Hewlett Packard Enterprise

Rapport annuel 2023 sur la cybersécurité

Chez HPE, nous pensons que notre réussite individuelle et collective repose sur notre capacité à partager nos connaissances, nos idées et nos opportunités. Lorsqu'il s'agit de sécuriser nos organisations respectives, nous sommes tous confrontés aux mêmes défis : une pénurie mondiale de compétences en cybersécurité, une surface d'attaque en expansion, des données distribuées et une demande croissante de transparence de la part des parties prenantes. Et pour assurer la protection de la périphérie au cloud, comment décider qui fait quoi ? Nous pensons que la cybersécurité est devenue une responsabilité partagée, car un seul maillon faible peut avoir un impact sur chacun d'entre nous. Ce rapport présente une partie du travail que nous avons accompli sur ce front en 2022 et quelques prévisions pour 2023. Nous avons le plaisir de le partager avec vous, nos clients, nos partenaires et nos pairs.

Sommaire

2022 en chiffres

2,6 Mds

Notre SIEM d'entreprise a enregistré plus de 2,6 milliards d'événements par jour, ce qui a permis à notre Cyber Fusion Center de les trier, de les examiner et de les résoudre.

2 200

La plateforme Edge to Cloud HPE GreenLake applique en permanence plus de 2 200 contrôles de sécurité distincts pour protéger les clients et leurs données en temps réel.

1 900

Nous avons amélioré la visibilité de notre parc de serveurs cloud, en surveillant en permanence plus de 1 900 contrôles de sécurité.

1 060

Nous avons bloqué en moyenne 1 060 courriers électroniques d'hameçonnage reçus chez HPE chaque jour. Au total, nous avons bloqué environ 1 milliard de vecteurs de menaces par courrier électronique.

334

L'équipe de réponse à la sécurité des produits de HPE a publié 187 bulletins de sécurité, couvrant 334 CVE (Common Vulnerability & Exposure / failles et vulnérabilités communes) sur 450 produits, dont 46 CVE émis par HPE. Tous les CVE ayant un impact ont été corrigés conformément aux politiques de sécurité de HPE, et des correctifs ont été mis à disposition afin de garantir un impact minimal sur la sécurité et la disponibilité des environnements des clients.

58

HPE détient des certificats globaux ISO 27001 sur 58 sites dans 36 pays, ajoutant 11 sites en 2022 avec l'approbation de 16 sites supplémentaires en attente en 2023. Notre programme de conformité s'est élargi pour inclure l'attestation SOC 1 et SOC 2 pour un certain nombre de nos centres d'assistance à la clientèle, ainsi que FedRAMP pour Aruba Central et les évaluations CSA STAR pour nos plateformes de gestion cloud.

33

HPE a entrepris 33 chasses aux menaces dans le but de découvrir des acteurs de menaces persistantes avancées au sein du réseau. Les résultats de ces chasses aux menaces ont été utilisés pour améliorer nos ensembles de règles de surveillance.

98 %

Plus de 55 000 employés de HPE, soit 98 %, ont suivi la formation annuelle de sensibilisation à la cybersécurité.

+50 %

Conformément aux tendances du secteur, plus de la moitié des incidents de cybersécurité examinés par le Cyber Fusion Center de HPE peuvent être attribués à des actions d'utilisateurs telles que la tentative d'installation de logiciels infectés, la désactivation d'outils de sécurité ou l'exécution de logiciels de cryptominage, qui ont été bloquées par nos contrôles de sécurité.

Antonio Neri
Président-directeur général
HPE

La sécurité est notre priorité

Chez Hewlett Packard Enterprise, nous aidons nos clients à utiliser la technologie pour transformer leurs idées en valeur. Ces idées ont besoin d'un endroit sûr pour être cultivées. Nous avons donc mis l'accent sur la protection de ces idées et des systèmes où elles sont développées.

Aujourd'hui, nous gérons plus de deux millions d'appareils et plus d'un exaoctet de données via la plateforme HPE GreenLake. C'est une responsabilité que nous prenons au sérieux. Au cours de l'année écoulée, nous avons renforcé notre position dans toutes les catégories de sécurité et avons assidûment investi dans la recherche, les contrôles et le développement des talents en matière de cybersécurité.

Pour mieux démontrer notre engagement dans la sécurité, nous avons récemment acquis Axis Security. Cette opération nous permettra d'étendre nos capacités de sécurité de la périphérie au cloud, ainsi que de répondre aux besoins d'amélioration des performances des applications et de renforcement de la sécurité des réseaux, à mesure que les entreprises continuent de migrer leurs applications vers le cloud.

Ce rapport souligne l'engagement de Hewlett Packard Enterprise en faveur de la cybersécurité et de la responsabilité que nous partageons tous.

