

POUR DES RECRUTEMENTS SUR-MESURE en Cybersécurité

C'est à l'aune du digital que les besoins des entreprises en termes de compétences en IT et en cybersécurité sont en perpétuelle évolution. **Rencontre avec Hervé Mafille, Président fondateur d'uVu Group.** Il nous en dit plus sur le cabinet et les principales tendances qui marquent le marché.



Hervé Mafille

Bio express

Après 15 ans d'expériences évolutives en cabinet de conseil et ESN avec un périmètre de responsabilité jusqu'à 140 ingénieurs, Hervé Mafille a créé le cabinet uVu Group en 2016 dans une volonté d'entreprendre et de tester de nouveaux modèles en réseau. 4 années riches pendant lesquelles il s'est également formé en parallèle notamment sur ISO 27001 et auprès du CRA (LBO), de la FFA (Franchise) puis de l'ESSEC (Finance) afin de pouvoir comprendre et challenger des candidats de haut niveau. Hervé Mafille est par ailleurs membre de plusieurs cercles de réflexion dont le Cluster maritime, Clusif (Cybersécurité), Medef et IFA (Gouvernance)...

Présentez-nous uVu Group et ses principaux vecteurs de différenciation.

Cabinet de chasse de tête et de management de transition spécialisé en cybersécurité, uVu Group a vu le jour en 2016. Fort d'un réseau d'experts, managers et dirigeants confirmés des secteurs de l'IT et de la Cybersécurité, le cabinet accompagne les ETI et les groupes internationaux à trouver les compétences en adéquation avec leurs besoins et valeurs, et ce, de manière durable.

Nous sommes un cabinet français qui intervient en Europe de l'ouest, Montréal et Singapour avec un fonctionnement de confiance conformément à nos valeurs fondatrices notamment :

- L'écoute pour comprendre le plus finement possible les attentes, potentiels et besoins de nos clients et candidats ;
- La bienveillance pour apporter une véritable plus-value et un impact positif dans nos prestations ;
- L'humanisme avec la quête de sens et la recherche constante d'un leadership positif ;
- Le pragmatisme pour assurer la parfaite adéquation entre les compétences / motivations des candidats avec les attentes / projets d'entreprises ;
- L'indépendance pour proposer à nos candidats et clients des échanges équilibrés, sans pensée unique ni lien de dépendance.

Dites-nous-en plus sur votre positionnement.

Notre mission est d'accompagner les dirigeants d'ETI et groupes internationaux dans leurs stratégies de croissance à la fois interne via des offres de recrutement et de management de transition mais aussi externes avec des offres de Cyber Due Diligence. De notre point de vue, la chasse de tête est un moyen d'accompagner

le dirigeant dans sa stratégie, notre spécialisation concerne la gestion des risques d'entreprise et cybersécurité, des profils techniques aux profils de direction. Sur les fonctions de sécurité et de sûreté, nous sélectionnons notamment des officiers généraux issus des différents corps d'Armées.

Convaincus de l'importance de travailler en réseau et en bonne intelligence sur la durée, nous animons une communauté de professionnels de l'IT et la Cybersécurité (pour des recrutements avec validation par des pairs) et sélectionnons des partenaires pour leurs complémentarités. Nos candidats sont majoritairement issus de cursus ingénieurs et grandes écoles, et nous avons un focus tout particulier sur les profils ayant une expérience de 7 ans et plus.

Sur un plan plus opérationnel, quels sont vos principaux axes d'interventions ?

Nous intervenons le plus fréquemment sur mandat d'une DG ou d'une DSI pour des chasses de profils dont l'adéquation entre les personnes et le partage de la vision-mission sont prégnantes.

