LE RISQUE CYBER
ou la nécessité de former ses collaborateurs

Interview croisée entre Joël Courtois, Directeur Général de l'EPITA, et Marie Moin, Directrice de SECURESPHERE by EPITA. Ils reviennent pour nous sur la proposition de valeur de l'EPITA dans le domaine de la cybersécurité, qui est devenu en quelques années un enjeu stratégique pour les entreprises.

Joël Courtois

Marie Moin

Où se situe l'EPITA dans le paysage de la formation ?
L'EPITA est une grande école d'ingénieur spécialisée dans le domaine du numérique. L'école forme des jeunes issus de terminale scientifique, sur un cursus de 5 ans, et elle propose aussi des cursus de 3 ans pour des personnes issues de classes préparatoires classiques (CPGE). Elle forme également par l'apprentissage et a développé un centre de formation professionnelle continue.

Actuellement, sur le marché, il y a un manque évident d'ingénieurs en IT. Comment appréhendez-vous cette situation ?
Depuis quelques années, nous assistons à une véritable pénurie d'ingénieurs en IT. Forts de ce constat, nous avons triplé nos promos sur ces dernières années. Mais cette initiative ne permet pas de répondre à une demande des entreprises en constante hausse.
En parallèle, les ingénieurs français sont très prisés sur le marché du travail international, notamment au Canada, aux États-Unis ou encore au Royaume-Uni.
D'ailleurs, sur la promotion 2017, nous avons enregistré 1/3 des premiers emplois à l'étranger.
Suite à nos échanges avec les industriels et les entreprises, nous avons fait le choix de développer la formation professionnelle en nous concentrant sur deux axes :

- Apporter une double compétence à des jeunes issus d'autres domaines ;
- Développer le « Reskilling » en formant des informaticiens qui ont besoin d'une remise à jour de leurs connaissances afin d'être en adéquation avec les évolutions technologiques et les besoins actuels du marché.

L'EPITA couvre tous les champs de l'informatique (cybersécurité, intelligence artificielle, robotique, embarqué, télécoms, systèmes d'information, multimédia, réalité virtuelle et augmentée, imagerie…) mais nous avons décidé dans un premier temps, pour la formation professionnelle, de privilégier la cybersécurité, domaine historique d'expertise de l'école générant la plus forte demande des entreprises.

Que proposez-vous donc comme formation continue ?
Nous proposons une offre de formation professionnelle étendue :

- Une formation diplômante en partenariat avec l'UTT (un diplôme d'université) ;
- Une offre « Secure by Design » sur mesure en co-construction avec les entreprises (programme de chaque formation imaginé et conçu sur mesure en fonction des besoins exprimés par l'entreprise). Les programmes sur 10 jours sont ciblés pour trois profils de participants : les collaborateurs de toutes fonctions confondues, les collaborateurs de profils techniques IT, mais aussi les experts en cybersécurité.

En parallèle, nous proposons aussi des formats courts, sur 2 ou 3 jours, pour faire monter en compétences les collaborateurs rapidement sans impacter le fonctionnement et l'activité de l'entreprise.
Si nous organisons ces formations pour divers secteurs d'activité (automobile,

aéronautique, militaire, banque et assurance), l'enjeu reste le même : avoir des ingénieurs capables d'implémenter la sécurité informatique dès la conception de leurs environnements.
En parallèle, nous avons vu la demande pour nos formations croître avec l'entrée en vigueur du RGPD et les sanctions appliquées en cas de non-conformité, notamment en termes de sécurisation de données. Cela a entraîné une hausse des demandes pour des formations autour de la sécurité des outils.

Quelle est la valeur ajoutée de vos formations ?