Bobby Ford
Directeur de la sécurité
HPE

Une nouvelle approche de la cybersécurité

Il n'est pas fréquent, dans la carrière d'un directeur de la sécurité, d'avoir l'opportunité de rejoindre une entreprise technologique mondiale qui transforme et crée activement un nouveau marché. C'est passionnant et stimulant, et je crois que chez Hewlett Packard Enterprise, nous sommes en train de changer la façon dont l'industrie voit le cloud. Le cloud n'est pas seulement une destination, c'est aussi une expérience. Avec HPE GreenLake, c'est une expérience qui peut être amenée jusqu'à vous.

Une chose qui m'est apparue clairement lorsque j'ai rejoint HPE, c'est que la cybersécurité et la gestion des risques numériques seraient responsables non seulement de la protection des activités de HPE, mais aussi de la sécurisation de l'expérience cloud que nous offrons à nos clients. Une grande partie du travail de mon équipe au cours des 18 derniers mois s'est donc concentrée sur la compréhension des risques qui apparaissent lors de la migration des charges de travail des datacenters sécurisés sur site vers le cloud public, l'edge et à d'autres emplacements entre les deux, dans le cadre d'une expérience de cloud hybride.

À l'aube de 2023, l'évolution du climat économique a resserré les budgets dans tous les secteurs d'activité. En outre, la pénurie mondiale de candidats disponibles pour pourvoir les nombreux postes vacants continue d'étouffer les programmes de cybersécurité, même les plus matures.

En tant que leaders de la cybersécurité et de la technologie, nous avons la possibilité d'avoir un impact sur nos entreprises et nos collaborateurs en nous attaquant à toutes ces questions. Ce rapport présente certaines des initiatives que nous avons lancées en 2022 pour relever ces défis et offrir à nos clients une expérience sécurisée de la périphérie au cloud. Ces initiatives ont posé les bases sur lesquelles nous nous appuierons en 2023 et au-delà, toujours dans le but de vous aider à transformer votre entreprise.

De nouvelles menaces de plus en plus graves se profilent

HPE n'est pas seulement une organisation technologique mondiale de premier plan, c'est aussi une cible que les cybercriminels tentent d'infiltrer et d'attaquer tous les jours. Nous savons que nous devons garder une longueur d'avance sur nos adversaires. Par conséquent, nous surveillons activement les différents vecteurs de menace, notamment les suivants :

Les États-nations hostiles se multiplient.

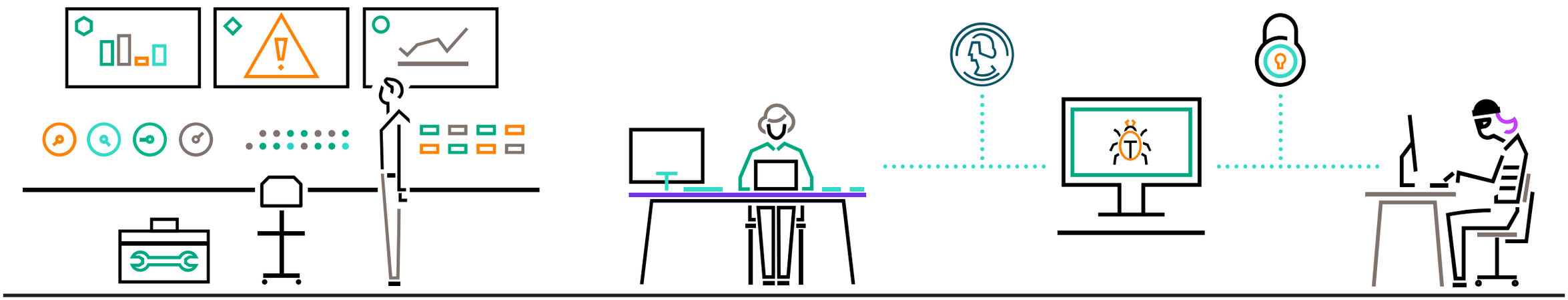
Les menaces persistantes significatives (APT) continuent de susciter des inquiétudes dans de nombreux secteurs à l'échelle mondiale. Les acteurs responsables de la création des APT sont richement financés, hautement qualifiés, bien organisés et peuvent être des organisations militaires ou des professionnels de la sécurité sous contrat. Alors que ces acteurs hostiles continuent de cibler les secteurs des semi-conducteurs, des télécommunications et des infrastructures à la recherche d'informations liées au calcul haute performance, au Big Data, au ML et à l'IA, HPE continue de suivre et de se protéger contre les activités liées aux APT dans le but de prévenir l'espionnage économique.

L'hameçonnage reste une épidémie.

L'élément humain est toujours le maillon faible des défenses de sécurité d'une entreprise. L'hameçonnage est depuis longtemps un problème critique de cybersécurité< ; Un nouveau site d'hameçonnage apparaît toutes les 20 secondes sur Internet. Chez HPE, nous bloquons plus de 1 000 tentatives d'hameçonnage par jour, ce qui en fait le plus grand vecteur de menace utilisé contre l'entreprise. Si l'utilisation de la technologie pour identifier et bloquer la quasi-totalité de ces attaques est essentielle, la formation des membres de l'équipe à la reconnaissance de ces attaques de plus en plus élaborées reste une priorité. Nous organisons un programme annuel de sensibilisation à la cybersécurité et déployons régulièrement des campagnes d'hameçonnage pour tenir les membres de l'équipe au courant.

