CYBERSUP

ÉCOLE SUPÉRIEURE DE CYBERSÉCURITÉ ET IA

CONSTRUIRE SON AVENIR EN CYBERSÉCURITÉ

DÉCOUVREZ

10 PARCOURS

INSPIRANTS

Édition - 2025


BERSUP
ÉRIEURE DE CYBERSÉCURITÉ ET IA
CYBERS
ÉCOLE SUPÉRIEURE DE CYBER

ÉDITO

Manon Pellat, Directrice de Cybersup

Vous souhaitez suivre ou poursuivre des études en cybersécurité ? Bienvenue dans un secteur exigeant, fascinant, terrain d'exploration sans cesse renouvelé. Quel que soit votre établissement de formation actuel ou futur, vous pourrez certainement y développer une expertise technique pointue, au sein d'une communauté de passionnés et d'un écosystème dynamique.

Cette passion commune anime nos étudiants et formateurs chez Cybersup. Avec une conviction forte : il existe de multiples métiers en cybersécurité, qui requièrent des compétences diverses et objectivement, une courbe d'apprentissage assez raide… La cyber n'est pas un secteur que l'on choisit par défaut, bien au contraire ! Nos étudiants ont ainsi tous la volonté d'apprendre vite, de s'adapter et de contribuer à un monde numérique plus sûr.

Analyste SOC, assistant RSSI, développeur DevSecOps, consultant en GRC… Pour tous ces métiers, nous devons former des professionnels experts, agiles, complets, capables d'avoir une vraie hauteur de vue sur les enjeux techniques et organisationnels de la sécurité informatique. Reconnaissons-le cependant : se projeter parmi ces métiers est loin d'être évident pour tous les étudiants, surtout lorsqu'on leur explique que le secteur ne recrute que des "juniors expérimentés"…

Ce livre blanc, fruit d'un travail collaboratif avec Leslie Fornero et son podcast Le Monde de la Cyber, vise précisément à guider l'étudiant en cybersécurité dans ce paysage. À travers les récits de parcours de Candice Tran Dai, Julien Charlent, Joséphine Delas, Morgane Nguyen, Imane Dahou et cinq autres acteurs clés du secteur, nous dévoilons des trajectoires professionnelles et des chemins de vie aussi diversifiés qu'inspirants pour les étudiants, pour montrer qu'il n'y a pas une seule voie, mais une multitude de chemins possibles vers la cybersécurité.

Chez Cybersup, nous croyons à une formation exigeante, qui ne sacrifie ni la technique, ni la compréhension des enjeux humains, réglementaires et stratégiques. Et malgré tout, la technique seule ne suffit pas. Nos programmes, enrichis par l'expertise de Lefebvre Dalloz et intégrant pleinement les enjeux de l'intelligence artificielle, incluent également une dimension réglementaire et comportementale indispensable dans la quasi-totalité des métiers de la cyber. Les témoignages rassemblés ici illustrent cette nécessité de conjuguer compétences opérationnelles, connaissance des normes (RGPD, NIS2, CRA, IA Act…) et sensibilité aux enjeux du changement en entreprise. Les récits rassemblés ici illustrent cette nécessité d'allier savoir-faire technique, conformité et agilité.

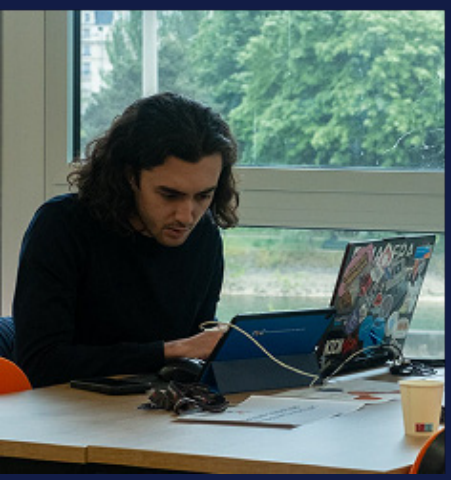
Merci à Leslie Fornero d'avoir capté, avec son regard affûté, la pluralité des voix qui font la richesse de notre écosystème. Puissent ces récits inspirer et éclairer celles et ceux qui envisagent une carrière dans la protection numérique, et rappeler à tous que la cybersécurité est avant tout, une aventure collective faite d'excellence et d'engagement.

