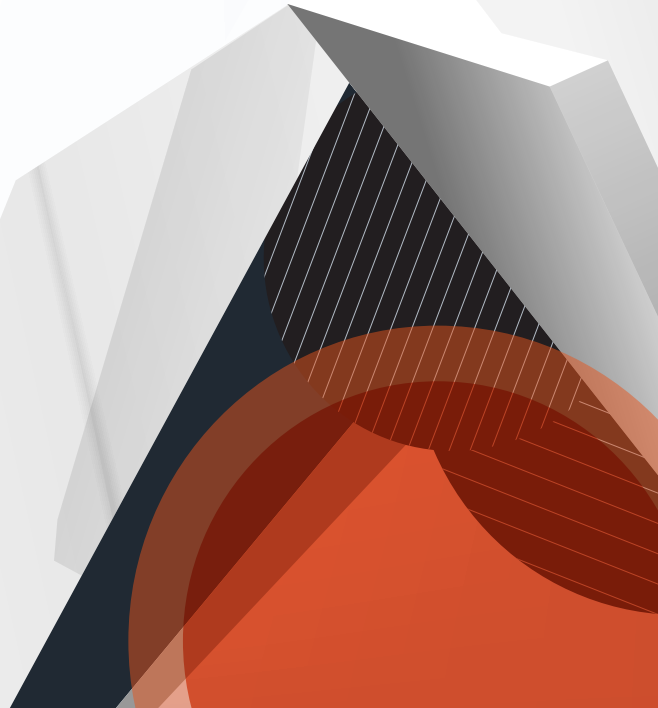
FIREEYE™

LIVRE BLANC

Cybersécurité : combattre la pénurie de compétences



ONE

des entreprises interrogées ont subi au moins une compromission en 2018

2 100 milliards $
Coût total estimé du cybercrime en 2019

3,5 millions
Pénurie estimée à l'échelle mondiale d'ici 2022

Introduction

Le facteur humain occupe une place prépondérante dans l'efficacité d'une cybersécurité. Derrière les technologies se cachent en effet des professionnels dotés d'une expertise et de compétences techniques essentielles à la mise en œuvre de stratégies de défense et de traque proactive. Les technologies jouent certes un rôle crucial dans la guerre contre les cyberattaques, mais le facteur humain reste l'élément catalyseur des attaques et des ripostes.

En 2018, le nombre des cyberattaques s'est envolé avec 77 % d'entreprises ayant déclaré avoir subi au moins une compromission au cours des 12 mois précédents[1]. Bien que les dépenses mondiales liées à la sécurité de l'information devraient atteindre 124 milliards de dollars, certains chercheurs estiment que le coût total du cybercrime devrait quadrupler en 2019. Il devrait ainsi s'élever à 2 100 milliards de dollars, soit 16 fois plus que les dépenses en cybersécurité[2].

L'intensification des menaces stimule la demande en personnel qualifié, créant une dynamique de l'emploi sans précédent dans ce secteur relativement récent. Tant et si bien que le taux de chômage mondial dans la cyber-sécurité ne dépasse pas les 2 % (1 % en Europe). Ainsi, entre 2018 et 2019, 53 % des entreprises (11 % en 2015) disaient pressentir une pénurie de compétences problématique dans le domaine de la cybersécurité[3] .

Une pénurie qui devrait d'ailleurs s'élever dans le monde à 3,5 millions de personnes d'ici 2022[4].

Diverses mesures sont prises pour pallier ce problème. Toutefois, plusieurs années d'efforts soutenus seront nécessaires pour maîtriser pleinement la situation. D'ici là, les entreprises devront revoir leurs stratégies à court et long terme pour y faire face en toute sécurité. Quitte à accepter quelques souffrances temporaires, le temps que des solutions plus pérennes voient le jour.

Ce livre blanc évalue et analyse l'impact de la pénurie de compétences en cybersécurité sur les entreprises et leurs salariés. Il examine également un certain nombre de stratégies pouvant être déployées pour réduire le risque de compromission.

