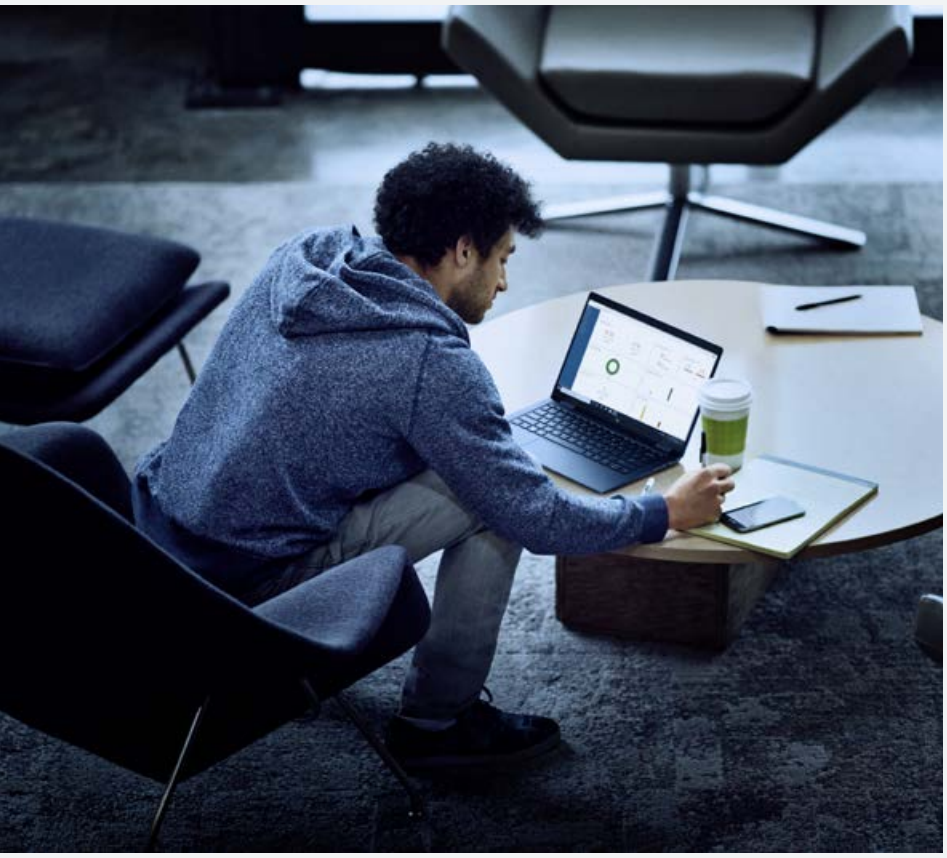
APPORTEZ UNE RÉPONSE AU MANQUE D'EXPERTS EN CYBERSÉCURITÉ :

COMMENT RENFORCER LES COMPÉTENCES DE VOTRE ÉQUIPE ET TIRER PARTI DES DONNÉES ANALYTIQUES POUR ACCROÎTRE VOS CAPACITÉS EN MATIÈRE DE CYBERSÉCURITÉ

LES ENTREPRISES DU MONDE ENTIER SONT AUJOURD'HUI CONFRONTÉES À UN MANQUE DE PERSONNEL INFORMATIQUE.
QUE POUVEZ-VOUS FAIRE POUR RENFORCER LES COMPÉTENCES DE VOS ÉQUIPES ?



85 %

DES ENTREPRISES DÉCLARENT UN MANQUE DE COMPÉTENCES EN CYBERSÉCURITÉ[2]

La cybercriminalité est un sujet qui fait souvent la une. De nouvelles menaces de sécurité semblent en effet apparaître tous les quelques mois, entraînant un processus coûteux et complexe pour les professionnels de l'informatique chargés d'y apporter une réponse.