Ce livre blanc ne vous donnera pas de recette miracle. Mais il vous aidera, je l'espère, à mieux comprendre les métiers, à mieux cerner vos envies, et à construire, pas à pas, un projet professionnel à votre image.

Bonne lecture,

Manon Pellat, Directrice de Cybersup – École de la Protection Numérique

CAMPUS
PARIS – LA DÉFENSE



Suivez-nous sur nos réseaux sociaux

SOMMAIRE

CANDICE TRAN DAI *Directrice cybersécurité* 6

JULIEN CHARLENT *SOC Analyst & Consultant en cybersécurité* 8

MORGANE NGUYEN *Adjointe RSSI* 10

JOSÉPHINE DELAS *AI Engineer* 12

IMANE DAHOU *Manager Cybersecurity, Data Protection & IT Risks* 14

LIVIA TIBIRNA *Analyste Cyber Threat Intelligence* 16

ROMAIN MARCOUX *Expert en cybersécurité transverse, consultant indépendant* 18

MAKSYM ZAITSEV *Consultant indépendant en cybersécurité, formateur et développeur open source* 20

CÉCILE DEGRUGILLIER *Lead CTI & Senior Incident Handler* 22

SOPHIE THÉNOT *Head of Group CISO Office* 24

interviews réalisées par Leslie Fornero

Candice TRAN DAI

Directrice Cybersécurité

“La cybersécurité se vit à un rythme effréné, loin de toute routine. Elle éprouve votre goût pour l’inattendu, votre agilité dans le changement et votre appétit pour des sujets foisonnants. C’est toute sa richesse.”

PARCOURS

1. **Formation initiale** en relations internationales, géopolitique, géostratégie et géo-économie.
2. **Débuts dans le monde de l’Enterprise Risk Management et de l’Intelligence Stratégique** avec une forte composante sécurité globale de l’information.
3. **Activités parallèles dans la recherche académique,** centrées sur les enjeux géopolitiques du cyberespace, notamment en Asie-Pacifique.

Découverte de la cybersécurité dès 2005, au croisement de toutes ces thématiques.

COMMENT DÉFINISSEZ-VOUS VOTRE MÉTIER AUJOURD’HUI ?

Je suis Directrice Cybersécurité. Mon rôle englobe une vaste étendue de dimensions, qui incluent et dépassent le cadre traditionnel du rôle de RSSI.

Ma mission consiste prioritairement à gérer les risques cyber de l’entreprise dans une logique d’intégration dans la gestion globale des risques business. Je couvre un spectre très large, de la technique à la stratégie, en passant par les enjeux humains.

C’est un métier qui demande de la vision, de la pédagogie, et beaucoup de capacité d’adaptation. Aucun jour ne ressemble au précédent, tout comme chaque semaine apporte son lot de nouveautés. Un attrait pour l’action est indispensable.

QUELLES SONT LES COMPÉTENCES CLÉS POUR EXERCER CE MÉTIER ?

Côté hard skills : une solide expertise technique, une vraie culture de la gestion du risque, et une maîtrise concrète des enjeux réglementaires.

Côté soft skills : du leadership, une excellente capacité de communication, et la force d’embarquer à la fois ses propres équipes cyber et toutes les autres au sein de l’entreprise.

Il faut aussi savoir communiquer la complexité des enjeux cyber de manière claire et accessible auprès du COMEX ou du Board. C’est un métier de liaison autant que de protection. Et surtout, ne jamais réduire la cyber à des checklists : elle nécessite une approche systématique, tout en faisant appel à l’intuition, à une capacité d’analyse poussée et à une solide expérience pratique.

QU’EST-CE QUI VOUS PLAÎT LE PLUS DANS VOTRE MÉTIER ?

J’aime être au cœur des enjeux stratégiques de l’entreprise, avoir un impact réel. J’aime la diversité des sujets que je traite, ce grand écart permanent entre technique, stratégie, humain. C’est stimulant intellectuellement, mais aussi exigeant. Ce n’est pas un métier de routine. Il faut savoir passer d’un sujet à un autre, d’un interlocuteur à un autre, sans perdre le fil.

COMMENT AVEZ-VOUS VU LE SECTEUR ÉVOLUER DEPUIS VOS DÉBUTS ?