Les attaques par rançongiciels sont plus simples que jamais.

Il y a quelques années, les cybercriminels devaient être des experts en programmation, conception de matériel, mise en réseau, etc. Tout cela a changé, car des équipes de cybercriminels développent des boîtes à outils de logiciels malveillants et les mettent à la disposition des criminels « as-a-service ». Le lancement de cyberattaques, telles que les rançongiciels, s'effectue désormais en quelques clics. Les attaquants n'ont plus besoin d'un réel niveau de savoir-faire pour mener à bien ces initiatives, mais seulement d'une cible et du désir de planifier une attaque. Cette situation a entraîné une explosion des cyberattaques par rançongiciels au cours des derniers mois. Chez HPE, nous disposons de défenses élaborées contre ces vecteurs d'attaque. Nous fournissons également des services de conseil et élaborons des solutions pour nos clients qui recherchent les meilleures pratiques en matière de défense et de récupération contre les rançongiciels.



De nouvelles menaces de plus en plus graves se profilent

Les attaques internes augmentent.

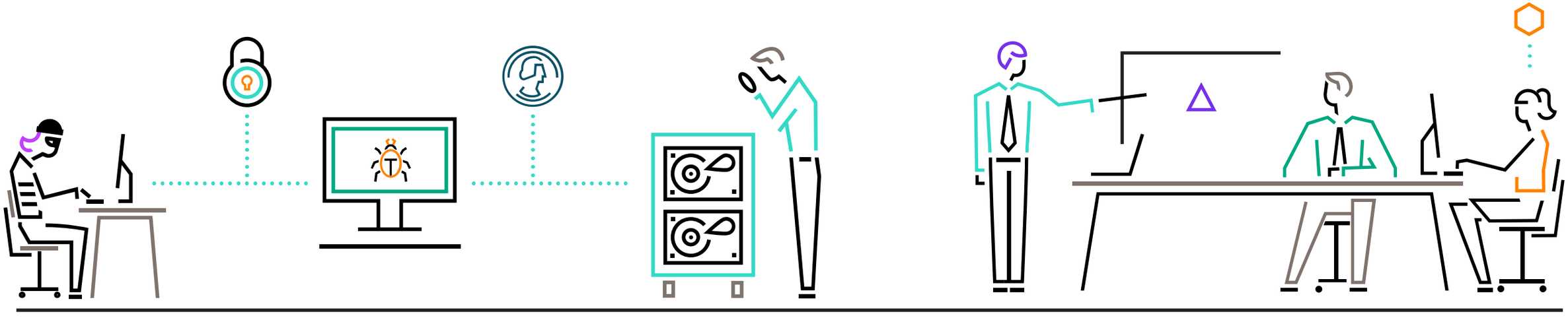
Que ce soit par malveillance ou par simple négligence, les employés restent un vecteur clé pour les attaques de tous types. Ces attaques peuvent être beaucoup plus difficiles à détecter et, par conséquent, peuvent infliger des dommages beaucoup plus importants que les attaques extérieures habituelles. De nombreuses organisations négligent les dangers des menaces internes, mais les attaques internes représentent une autre menace clé qui doit être atténuée. En tant que grande entreprise technologique, nous devons non seulement être conscients des employés mécontents qui souhaitent nuire à HPE, mais aussi de la possibilité que des membres de l'équipe soient incités à participer au vol d'informations par des parties bien financées. Les formations de sensibilisation à la cybersécurité continuent de jouer un rôle important à cet égard.

Les vulnérabilités atteignent un niveau record.

Le nombre de failles de sécurité signalées dans le matériel et les logiciels est stupéfiant et ne cesse de croître : plus de 22 000 signalements en 2022, contre 20 000 en 2021. En conséquence, les entreprises se débattent avec la gestion des correctifs, ce qui rend la correction et le triage rapides plus critiques que jamais, ainsi que les contrôles compensatoires appropriés. Chez HPE, la gestion des vulnérabilités est un triptyque qui consiste à surveiller les vulnérabilités de l'ensemble de l'organisation, celles de nos plateformes de gestion cloud et celles des produits et services que nous vendons à nos clients.

La structure d'approvisionnement complique la sécurité.

Les entreprises établissent de plus en plus de partenariats avec d'autres organisations dans le cadre de collaborations, d'externalisations et d'autres accords. Elles doivent donc accorder une importance accrue à la gestion de la sécurité des tiers. Les services de gestion des risques tiers de HPE se sont étendus à la chaîne d'approvisionnement et à la sécurité des achats mondiaux, offrant un cadre pour atténuer les perturbations logistiques et protéger à la fois la propriété intellectuelle des clients et la nôtre. En outre, en tant que fournisseur de nos clients, nous reconnaissons le rôle important que joue la sécurité de la chaîne d'approvisionnement dans les relations avec les clients. Nous avons développé nos capacités pour répondre aux questions des clients en conséquence.



