

COMMUNIQUÉ DE PRESSE

Paris, le 25/03/2024

Nouvelle enquête de l'Observatoire des métiers de la cybersécurité : 3 actions essentielles pour faire face à la pénurie de talents

Pour la troisième année consécutive, l'ANSSI présente sa nouvelle enquête sur [« L'attractivité et la représentation des métiers de la cybersécurité vues par les professionnels »](#) de l'Observatoire des métiers de la cybersécurité, réalisée en collaboration avec la DGEFP et l'AFPA, qui aide les entreprises dans leur politique de recrutement, les organismes de formation ainsi que les étudiants et salariés en reconversion. Vouée à mettre en miroir la « réalité de terrain » vécue par les professionnels du secteur et la perception des jeunes en formation, cette étude effectuée en 2023 met en lumière 3 actions indispensables pour faire face à la pénurie de talents cyber : travailler l'image du secteur, mieux structurer la filière et améliorer les conditions de travail.

Une évolution constante de la menace cyber qui oblige à l'action sur le terrain pour contrer la pénurie de talents

Alors que le [Panorama de la cybermenace 2023](#) de l'ANSSI fait état d'un niveau de la menace en constante augmentation, avec des attaquants qui ne cessent de s'améliorer et de saisir toutes les opportunités, entreprises et administrations se doivent de renforcer leurs capacités de défense. En conséquence il apparaît indispensable pour chaque organisation de pouvoir s'appuyer sur des professionnels qualifiés dans le domaine de la sécurité des systèmes d'information (SSI).

Or, la pénurie de talents en cybersécurité que connaît actuellement le secteur engendre de grandes difficultés dans le recrutement et une forte tension sur le marché du travail. Dans son enquête menée auprès de plus de 2 250 personnes, en 2023, l'Observatoire des métiers de la cybersécurité de l'ANSSI dévoile 3 leviers indispensables pour y faire face.

Une image du secteur à travailler

Si professionnels et jeunes en formation s'accordent à dire que la cybersécurité est un domaine d'importance majeure, d'avenir, créateur d'emploi et en évolution permanente, la comparaison de leurs visions respectives démontre une certaine méconnaissance de la réalité du terrain par les étudiants.



**RÉPUBLIQUE
FRANÇAISE**

*Liberté
Égalité
Fraternité*



À titre d'exemple, 80% des professionnels estiment que l'exercice des métiers requière un fort relationnel, tandis qu'ils ne sont que 62% parmi les jeunes en formation « cybersécurité » à le penser, et seulement

48% parmi les jeunes en cursus « informatique ». Par ailleurs, si les publics en formation pensent que la cybersécurité n'est exercée majoritairement que par des personnels très qualifiés dans ce domaine (à plus de 83% toutes disciplines de formations confondues), les professionnels ne sont d'accord avec cette proposition qu'à 65%. L'étude démontre également que seuls quelques métiers sont facilement identifiables par les jeunes en formation ou par le grand public : consultant en cybersécurité ou encore *pentester* (même s'ils sont loin de représenter la majorité des emplois dans ce domaine), notamment parce que l'on entend davantage parler d'eux dans les médias ou l'actualité.

Face à ces constats, l'essentiel des propositions faites par les professionnels au cours de l'enquête visent à améliorer la communication sur la filière. Pour favoriser l'orientation vers les cursus numériques et la cybersécurité, il conviendrait selon eux d'aller vers une éducation aux usages numériques et à la cybersécurité, de démystifier et diversifier les représentations du secteur, ou bien encore de développer une culture cyber sociétale et professionnelle.

Une filière à mieux structurer

L'image élitiste et très technique des métiers reste prégnante. Si les professionnels sont, en majorité, qualifiés, ils plaident pour une démocratisation des profils et des parcours pouvant amener à la cybersécurité. En effet, les professionnels ne sont pas tous des « natifs cyber ». Les professionnels issus du secteur du public mettent également en avant le manque de parcours d'expertise « cybersécurité » au sein de la fonction publique. De leurs côtés, les professionnels du privé constatent le manque de lisibilité des possibilités d'évolution entre les métiers ou les domaines de compétences. Enfin, l'offre de formation paraît assez peu lisible. Elle est difficile à identifier et à apprécier.

Pour pallier ces problèmes, les professionnels suggèrent d'élargir les profils recrutés en favorisant les reconversions professionnelles ou la prise en compte des compétences acquises en dehors des cursus de formation habituels. Ces derniers suggèrent aussi de proposer des carrières en accompagnant les mobilités et les recrutements par le biais d'une structuration de métiers de différents niveaux de qualification, ou encore un travail sur les offres d'emploi ou les opportunités de recrutement qui ne semblent pas aujourd'hui être en correspondance avec les pratiques des employeurs pour ce type de poste. Enfin, les professionnels invitent à développer les filières de formation en mettant notamment en place des spécialisations dès le lycée.

Des conditions de travail à améliorer

Enfin, les conditions de travail doivent être améliorées en proposant notamment un meilleur équilibre vie privée / vie professionnelle, certains métiers (tels que ceux du conseil) semblant permettre actuellement une meilleure balance que d'autres (tel que la gestion et sécurité de projets). Par ailleurs, seuls 63% des professionnels sondés estiment avoir un métier reconnu et valorisé socialement. Dans les entités non spécialisées, les professionnels soulignent le manque de considération interne pour leurs métiers.



**RÉPUBLIQUE
FRANÇAISE**

*Liberté
Égalité
Fraternité*



Outre le développement dans le secteur privé d'une culture cyber essentielle pour pallier ce ressenti – tant sur l'acculturation des directions pour que la cyber devienne un enjeu stratégique que sur le besoin de susciter l'adhésion de l'ensemble des collaborateurs – le levier de la rémunération n'est pas à négliger dans le secteur public. Le déficit de rémunération et le type de contrats, parfois qualifiés de peu attractifs, sont les leviers principaux à faire évoluer afin de parvenir à conserver les talents. Travailler sur l'attractivité des contrats proposés et sur les différences de rémunération permettra de mieux fédérer les professionnels du secteur public sur un marché du travail en forte tension.

« Si le travail mené par l'Observatoire met en lumière les grandes différences entre une vision « stéréotypée » des jeunes et la réalité du terrain vécue par les professionnels, elle permet également de se projeter sur les actions indispensables pour faire face à la pénurie de talents. Ces leviers sont un défi que nous devons tous relever pour continuer à renforcer nos capacités de défense de la Nation. » précise Vincent Strubel, Directeur général de l'ANSSI.

À PROPOS DE L'ANSSI

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée par le décret n°2009-834 du 7 juillet 2009 sous la forme d'un service à compétence nationale.

L'agence est l'autorité nationale en matière de cybersécurité et de cyberdéfense. Elle est rattachée au Secrétaire général de la défense et de la sécurité nationale (SGDSN), sous l'autorité du Premier ministre.

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI - 51, boulevard de la Tour-Maubourg - 75700 PARIS 07 SP

www.ssi.gouv.fr   

Contacts Presse

presse@ssi.gouv.fr

06 49 21 63 80

Roxane ROSELL

roxane.rosell@ssi.gouv.fr

Leïla LEGRAND

leila.legrand@ssi.gouv.fr

Victor PLOUÉ

victor.ploue@ssi.gouv.fr