

## Les jeunes et l'univers de la cyber



**Charles BLANC ROLIN**

*Chef de projet sécurité numérique en santé*

*GCS e-santé Pays de la Loire*

Offres d'emplois qui restent publiées pendant des mois, et parfois même des années sans qu'un recrutement n'aboutisse, salaires qui ne cessent d'augmenter, conditions de travail de plus en plus flexibles, salariés qui bougent beaucoup... Je ne vous apprends rien en vous disant que le domaine de la sécurité numérique, ou cybersécurité puisque nous l'appelons ainsi désormais, manque cruellement de compétences.

Pour répondre à ce besoin, nous comptons sur la relève, par conséquent, de plus en plus de formations spécialisées comme celles labellisées SecNumedu<sup>1</sup> ou intégrant la sécurité avec la labellisation CyberEdu<sup>2</sup>, sont proposées aux jeunes.

Cela va-t-il nous permettre de nous sortir rapidement de cette ère chiffrante où il ne se passe pas une semaine sans qu'une cyber-météorite ne tombe sur le coin de nos données ? Pas si simple.

**« Quand je serai grand, je serai hacker éthique ! »**

Beaucoup de jeunes fantasment sur les métiers de l'offensif, et c'est parfaitement compréhensible, c'est

fun, c'est gratifiant, ça donne l'impression d'avoir un pouvoir immense (ce qui n'est pas totalement faux) et en plus, on est adulé comme une rockstar (quand on est bon, et qu'on a bossé) !

À quinze ans, on ne rêve pas forcément de devenir analyste SOC de niveau 1 et manger des lignes de logs toute la journée, on ne rêve pas non plus d'analyses d'impacts sur les traitements sensibles de données à caractère personnel ou d'analyses de risques Ebios RM, et en même temps, on s'en fiche car on ne sait pas ce c'est, et qu'il est quand même bien plus amusant de découvrir le cyberspace et ses vulnérabilités à l'aide d'une distribution Kali Linux.

<intermède>

On constate à ce point déjà, qu'il y a plusieurs métiers et que le titre « expert en cybersécurité » n'apporte pas plus de détails que le terme « professionnel de santé ». Sauf qu'un professionnel de santé n'écrira jamais « professionnel de santé » sur son CV, sa carte de visite ou ses ordonnances.

</intermède>

**Alors, former les jeunes aux métiers de « pentesters », est-ce une bonne chose ?**

Déjà, nous en avons besoin, il n'y pas vraiment de doutes sur le sujet.

Même si nous avons un besoin urgent de ressources, pas sûr que ce soit dans le domaine de l'offensif que le manque soit le plus important d'ailleurs, ne va-t-on pas trop vite dans certaines formations ? Avant d'apprendre à exploiter des vulnérabilités ou des erreurs de configuration à l'aide d'outils prêts à l'emploi, il me semble primordial d'acquérir des bases en informatique, connaître le fonctionnement des systèmes, les protocoles réseau, le développement... Reproduire les actions présentées dans un tuto Kali sur YouTube, il n'y a pas besoin de formation pour ça, comprendre ce qu'il se

<sup>1</sup> <https://www.ssi.gouv.fr/particulier/formations/secnumedu/>

<sup>2</sup> <https://www.ssi.gouv.fr/entreprise/formations/cyberedu/>

passer concrètement en arrière-plan et les actions à mettre en place pour y remédier, c'est une autre affaire. Pour les jeunes qui pensent que les missions d'un pentester s'arrêtent au fait de tout casser, ils risquent d'être déçus.

Si tout le monde suit le même cursus de formation à l'offensif, ne risque-t-on pas de perdre en « innovation » si les jeunes diplômés ne sont pas un minimum curieux, passionnés, investis et créatifs ? Les gens qui se démarquent, qui sont très bons dans leur domaine, sont de vrais passionnés, peu importe le cursus qu'ils ont suivi, ils ont passé du temps à potasser, à chercher, à tester. Certaines entreprises ou la DGA l'ont bien compris et ne s'attardent pas spécialement sur les diplômes dans leurs processus de recrutement, mais en France, cet état d'esprit reste encore à la marge et il est assez fréquent de lire des offres d'emploi où l'on demande un « bac+5 en cybersécurité » pour une mission consistant à pousser des alertes à un niveau supérieur.

En opposition totale, j'adore voir des personnes avec des parcours atypiques, comme celui de Lionel GILLES, retracé dans son interview au micro de NoLimitSecu<sup>3</sup>.

Je ne dis pas qu'il ne faut pas que les jeunes soient formés, bien au contraire, mais la formation doit être adaptée et les profils bien orientés, sans fermer la porte à celles et ceux qui se sont construits seuls. En médecine, il y a un tronc commun avant de partir dans des spécialités, en informatique, cela doit être pareil, il faut des bases solides avant de se spécialiser dans un domaine.

D'autre part, nous pouvons également observer des recruteurs qui demandent désormais un classement sur Root-Me à leurs candidats. La plateforme est géniale pour les curieux qui ont soif d'apprendre et l'idée me semble plutôt intéressante pour se faire une première idée des connaissances du candidat. Maintenant, il faut peut-être faire preuve d'indulgence, notamment en fonction du poste proposé.

Même si les mentalités évoluent, je regrette qu'on ne mette pas plus en avant les métiers des défenseurs et de la réponse à incident, ils restent encore trop souvent les héros oubliés, et nous en manquons certainement

encore plus que des profils offensifs.

N'oublions pas non plus les métiers de la gouvernance et de la conformité qui peuvent peut-être paraître moins fun au premier abord, mais indispensables eux aussi. Il n'y a pas forcément besoin d'avoir une expertise technique pour faire de la sécurité numérique et chacun peut amener sa pierre à l'édifice.

Ce que j'affectionne particulièrement dans le domaine de la cyber, c'est que l'on apprend constamment, et que l'on apprend de tous ! D'une conférence de Gérard PELIKS au « write-up » d'un jeune étudiant. D'un podcast des amis de NoLimit et du Comptoir Sécu, en passant par un échange interminable avec un pentester insomniaque, les connaissances, la passion et la créativité font que nous sommes tous rapidement sur un pied d'égalité (ou presque), peu importe la différence d'âge !

---

<sup>3</sup> <https://www.nolimitsecu.fr/interview-topotam/>