[1] CyberEdge Group, LLC (2018). 2018 Cyberthreat Defense Report. *https://cyber-edge.com/wp-content/uploads/2018/03/CyberEdge-2018-CDR.pdf*
[2] Gartner (15 août 2018). Selon Gartner, les dépenses mondiales en matière de sécurité de l'information dépasseront les 124 milliards de dollars en 2019. *https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019*
[3] ESG, Blog (10 janvier 2019) The Cybersecurity Skills Shortage Is Getting Worse *https://www.esg-global.com/blog/the-cybersecurity-skills-shortage-is-getting-worse*
[4] Herjavec Group (2017), Cybersecurity Jobs Report. *https://www.herjavecgroup.com/wp-content/uploads/2018/07/HG-and-CV-The-Cybersecurity-Jobs-Report-2017.pdf*

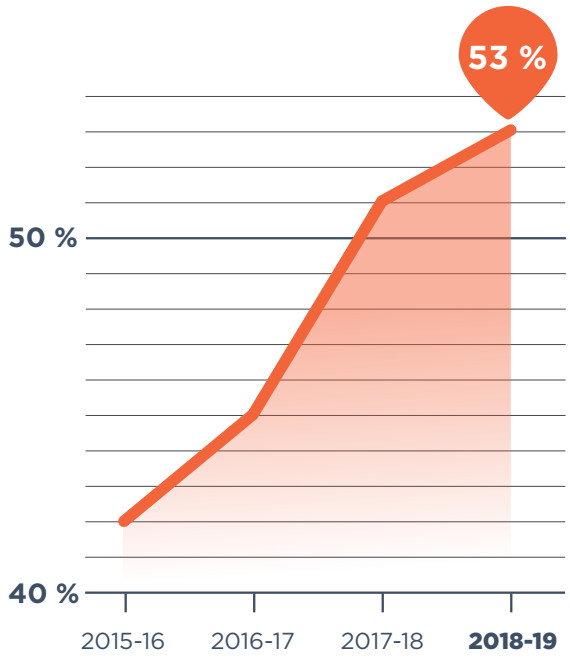
Cybersécurité : une pénurie de compétences bien réelle

Réalités commerciales

Traditionnellement, les entreprises ont vu dans les technologies la réponse aux besoins de cybersécurité. Ainsi, nombre d'entre elles pensaient que l'acquisition du dernier logiciel antivirus suffisait à protéger efficacement leurs données sensibles. Or aujourd'hui, la vérité est tout autre. En effet, tandis que les hackers travaillent sans relâche pour craquer les logiciels de sécurité disponibles dans le commerce, les solutions de mise en conformité continuent elles de présenter des brèches pour les attaquants. Côté entreprises, les salariés formés sont chargés d'intervenir en complément des outils de cybersécurité, ces derniers étant censés collecter les données, mais aussi interpréter et signaler les alertes et autres événements pour réagir de façon appropriée.

Les professionnels de la cybersécurité, eux, semblent toujours avoir un temps de retard sur les menaces qu'ils combattent. Les technologies et l'ingéniosité des cybercriminels se développent à une telle vitesse qu'elles dépassent le niveau de disponibilité et de compétences des nouveaux talents.

Figure 1 : Pourcentage des entreprises signalant une pénurie de compétences en cybersécurité



Par ailleurs, compte tenu de la diversité des besoins de cybersécurité, aucun expert ne peut prétendre à lui seul posséder toutes les compétences nécessaires à la protection d'une entreprise. Les organisations ont en effet besoin d'une très vaste palette de professionnels : analystes en traque des menaces, analystes CTI, spécialistes du désassemblage des malwares, spécialistes de la simulation d'attaques, experts de la réponse à incident, analystes des programmes de sécurité, etc.[5] Or, la pénurie croissante de ces profils ne rend la cybersécurité que plus difficile.

La multiplication des cas de burnout, la difficulté à fidéliser les talents et l'augmentation des risques de violation de sécurité sont autant d'éléments qui traduisent l'impact de cette pénurie sur les secteurs public et privé dans le monde. Certes, toutes les attaques n'aboutiront pas, mais les entreprises qui manquent de personnel qualifié auront du mal à faire face au volume et à la sophistication des menaces.