Et ces menaces génèrent des coûts très importants pour les victimes. Le coût moyen d'une attaque est de 8,7 millions de dollars aux États-Unis et de 3,86 millions de dollars dans le monde. En ajoutant à cela les nombreux terminaux distants utilisés dans l'environnement professionnel hybride d'aujourd'hui, ces coûts deviennent encore plus élevés.[1]

Les pertes constatées ne sont pas uniquement liées aux revenus perdus à cause des périodes d'indisponibilité : elles incluent également d'autres éléments plus difficiles à quantifier, comme l'augmentation de la perte de clients et le coût lié aux efforts accrus pour signer de nouveaux contrats après la dégradation de la réputation de l'entreprise.[1]

Si les failles de sécurité sont un problème, la solution évidente est d'engager plus de spécialistes capables de protéger l'entreprise. Mais l'un des principaux obstacles à la défense efficace des terminaux est le manque de personnel informatique spécialisé en sécurité.[2]

Ce manque est lié en partie au marché lui-même. Il existe un manque notable de professionnels spécialisés en cybersécurité : en effet, à l'échelle mondiale, il manque plus de 3 millions d'employés dans ce secteur.[3] Et malgré des attaques croissantes et 85 % des entreprises déclarant un manque de compétences en cybersécurité,[2] les recrutements de professionnels du domaine sont en réalité en baisse.[3] Il est possible que vous vouliez engager du personnel spécialisé en cybersécurité, mais il est difficile de trouver des experts que vous pouvez vous permettre de recruter.

HP WOLF SECURITY

LES CYBERMENACES SONT EN AUGMENTATION

102 MILLIONS

DE NOUVELLES MENACES LIÉES AUX MALWARES CHAQUE MOIS[4]

60 %

NOMBRE D'ENTREPRISES TOUCHÉES PAR DES ATTAQUES SE PROPAGEANT D'UN À PLUSIEURS EMPLOYÉS[5]

+58 %

D'ATTAQUES DE HAMEÇONNAGE AU COURS DE L'ANNÉE PASSÉE[5]

+63 %

DE CAMPAGNES DE HAMEÇONNAGE ET DE FAUSSES PUBLICATIONS SUR LES RÉSEAUX SOCIAUX LIÉES À LA PANDÉMIE DE COVID-19[6]

COÛT MOYEN D'UNE VIOLATION DE DONNÉES :[1]

- 2,01 MILLIONS DE $ POUR LES COMMERCES
- 3,9 MILLIONS DE $ POUR LE SECTEUR DE L'ÉDUCATION
- 5,85 MILLIONS DE $ POUR LES SERVICES FINANCIERS
- 7,13 MILLIONS DE $ POUR LE SECTEUR DE LA SANTÉ

