Pénurie de compétences : quelles solutions ?

Étude sur la pénurie internationale de compétences en cybersécurité

La pénurie mondiale de talents formés et qualifiés ne fait qu'exacerber le problème tout aussi complexe de la protection contre un volume croissant de menaces toujours plus avancées et sophistiquées. Le CSIS (Center for Strategic and International Studies) a mené une étude afin de quantifier le manque de personnel de cybersécurité dans huit pays, à savoir l'Allemagne, l'Australie, les États-Unis, la France, Israël, le Japon, le Mexique et le Royaume-Uni. Menée auprès des décideurs informatiques des secteurs public et privé, l'étude portait sur quatre aspects clés du développement des talents en cybersécurité : les dépenses en sécurité, les programmes d'études et de formation, la dynamique des employeurs et les politiques gouvernementales. Elle offre des informations précieuses susceptibles d'aider les entreprises et les pouvoirs publics à développer un vivier plus riche et durable de talents dotés des compétences requises. L'étude propose également plusieurs recommandations concrètes pour pallier la pénurie de talents actuelle et améliorer la cybersécurité à l'échelle mondiale.

Principales observations

- La pénurie de talents en cybersécurité est généralisée. D'après l'étude menée par le CSIS, 82 % des participants reconnaissent être confrontés à une pénurie de compétences en cybersécurité au sein de leur entreprise. L'offre limitée et la demande élevée de professionnels de la cybersécurité a également contribué à une hausse des salaires. Aux États-Unis, les emplois dans ce domaine offrent une rémunération près de 10 % supérieure à celle d'autres fonctions informatiques.
- La pénurie de talents rend les organisations plus vulnérables aux attaques. C'est en tout cas l'avis de 71 % des personnes interrogées. Un répondant sur quatre estime que le manque de personnel de cybersécurité a joué un rôle dans le vol ou les fuites de données et l'atteinte à la réputation.
- La demande de certaines compétences est forte. Parmi les compétences les plus demandées dans les huit pays, citons la détection des intrusions, le développement de logiciels sécurisés et la neutralisation des attaques.

- Une formation pratique est le meilleur moyen d'acquérir des compétences en cybersécurité. Alors qu'environ 50 % des décideurs interrogés considèrent un baccalauréat dans une discipline technique pertinente comme un critère minimum d'embauche pour un poste de premier échelon, la plupart des répondants estiment que l'expérience, les compétitions de piratage éthique et les certifications professionnelles sont préférables à un diplôme pour acquérir des compétences en cybersécurité.
- La technologie peut compenser dans une certaine mesure la disette de talents. Près de neuf répondants sur dix ont déclaré que les technologies de sécurité peuvent contribuer à pallier les lacunes et 55 % d'entre eux estiment que, d'ici cinq ans, les solutions de cybersécurité seront suffisamment évoluées pour répondre aux besoins de leur entreprise. Par ailleurs, ils externalisent les processus et fonctions de sécurité susceptibles d'être automatisés.
- Les pouvoirs publics n'investissent pas suffisamment dans la cybersécurité. 76 % des personnes interrogées estiment que leur gouvernement n'investit pas assez dans des initiatives de développement des talents en cybersécurité et que la législation et les réglementations de leur pays en matière de sécurité informatique sont inadaptées.

Les quatre dimensions de la pénurie en personnel de cybersécurité

Dépenses en cybersécurité

Selon les estimations, les dépenses mondiales en cybersécurité devraient franchir la barre de 100 milliards de dollars d'ici quatre à cinq ans[1]. Ce sont les pouvoirs publics américains et les services financiers, cibles de choix des pirates, qui consomment et dépensent le plus en technologies et services de cybersécurité. Grâce à leurs investissements considérables en cybersécurité, ces deux secteurs sont mieux armés pour faire face à la pénurie de personnel et définir de bonnes pratiques de formation et d'embauche.

Études et formations

Comme le CSIS le souligne dans son rapport, si un diplôme universitaire peut être une condition requise pour les emplois de cybersécurité, la plupart des décideurs estiment qu'un apprentissage pratique axé sur l'expérience est la meilleure formation qui soit. Seuls 23 % des répondants estiment en effet que les programmes d'enseignement préparent les étudiants à un travail dans le secteur. D'après l'étude, ce sont les États-Unis et le Royaume-Uni qui investissent le plus à l'heure actuelle dans les études en cybersécurité, tandis que le Mexique, la France et le Japon arrivent en queue de peloton. Plus de trois quarts des personnes interrogées considèrent les certifications professionnelles comme un moyen efficace de démontrer des compétences. Et deux répondants sur cinq déclarent que les compétitions de piratage éthique constituent une excellente formule pour acquérir des compétences.