Les services DRH font appel à nos services en soutien et en collaboration de leurs équipes pour des compétences très pointues en cybersécurité, gourmandes en temps de recherche et difficiles à qualifier. Notre approche est assez spécifique et nous intervenons assez souvent sur des créations de postes. C'est une démarche que je trouve particulièrement stimulante car elle mixe d'une part la compréhension de la stratégie de l'entreprise pour comprendre projets, types de compétences et tempéraments adaptés, et d'autre part l'accompagnement en amont et sur la durée des candidats afin de maximiser les chances d'une adéquation entre compétences ;

motivation ; projet ; valeurs mutuellement bénéfiques. S'impliquer auprès des dirigeants en tant qu'un vrai business partner nous semble une clé essentielle pour identifier et orienter les compétences adaptées à leurs croissances.

Qu'en est-il des principaux challenges auxquels vous êtes confrontés dans ce cadre ?

Dans le domaine de la cybersécurité, nous pouvons parler d'un vrai marché caché et d'une rareté des profils, car certains profils ne sont bien évidemment pas visibles des réseaux sociaux classiques. Sur la question de la rareté des profils, nous partons d'un simple constat : les 140 000 PME, ETI et grandes entreprises en France se partagent les compétences en cybersécurité d'environ 50 000 experts et professionnels, chacun avec des expertises spécifiques, des étapes de carrière variées, des valeurs et des souhaits de réalisation différents. Ensuite, pour la plupart des candidats dans ce secteur la question n'est pas de savoir s'ils vont trouver un emploi ou s'ils vont pouvoir être augmenté, la question est le plus souvent de savoir comment la mise en action de leurs compétences peut avoir du sens. Un besoin d'autonomie apparait également pour certains qui prennent un statut freelance, réduisant d'autant les possibilités d'embauche pour les entreprises.

Enfin, la cybersécurité évoluant constamment, il faut d'une part que nous nous tenions informés des nouveautés, et d'autre part que nous détections dans les candidats cette capacité à évoluer dans le temps aux côtés de nos clients.

De par votre expertise, quels conseils prodigueriez-vous à une entreprise pour recruter des compétences en cybersécurité ?

Un conseil semble compliqué devant l'asymétrie existante dans ce domaine ! Cependant, il y a des pistes de réflexions qu'il me semble important à prendre compte. En effet, la cybersécurité est un domaine de haute technicité, mais ce mot est devenu une notion plus globale dont l'ensemble des salariés de l'entreprise doit



s'approprier, et à fortiori les dirigeants afin de pouvoir insuffler une bonne gouvernance et prendre des décisions éclairées.

Bâtir une stratégie de recrutement de compétences rares en cybersécurité sur un modèle de gestion du turnover ne me semble pas le plus efficient, je crois plus dans le sur-mesure. Nous le voyons quotidiennement sur les raisons évoquées pour changer d'entreprise, la gestion individualisée et prospective des talents en cybersécurité est devenue essentielle. Enfin, peut-être qu'une des pires choses est de survendre un projet par ce qu'il y a un poste vacant... et que les candidats se rendent compte à leur prise de fonction que la réalité est bien différente de ce qui leur a été vendu. La cybersécurité est et reste une question de confiance.

Notre cabinet intervient comme facilitateur. Convaincu de l'importance d'une démarche long terme, nous portons une attention toute particulière au projet de carrière des candidats afin de favoriser une mise en situation de réussite sur la durée avec les valeurs et les projets de l'entreprise. Nous sommes intimement convaincus que ce qui a du sens pour nos candidats aura un impact positif sur les projets de nos clients.

Quelques mots sur vos projets à venir.

Les incidents de carrière après les 45-50 ans sont un sujet qui m'interpelle. Cette étape n'est pas le plus souvent le reflet d'un manque de qualifications, compétences, résultats ou d'engagements. Je rencontre chaque semaine des personnes formidables avec des parcours d'une richesse incroyable, mais qui parfois sont restées dans une posture "tête dans le guidon" pendant des années sans avoir un moment à soi pour prendre du recul, et sans avoir entretenu son réseau professionnel.

Devant ce constat, je réfléchis à une offre de service parallèle pouvant permettre à ces profils à haute valeur ajoutée d'avoir des conseils avisés, neutres et pragmatiques tout au long de leur carrière, et gagner ainsi en antifragilité. ×