Aperçu et résultats des efforts déployés en matière de sécurité

Soutenir la transformation Edge to Cloud

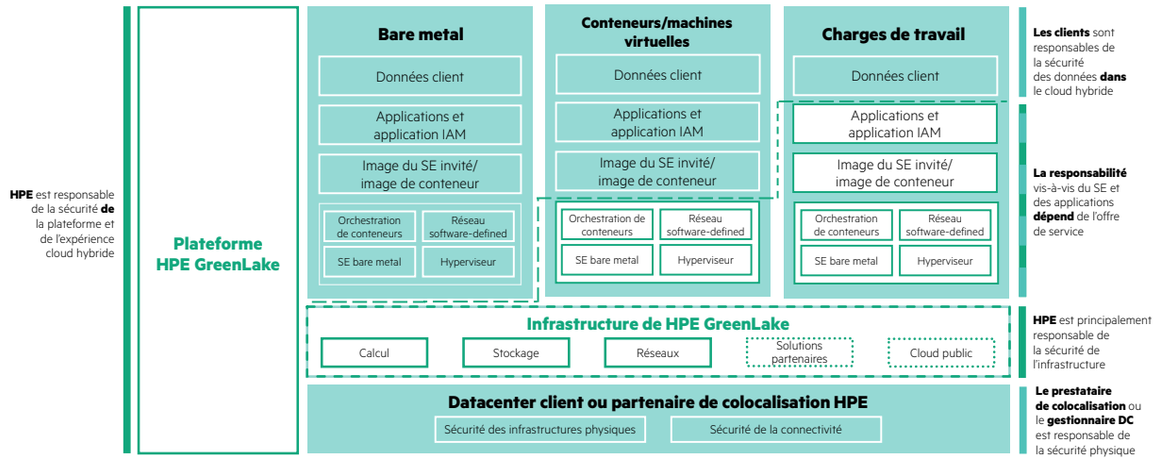
Le cloud a prouvé sa valeur en tant que ressource permettant de réduire les coûts d'infrastructure et d'assistance et de créer rapidement des applications et des services. Mais les incidents qui ont défrayé la chronique ces dernières années ont montré à quel point la sécurité et la conformité sont essentielles pour les écosystèmes basés sur le cloud.

Chez HPE, nous sommes bien conscients du besoin de sécurité entre la périphérie et le cloud et avons développé une architecture de sécurité qui y répond spécifiquement. Nous faisons de la sécurité une priorité sur notre plateforme cloud, HPE GreenLake. Nous sommes déterminés à la fois dans nos principes de plateforme sécurisée par conception et dans la protection des données des clients en tant que premier critère de conception.

Pour atteindre nos objectifs de sécurité, nous nous appuyons sur une approche de la cyber-résilience et de la protection des données fondée sur les risques et la conformité. Notre plateforme est entièrement alignée sur les normes et les meilleures pratiques du secteur.

Cet axe a été crucial, car les charges de travail se sont éloignées des environnements de clouds publics purs, que les clients considèrent de plus en plus comme une solution imparfaite pour toutes les opérations, pour diverses raisons, notamment les défis liés à la confidentialité et à la souveraineté des données. Alors que le cloud hybride devient un choix de plateforme de plus en plus populaire et flexible, HPE est entièrement prêt à sécuriser ces charges de travail, quelles que soient les spécificités des opérations du client.

Tout au long de ce parcours, nous avons appris qu'il faut déterminer où s'arrête notre responsabilité et où commence celle du client. Tout malentendu ou manque de clarté concernant ces lignes de démarcation peut introduire des vulnérabilités de sécurité et accroître l'exposition à de nouveaux vecteurs d'attaque. Pour atténuer ces risques, nous avons mis au point le modèle de responsabilité partagée pour la sécurité HPE GreenLake, qui définit clairement les rôles de HPE et des consommateurs de nos services, contribuant ainsi à réduire la surface d'attaque potentielle.



Modèle de responsabilité partagée pour la sécurité HPE GreenLake

Parallèlement, nous soutenons nos initiatives de cybersécurité en constituant une équipe de sécurité interfonctionnelle qui soutient à la fois nos activités internes et nos opérations as-a-service, sous la direction de notre directeur de la sécurité, Bobby Ford, qui remet activement en question le rôle traditionnel du directeur de la sécurité. Selon Bobby, la sécurité est une fonction que le directeur de la sécurité doit utiliser pour permettre à l'entreprise de fonctionner (et pas seulement en appliquant des contrôles arbitraires), en donnant à tous les membres de l'entreprise les outils dont ils ont besoin pour intégrer la sécurité à toutes les opérations. En outre, Bobby s'est concentré sur une approche non conventionnelle de l'acquisition de talents, reconnaissant le nombre élevé de postes vacants dans le domaine de la cybersécurité que l'industrie doit collectivement combler (voir également la section « Repenser les talents » à la page 12.) En positionnant HPE comme un faiseur de talents et non comme un preneur de talents, il se tourne vers des endroits inattendus pour recruter des équipes de sécurité.