L'économie du recrutement

De nos jours, la pénurie d'experts en cybersécurité élève le salaire moyen de ces professionnels à un niveau inaccessible pour beaucoup d'entreprises. C'est particulièrement vrai pour le secteur public dont les salariés, extrêmement convoités par les cabinets de recrutement, se tournent en masse vers le privé, plus rémunérateur. Ainsi, 44 % des professionnels de la cybersécurité interrogés admettent être sollicités par un recruteur au moins une fois par semaine[6]. Autrement dit, une équipe soigneusement bâtie peut très vite partir en fumée. Dans une étude IBM de 2019, seules 30 % des entreprises déclaraient avoir dans leurs rangs suffisamment de personnel de cybersécurité, tandis que 75 % qualifiaient de « plutôt difficile » à « difficile » le recrutement et la fidélisation de salariés compétents[7].

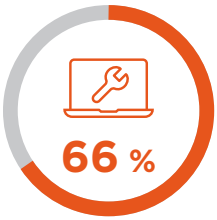
La plus forte pénurie se situe au niveau des profils de débutant à cadre moyen, c'est-à-dire du personnel en charge des tâches de sécurité tactiques et opérationnelles. Les équipes RH doivent par conséquent adopter des processus de recrutement plus rapides et plus efficaces tout en élargissant les critères de sélection des candidats. Résultat : de nombreuses entreprises se retrouvent à devoir embaucher et former des salariés débutants plutôt qu'à recruter des personnes possédant le niveau approprié de compétences en cybersécurité.

Figure 1 : ESG, ISSA (Avril 2019). Life of Cybersecurity Professionals

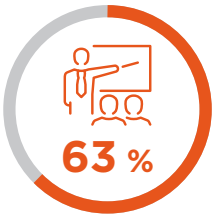
[5] FireEye – Comment renforcer votre équipe de sécurité *https://content.fireeye.com/expertise-on-demand/eb-expertise-on-demand.*

[6] ESG, ISSA (2018). The Life and Times of Cybersecurity Professionals.

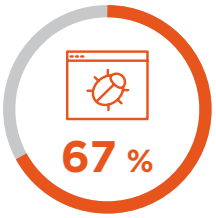
[7] IBM Security (11 avril 2019). Study on the Cyber Resilient Organization.



de professionnels de la cybersécurité reconnaissent avoir du mal à maintenir leurs compétences à jour compte tenu des impératifs de leur métier[8]



des entreprises ne proposent pas des formations adaptées aux professionnels du secteur[9]



des personnes interrogées déclarent ne disposer ni du temps ni des ressources pour résoudre chaque problème[10]

Facteurs professionnels de stress

Un gros chèque de paie ne suffit pas toujours à compenser le niveau de pression que subit un salarié. Les équipes de sécurité en manque d'effectifs et de personnels qualifiés peuvent passer un temps disproportionné à résoudre les incidents et autres problèmes prioritaires. Il n'en reste donc que très peu à consacrer à la planification, au développement de stratégies et à la formation continue.

Or, lorsque les salariés n'ont pas le temps d'actualiser leurs compétences ou qu'aucun budget n'est mis en place pour faciliter la formation, la responsabilité d'une compromission peut être injustement attribuée à l'équipe de cybersécurité. Et les conséquences sont multiples : baisse de la satisfaction au travail, taux élevé de burnout, exode des salariés vers d'autres secteurs… Pas étonnant que seuls 39 % des professionnels de la cybersécurité se disent très satisfaits de leur travail[11].

Enfin, les répercussions de la crise de personnel sur le moral des salariés peut constituer un facteur de stress supplémentaire pour les professionnels fraîchement recrutés dans le secteur.

Formation et adaptation : deux impératifs

Contrairement à de nombreux secteurs, les règles d'engagement en matière de cybersécurité ne cessent d'évoluer. Les professionnels de ce domaine doivent constamment actualiser leurs connaissances sur les nouvelles méthodes d'attaque pour protéger efficacement leurs employeurs. Seul bémol, ces derniers ne les forment pas toujours.

Ce manque de formation et de partage des connaissances représente le facteur le plus courant d'incidents de sécurité[12]. En effet, des professionnels non formés auront du mal à contrecarrer les attaquants. Selon une étude ESG récente, 47 % des professionnels de la cybersécurité se disaient incapables d'exploiter tout le potentiel de certaines de leurs technologies de sécurité en place[13]. Autrement dit, ils manquent non seulement de temps pour adopter et mettre à profit toutes les fonctionnalités, mais ils ne sont pas non plus en mesure d'utiliser et d'intégrer ces outils dans leurs systèmes.

Un cercle vicieux

Briser cette spirale négative n'est pas chose facile. Les entreprises peinent à trouver et à fidéliser du personnel qualifié. Et bien que débordés, ces professionnels ont besoin que leur employeur investissent dans la mise à jour de leurs connaissances et compétences.

Enfin, le recrutement de personnel non qualifié obère tant les salariés existants que les nouvelles recrues. Pour les premiers, cette situation se traduit généralement par une surcharge de travail pour combler l'écart. Pour les seconds, le rythme d'apprentissage et d'application des connaissances fraîchement acquises est tout simplement irréaliste. Tout cela ne fait qu'alourdir la pression qui pèse sur les équipes.

[8] ESG, ISSA (2018). The Life and Times of Cybersecurity Professionals.
[9] ESG, ISSA (2018). The Life and Times of Cybersecurity Professionals.
[10] C.Osborne (February 2 2019). One In Three Enterprises Can't Protect Themselves From Data Breaches. https://www.zdnet.com/article/one-in-three-enterprises-cant-avoid-data-breaches/
[11] ESG, ISSA (Novembre 2017). The Life and Times of Cybersecurity Professionals.
[12] ESG, ISSA (Novembre 2017). The Life and Times of Cybersecurity Professionals.
[13] ESG, ISSA (Novembre 2017). The Life and Times of Cybersecurity Professionals.

Solutions à la pénurie

SOLUTIONS À LONG TERME

Formation, modification des processus de recrutement, intelligence artificielle, externalisation des tâches spécialisées… les entreprises de toutes tailles peuvent prendre différentes mesures pour réduire leur risque.

Réduction du risque : expertise vs expérience

Pour les entreprises, une manière de combler la pénurie de compétences consiste à mettre en place un programme détaillé avec des experts et à combiner des exercices fondés sur des cas réels à des données de Threat Intelligence directement exploitables. Elles peuvent également fournir des ressources en continu pour aider les équipes à se tenir informées des tendances en matière d'attaques. Associé à de solides stratégies de fidélisation, ce type d'investissement dans le personnel existant peut se révéler rentable à long terme.

Des débutants et jeunes diplômés au personnel plus chevronné capable de se reconvertir dans la sécurité, des formations et stages en sécurité peuvent être proposés à un large éventail de profils. Naturellement, un salarié passionné et dévoué sera un excellent élève. Mais avec un programme de formation et de développement totalement immersif, il pourra devenir un atout encore plus précieux pour l'entreprise.

Toutefois, les entreprises doivent d'abord évaluer leurs besoins avant de développer ou déployer un quelconque programme de formation. Elles pourront ainsi mieux cibler et développer les compétences requises. Un plan de mentorat et d'apprentissage clair, ainsi de que des programmes agréés comportant un processus reproductible à l'arrivée de nouveaux employés, peut changer le sort d'une entreprise confrontée à une crise de compétences.

De par sa flexibilité, la formation représente une solution applicable aux entreprises de toutes tailles. Cependant, les entreprises ont besoin de protection même pendant les formations. S'associer à un partenaire externe leur permettra d'obtenir la valeur ajoutée dont elles ont besoin à court terme, surtout si ce partenaire peut assurer le mentorat de son personnel. Les plus grandes structures pourront également témoigner un intérêt pour certaines solutions d'intelligence artificielle (IA).

