• ENSEIGNEMENT SUPÉRIEUR

Les profils recherchés dans le secteur de la cybersécurité : « Il faut sortir du cliché de l'expert en sweat à capuche façon Mr. Robot »

Alors que les enteprises ont du mal à recruter et que les cyberattaques se multiplient, l'école d'ingénieurs Epita a ouvert une nouvelle formation à la Défense, sur un site où se côtoient tous les acteurs du milieu.

Par Séverin Graveleau

Publié hier à 12h15, modifié hier à 17h17 • Lecture 5 min.

Article réservé aux abonnés

XAVIER LISSILOUR

« A Paris-la Défense, l'avenir se construit aujourd'hui ». Le slogan orne les barrières du vaste chantier de réaménagement du sud du quartier d'affaires de la Défense (Hauts-de-Seine), où la fine fleur des entreprises françaises et internationales est installée. C'est ici, au milieu des grues et du brouhaha des travaux, que le Campus Cyber a ouvert ses portes, en février 2022. L'objectif, lancé par le président de la République sur le modèle du cybercampus de Beersheba, en Israël, est ici aussi de construire l'avenir. Mais plus particulièrement celui de la cybersécurité française, en réunissant sur un même site quelque 160 acteurs du secteur : entreprises, organismes de recherche, services de l'Etat et écoles spécialisées. L'idée est de susciter des synergies entre ces acteurs pour répondre plus efficacement à l'explosion des attaques informatiques contre les entreprises et les services publics.

Dans le hall du bâtiment flambant neuf, où l'ambition de créer *« une grande nation cyber »* est même affichée sur les murs, Hugo, étudiant de 19 ans (qui n'a pas souhaité que son nom apparaisse), croise tous les jours de possibles futurs collègues ou employeurs : experts en cybersécurité, entrepreneurs

du numérique ou responsables d'administration. *« A la cantine, lors de conférences ou "afterworks" accessibles à tous, on discute parfois avec eux, on voit quels sont leurs problématiques et besoins, on commence à se faire un réseau… »*, confie le jeune homme, qui est inscrit en deuxième année de bachelor cybersécurité à l'Epita. Cette école d'ingénieurs spécialisée dans les métiers de l'informatique est membre fondateur du Campus Cyber, et fait partie des quelques établissements de formation présents sur le site (Efrei, Esilv, Institut Mines-Télécom, etc.). Au deuxième étage du bâtiment, l'Epita partage le palier avec l'entreprise Gatewatcher, un éditeur de logiciels de cybersécurité, partenaire de l'école.

Passionné de développement informatique depuis le collège, Hugo a découvert les enjeux de la cybersécurité pendant le confinement de 2020 en *« s'amusant »* sur son ordinateur avec son père, ingénieur en informatique. Un an plus tard, sur Parcoursup, il a *« choisi au tout dernier moment cette passion »*, plutôt que la filière médecine, dans laquelle ce bachelier au profil scientifique aurait, sans doute, aussi réussi. A l'avenir, il se verrait bien fonder sa *« société de cybersécurité blockchain »*, une technologie de stockage et de transmission d'informations.

Professionnalisation rapide

Le profil d'Hugo est à l'image de celui de ses 25 camarades de promo de deuxième année, réunis cette matinée de mars dans une salle de cours ensoleillée de l'Epita. Une enseignante, salariée d'une entreprise du secteur, leur présente le fonctionnement d'un logiciel de détection des *ransomwares*. Ces attaques informatiques, visant à prendre en otage des données personnelles pour obtenir une rançon, représentent une part importante des cyberattaques aujourd'hui. Dans les rangs, certains pianotent en parallèle sur leur ordinateur des lignes de code pour avancer sur des projets à rendre prochainement. *« On a tous choisi ce bachelor en trois ans pour faire tout de suite de la cybersécurité, être dans la pratique, rapidement opérationnel pour travailler, là où un cursus ingénieur en cinq ans commence par deux années plus théoriques »*, commente Nicolas, 19 ans. Cet autodidacte en programmation informatique s'imagine, quant à lui, travailler *« dans le renseignement »* ou dans la cybersécurité des infrastructures publiques.

Lire aussi : « La cyberdéfense de la France a besoin de moyens humains et technologiques »

Si la première année de formation ici vise à donner à tous les mêmes bases en programmation, en connaissance des systèmes informatiques et réseaux, ou en mathématiques, les étudiants sont, dès la deuxième année, exclusivement plongés *« dans la cybersécurité, la cryptologie, les techniques d'attaque et de défense informatique, etc. »*, décrit Nicolas. Les projets pratiques *« comme développer un petit réseau social sans aucune faille de sécurité »* sont omniprésents durant la scolarité, avant une dernière année qui se fait en alternance en entreprise.

Le nouveau bachelor de l'Epita *« vise à répondre à la demande de certains jeunes de se professionnaliser rapidement, mais aussi aux besoins urgents de recrutement des entreprises »*, commente Philippe Dewost, directeur général de l'école. Le contexte explique cette urgence. L'Agence nationale de la sécurité des systèmes d'information (Anssi), le gendarme français de la sécurité numérique, présente aussi sur le Campus Cyber, notait en janvier une stabilisation sur un palier haut des cyberattaques (831 en 2022), à la suite de leur forte augmentation les années précédentes sur fond de numérisation de l'économie, de pandémie et de guerre en Ukraine. Mais elle soulignait en même temps du doigt que ces menaces, de plus en plus sophistiquées, concernent maintenant, aussi, des entités publiques

ou privées *« moins bien protégées »* : hôpitaux, prestataires d'entreprise, fournisseurs, sous-traitants, etc.

