Le 22 mai 2012

INTerview de Julie GRASSIN (TSP 10)

Pourriez-vous nous raconter votre parcours depuis la sortie de l'école ?

En réalité, tout commence à Télécom SudParis, avec le cours sur **l'intelligence économique** de Monsieur BRUNEAU. Pendant deux mois je découvre un domaine que je ne connaissais pas et qui me plait vraiment. Je décide donc de faire un stage dans ce secteur pour voir concrètement ce que cela représente.

Je pars deux mois et demi à Digimind (spécialiste des logiciels de veille stratégique et des logiciels e-réputation) dans les bureaux de Boston (la société est basée à Paris) en tant que consultante **avant-vente pour la solution Digimind**. J'en sors totalement séduite.

Pour mon stage de fin d'étude, je choisis **l'ADIT,** un **cabinet d'intelligence économique de renom,** afin de parfaire la réorientation de mon parcours. **Dans ce cabinet je réalise des « due diligence commerciales »** mais je n'ai plus aucun aspect "technique", ce que je regrette.

C'est pour cette raison que j'ai choisi, il y a deux ans, d'intégrer **LEXSI (cabinet indépendant de protection du patrimoine informationnel) en tant qu'analyste cybercriminalité**.

Quels savoir-faire/savoir-être acquis dans vos écoles, vous ont été utiles dans votre carrière?

Pour ce poste d'analyste cybercriminalité, **les acquis de la VAP "sécurité des réseaux"** m'ont été particulièrement utiles ! Je disposais en effet d'un bagage technique important ainsi que d'une connaissance approfondie des problématiques de sécurité. Cela m'a permis de me former très rapidement au poste.

En quoi consiste exactement le métier d'un analyste en cyber criminalité ?

Aujourd'hui j'ai deux axes de travail : celui d'analyste cybercriminalité et un travail sur les réseaux sociaux.

Nous travaillons au sein d'un CERT : « Computer Emergency Response Team », une équipe agréée pour les réponses à incidents informatiques. Nous nous penchons concrètement sur les problématiques de fraudes bancaires.

Les banques sont responsables de leurs plateformes de paiement en ligne et il est interdit d'y réaliser des paiements pour des objets à caractère pornographique, des objets de contrefaçon etc. **Nous les aidons donc à la détection de ventes d'objets non autorisés sur les plateformes de paiement en ligne.**

INTerview de Julie GRASSIN (TSP 10)

(Suite) En quoi consiste exactement le métier d'un analyste en cyber criminalité ?

Nous travaillons aussi à détecter la mise en ligne de sites de « phishing » (ou hameçonnage). Ces sites imitent le site d'une banque et demandent à la victime son numéro de carte bancaire complet, la date de péremption et éventuellement le code PIN. Pour cela nous avons des outils, qui génèrent des alertes, et nous qualifions manuellement les sites (phishing ou non). Une fois le site de phishing détecté, nous travaillons à sa signalisation et à sa fermeture.

Ainsi dès qu'un internaute se rend sur le site de phishing, il est prévenu du danger par le navigateur. Ensuite, nous prenons contact avec l'hébergeur afin qu'il procède à la suspension du site (contact...pas toujours facile, hébergeur...pas toujours coopératif!).

J'en profite ici pour signaler **l'existence du site Phishing Initiative (http://phishing-initiative.fr/)** qui permet à tout internaute de signaler un site. Il lui suffit de soumettre l'URL suspecte, celle-ci est ensuite qualifiée par l'un de nos analystes et si besoin, des contre-mesures sont lancées.

Parallèlement à cela, **nous analysons également les grandes tendances de la cybercriminalité bancaire dans le monde**, ce qui donne lieu à la production de rapports mensuels.

L'équipe d'analystes travaille également sur les problématique de lutte contre la contrefaçon et de "veille image". **Nous maintenons nos clients à jour sur les problématiques d'atteinte à l'image et dénigrement qui peuvent avoir lieu sur internet.**

En plus de tout cela, **je travaille aussi sur les problématiques de réputation sur les réseaux sociaux professionnels comme personnels.** Nous évaluons à un moment donné le niveau d'exposition d'une société sur ces réseaux : quelles sont les informations sensibles voire confidentielles qui sont diffusées sur la toile, quel est l'impact pour la société et ses salariés, etc.

Pour conclure, vous diriez que...

... j'adore mon métier. Actuellement, certaines tâches sont encore manuelles et répétitives mais elles auront très probablement vocation à être automatisées un jour. Ce qui m'attire particulièrement est de pouvoir travailler dans un domaine nouveau, où tout reste encore à faire. D'autre part, ce métier me permet de maîtriser quotidiennement les problématiques techniques liées à la sécurité des réseaux. En ce qui concerne la cybercriminalité, ce qui est passionnant ce n'est pas tant la pratique technique, mais c'est d'être toujours en position de veille.