Adapter le processus de recrutement

La chasse aux professionnels de la cybersécurité exige des équipes RH de revoir leurs critères de recherche et méthodes de recrutement. Ici, de petits ajustements de stratégie et d'attitude pourront faire affluer une main-d'œuvre jusque-là latente. Côté processus, le recrutement de personnel qualifié et formé doit s'effectuer de manière plus réactive et proactive. De nombreuses étapes d'entretien au long cours doivent être remplacées par des procédures dynamiques et instinctives qui accélèrent la prise de décisions pour conduire à des offres d'embauche rapides. Plus une entreprise s'adapte vite, plus elle aura de chances d'accéder à des candidats mieux qualifiés.

Lorsqu'une entreprise est disposée à former ses nouvelles recrues par le biais de l'apprentissage, du mentorat ou d'une formation certifiée, ses équipes RH doivent élargir leurs critères de recherche pour identifier des pools de candidats plus vastes et plus solides. En ce sens, les universités et autres établissements d'enseignement supérieur constituent un point de départ naturel, notamment en matière d'apprentissage. De nombreuses entreprises se tournent aussi vers d'anciens combattants qui reviennent à la vie civile. Les militaires sont familiarisés avec les derniers outils informatiques. Et chez eux, mettre en œuvre des bonnes pratiques et protocoles de sécurité est une seconde nature.

Encourager la diversité dans le secteur peut également représenter un moyen de combler la pénurie de compétences. En effet, la cybersécurité ne compte aujourd'hui que 11 % de femmes. Il existe donc là une opportunité d'augmenter ce chiffre[14]. Selon une étude récente, les femmes intègrent ce secteur avec un niveau de qualification supérieur à celui des hommes. Cependant, 51 % déclarent avoir été victimes de diverses formes de discrimination[15], ce qui affaiblit leur motivation à rester dans le secteur.

Des solutions pratiques et proactives aux questions de recrutement peuvent être appliquées aux entreprises de toute taille. Les méthodes pourront varier en fonction du budget et des ressources, mais la stratégie et l'approche sous-jacentes resteront les mêmes.

[14] Frost & Sullivan (2017). Frost & Sullivan - 2017 Global Information Security Workforce Study Women In Cybersecurity.
[15] Frost & Sullivan (2017). Frost & Sullivan - 2017 Global Information Security Workforce Study Women In Cybersecurity.

SOLUTIONS À COURT TERME

Développement d'une main d'œuvre automatisée

Le potentiel de l'intelligence artificielle (IA) est évident même dans ses phases d'exploitation initiales. Les équipes novices peuvent s'en servir notamment pour analyser les menaces ou traiter des volumes massifs de données.

En matière de sécurité, l'IA suscite deux points de vue distincts. Tandis que certains la perçoivent comme difficile à adopter et à maîtriser sans formation adéquate, d'autres pensent qu'elle pourrait bonnement et simplement remplacer toute une équipe de sécurité. Ce dernier point de vue semble toutefois irréaliste. Bien qu'un dispositif de sécurité orienté IA soit capable de prédire et de détecter les premières étapes d'une attaque, voire de la neutraliser, les cybercriminels chercheront sans cesse un moyen de le renverser ou le contourner.

Il est peu probable que l'IA remplace un jour une équipe en chair et en os. Elle peut toutefois servir à automatiser les tâches de routine répétitives.

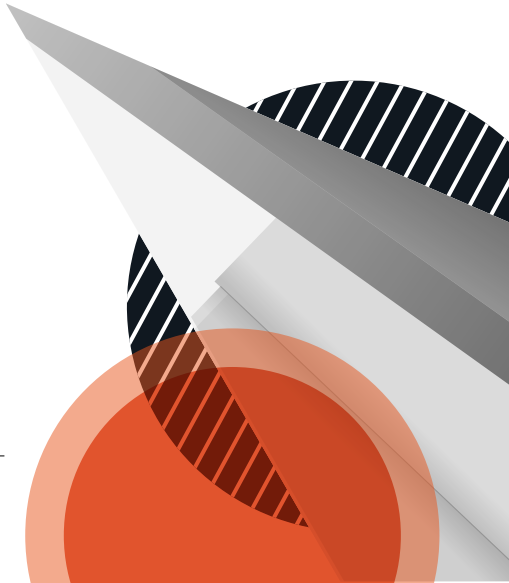
L'intégration de l'IA permet aux équipes de sécurité de se recentrer sur la planification stratégique, et sur l'analyse et la neutralisation en temps réel des menaces pour mieux protéger leur entreprise. L'IA ne convient peut-être pas à tout le monde, mais elle peut avoir une valeur inestimable pour certains.