Aujourd'hui, nous avons des retours très positifs de la part des entreprises et des collaborateurs qui suivent nos formations. C'est une grande fierté pour nous que les participants soient satisfaits d'avoir pu développer et acquérir des compétences au sein de l'EPITA, devenues opérationnelles dans leurs entreprises. Chacune de nos formations est précédée d'une phase d'ingénierie pédagogique pour identifier le besoin des entreprises. Cette démarche réalisée avec les formateurs, permet de concevoir le syllabus et de réaliser des tests avant de déployer la formation. Nous avons fait le choix de ne pas dissocier l'ingénierie pédagogique de l'instruction.
Au-delà d'une démarche d'agilité, c'est aussi un gage de qualité. Dans un domaine aussi sensible que la sécurité et la cybersécurité, la confiance et la compétence sont des prérequis. Ainsi, nous comptons de nombreux enseignants chercheurs issus de l'ANSSI parmi notre corps enseignant.

Quels sont les enjeux qui persistent ?

Il n'y a que quelques écoles qui, comme l'EPITA, ont pris la mesure des risques cyber. Une très grande majorité des écoles continuent de former des développeurs comme cela se faisait il y une quinzaine d'années en leur rappelant en fin de formation l'importance de sécuriser leur produit. Aujourd'hui, cette approche ne fonctionne plus, elle est obsolète. La sécurité doit être prise en compte dès le départ en utilisant les bons outils et environnements, en étant vigilants sur tous les aspects.
Au sein des entreprises, il y a donc un travail de pédagogie à mener pour permettre une vraie prise de conscience au niveau des cyber risques. Plus que jamais, la formation doit cibler tous les collaborateurs de l'entreprise, avec un véritable focus sur les équipes IT, dont celles en charge de concevoir les applications.

Vos perspectives ?

Un fort développement avec notre implication dans le « Cyber Campus France », initié à la demande du Président Macron, où nous serons au centre de cet écosystème constitué par toutes les grandes entreprises de la cyber, les grands utilisateurs et les startups les plus innovantes.
Nous allons continuer d'étoffer notre catalogue de formations du diplôme d'ingénieur aux formations courtes spécialisées en passant par les bachelors cyber et cela en fonction des attentes des entreprises.
Par ailleurs, nous avons déjà fait accréditer un diplôme BADGE de la Conférence des Grandes Écoles (CGE) sur la conception et le développement dans le domaine des technologies de l'information et de la communication. Nous nous inscrivons dans une démarche globale de veille continue et nous organisons deux fois par an un conseil de perfectionnement qui veille à la pertinence de nos programmes.

Nicolas Ioss (2010), Auditeur en sécurité des systèmes d'information à l'ANSSI et formateur pour SECURESPHERE by EPITA

« Après avoir appris à l'X comment fonctionne théoriquement un réseau informatique et un ordinateur, je me suis intéressé à la sécurité des systèmes d'information (SSI). Je me suis rendu compte à quel point celle-ci était vitale pour les organisations (entreprises, administrations, etc). Un des objets de la SSI est l'usage de mécanismes qui garantissent des propriétés de sécurité (confidentialité, intégrité, authenticité, disponibilité, etc.) et mon travail à l'ANSSI consiste entre autres à aider des organisations dans la conception et l'utilisation de tels mécanismes.
Cela permet à ces bénéficiaires d'améliorer le niveau de sécurité de leurs systèmes, mais cela ne peut pas être pérenne si les collaborateurs de ces organisations ne comprennent pas les notions sous-jacentes. Ainsi, je crois beaucoup dans le fait que la sécurité est l'affaire de tous et qu'une manière efficace pour que les propriétés de sécurité fonctionnent correctement sur le long terme consiste à former les personnes qui conçoivent, construisent et administrent des systèmes, logiciels, produits, etc. C'est principalement pour cette raison que j'anime des formations dans lesquelles je transmets des connaissances et des compétences à des architectes de projet, développeurs, administrateurs système, etc.
Le but des formations que je donne n'est donc pas de transformer les participants en des experts de la SSI, mais de donner les éléments de base qui permettent d'intégrer des notions de SSI dans un projet. J'espère ainsi que le monde de demain sera constitué de systèmes dans lesquels il sera possible d'avoir confiance ».