Réalisations et investissements

Où nous investissons notre argent et notre temps

Répondre aux attentes de sécurité de l'industrie

Le décret présidentiel américain 14028 a établi de nouvelles règles pour garantir la sécurité de la chaîne d'approvisionnement, en particulier au niveau des logiciels. La nomenclature logicielle décrit en détail les composants utilisés dans la construction d'une application logicielle. HPE a redoublé d'efforts pour développer des processus de collecte d'informations afin de remplir les nomenclatures logicielles et de les fournir pour les produits HPE lorsque cela est nécessaire. Par ailleurs, notre initiative « Chaîne d'approvisionnement de confiance » est désormais disponible dans le monde entier. Cette initiative élargit et sécurise notre chaîne d'approvisionnement, garantissant aux clients que nos produits sont fabriqués à partir de pièces authentiques et vérifiables. Aujourd'hui, nous restons le seul grand fabricant de serveurs à produire des serveurs standard avec une désignation de pays d'origine américaine.

Adopter une approche multicouche de la protection

Nous avons créé une chaîne de confiance pour protéger les données des clients (et les nôtres) tout au long du cycle de vie. Cela commence aux niveaux les plus élémentaires du silicium, où notre base de confiance gravée dans le silicium (Silicon Root of Trust) unique donne aux serveurs une empreinte digitale immuable qui empêche les codes malveillants de corrompre le firmware. Nous contrôlons minutieusement les fournisseurs et les tiers pour réduire le risque de menaces tout au long de la chaîne d'approvisionnement. Nos dispositifs de réseau utilisent également l'identité du matériel et la protection du firmware renforcée par le matériel pour protéger l'intégrité du dispositif. Notre programme de fin de vie détaille les politiques de mise hors service, de remise en état et de recyclage des actifs en toute sécurité. Des analyses et des tests de pénétration effectués par des tiers indépendants garantissent que tous ces programmes sont très efficaces et conformes aux contrôles 800-53 du National Institute of Security and Technology (NIST).

Engager le dialogue sur la sécurité avec les clients

Du point de vue de la sécurité, nous reconnaissons que notre relation avec les clients évolue à mesure que l'industrie adopte des plateformes de cloud hybride et que cela soulève des questions quant à la responsabilité de chacun. Lors de HPE Discover 2022, notre plus grand événement de l'année pour les clients et les partenaires, nous avons abordé ces questions de front, avec une session de Bobby Ford, directeur de la sécurité. Il a dévoilé le modèle de responsabilité partagée de HPE, soulignant l'importance d'un langage commun que les fournisseurs et les clients peuvent utiliser pour comprendre les besoins des uns et des autres. Bobby a également animé une session avec un panel de clients et d'experts de l'industrie pour discuter du battage médiatique et de la réalité du modèle zero trust, ainsi que de la façon dont la transformation vers une culture de la sécurité est essentielle à l'amélioration de la cyber-résilience.

Notre nouveau cercle des RSSI a rassemblé les plus grands spécialistes de la cybersécurité dans de nombreux secteurs d'activité afin qu'ils partagent en privé leur sagesse et leurs meilleures pratiques. Pour une consommation plus large, nous avons produit de nombreux livres blancs, webinaires et articles en ligne offrant des conseils sur les dernières tendances, menaces et solutions de cybersécurité. Nous avons également été heureux de rencontrer nos clients dans notre nouveau siège de Houston, où nous avons organisé des visites de notre Cyber Fusion Center et discuté des meilleures pratiques de cybersécurité de la périphérie au cloud.

Pleins feux sur les membres de l'équipe

Rencontrez **McKaela Doherty, vice-présidente, Centre d'excellence en cybersécurité**

McKaela a occupé diverses fonctions de direction chez HPE au cours de ces dix dernières années. En tant que vice-présidente du Centre d'excellence en Cybersécurité, McKaela applique son sens des affaires à la création d'une cybercommunauté à l'échelle de HPE, à la consultation des équipes commerciales et à la mise en place de solides habitudes de sécurité parmi les 60 000 employés de HPE. Elle a poussé l'organisation à se tourner davantage vers l'extérieur, en démontrant les capacités cybernétiques de HPE et en s'engageant auprès des clients pour partager des idées et des bonnes pratiques. « Mais ce qui me passionne le plus, ce sont les gens », confie-t-elle. « Nos programmes de cyber-talents consistent à trouver des moyens créatifs de recruter, de motiver et d'améliorer les compétences des membres de l'équipe, ainsi que de contribuer à faire de HPE un endroit où il fait bon travailler.»

