Chapitre 5 : La cybersécurité dans votre futur

Ce chapitre aborde les enjeux éthiques et juridiques dans le domaine de la cybersécurité. Il traite également des cursus de formation et des parcours professionnels dans le domaine de la cybersécurité. Certains parcours de formation proposés à la Cisco Networking Academy mènent à des certifications. Certaines de ces certifications sont des prérequis aux certificats de spécialisation dans de nombreux domaines de réseaux, notamment la cybersécurité.

Sur la page Networking Academy Talent Bridge (sur le site netacad.com sous Ressources), vous trouverez des informations de qualité pour vous aider à écrire votre CV et à vous préparer à un entretien d'embauche. Elle contient également une liste des emplois chez Cisco et chez les partenaires Cisco. Trois moteurs de recherche d’emploi en ligne sont mis à votre disposition.

# Enjeux juridiques en matière de cybersécurité

Les professionnels de la cybersécurité doivent avoir les mêmes compétences que les pirates informatiques, surtout les pirates Chapeaux noirs, afin de pouvoir mettre en place des protections contre les attaques. L’une des différences entre un pirate informatique et un professionnel de la cybersécurité est que le dernier doit travailler dans le cadre légal.

**Enjeux juridiques et personnels**

Pas besoin d’être un employé pour être soumis aux législations régissant la cybersécurité. Dans votre vie privée, vous pouvez avoir l’opportunité et les compétences pour pirater l’ordinateur ou le réseau d’une autre personne. Mais selon un vieux dicton, « Ce n’est pas parce que vous savez comment le faire que vous devez le faire ». Souvenez-vous de cela. La plupart des pirates laissent des traces, délibérément ou non, et ces traces peuvent servir pour le traquer.

Les professionnels de la cybersécurité développent de nombreuses compétences pouvant être utilisées pour le bien ou pour le mal. Ceux qui utilisent leurs compétences dans le cadre légal, pour protéger l’infrastructure, le réseau et la confidentialité sont toujours très demandés.

**Enjeux juridiques et professionnels**

La plupart des pays mettent en place des lois régissant la cybersécurité. Ils doivent en élaborer avec les infrastructures critiques, les réseaux et la confidentialité professionnelle et personnelle. Les entreprises sont amenées à respecter ces lois.

Dans certains cas, si vous enfreignez les lois régissant la cybersécurité pendant votre travail, c’est l’entreprise qui est punie et vous risquez de perdre votre emploi. Dans d’autres cas, vous risquez d’être poursuivi, de payer une amende et probablement d’être condamné.

En général, si vous vous sentez incapable de déterminer si une action ou un comportement pourrait être illégal, considérez cette action ou ce comportement comme illégal et ne le faites pas. Votre entreprise peut être dotée d’un service juridique ou une personne du département des ressources humaines peut répondre à vos questions avant que vous ne fassiez quelque chose d’illégal.

**Législation internationale et cybersécurité**

Le domaine de la législation régissant la cybersécurité est plus récent que la cybersécurité elle-même. Comme mentionné précédemment, la plupart des pays ont mis en place certaines législations, et d’autres lois sont en vue.

# Enjeux éthiques en matière de cybersécurité

En plus de travailler dans le cadre de la loi, les professionnels de la cybersécurité doivent également démontrer un comportement éthique.

**Enjeux éthiques et personnels**

Une personne peut agir contrairement à l’éthique et ne pas être sujette à des poursuites, à des amendes ou à l’emprisonnement. C’est parce que l’action n’a peut-être pas été techniquement illégale. Mais cela ne signifie pas pour autant que le comportement est acceptable. Le comportement éthique est assez facile à déterminer. Il est possible de lister tous les différents comportements contraires à l’éthique qu’une personne disposant de compétences en cybersécurité peut avoir. Voici deux exemples. Posez-vous les questions suivantes :

* Est-ce que je souhaite découvrir que quelqu’un a piraté mon ordinateur et altéré mes images dans mes sites de réseaux sociaux ?
* Est-ce que je souhaite découvrir qu’un technicien informatique à qui j’ai confié le dépannage de mon réseau a communiqué à ses collègues des informations personnelles me concernant qu’il a obtenues lorsqu’il travaillait sur mon réseau ?

Si vous répondez « non » à ces questions, ne faites pas ce genre de chose à d'autres personnes.

**Enjeux éthiques et professionnels**

L’éthique est constituée de codes de comportement qui sont parfois renforcés par la loi. Il existe plusieurs domaines dans la cybersécurité qui ne sont pas visés par la législation. Cela signifie qu'une action techniquement légale peut néanmoins s’avérer ne pas être l’action éthique à effectuer. Puisque de nombreux domaines de la cybersécurité ne sont pas (ou pas encore) visés par la loi, de nombreuses organisations professionnelles du secteur informatique ont créé des codes d’éthique pour les personnes travaillant dans le secteur. Voici une liste de trois organisations disposant de codes d’éthique :

* Le CyberSecurity Institute (CSI) a publié un code d’éthique que vous pouvez lire [ici](http://csisite.net/training/ethicsconduct.htm).
* L’ISSA (Information Systems Security Association) dispose d’un code d’éthique disponible [ici](http://www.issa.org/?page=CodeofEthics).
* L’Association des professionnels des technologies de l’information (AITP) dispose d’un code d’éthique et d’un code de conduite accessible [ici](http://www.aitp.org/?page=EthicsConduct).