APPORTEZ UNE RÉPONSE AU MANQUE D'EXPERTS EN CYBERSÉCURITÉ

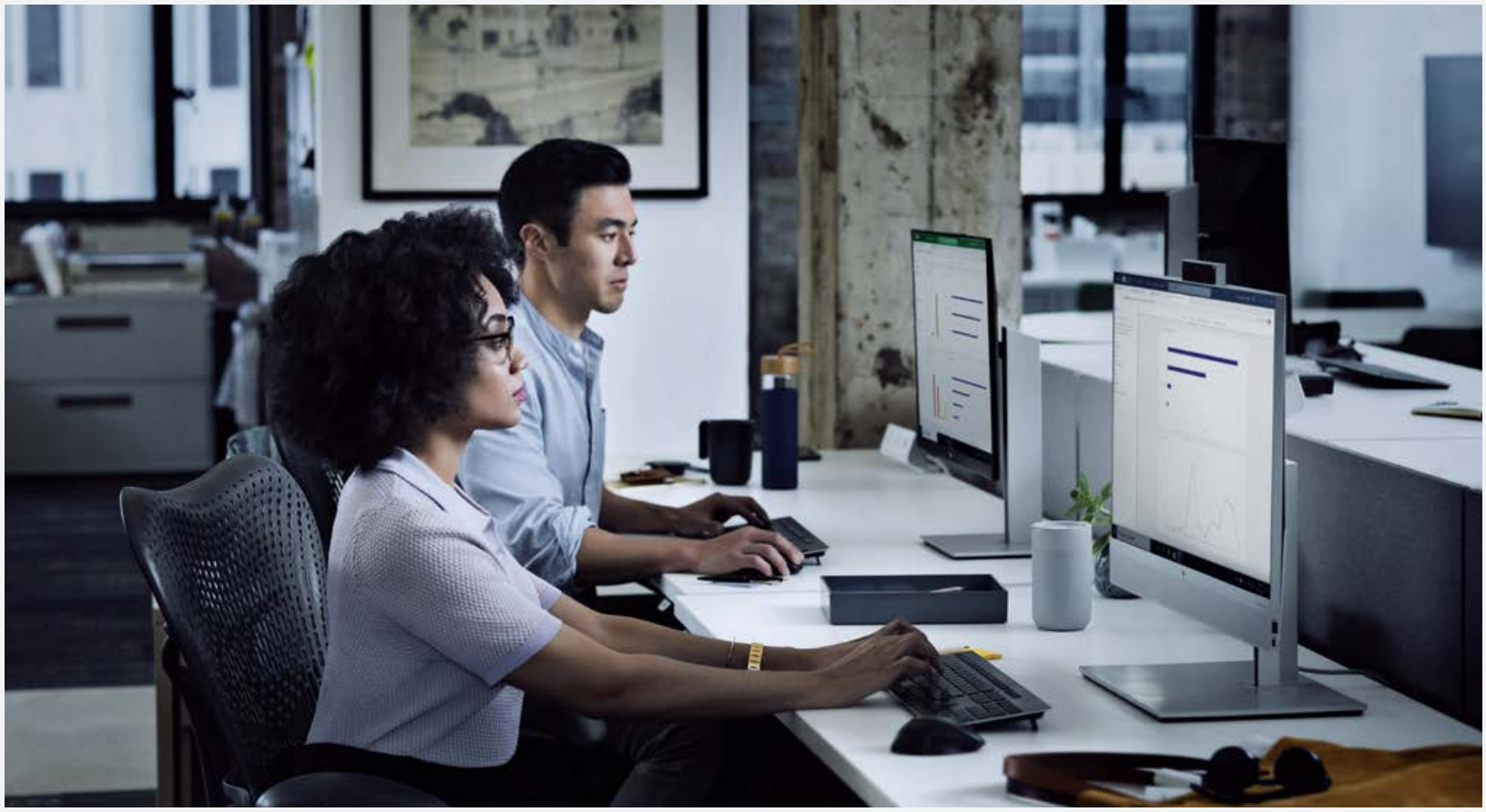
POURQUOI IL EST COMPLEXE DE DÉVELOPPER UNE COMMUNAUTÉ DE TALENTS SPÉCIALISÉS EN CYBERSÉCURITÉ

Les compétences en cybersécurité sont une spécialité, et tous les programmes de formation en informatique n'y accordent pas la même importance. Si les responsables de formations en informatique redoublent d'efforts pour renforcer les compétences en cybersécurité, développer une communauté de nouveaux talents nécessite du temps. Cybercrime Magazine déclare qu'aux États-Unis, seulement 3 % des personnes qui possèdent une licence universitaire ont des compétences en cybersécurité.[7]

James Hadley, fondateur et PDG d'Immersive Labs, explique que plus d'efforts sont nécessaires pour promouvoir la grande variété des rôles existant dans ce domaine.

« La majorité des pays développés mettent en œuvre des initiatives destinées à augmenter le nombre de personnes envisageant de faire carrière dans la cybersécurité, en commençant par les enfants dans les écoles », précise James Hadley. « Le secteur ne se limite pas aux hackers. Mais étant donné qu'il est souvent présenté sous cet angle, il est difficile de rentre ce domaine attractif, en particulier pour les femmes. Plus d'efforts doivent être mis en œuvre pour corriger ce déséquilibre de genre. »

En attendant, voici quelques conseils pratiques destinés aux entreprises qui savent qu'elles doivent faire appel à des experts en cybersécurité.