Réalisations et investissements

Où nous investissons notre argent et notre temps

Donner en retour

HPE s'efforce d'être une force positive, en aidant les communautés du monde entier par le biais du bénévolat, des dons et du soutien par la fondation de l'entreprise. Mais l'une des façons les plus efficaces dont nous pouvons rendre service en tant qu'entreprise technologique est de mettre notre savoir-faire approfondi au service de ceux qui peuvent en bénéficier. C'est ce qu'a fait cette année l'équipe HPE de Galway, en Irlande, en s'associant à Safe Ireland pour sensibiliser à la cybersécurité. L'équipe a créé une campagne d'affichage, #RedFlagsAreAbuse, et un ensemble de ressources en ligne destinées à empêcher les groupes vulnérables d'être victimes d'abus facilités par la technologie. Elle a été lancée en octobre 2022 et a fait l'objet d'une attention médiatique nationale.

Investir dans les normes

Nous investissons dans la normalisation de notre approche de l'architecture de nos propres applications de cloud hybride en suivant et en certifiant selon les normes de l'industrie. Notre équipe de services aide également nos clients à s'aligner sur ces mêmes normes grâce à ses missions de conseil en sécurité. Il s'agit notamment de développer de nouvelles architectures et méthodologies de sécurité pour fournir une approche reproductible et éprouvée de la protection qui s'aligne sur les normes, notamment celles du NIST, de la CSA et de l'ISO. Ceux-ci ont été codifiés dans notre modèle de référence pour la sécurité d'entreprise, que nous présentons lors d'ateliers stratégiques sur la sécurité qui couvrent une variété de sujets allant du modèle zero trust à la cyber-résilience.

Pleins feux sur les membres de l'équipe

Rencontrez **Ankush Chowdhary, RSSI des services cloud**

Ankush fait partie du monde de la cybersécurité depuis plus de 20 ans, mais il est aujourd'hui confronté à son défi le plus important en tant que responsable de la transformation de la sécurité du cloud pour la plateforme HPE GreenLake. En tirant parti de son expérience antérieure dans la création de centres d'opérations de sécurité, de programmes de surveillance de la sécurité, de réponse aux incidents et de programmes de renseignement sur les menaces pour les principaux fournisseurs de cloud public, Ankush a apporté une approche pluridisciplinaire indispensable aux opérations de sécurité Edge to Cloud de HPE. « La modernisation axée sur les données est la clé du succès dans les entreprises d'aujourd'hui », déclare-t-il, « mais les entreprises ne réussiront jamais si elles ne disposent pas d'une plateforme sécurisée sur laquelle travailler. »

Repenser les talents

Changer la façon dont nous investissons dans les membres de l'équipe

De nombreux secteurs sont confrontés à une grave pénurie de talents, et c'est particulièrement vrai dans le domaine de la cybersécurité. Comme le fait remarquer Bobby Ford, directeur de la sécurité de HPE, les rapports faisant état d'une pénurie de talents dans la cybersécurité ne sont pas tout à fait exacts. Il y voit un manque d'expérience. Voici les principaux moyens que nous avons mis en œuvre pour créer et développer nos professionnels de la sécurité en 2022.

Ouvrir les portes aux talents ignorés

Il y aura plus de 3,5 millions de postes à pourvoir dans le domaine de la cybersécurité d'ici à 2025, mais une liste interminable d'exigences empêche la plupart de ces postes d'être pourvus. Il en résulte une guerre sans fin entre les entreprises pour attirer ces talents. Et si nous cherchions à créer nous-mêmes des talents en donnant des opportunités à ceux qui en ont besoin ? Cette année, nous avons lancé le programme Cybersecurity Career Reboot. Il recherche activement des candidats susceptibles d'être négligés parce qu'ils n'ont pas l'expérience requise pour décrocher un emploi de débutant dans ce domaine, ou qui considèrent la cybersécurité comme un nouveau parcours professionnel ou qui ont des difficultés à obtenir un emploi dans une entreprise. Ce qui n'est pas indispensable : un diplôme universitaire ou une expérience en cybersécurité. Au cours d'un programme intensif de six mois, les participants sont rémunérés tout en apprenant les rouages de la cybersécurité, en étant intégrés dans diverses fonctions cybernétiques au sein de HPE, et en prenant en charge des projets tout en étant encadrés par les membres de notre équipe. Notre première cohorte Career Reboot a fait l'objet d'une attention nationale. Les participants ont obtenu leur diplôme à la fin de l'année 2022. Ce qui n'était au départ qu'un projet pilote est aujourd'hui un programme permanent en pleine expansion.

Donner aux nouveaux diplômés un premier aperçu des opérations de cybersécurité

De même, notre programme de rotation professionnelle (PREP) est conçu pour recruter des jeunes diplômés dans le cadre d'un programme de rotation de deux ans qui comprend une exposition globale à toutes nos fonctions de cybersécurité. Les participants au programme PREP acquièrent une expérience des fondements de la cybersécurité par le biais de projets concrets, d'une exposition à une variété d'expériences, ainsi que d'une formation et d'un développement novateurs, en passant par les différentes équipes de cybersécurité tous les six mois au cours du programme.

