5 bonnes raisons de se former à la cybersécurité

Le même refrain se répète d'année en année : les experts en cybersécurité sont en nombre insuffisant au regard des besoins des entreprises. Face à cette pénurie, une solution : se former.

Les cyberattaques se multiplient en France comme à l'international. Un fléau invisible qui préoccupe autant les entreprises que les États. Face à cette menace, *« il manque 18.000 personnes dans les entreprises sur le secteur de la cybersécurité* », souligne Arthur Bataille, CEO de Seela, plateforme de formation en cybersécurité pour les acteurs de la tech.

Pour se constituer des remparts et pallier le manque de ressources, les entreprises misent donc sur l'évolution des compétences en attirant des professionnels de l'informatique tels que les développeurs qui n'ont pas encore les compétences adéquates aujourd'hui, mais peuvent devenir des profils compétents demain. La demande est telle que 70% des professionnels de la cybersécurité assurent être sollicités par des recruteurs au moins une fois par mois. Voici les raisons pour lesquelles se former à la cybersécurité est une bonne idée.

1. Il y a une urgence locale, nationale et internationale

Vols de données de santé aux Hôpitaux de Paris, attaques contre les

assurances, mais aussi contre les collectivités territoriales… En 2021, l'Agence nationale des systèmes d'information (ANSSI) a enregistré 1082 intrusions qui auraient pu atteindre la sécurité du pays. D'après Seela, formation en ligne de cybersécurité pensée comme une plateforme de streaming, les cyberattaques ont augmenté de 500% ces deux dernières années. Et les tensions internationales, comme la guerre en Ukraine, ont montré que désormais, le cyberespace était aussi un terrain de combat lors d'un conflit. Les entités françaises tout comme les entreprises, ont de plus en plus besoin d'anticiper ces événements et de limiter leurs conséquences.

2. On manque de ressources

« De nombreuses entreprises ont des besoins en cybersécurité mais n'arrivent pas à trouver des personnes compétentes », assure Arthur Bataille. Il y a donc une réelle pénurie de ressources humaines. On estime d'ailleurs que 70% des entreprises dans le monde manquent de spécialistes en sécurité informatique et qu'il faudrait en former plus de quatre millions pour répondre aux besoins du marché actuel. Problème : *« nous ne sommes structurés ni en France, ni à l'étranger pour faire face à cela »*. Les entreprises françaises n'ont donc pas la possibilité de recruter des talents venant d'autres pays qui auraient pu être davantage spécialisés dans le domaine car *« ils sont déjà ultra sollicités dans leur propre pays »*. C'est dans ce contexte que Seela collabore d'ailleurs avec le gouvernement français pour mieux former les acteurs de la tech sur ce sujet prioritaire.

3. C'est un secteur d'activité en plein boom

76% des organisations estiment alors qu'il est extrêmement difficile de recruter des professionnels en cybersécurité, compte tenu du décalage entre l'offre et la demande. Le secteur de la cybersécurité est donc en plein recrutement et Arthur Bataille l'assure : *« s'engager dans la cybersécurité est promesse d'augmenter fortement son salaire et de n'avoir aucun problème d'employabilité. »* D'autant que les dépenses allouées à la cybersécurité ont été majorées de 40% entre 2020 et 2021, pour les entreprises et les administrations.

À lire aussi

Les 10 erreurs de cybersécurité des startups technologiques

4. On peut se former en ligne

Les entreprises se tournent de plus en plus vers des organismes de formation pour permettre à leurs collaborateurs de faire évoluer leurs compétences. Et la cybersécurité n'échappe à la règle. Plateforme moderne et ludique à la Netflix, Seela propose par exemple une formation 100% online qui allie théorie (plus de 700 heures de cours) et pratique (grâce à des travaux dirigés, pratiques et "Capture the flag", jeu qui consiste à exploiter des vulnérabilités affectant des logiciels de manière à s'introduire sur des ordinateurs pour récupérer des drapeaux). Celle-ci est accessible 7 jours sur 7, 24 heures sur 24. Ce qui permet aux participants de se former quand ils le souhaitent de façon indépendante.

Un soulagement pour les 59% de professionnels de la cybersécurité qui reconnaissent qu'il est compliqué de trouver des formations adaptées à leur emploi du temps. *« Les parcours de formation sont également pensés pour différents métiers – DevSecOps, NetSecOps, Lead Auditor et Ethical Hacker – et un test de positionnement à l'arrivée sur la plateforme permet de cibler le niveau de la personne. Un débutant sera accompagné afin de progresser, quand une personne plus avancée pourra mettre à jour ses compétences et continuer à les développer »*, précise Arthur Bataille.

Et pour cause, 91% des professionnels pensent qu'il est nécessaire de maintenir à jour ses compétences en cybersécurité pour protéger leur organisation des cyber-adversaires. *« Aujourd'hui, des aptitudes en cybersécurité rendent un profil très employable mais demain cela sera un prérequis donc si les professionnels du domaine ne veulent pas assister à une obsolescence de leurs connaissances, ils doivent se former et monter en compétences »,* prévient le dirigeant de Seela.

5. Se spécialiser selon son territoire, c'est possible

L'ancrage territorial est primordial lorsqu'on se forme à la cybersécurité. En effet, dans certaines régions du sud, la cybersécurité sera davantage axée sur les données spatiales que dans la région grenobloise, où il s'agira plutôt de cybersécurité industrielle. Une formation adaptée permet ainsi de se spécialiser dans les problématiques et les enjeux du territoire où l'on vit.

AUTRES OPTIONS POUR SE FORMER À LA CYBERSÉCURITÉ

En plus de plateformes comme Seela, il est possible de devenir ingénieur en cybersécurité grâce à des masters d'écoles d'ingénieurs telles que Télécom ParisTech, Epita ou l'ESIEA. Il existe un label, SecNumedu, qui permet d'encadrer et d'améliorer le référencement des formations en cybersécurité de l'enseignement supérieur, que ce soit pour des cursus classiques ou des alternances. Ce label s'appuie sur un référentiel élaboré par l'ANSSI avec la contribution d'industriels, d'écoles, du Pôle d'Excellence Cyber (PEC) et du ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche.

Maddyness, partenaire média de Seela

Article écrit par MADDYNESS, AVEC SEELA