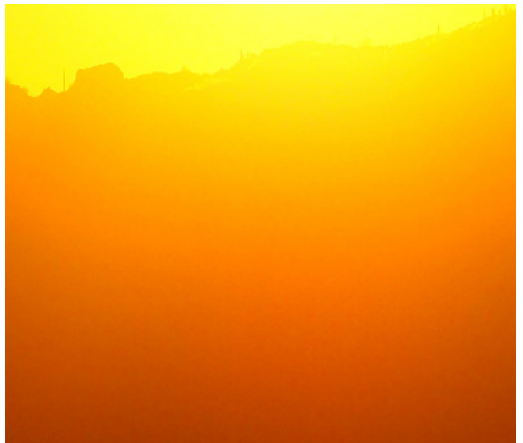
Robert Pizzari affirme qu'il observe les mêmes défis et solutions dans la région Asie-Pacifique : « On commence à rechercher des profils qui sont curieux de nature et qui ont un désir inné de comprendre le comportement humain. L'idée de mobiliser des personnes d'horizons divers fait son chemin et les organisations expérimentent avec cette approche. »

Et ça marche. Malgré l'éternelle pénurie de talents, M. Kovar raconte qu'un récent effort de recrutement pour un poste en début de carrière, visant à attirer un bassin de candidats plus diversifié, a presque trop réussi. « Les RH ont dû nous arrêter plus tôt parce que nous avions pratiquement fait planter le système. »

M. Baccio affirme : « Je suis vraiment optimiste quant à la nouvelle génération de cybertalents. Nous voyons des gens vraiment passionnés avec une diversité d'expériences et d'horizons, et je suis impatient de voir ce que sera l'avenir de la cybersécurité. »

Bienvenue dans l’âge d’or

C’était dense, non ? Comme l’a dit Ryan Kovar, s’il y a une chose sur laquelle les professionnels de la sécurité peuvent compter, c’est qu’ils seront toujours indispensables. Et il est également vrai que la vigilance de base en matière de sécurité, que ce soit en installant les correctifs sans attendre ou en formant les employés pour qu’ils n’achètent pas de cartes-cadeaux pour des PDG obsédés par les webinaires, arrête la plupart des menaces.



Mais il faut tout de même reconnaître qu'il n'y a pas de panacée aux nombreux maux de notre écosystème numérique. Quand l'agence fédérale américaine CISA débarque avec son programme exhaustif « Shields Up », vous êtes en droit de vous demander ce qu'ils pensent que nous faisons le reste du temps. Mick Baccio déclare : « Shields Up n'est pas un plan de cyberdéfense. C'est une feuille de route vers le burn-out. »

Le cadre Zero Trust fait l'objet d'une adoption de plus en plus large, et c'est très encourageant, mais les organisations doivent garder en tête que la partie « zéro » est ambitieuse.

M. Baccio dit : « Pour mettre en place un véritable modèle Zero Trust, il faut démolir la maison pour en construire une autre. Et qui peut faire ça ? »

M. Kovar note : « Google l'a fait. Mais si vous n'avez pas les moyens de Google, c'est plus difficile. Le Zero Trust est le Six Sigma de la défense du réseau : si vous avez un bon réseau Zero Trust, vous êtes nettement mieux loti qu'une organisation sans Zero Trust. Mais en matière de Zero Trust, la perfection est hors de portée. »

Malgré cela, l'optimisme est au rendez-vous. À un degré surprenant. Selon M. Kovar, si les menaces ne cessent de s'aggraver, les outils de sécurité et la discipline même de la cybersécurité sont en revanche bien meilleurs qu'ils ne l'étaient il y a vingt, dix, voire cinq ans. Lily Lee confirme.

005 2010 2015 2020 2025

Elle déclare : « L'univers de la cybersécurité a toujours des relents de fin du monde, parce que l'industrie est fondée sur la peur, mais je suis très prudemment optimiste. Chaque processus de cyberincident se termine par une session sur les enseignements qu'on peut en tirer. Nous apprenons de nos erreurs, nous comblons nos lacunes, nous nous améliorons. »

La sécurité repose sur la constance et la régularité des victoires, dit-elle. « Ces victoires sont éclipsées par les gros titres catastrophiques, mais notre industrie est là où elle en est aujourd'hui parce que ces victoires ont contribué à la façonner. »

Patrick Coughlin nous confie : « Nous le voyons déjà : les technologies essentielles à la protection de la cyber-résilience convergent, et la structure organisationnelle se décloisonne. Les données convergent depuis une décennie. Mais ce qui est formidable, c'est que nous entrons selon moi dans un âge d'or, un véritable tournant dans notre façon de penser les talents et les ressources en sécurité. »

Et nous conclurons sur cette prévision.

