



Votre bulletin mensuel sur la sensibilisation à la sécurité

Une carrière dans la cybersécurité.

Aperçu

Nous entendons régulièrement parler de cybersécurité aux actualités, pendant que des organisations et des gouvernements dans le monde continuent de se faire pirater. Il y a une forte demande de personnes formées en cybersécurité afin d'aider à se défendre devant cette menace grandissante. En effet, les ouvertures sont estimées à près de trois millions au niveau global. Avez-vous considéré une carrière comme professionnel de la cybersécurité ? C'est un secteur hautement dynamique, avec un très grand choix de spécialisations, tel que le judiciaire, la sécurité, les cellules de crise, la programmation sécurisée et la sensibilisation et la formation. De plus, une carrière en cybersécurité vous permet de travailler de n'importe où dans le monde, avec des avantages multiples et une opportunité de changer les choses.

Mais dois-je avoir un diplôme en informatique ?

Pas du tout. Les plus grands professionnels de la sécurité ont des parcours variés : des diplômés en Lettres, Médecine, Histoire, ou encore des mécaniciens, artistes ou mères au foyer. La clé est la passion d'apprendre : la cybersécurité, c'est apprendre comment les choses fonctionnent. Dès qu'on sait comment la technologie fonctionne, on peut mieux la sécuriser. L'avantage de la cybersécurité c'est qu'on peut apprendre comment ces technologies fonctionnent, de la maison et à notre rythme.

Comment commencer

Pas sûr où commencer ? Commencez par explorer les différentes technologies et voyez ce qui vous intéresse.



Codage : Apprenez les bases de la programmation, en commençant avec Python, HTML ou Javascript. Pas sûr où commencer votre apprentissage ? Optez pour un site de formation en ligne ou un livre de programmation pour débutants.



Systèmes : Apprenez les bases d'administration d'un système d'exploitation, comme Linux ou Windows. Si vous voulez faire geek, commencez par Linux. Apprendre à administrer un système Linux par la ligne de commande est une compétence qui vous aidera, qu'importe la voie que vous prendrez.



Applications: Apprenez à configurer, exécuter et maintenir des applications, comme un serveur web ou DNS.



Réseautage : Apprenez comment un réseau fonctionne, y compris comment les appareils discutent entre eux grâce à la capture et l'analyse du trafic réseau. Ça peut être amusant vu que votre maison est sûrement déjà un environnement réseau avec toutes sortes d'appareils connectés.

Une bonne manière d'apprendre est de monter votre propre labo à la maison. C'est assez simple, car vous pouvez créer des systèmes d'exploitation virtuels multiples d'un même ordinateur, ou monter un labo avec un cloud, comme AWS d'Amazon ou Azure de Microsoft. Une fois vos systèmes d'exploitation opérationnels, commencez à interagir avec eux et apprenez autant que possible. Une autre manière est de rencontrer des personnes dans la cybersécurité. Songez à aller dans des conférences sur la cybersécurité (appelées "con") près de chez vous. Presque toutes les grandes villes proposent des événements. Un type d'évènement sur la cybersécurité connu pour aider les débutants s'appelle Bsidés. Le plus dur est de trouver le premier évènement ou la première rencontre. Une fois que vous y participez, votre réseau va s'étendre graduellement. Il y a d'autres manières d'apprendre : les vidéos YouTube, les forums en ligne, les blogs de professionnels ou les événements "Capture the Flag" (CTF). Enfin, il existe pleins de programmes pour vous aider à commencer votre carrière, comme CyberTalent Immersion Academies, Cyber Aces, ou Cyber Patriot.

Ne vous arrêtez donc pas à votre éducation ou parcours. Peu importe votre parcours, il vous apporte quelque chose d'unique et spécial dont la cybersécurité a besoin. La clé est la passion d'apprendre. Dès que vous commencerez à développer vos compétences et à faire des rencontres, vous aurez des opportunités.

Rédacteur Invité

Heather Mahalik (@heathermahalik) est directrice, ingénieure légiste à ManTech CARD et instructrice / auteur principal pour les formations SANS Digital Forensics et Incident Response (DFIR). Elle est dans la cybersécurité depuis 17 ans et adore son métier. Elle écrit un blog sur www.smarterforensics.com.



Ressources

Bsidés: <http://www.securitybsides.com>
CyberTalent Immersion Academies: <https://www.sans.org/cybertalent/cybersecurity-career/seekers>
Cyber Aces: <https://www.cyberaces.org>
Cyber Patriot: <https://www.uscyberpatriot.org/>
Code Academy: www.codeacademy.com

OUCH! est publiée par le programme SANS (Security Awareness) et est distribuée sous la licence « [Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/) ». La distribution de cette lettre d'information est autorisée tant que vous faites référence à la source, qu'elle n'a subie aucune modification et qu'elle n'est pas utilisée à des fins commerciales. Afin d'obtenir des traductions ou plus d'informations, merci de contacter www.sans.org/security-awareness/ouch-newsletter.
Comité de rédaction : Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley