CYBERSÉCURITÉ ET EMPLOI : « La demande des entreprises devrait être forte et stable pour plusieurs années »

Hervé Mafille, fondateur du cabinet UVU GROUP spécialisé dans le recrutement sur les métiers de la cybersécurité. Actif depuis 2016 dans ce domaine, il nous livre sa lecture de ce marché en pleine explosion marquée par un véritable déséquilibre entre la demande des entreprises et les profils à recruter. Explications.

Hervé Mafille

Bio express
Hervé Mafille, après 15 années évolutives en conseil IT et digital, fonde un cabinet de recrutement et management de transition spécialisé en cybersécurité en 2016. Membre de plusieurs centres de réflexion pour dirigeants et dans le domaine de la cybersécurité – sûreté, il est également intervenant extérieur en formation Bac+5, et mène en parallèle des activités de conseil et coaching auprès de dirigeants.

Dans un contexte où le risque cyber est de plus en plus prégnant et important se pose la question des compétences et des talents. Comment se porte le marché et quelles sont les perspectives de carrière qu'il peut offrir ?
Globalement, le recrutement des cadres en 2022 est très actif. En cybersécurité, le constat semble encore plus sensible, car la pénurie de profils dans ce domaine présente une asymétrie durable encore pour quelques années. Le marché est certes tendu, néanmoins, les entreprises ne veulent pas non plus recruter des talents ne répondant pas à leurs attentes (soft skills et hard skills).
Côté candidats, nous voyons deux optiques. Nous accompagnons parfois des candidats en reconversion en cybersécurité qui peinent à trouver des entreprises. Pour les candidats présentant les qualifications et compétences souhaitées par le marché, vous l'aurez compris, il y a un réel boulevard : des projets de transformation très intéressants, des budgets, et des parcours qui peuvent avoir un accélérateur formidable à condition de faire les bons choix et d'avoir la bonne attitude. Les salaires sont alors en conséquence.

Comment les métiers de la cybersécurité ont-ils évolué au cours des dernières années ?
Je souhaite tout d'abord indiquer que l'ANSSI a publié une liste des métiers de la cybersécurité, cela pourra intéresser celles et ceux qui voudront creuser la question. Si nous prenons le terme de cybersécurité dans un sens large, il y a une multitude de métiers et d'expertises connexes. Ces métiers peuvent parfois évoluer avec les menaces et les avancées technologiques, c'est le cas notamment avec la sécurité cloud, le quantique l'IA… et parfois de nouveaux métiers apparaissent ou évoluent (négociateur de ransomware, expert en M&A Cyber Due Diligence…). Les solutions innovantes actuellement développées par les startups (FrenchTech, pôle d'excellence cyber, Campus Cyber…) vont probablement faire éclore de nouvelles expertises, de nouveaux métiers ou de nouvelles facettes de ces métiers.

Quels sont les profils mais aussi les compétences recherchées par vos clients ?
Les projets de transformation numérique trouvent dans la cybersécurité le point d'appui nécessaire à l'effet de levier recherché par les entreprises. Dès lors, il y a beaucoup de tension sur les expertises en sécurité cloud, et c'est également le cas pour les compétences en analyse des risques cyber et GRC. Nous accompagnons par exemple de plus en plus de star-up qui investissent et rassurent leurs parties prenantes avec une démarche ISO27001.

Comment appréhendez-vous la complexité du marché aujourd'hui ?
La question pour les candidats en cybersécurité n'est pas de savoir s'ils vont trouver

“Les entreprises qui veulent recruter aujourd’hui doivent avoir en tête qu’elles doivent proposer des projets de qualité, et être réactives pour mener les entretiens, car en général les candidats signent un nouveau poste en 2 à 3 semaines.”

un emploi, mais plutôt de savoir sur quel projet les candidats vont être stimulés, progresser, trouver du sens.
Il ne faut pas oublier que le domaine est en perpétuel mouvement.
Les entreprises qui veulent recruter aujourd’hui doivent avoir en tête qu’elles doivent proposer des projets de qualité, et être réactives pour mener les entretiens, car en général les candidats signent un nouveau poste en 2 à 3 semaines.
La période de Covid a également mis en exergue des souhaits d’organisation du travail à distance, qui sur certains métiers de la cybersécurité sont possibles, mais sur d’autres semblent toutefois plus compliqués à mettre en œuvre.

Comment voyez-vous la demande évoluer sur les prochaines années ?
La demande des entreprises devrait être forte et stable pour plusieurs années.
Notre démarche est de faire l’adéquation entre des compétences et des souhaits de réalisation personnelle afin de les mettre en lumière sur des projets d’entreprise. Lorsque cette adéquation s’opère, les recrutements prennent une toute autre dimension.

Quelles pistes de réflexion pourriez-vous partager avec notre lectorat sur ce sujet ?
Parmi les sujets notables, il y a tout d’abord une augmentation de professionnels de la cybersécurité qui ont quitté le statut de salarié pour travailler en freelance. Il pourra certes se poser la question de l’employabilité à long terme sur certaines expertises en cybersécurité qui pourraient être automatisables, mais la demande du marché est bien présente.
De manière générale, la gestion de carrière individualisée sera importante à garder en tête, autant pour les freelances, que pour les entreprises, car il y a encore assez peu de démarche GPEC spécifique à ces expertises pointues. Ensuite, nous avons vu une réelle prise en compte par les instances dirigeantes des enjeux de cybersécurité. Certaines entreprises ont créé des fonctions de direction cybersécurité, ceci impliquant la prise en compte des enjeux de cybersécurité à un niveau stratégique, et non plus seulement tactique.
De même, le sujet de la cybersécurité se discute entre professionnels des fusions-acquisitions au-delà des grands cabinets de conseil accompagnant les entreprises du CAC40 et du SBF120. Nous accompagnons d’ailleurs plusieurs RSSI/CISO qui ont renforcés leurs compétences sur des formations certifiantes en finance par exemple, ou encore en se formant sur des Executive MBA.

Cet ouvrage a été organisé de manière à faciliter les dialogues entre les différentes parties prenantes des fusions-acquisitions, d’une part les experts de la finance et de la cybersécurité entre eux, et d’autre part les fonctions dirigeantes à la fois avec ces experts, mais aussi entre cédants et repreneurs. À la lecture de ce livre, les experts en cybersécurité pourront envisager de nouveaux angles de vue sur les enjeux de finance et un vocabulaire leur permettant de démontrer l’importance des investissements qu’ils demandent, les experts en finance gagneront en compréhension des enjeux de cybersécurité et des indicateurs pour les mesurer, puis les dirigeants et administrateurs indépendants pourront mieux piloter la stratégie et avoir une influence sur les sujets majeurs.
Finance et cybersécurité étant des domaines de haute expertise, il importe aux dirigeants de pouvoir bien s’accompagner dans les opérations de fusions-acquisitions et d’avoir des points de repère pour piloter les équipes et prestataires. Il importe également aux dirigeants de faciliter les dialogues entre les intérêts parfois divergents des repreneurs et cédants, et c’est finalement en ce sens que ce livre pourra permettre une prise de hauteur sur les sujets majeurs à évoquer dans le cadre des négociations.
Ce livre ne prétend pas apporter une méthode seule et unique, chaque opération de M&A étant spécifique. Le livre permet d’ouvrir le débat sur la prise en compte des risques cyber en PME et ETI. Il permet d’identifier certaines mesures correctrices à prendre avant la signature d’un deal, et potentiellement ainsi d’éviter des écueils post-acquisitions.
Ce livre intéressera également tout étudiant se destinant à des métiers touchant à la sécurisation et la valorisation de l’entreprise.