Contributeurs

Mick Baccio
Mick Baccio, Stratège en sécurité mondiale, a rejoint l'équipe SURGe après avoir occupé des rôles dans la cybersécurité et la threat intelligence dans diverses agences fédérales à acronyme. Il a été le tout premier RSSI d'une campagne présidentielle américaine. Il aime la chasse aux menaces, les Air Jordan et les « cyber-légumes » sans ordre de préférence.

Patrick Coughlin
Patrick, Vice-président de la stratégie et de la spécialisation GTM de Splunk, a une solide expérience en sécurité. Il a été cofondateur et PDG de TruSTAR, une plateforme de gestion de cyber-intelligence acquise par Splunk. Auparavant, il a dirigé des équipes d'analystes en cybersécurité et contre-terrorisme pour le gouvernement américain et des clients du secteur privé.

Simon Davies
En tant que SVP et Directeur général en APAC, Simon est responsable du portefeuille complet de solutions Splunk sur les marchés de l'Asie-Pacifique et du Japon. C'est un ancien de Microsoft, de Salesforce, d'Oracle et de Citibank.

Dhiraj Goklani
Dhiraj est le Vice-président de l'observabilité de Splunk en APAC, où il applique plus de deux décennies d'expérience dans l'industrie technologique pour développer le marché de l'observabilité dans la région.

Petra Jenner
Petra est Vice-présidente senior et Directrice générale pour la région EMEA chez Splunk. Auparavant, elle a occupé des postes de direction chez Salesforce, Microsoft, Checkpoint et Pivotal. Elle est titulaire d'un master de commerce et d'IT, et a étudié le management international à la Stanford Graduate School of Business à Singapour.

Ryan Kovar
Ryan Kovar, Stratège en sécurité, dirige SURGe, le groupe de recherche en sécurité « blue team » de Splunk. Il a fait une carrière dans la recherche de sécurité et l'ingénierie, notamment comme ingénieur principal en sécurité pour la DARPA. Mais il n'a pas le droit de nous en parler.

Lily Lee
Lily est Responsable senior de la stratégie des solutions de sécurité chez Splunk. Elle dirige une équipe mondiale d'experts de l'industrie et des produits qui appuient les activités de sécurité de Splunk et jouent le rôle de leaders d'opinion et de conseillers de confiance pour les clients, les partenaires et la communauté de sécurité.

Robert Pizzari
Robert est le Vice-président de la sécurité de Splunk dans la région APAC. Auparavant, il a occupé des postes de direction chez Check Point, FireEye, Trustwave et Cisco.

Subho Majumdar
Subho est Chercheur principal en ML appliqué au sein du groupe de science des menaces de Splunk. Auparavant, il a travaillé au sein de l'équipe de recherche en science des données et IA d'AT&T. Cofondateur de plusieurs efforts communautaires en ML, Subho a récemment coécrit Practicing Trustworthy Machine Learning.

Gary Steele
Gary est PDG de Splunk, et membre de notre conseil d'administration. Avant de rejoindre Splunk en 2022, Gary a été le PDG fondateur de Proofpoint, où il a dirigé la croissance de cette jeune start-up pour en faire un leader de sécurité en tant que service, coté en bourse.

Tom Martin
En tant qu'Ingénieur principal des solutions au sein de l'équipe blockchain de Splunk, Tom est un ambassadeur des nouvelles technologies et assure un rôle d'agent de liaison entre les clients et la gestion des produits dans les domaines des technologies blockchain et Web3. Auparavant, il a travaillé chez Silverstream, VMware, Pivotal Software, Wily Technology et New Relic.

Mark Woods
Conseiller technique en chef de Splunk dans la région EMEA, Mark a été ingénieur, consultant, entrepreneur et directeur technique. Il aide les équipes de direction et les décideurs internationaux à comprendre le potentiel considérable des approches basées sur les données.

Pour connaître d'autres prévisions pour 2023, consultez les rapports sur l'IT/l'observabilité ainsi que les tendances du leadership et les technologies émergentes.

En savoir plus

22-25648-Splunk-Data Sec Predictions 2023-EB-106-AW