Cyber Security Specialist BF

observer, analyser, intervenir, protéger, sensibiliser, conseiller

Le monde de plus en plus connecté numériquement ne change pas la vie que pour le mieux. Les cyber-attaques sont devenues un problème quotidien pour les organisations privées et publiques. L'importance croissante de l'information et de la technologie augmente également le risque d'abus avec un potentiel de nuisance considérable pour l'économie et la société.

Par leur travail, les Cyber Security Specialists contribuent à protéger les systèmes, les applications et les données contre les abus et à minimiser ainsi les dommages causés au patrimoine, aux objets, aux connaissances et aux personnes. Ils surveillent les systèmes, analysent les menaces et détectent les éventuelles failles. S'ils constatent un incident de sécurité, ils réagissent immédiatement en prenant les mesures de protection appropriées. En outre, ils planifient et mettent en œuvre des projets dans le domaine de la cybersécurité.

Les Specialists travaillent souvent en équipe avec d'autres spécialistes dans le domaine de la sécurité ICT de l'entreprise, appelé Security Operations Center. Ils dirigent de petites équipes et assument la responsabilité de projets partiels.

Quoi et pourquoi?

- Afin que les systèmes d'information et de communication de l'organisation soient protégés contre les attaques provenant du cyberespace, le Cyber Security Specialist observe attentivement toutes les opérations et intervient en temps réel si nécessaire.
- Afin de pouvoir développer le circuit de protection professionnel interne à l'entreprise, la Cyber Security Specialist analyse les connaissances acquises lors des attaques et les documente consciencieusement.
- Afin qu'il agisse toujours dans l'intérêt de son entreprise, le Cyber Security Specialist respecte les directives issues de la stratégie de sécurité de la direction et les directives de sécurité qui en découlent (Information Security Policy).
- Afin que les cyber-attaques ne causent pas de dommages durables, la Cyber Security Specialist conseille, sensibilise et forme les collaborateurs et la clientèle.

Les faits

Admission En passant l'examen:
a) formation professionnelle initiale avec CFC dans une profession ICT et au moins 2 ans de pratique dans le domaine de la sécurité ICT
b) Formation avec CFC dans une autre profession, diplôme de niveau secondaire II ou diplôme équivalent et au moins 4 ans de pratique dans le domaine des TIC (dont au moins 2 ans dans la sécurité des TIC).
c) Autre formation préalable et au moins 6 ans de pratique dans le domaine des TIC (dont au moins 2 ans dans la sécurité des TIC).
d) Stage de formation cybernétique de l'armée suisse et au moins 1 an de pratique dans le domaine de la sécurité des TIC.

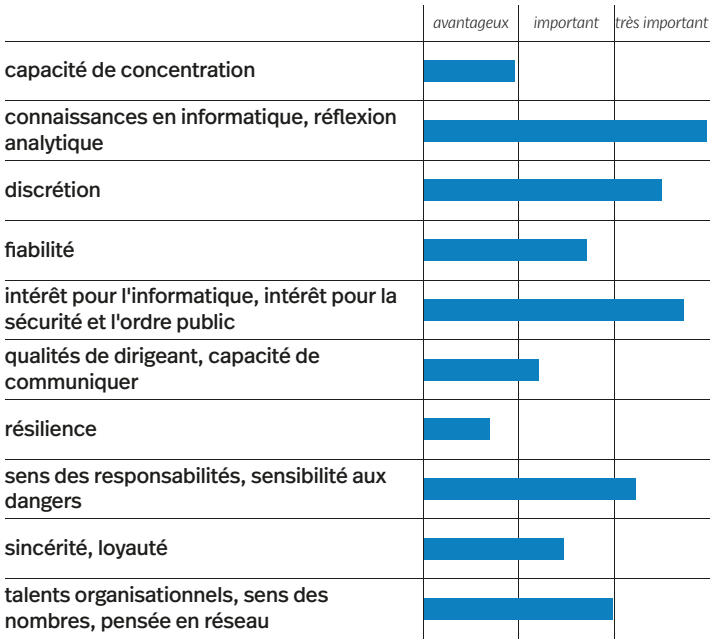
Formation 2 à 3 semestres de formation continue en cours d'emploi. Selon le prestataire, sur place ou en ligne. L'armée suisse propose un stage de formation cyber qui peut être suivi dans le cadre de l'école de recrues. Remarque: Les frais de cours sont partiellement couverts par la Confédération.

Les aspects positifs La méga-tendance de la numérisation touche tous les domaines de la vie. Comme l'utilisation des technologies de l'information et de la communication ne cesse d'augmenter, le risque potentiel d'une utilisation abusive de ces technologies augmente également et le besoin de sécurité numérique se fait de plus en plus sentir. Les Cyber Security Specialists sont donc très recherchés, car ils peuvent aborder et atténuer le problème de la criminalité dans le cyberespace.

Les aspects négatifs Le risque de criminalité dans le cyberespace est omniprésent et concerne les entreprises et les institutions de toutes tailles. Les attaques ont un potentiel de dommages immensément élevé. Cela signifie une pression pure pour les spécialistes.

Bon à savoir Les Cyber Security Specialists travaillent généralement dans des entreprises privées de taille moyenne ou grande et dans des institutions publiques.

Profil requis



Plans de carrière