Mettre l'accent sur la diversité et le mentorat

Grâce à un solide programme de mentorat et de stages, nous constatons que la cybersécurité suscite plus d'intérêt que jamais chez un nombre croissant de travailleurs. Chez HPE, nous savons que les personnes sont nos plus grandes forces et nous considérons que l'équité, l'inclusion et la diversité sont primordiales pour réussir dans le domaine de la cybersécurité. Nous pensons que la diversité des vécus améliore les opérations de cybersécurité, en nous aidant à surmonter les préjugés inhérents aux méthodes de travail traditionnelles et à remettre en question le statu quo. Ce type de réflexion innovante devient de plus en plus incontournable, car les attaquants adaptent leurs techniques, qui exigent des réponses tout aussi créatives.

Notre point de vue sur les directions à privilégier par le secteur

Priorités

La cybersécurité est une question stratégique qui a un impact sur la prise de décision à tous les niveaux de l'entreprise.

- Définir des **objectifs d'amélioration de la maturité cybernétique** qui s'alignent sur un cadre de cybersécurité standard de l'industrie, créant ainsi un langage commun entre les équipes de cybersécurité.

- Établir un **cadre de risque de cybersécurité** en définissant des critères permettant de mesurer de manière objective et cohérente l'importance des actifs, en accord avec les équipes chargées de la gestion des risques et les dirigeants d'entreprise.

- Adopter une approche basée sur des mesures pour **évaluer l'efficacité des contrôles de sécurité**, les responsables peuvent ainsi prendre des décisions éclairées en fonction des priorités de l'entreprise et de leur goût du risque.

- Investir dans **la création et le développement de talents** pour palier la pénurie de talents dans le domaine de la cybersécurité.

- **Protéger les infrastructures critiques** contre les menaces croissantes, sans oublier les perturbations économiques qui en découlent, afin de garantir la sécurité nationale.

- Gérer **les tensions géopolitiques** et les logiciels malveillants évolués qui en résultent et se multiplient pour menacer toutes les entreprises.

Perspectives en matière de sécurité : 2023 et au-delà

Prévisions

« Les cybercriminels vont redoubler d'efforts en matière d'automatisation face à des attaques devenant de plus en plus automatiques et reproductibles. Les marchés de la cybercriminalité qui vendent des attaques de déploiement de logiciels malveillants prêtes à l'emploi as-a-service vont se développer, ce qui multipliera les attaques d'opportunité et pèsera de plus en plus lourd sur les opérations cybernétiques. »

– Daniel Frye, RSSI de l'entreprise

« Nous voyons un risque dans les chaînes d'approvisionnement distribuées comprenant des sites de fabrication et d'assemblage dans des pays géopolitiquement adversaires ou dans des pays qui risquent d'être envahis par des forces géopolitiques. Cela peut à son tour augmenter le risque que des composants contrefaits ou malveillants entrent dans le cycle de vie de la production. »

– CJ Coppersmith, directeur de la sécurité des produits

« Alors que les organisations adoptent la transformation numérique et l'IoT, les pirates continueront probablement à tirer parti de la surface d'attaque qu'elles créent. Ainsi, les attaques destructrices pourraient devenir encore plus préjudiciables. »

– Sandya Bhoajaraj, conseillère technique stratégique, cybersécurité et gestion des risques numériques

« Alors que les conseils d'administration font l'objet d'un examen de plus en plus minutieux, la sécurité restera une préoccupation majeure. Les pressions budgétaires obligeront les équipes de sécurité à faire plus avec moins et à se concentrer sur ce qui compte le plus pour l'entreprise. »

– Paul De Luca, directeur de la gestion du risque cybernétique

« À la lumière des nouvelles réglementations et des décisions de justice, les RSSI, les directeurs de la sécurité et les autres professionnels du domaine seront de plus en plus souvent tenus personnellement responsables de leur incapacité à fournir les informations requises sur les violations ou à sécuriser de manière adéquate les données sensibles. »

– Brian Schmitt, avocat général associé, cybersécurité

Perspectives en matière de sécurité : 2023 et au-delà

Prévisions

« L'environnement propice aux cybermenaces continue de se développer à un rythme exponentiel. Les acteurs de la menace, tels que les États-nations et les cybercriminels, continueront à faire progresser les technologies émergentes. Les recherches sur la sécurité indiquent que les acteurs de la menace font évoluer leur savoir-faire grâce à l'intelligence artificielle et à l'informatique quantique. Les organisations devront adopter des technologies telles que la cryptographie à résistance quantique (ou post-quantique) pour sécuriser leurs données dans un avenir proche. »

– Travis Murray, chef de l'équipe des renseignements cybernétiques

« L'utilisation croissante de l'IA et des opérations d'apprentissage machine (MLOps) dans la cybersécurité facilitera la découverte et la correction des activités inhabituelles dans l'entreprise. »

– Rohini Chavakula, scientifique des données

« Les organisations devront se concentrer davantage sur la mise en place d'architectures informatiques capables de résister, de réagir et de se remettre de toutes sortes de menaces informatiques et cybernétiques, en particulier à la lumière de nouvelles réglementations telles que la loi européenne sur la résilience opérationnelle numérique pour le secteur financier. »

– Lois Boliek, directrice des services de cybersécurité

« Le périmètre de l'entreprise va encore s'étendre et, dans certains cas, disparaître, car les organisations investissent dans le modèle Edge to Cloud, et le télétravail reste le nouveau mode de fonctionnement. Les technologies telles que SASE et SD-WAN, ainsi que le zero trust, joueront un rôle essentiel dans le développement de contrôles de niveau efficaces. »

– Tim Ferrell, technologue émérite, services de cybersécurité

« L'assurance cybersécurité deviendra une exigence standard dans la plupart des secteurs d'activité. Cependant, face à un nombre croissant de demandes de remboursement, les courtiers augmenteront les primes de manière exponentielle et introduiront des critères de pré-acceptation concernant la conformité et les niveaux minimums de sécurité. »

– Simon Leech, directeur de la cybersécurité et de la gestion des risques numériques

Pleins feux sur les membres de l'équipe

Rencontrez **Carlos Camarillo, programme Cybersecurity Career Reboot**

Carlos est né à Mexico et a grandi dans le sud du Mexique. Après un passage à l'Université Ibéro-américaine, il a finalement été transféré à l'Université Heidelberg de l'Ohio où il a terminé ses études de premier cycle, avant d'obtenir un MBA à l'Université de Findlay, située non loin de là. Carlos est retourné au Mexique à la suite d'une urgence familiale et a dirigé un restaurant local pendant plus de dix ans, jusqu'à la pandémie, après quoi il a vendu l'affaire. Grâce au programme Career Reboot de HPE, Carlos a reçu une offre d'emploi en tant qu'analyste en cybersécurité dans notre bureau de Houston, malgré un manque de formation formelle en cybersécurité. « Je suis ravi d'être de retour dans le monde de l'entreprise », déclare-t-il, « et de travailler pour un leader technologique d'envergure mondiale. »

Perspectives en matière de sécurité : 2023 et au-delà

Recommandations

Renforcer la résilience et adopter une politique zero trust

Clarifier le modèle de sécurité partagée de vos opérations cloud pour comprendre où commencent vos responsabilités et où s'arrêtent celles de vos fournisseurs.

S'efforcer de rapprocher les équipes de sécurité de l'entreprise afin qu'elles comprennent mieux comment leur travail peut contribuer à atténuer les risques pour l'organisation.

Passer d'une protection des données basée sur les appareils à une auto-protection des données.

Embaucher pour le talent, pas nécessairement pour l'expérience. Cette dernière peut être développée ou acquise, contrairement au talent.

Tirer parti du zero trust et du service d'accès sécurisé à la périphérie (SASE) pour accroître la résilience de votre infrastructure en matière de cybersécurité et mieux préparer l'organisation face aux menaces.

Comprenez votre chaîne d'approvisionnement dans son intégralité et identifiez où se situent les cyber-risques liés à des tiers.

Investir dans l'analyse du comportement des utilisateurs, qui modélise les activités des utilisateurs au fil du temps et met en évidence les écarts par rapport aux modèles établis, pour révéler les attaques potentielles en cours.

Instaurez une culture de la sécurité au sein de l'organisation, jusqu'au niveau du conseil d'administration, et mettez en place un solide programme de sensibilisation à la cybersécurité.

Les techniques de chiffrage, de création de jetons et de pseudonymisation peuvent protéger et masquer les données sous toutes leurs formes jusqu'au moment où elles doivent être consommées.

La sécurité n'est possible que par la combinaison de l'automatisation et de l'assiduité des personnes, en veillant à ce que les correctifs critiques soient appliqués en premier et que toutes les vulnérabilités ayant un impact soient traitées dans un délai approprié.

Ressources du Centre d’excellence en cybersécurité de HPE

Rapports HPE et contenu en ligne

- Responsabilité partagée pour la sécurité avec HPE GreenLake
- La cybersécurité Edge to Cloud vue par les spécialistes de la sécurité HPE
- Rapport annuel HPE Living Progress
- Alertes de vulnérabilité de sécurité des produits critiques HPE
- Services de cybersécurité HPE
- Formation à la cybersécurité HPE
- Sécurité HPE GreenLake
- Carrières chez HPE

Évaluations externes

UpGuard

Commentaires

Nous attendons avec impatience vos commentaires sur tout sujet lié à la sécurité, au fil de l’évolution de notre monde Edge to Cloud. Veuillez nous contacter ici.

Visiter **HPE GreenLake**

Hewlett Packard Enterprise

a00130859FRE, rév. 1