Externaliser la cybersécurité

Les fournisseurs de services de sécurité managés (MSSP) peuvent apporter un coup de pouce immédiat ou carrément remplir les missions des équipes de sécurité internes. Pare-feu, détection d'intrusion, réseaux privés virtuels, analyse des vulnérabilités, services antivirus… les MSSP offrent une grande variété de services destinés à réduire les dépenses globales tout en donnant accès à des professionnels spécialisés. Ainsi, près de 90 % des entreprises interrogées font appel à des experts externes pour les accompagner dans leurs activités[16].

Le marché des services de cybersécurité se transforme au fur et à mesure qu'il se développe. Les offres des MSSP se dynamisent. Il devient aussi de plus en plus courant de combiner des produits de sécurité et des services opérationnels à une Threat Intelligence de première ligne. Les entreprises peuvent ainsi exploiter tout le potentiel de leurs solutions de sécurité tout en améliorant leurs compétences internes.

Le nombre de MSSP sur le marché est en pleine explosion, une hausse qui tient en partie à la décision de professionnels de la sécurité déçus et épuisés d'opter pour un parcours plus lucratif.



[16] CyberEdge Group, LLC (2017). 2017 Cyberthreat Defense Report. *https://cyber-edge.com/wp-content/uploads/2017/03/CyberEdge-2017-CDR-report.pdf*

Conclusion

La nature et la sévérité de la pénurie de compétences en cybersécurité sont depuis quelques temps au cœur de nombreux débats sur les réseaux sociaux, dans les organismes sectoriels et dans les entreprises.

Aujourd'hui, très peu de secteurs sont confrontés à un paysage aussi dynamique et destructeur que celui de la cybersécurité. Et à cela il n'existe pas de solution miracle, pour la simple et bonne raison que les professionnels du secteur, aidés des technologies, sont encore loin de maîtriser la situation.

Toutefois, un certain nombre de solutions à court et à long terme visant à réduire le risque de violation de sécurité sont disponibles pour les entreprises de toutes tailles – la formation du personnel étant la plus répandue. Qu'il s'agisse de former de nouvelles recrues motivées, mais manquant de l'expertise nécessaire, ou de mettre à jour les connaissances d'équipes en place, la formation s'est révélée maintes fois comme la solution par excellence au déficit de compétences. Accessible aux petites comme aux grandes entreprises, la formation représente un moyen efficace de fidéliser les équipes à l'heure où les pressions professionnelles et les techniques agressives de recrutement sont à leur maximum.

Pour les PME et grandes entreprises, la Threat Intelligence et le support de première ligne fournis par les MSSP constituent une voie privilégiée. Très réactifs au marché, de nombreux fournisseurs proposent des services qui protègent et forment simultanément leurs clients.

La bonne combinaison de solutions ne peut être déterminée que par chaque entreprise, en fonction de ses besoins, de son exposition perçue au risque et, bien entendu, de ses budgets. Et pour réussir, chacune d'elles doit être consciente des risques et des avantages générés par les solutions actuellement disponibles, à court et à long terme.

Pour en savoir plus sur le service FireEye Expertise On Demand, rendez-vous sur **www.fireeye.fr/solutions/expertise-on-demand**

FireEye, France
Nextdoor Cœur Défense,
110 Esplanade du Général de Gaulle,
92931 Paris La Défense Cedex 92974
+33 1 70 61 27 26
france@FireEye.com

À propos de FireEye

FireEye est spécialisé dans la cybersécurité axée sur la Cyber Threat Intelligence (CTI). Prolongement naturel et évolutif des opérations de sécurité des clients, la plateforme unique de FireEye combine des technologies de sécurité innovantes, des services de CTI d'envergure internationale et les services réputés de Mandiant® Consulting. FireEye simplifie ainsi la cybersécurité et son administration, devenant un allié précieux des entreprises confrontées au casse-tête que représentent la prévention et la neutralisation des cyberattaques.

FIREEYE™