Dynamique des employeurs

Quelles sont les principales stratégies de recrutement pour attirer et retenir les professionnels de la sécurité informatique ? Le salaire arrive en tête de liste, suivi de la formation, de la réputation du service informatique et des possibilités de promotion. Près de 50 % des participants déclarent que le manque de formation ou de soutien des programmes de certification est l'un des motifs de départ les plus souvent invoqués par les employés. Comme il faut souvent du temps pour mettre en place une équipe de cybersécurité compétente et expérimentée, les entreprises se tournent vers les technologies pour pallier les lacunes. Environ neuf répondants sur dix estiment que les avancées technologiques en cybersécurité pourraient compenser le manque de compétences du personnel. L'externalisation de certaines fonctions de sécurité, notamment l'évaluation et la limitation des risques, la gestion de l'accès et la surveillance réseau ainsi que la restauration des systèmes compromis, est aussi une alternative largement acceptée. Plus de 60 % des répondants externalisent au moins une partie de leurs processus et fonctions de cybersécurité.

Politiques gouvernementales
De nombreux pays, dont les États-Unis, le Royaume-Uni, Israël et l'Australie, soutiennent de plus en plus les initiatives cherchant à résoudre le problème de pénurie de talents en cybersécurité. La plupart des pays possèdent aussi une législation visant tout particulièrement à améliorer les cursus de formation en cybersécurité. Cependant, plus de 75 % des répondants estiment que leur gouvernement n'investit pas suffisamment dans le développement de talents dans ce domaine et un pourcentage identique juge que les lois et les réglementations nationales en matière de cybersécurité sont insuffisantes.

Recommandations

Redéfinissez les conditions minimales d'embauche pour des postes de cybersécurité de premier échelon et acceptez les sources non traditionnelles de formation.
Comme il existe très peu d'universités et hautes écoles proposant des cursus en cybersécurité, tous pays confondus, les résultats de l'étude de CSIS suggèrent que les responsables de l'embauche devraient accorder une plus grande valeur aux certifications professionnelles et à l'expérience pratique par rapport aux diplômes. Les universités et les lycées devraient commencer à offrir ce type de formation pratique en cybersécurité pour aider les jeunes talents à perfectionner leurs compétences. Ce type de programmes représente, pour les pouvoirs publics, le secteur privé et celui de l'enseignement, l'occasion de collaborer ensemble à l'amélioration des cursus et de proposer des formations et des stages.

Améliorez la diversité dans le secteur de la cybersécurité.
Plusieurs études révèlent que les femmes et les minorités sont sous-représentées dans ce secteur. En outre, des politiques d'immigration strictes réduisent le réservoir de personnel hautement qualifié dont a cruellement besoin le secteur de la cybersécurité. Il est possible d'enrichir rapidement le vivier de talents en cybersécurité aux États-Unis et dans d'autres pays présentant des conditions d'immigration similaires en augmentant le nombre de permis de travail et en incluant les minorités et les femmes. Un autre obstacle au développement du personnel dans ce domaine est l'ostracisme vis-à-vis des anciens pirates informatiques. Les employeurs doivent faire preuve de plus d'indulgence vis-à-vis des anciens « hackers » car ils possèdent souvent des connaissances et des compétences inestimables.

Proposez davantage d'opportunités de formation externe.
Les programmes de formation continue sont essentiels pour conserver les talents dans la mesure où l'absence de telles initiatives incite souvent les collaborateurs à chercher un emploi ailleurs. Les pouvoirs publics et le secteur privé devraient envisager de collaborer afin d'améliorer les opportunités de formation pour les étudiants et les employés qui souhaitent perfectionner leurs compétences.

Développez de nouvelles compétences en vue de l'automatisation.
L'étude du CSIS révèle que les entreprises cherchent à automatiser certaines fonctions de cybersécurité afin de compenser le manque de compétences. Dès lors, le personnel de cybersécurité se verra contraint d'adapter ses compétences à ces nouveaux processus. Comme l'automatisation optimise l'efficacité opérationnelle, les professionnels du secteur pourront consacrer davantage de temps et mieux exploiter leurs compétences dans d'autres domaines, notamment la détection, l'analyse et la neutralisation de menaces plus évoluées.

Collectez des données et développez des indicateurs plus précis.
La collecte de données sur le marché de l'emploi dans le domaine de la cybersécurité et la normalisation des fonctions peuvent permettre au secteur privé, aux pouvoirs publics et au secteur de l'enseignement de développer une taxinomie commune de compétences en cybersécurité clairement définies et applicables à tous les secteurs de l'industrie.

Conclusion

La compétence du personnel est plus indispensable que jamais au déploiement d'une sécurité efficace. Il est possible de pallier la pénurie mondiale de talents en cybersécurité en dirigeant des personnes plus talentueuses dans cette voie grâce à des cursus mieux conçus, à une plus grande diversité, à de nouvelles opportunités de formation, à l'adoption de technologies de sécurité et à la collecte de données.

Consultez la page **mcafee.com/skillsshortage** pour lire le rapport complet.

1. http://www.forbes.com/sites/stevemorgan/2016/02/12/cybersecurity-market-outlook-for-2016-to-2020/#185c567a74a4

McAfee. Part of Intel Security.
Tour Pacific
13, Cours Valmy - La Défense 7
92800 Puteaux
France
+33 1 47 62 56 09 (standard)
www.intelsecurity.com