APPORTEZ UNE RÉPONSE AU MANQUE D'EXPERTS EN CYBERSÉCURITÉ

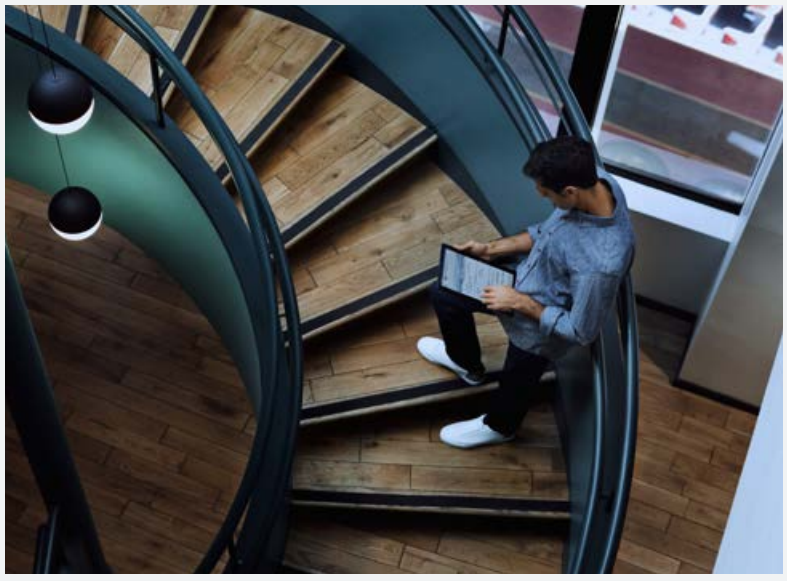
TIREZ PARTI DE VOS TALENTS DÉJÀ EXISTANTS

CE SONT DES QUALITÉS COMME L'ESPRIT ANALYTIQUE, LA CAPACITÉ DE RÉSOLUTION DE PROBLÈMES ET LA PERSÉVÉRANCE QUI COMPTENT LE PLUS.

Ne négligez pas une source naturelle de talents : vos employés déjà existants qui peuvent être stratégiquement formés à des compétences très demandées comme la cybersécurité. Évaluez le potentiel caché des membres de votre personnel, puis développez leurs compétences afin de leur attribuer de nouvelles responsabilités.

Les entreprises possèdent une opportunité clé d'assigner à leur personnel de nouveaux rôles liés à la cybersécurité, si elles savent où chercher de nouveaux talents. M. Hadley précise que la formation universitaire d'un individu a une influence minime sur son potentiel. « Ce sont des qualités comme l'esprit analytique, la capacité de résolution de problèmes et la persévérance qui comptent le plus », explique-t-il. « Si un individu possède ces attributs, il y a de fortes chances qu'il ou elle excelle dans le secteur de la cybersécurité. »

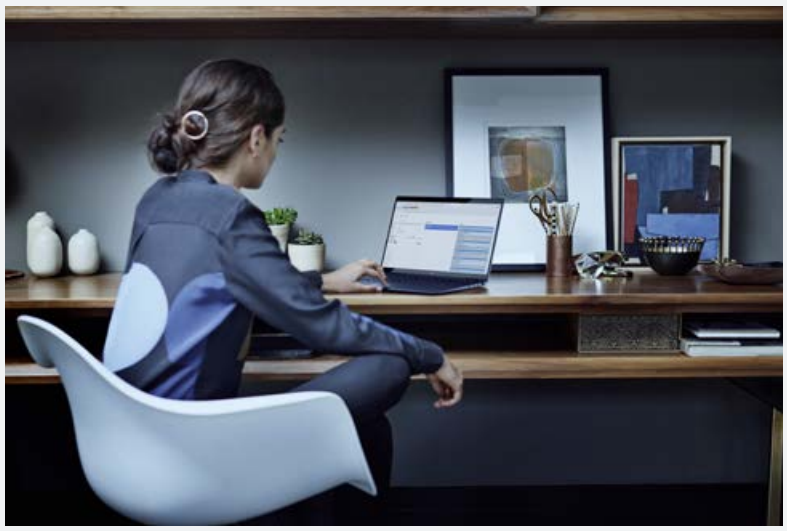
D'autres avantages existent également. Former à nouveau le personnel peut permettre de peaufiner la formation en fonction des besoins spécifiques de l'entreprise. Les formations payées par l'employeur permettent également d'accroître la fidélité des employés.[8] Elles impliquent les employés qui souhaitent développer leurs qualifications, ajouter de nouvelles compétences à leur CV et profiter d'une meilleure rémunération potentielle.