Cisco dispose d’une équipe dédiée exclusivement à la conduite professionnelle éthique. Allez [ici](http://csr.cisco.com/pages/governance-and-ethics) pour lire les détails sur cette équipe. Ce [site](http://investor.cisco.com/investor-relations/governance/code-of-conduct/default.aspx) contient un livre électronique sur le Code de conduite professionnelle de Cisco, ainsi qu’une version PDF. Les deux fichiers renferment un « Organigramme décisionnel sur l’éthique » comme illustré dans la figure. Même si vous ne travaillez pas pour Cisco, les questions et réponses dans cet organigramme décisionnel peuvent facilement être appliquées à votre lieu de travail. Comme avec les questions juridiques, en général, si vous n’arrivez pas à déterminer si une action ou un comportement pourrait être contraire à l’éthique, considérez que cette action ou ce comportement est contraire à l’éthique et ne le faites pas. Une personne du département des ressources humaines ou du département juridique devrait pouvoir clarifier votre situation avant que vous ne fassiez quelque chose qui pourrait être interprété comme étant contraire à l’éthique.

Faites des recherches en ligne pour trouver d’autres organisations liées au secteur de l’informatique et qui disposent de codes d’éthique. Essayez de découvrir ce qu’elles ont en commun.

Emplois dans le domaine de la cybersécurité

Beaucoup d’autres entreprises et industries embauchent des professionnels de la cybersécurité. Il existe plusieurs moteurs de recherche en ligne qui peuvent vous aider à trouver l'emploi qui vous convient dans le domaine de la cybersécurité :

* [ITJobMatch](https://itjobmatch.com/) : le moteur de recherche ITJobMatch se spécialise dans les emplois en informatique de tout type, dans le monde entier.
* [Monster](http://jobs.monster.com/search/?q=cybersecurity) : Monster est un moteur de recherche pour tous les types d'emplois. Le lien fourni redirige directement vers des emplois dans le domaine de la cybersécurité.
* [CareerBuilder](http://www.careerbuilder.com/jobs/keyword/cyber-security) : CareerBuilder est également un moteur de recherche pour tous les types d'emplois. Le lien fourni redirige directement vers des emplois dans le domaine de la cybersécurité.

Il ne s’agit que de trois sites parmi les nombreux sites de recherche d’emploi en ligne. Même si vous commencez tout juste votre formation en informatique et en cybersécurité, la consultation des moteurs de recherche d’emploi est un moyen efficace de prendre connaissance des types d’emplois disponibles, partout dans le monde.

En fonction de votre intérêt pour la cybersécurité, différents types d’emplois peuvent être à votre disposition, et ils peuvent exiger des certifications de compétences spécialisées. Par exemple, un testeur de pénétration, aussi connu comme un hacker éthique, recherche et exploite des vulnérabilités de sécurité dans les applications, les réseaux et les systèmes. Pour devenir un testeur de pénétration, vous aurez besoin d’acquérir de l’expérience dans d’autres emplois dans le domaine de l’informatique, tel qu’administrateur de la sécurité, administrateur réseau, et administrateur système. Chacun de ces emplois nécessite un ensemble de compétences propre qui vous aidera à devenir un atout précieux pour une entreprise.

Nous espérons que ce cours a stimulé votre intérêt de suivre une formation en informatique et en cybersécurité, et de continuer vers une carrière passionnante ! La Cisco Networking Academy propose plusieurs cours pour vous permettre de poursuivre votre formation dans le domaine de la cybersécurité. Nous vous encourageons à vous inscrire au prochain cours, Cybersecurity Essentials, pour approfondir vos connaissances de base en matière de cybersécurité. Accédez à la Cisco Networking Academy et affichez la liste des [cours](https://www.netacad.com/courses/) disponibles. Vous pouvez aussi accéder aux [ressources pour la recherche d'emploi](http://www.netacad.com/careers) disponibles sur la Cisco Networking Academy.

Juste pour le plaisir, cliquez [ici](http://newsroom.cisco.com/supersmartsecurity) pour lire un livre illustré à propos d’un super-héros de la cybersécurité !

# Conclusion

Ce chapitre a commencé par l'analyse des enjeux juridiques et éthiques que les professionnels de la cybersécurité rencontrent fréquemment. Il a également présenté les cursus de formation et les parcours professionnels pour ceux qui souhaitent devenir des professionnels de la cybersécurité. Trois moteurs de recherche d’emploi en ligne sont mis à votre disposition.

Si vous souhaitez découvrir plus en détail les concepts de ce chapitre, référez-vous à la page des [ressources et activités supplémentaires](https://contenthub.netacad.com/legacy/I2CS/2.1/fr/course/files/IntroCybersecurity%20-%20Additional%20Resources%20and%20Activities.pdf) dans les Ressources des étudiants.