Savoir se tenir à jour

Les besoins de recrutement en cybersécurité ne concernent plus seulement les grands groupes ou organismes étatiques. Résultat : quelque 15 000 postes ne seraient pas pourvus en France, faute de candidats, selon les calculs du cabinet de conseil Wavestone. La stratégie nationale d'accélération pour la cybersécurité, présentée en 2021, et dans laquelle l'ouverture du Campus Cyber s'intègre, prévoit même la création de 37 000 emplois dans le secteur d'ici à 2025. Hugo, Nicolas et leurs camarades savent donc que, dans un peu plus d'un an, s'offriront à eux une myriade de postes : architecte sécurité junior, spécialiste en développement sécurité, consultant en cybersécurité. Beaucoup se verraient bien aussi *pentester*, une forme de « hackeur éthique » employé pour tester la sécurité des installations informatiques, en essayant de les pirater. Les cours de sciences humaines et de droit du numérique sont parfois là pour tempérer les ardeurs *« et pour leur rappeler que, en matière de cybersécurité, il faut des années pour être identifié comme un expert, mais parfois un seul clic pour détruire sa réputation »*, souligne Philippe Dewost.

A quelques étages de là, on retrouve l'une des entreprises qui font rêver nombre d'étudiants : le groupe de défense français Thales. Sa branche cyber, forte de 1 200 experts en France, et 3 000 à l'étranger, a prévu de recruter 300 personnes supplémentaires cette année dans l'Hexagone, et autant dans le monde. Etre présent sur le Campus Cyber au côté des écoles *« nous permet de les accompagner pour que leurs cursus soient bien adaptés à nos besoins »*, commente Alexis Caurette, chargé de la stratégie et du marketing de l'activité cybersécurité de Thales. Mais dans un contexte de *« compétition sur le marché européen, autour de l'attractivité des talents »*, cette proximité géographique avec les étudiants permet aussi aux salariés qui interviennent parfois dans les cours *« d'identifier les meilleurs et de promouvoir les métiers à disposition pour eux »*, précise-t-il.

« Les menaces, comme les technologies, évoluent très vite dans notre milieu. L'enjeu de la formation, outre préparer ces jeunes à un instant T, est aussi de développer leur curiosité pour se tenir à jour, faire de la veille, etc., quand ils seront en poste », renchérit Floriane Alix, directrice des opérations chez HarfangLab, entreprise qui produit des logiciels de cybersécurité et dont les bureaux se trouvent au 5e étage du Campus Cyber. Pour cette ancienne de l'Epita, passée par Thales, relever le défi du recrutement et de la formation des talents cyber de demain doit passer par la promotion de la diversité des métiers du secteur, car *« on peut très bien, aujourd'hui, faire de la cybersécurité sans être un bon codeur »*. Mais il faut, aussi, *« sortir du cliché de l'expert cyber en sweat à capuche façon Mr. Robot »* qui peut faire peur, et, surtout, *« donner envie aux femmes de se lancer dans ces métiers »*.

Lire aussi : Parcours professionnels : Sarah Ruget, du casino à la cybersécurité via le poker et les études

A l'image de toutes les formations aux métiers du numérique, les deux premières promotions du bachelor cybersécurité d'Epita comptent seulement trois femmes, sur 80 étudiants, que l'école met en avant pour en inciter d'autres à se lancer. L'une d'elles, Elia, étudiante en première année, estime que *« la cybersécurité ne peut pas être efficace si elle n'est pensée que par des hommes. Les femmes ne doivent donc pas en avoir peur et y prendre toute leur place »*. Encore faut-il les attirer, au lycée, dans les spécialités scientifiques et techniques souvent nécessaires pour accéder aux formations en cybersécurité : un autre chantier d'avenir, colossal, pour le secteur…

Le vocabulaire de la cybersécurité

Blockchain. Les « chaînes de blocs » sont des bases de données en ligne dont la sécurité est, en théorie, assurée par le partage simultané

entre tous leurs utilisateurs, plutôt que par un organe de contrôle centralisé.

Faille de sécurité. Aussi appelée « vulnérabilité », elle désigne un défaut de conception d'un logiciel pouvant permettre à des hackeurs malveillants de l'exploiter pour mener une cyberattaque.

Hackeur. Spécialiste de l'informatique qui cherche à contourner les dispositifs de protection d'un matériel, d'un logiciel ou d'une base de données pour s'y introduire ou en détourner l'usage. S'il le fait à des fins bienveillantes, pour tester la sécurité informatique d'une entreprise par exemple, on parle de « hackeur éthique ».

Phishing. Arnaque informatique (aussi appelée « hameçonnage ») visant à se faire passer pour un tiers de confiance pour inciter un internaute à communiquer des informations personnelles.

Ransomware. Technique d'attaque informatique très répandue qui consiste à envoyer à une victime un logiciel malveillant (aussi appelé « rançongiciel ») qui va chiffrer ses données et mettre hors service ses ordinateurs tant qu'elle n'a pas payé de rançon.

Séverin Graveleau