DÉPLOIEMENT DE PROCESSUS D'AUTOMATISATION ET D'ANALYSE

Une autre méthode permettant d'offrir aux équipes informatiques existantes – même celles qui possèdent des connaissances moins développées en sécurité – les moyens de combattre les cyberattaques est de choisir des solutions technologiques complètes et permanentes. Laissez les processus d'automatisation faire ce pour quoi ils ont été conçus, et permettez aux humains de se focaliser sur les éléments clés.

Les entreprises qui ont intégré l'intelligence artificielle, l'apprentissage automatique et les données analytiques à leur stratégie de sécurité constatent bien moins de pertes que celles qui n'ont pas déployé ces technologies. Le coût moyen d'une attaque au sein d'une entreprise qui bénéficie d'un processus complet d'automatisation de la sécurité est de 2,45 millions de dollars, et de 6,03 millions de dollars pour les entreprises sans processus d'automatisation de la sécurité.[1] Il n'est donc pas étonnant que jusqu'à 43 % des entreprises déclarent préférer ces solutions de sécurité informatique plus avancées.[2]



Les solutions basées sur une gestion cloud centralisée permettent aux équipes informatiques de contrôler la sécurité des appareils grâce à des données basiques et plus avancées. Combiner des protections permanentes et une meilleure visualisation des données grâce à des données analytiques leur permet d'identifier bien plus facilement les failles, de maîtriser les violations et de profiter d'informations claires sur les risques liés au matériel et aux correctifs obsolètes.

HP TECHPULSE[9] AIDE LES PROFESSIONNELS DE L'INFORMATIQUE À DÉVELOPPER ET PERFECTIONNER DE NOUVELLES COMPÉTENCES

APPORTEZ UNE RÉPONSE AU MANQUE D'EXPERTS EN CYBERSÉCURITÉ

HP WOLF SECURITY

COMBLEZ VOS LACUNES EN CYBERSÉCURITÉ GRÂCE AU SERVICE DE SÉCURITÉ DES TERMINAUX LE PLUS AVANCÉ AU MONDE[10]

Vous pouvez désormais simultanément défendre vos terminaux et développer vos compétences informatiques. HP Wolf Pro Security Service[11,12] offre aux petites et moyennes entreprises une protection de pointe, sans nécessiter d'experts en sécurité internes.

PROFITEZ D'UNE GESTION DE LA SÉCURITÉ DES TERMINAUX COMPLÈTE ET FACILITÉE :

- Couches de protection renforcées de qualité gouvernementale et capacités antivirus avancées basées sur l'IA supérieures aux outils conventionnels[13,14] pour garantir la protection des données, des identifiants et des appareils de votre entreprise.
- Données précises et exploitables sur l'état complet des appareils, y compris les tentatives d'attaques et les menaces potentielles, grâce à un tableau de bord cloud centralisé.
- Connaissances de pointe en cybersécurité[15] offertes dans une solution en tant que service, afin de permettre à vos équipes informatiques internes de développer et perfectionner de nouvelles compétences.

NE LAISSEZ PAS UN MANQUE DE COMPÉTENCES DEVENIR UNE FAIBLESSE EXPLOITABLE.

En savoir plus sur hp.com/fr/wolf

APPORTEZ UNE RÉPONSE AU MANQUE D'EXPERTS EN CYBERSÉCURITÉ

Les services HP sont régis par les conditions de service HP en vigueur fournies ou notifiées au client au moment de l'achat. Le client peut disposer de droits supplémentaires selon les lois locales, qui ne peuvent en aucun cas être affectés par les conditions générales applicables au service HP ou par la garantie limitée accompagnant le produit HP.

HP WOLF SECURITY

[1] 15th Annual 2020 Cost of a Data Breach Study: Global Overview from IBM Security and Ponemon Institute (15e étude annuelle du coût des violations de données : aperçu mondial développé par IBM Security et le Ponemon Institute), juillet 2020

[2] CyberEdge 2020 Cyberthreat Defense Report (Rapport sur les défenses contre les cybermenaces CyberEdge 2020), mars 2020

[3] (ISC)² Cybersecurity Workforce Study (Étude du personnel spécialisé en cybersécurité (ISC)²), 28 avril 2019

[4] RAPPORT DE SÉCURITÉ AV-TEST 2019/2020, 26 août 2020

[5] Mimecast The State of Email Security 2020 (Évaluation de la sécurité liée aux e-mails 2020), juin 2020

[6] The Impact of the COVID-19 Pandemic on Cybersecurity (L'impact de la pandémie de COVID-19 sur la cybersécurité), ISSA, 30 juillet 2020

[7] https://cybersecurityventures.com/only-3-percent-of-u-s-bachelors-degree-grads-have-cybersecurity-related-skills/

[8] https://applied.economist.com/articles/a-route-map-for-retraining-workers

[9] HP TechPulse est une plateforme de télémétrie et d'analyses qui fournit des données clés sur les appareils et applications, et n'est pas vendu sous forme de service autonome. HP TechPulse respecte les normes rigoureuses relatives au respect de la vie privée et de la confidentialité instaurées par le RGPD, et est certifié conforme aux normes ISO 27001, ISO 27701, ISO 27017 et SOC 2 Type 2 en matière de sécurité des informations. Une connexion à Internet et au portail TechPulse est requise. Pour connaître la configuration système requise, rendez-vous sur http://www.hpdaas.com/requirements.

[10] Basé sur une analyse interne de HP concernant les services de sécurité des terminaux soutenus par l'isolation et l'apprentissage profond, y compris les services SaaS et gérés. La mention « le plus avancé » se base sur l'isolation des applications et l'apprentissage profond en matière de protection des terminaux sur les PC équipés de Windows 10 en juillet 2020.

[11] HP Security s'appelle désormais HP Wolf Security. Les fonctionnalités de sécurité peuvent varier selon la plateforme. Veuillez consulter la fiche technique du produit pour en savoir plus.

[12] HP Wolf Pro Security Service est vendu séparément. Pour connaître la configuration système requise, rendez-vous sur http://www.hpdaas.com/requirements. Les services HP sont régis par les conditions générales de service HP applicables, qui sont remises au client ou lui sont indiquées lors de l'achat. Le client peut disposer de droits supplémentaires accordés par les lois locales, qui ne peuvent en aucun cas être affectés par les conditions générales applicables au service HP ou la garantie limitée accompagnant le produit HP. Pour connaître la configuration système requise, rendez-vous sur www.hpdaas.com/requirements.

[13] HP Sure Click est disponible sur certains PC HP et requiert l'installation de Windows 10. Veuillez consulter la page https://bit.ly/2PrLT6A_SureClick pour plus d'informations.

[14] HP Sure Sense est disponible sur certains PC HP et n'est pas compatible avec Windows 10 Home.

[15] Les conseils experts en matière de sécurité sont fournis uniquement avec l'abonnement Proactive Security Enhanced.

4AA7-3855FRE, Rév. 1, avril 2021

APPORTEZ UNE RÉPONSE AU MANQUE D'EXPERTS EN CYBERSÉCURITÉ