Quand j'ai commencé, le secteur était très discret, presque de l'ombre. Aujourd'hui, il est beaucoup plus visible – ce qui a du bon (plus de talents, plus de moyens) mais cela comprend aussi des risques.

Une médiatisation parfois excessive peut apporter de l'eau au moulin des attaquants. Il faut garder en tête cette notion de discrétion stratégique. Côté technique, évidemment, l'IA est un game changer.

Je travaille aujourd'hui sur des produits intégrant de l'intelligence artificielle, et poser les bonnes mesures et règles de sécurité autour de cette technologie et de son usage est un défi quotidien

COMMENT OUVRIR LE SECTEUR À PLUS DE DIVERSITÉ SELON VOUS ?

J'ai toujours travaillé dans des milieux très masculins – industrie, défense… et j'ai toujours été très bien accueillie.

Ça n'a jamais été un frein pour moi mais je pense qu'il faut absolument ouvrir le secteur à d'autres profils.

Il ne faut pas juste recruter des ingénieurs issus des mêmes écoles. Il faut chercher des mindsets, des gens passionnés, curieux, parfois venus de domaines éloignés du monde numérique et informatique.

QUELS SONT LES DÉFIS À VENIR ?

L'intelligence artificielle en fait clairement partie : elle transforme nos outils, mais aussi ceux des attaquants. C'est un levier immense… des deux côtés.

Un autre sujet crucial, c'est la cryptographie post-quantique. Ce n'est plus un concept abstrait, c'est une vraie urgence. Les institutions comme l'ANSSI ou le NCSC UK ont déjà commencé à s'y pencher : on doit s'y préparer, maintenant. Il y a aussi les architectures Zero Trust, les objets connectés, la montée en puissance des ransomwares industrialisés (les fameux "RaaS"). Le terrain de jeu devient de plus en plus complexe, le tout dans un contexte où les fuites de données et en particulier celles à caractère personnel, n'a jamais été aussi dangereux.

VOS CONSEILS POUR LES ÉTUDIANTS QUI VEULENT SE LANCER ?

Cultivez votre résilience personnelle. La cyber, c'est un métier exigeant, parfois stressant, surtout dans l'opérationnel. Mais c'est aussi un métier passionnant. Si on aime apprendre, comprendre, et se dépasser, on s'y épanouit vraiment.

QUEL EST VOTRE CYBER-POUVOIR ?

" Mon intuition. Elle m'a toujours guidée dans les situations les plus complexes. Mais attention, ce n'est pas une intuition "magique" : elle repose sur l'expérience, le terrain, les années passées à lire entre les lignes. Dans ce métier, il faut savoir aller au-delà des process et des apparences. Il faut sentir, anticiper. C'est là que l'on fait la différence.

LA BOÎTE À OUTILS CYBER

Côté pratique :

Hack the Box
TryHackMe
RootMe

Côté théorie et cadre :

Le site de l'ANSSI : très utile, clair, et accessible.

Julien CHARLENT

SOC Analyst & Consultant en cybersécurité

"Analyste en cybersécurité, c'est comme être pompier du numérique : on arrive en premier, on éteint l'incendie, on sécurise les lieux, et on apprend pour mieux réagir demain."

PARCOURS

- **Passion pour la cybersécurité dès le collège**
- **1** BTS SIO option cyberdéfense au Lycée militaire de Saint-Cyr.
- **2** Licence 3 Professionnelle en cyberdéfense à Vannes.
- **3** Alternance chez Naval Group : intégration des solutions de cyberdéfense sur le système de combat du porte-avions Charles de Gaulle.
- **4** Alternance chez Alstom : missions d'audit, pentest, renforcement d'architecture.
- **5** École d'ingénieur à Paris
- **6** Alternance chez L'Oréal : assistant chef de projet cybersécurité intégré au CSIRT.
- **7** MBA 2 Spécialisé Risques Sûreté Internationale et Cybersécurité : diplômé de l'École de Guerre Économique.
- **8** SOC Analyst chez UBS & Consultant cybersécurité chez Luxoft : réponse à incident, conduite d'investigations, veille, rétro-ingénierie, rédaction de use case, forensic, CTI & threat hunting.
- **9** Intervenant en cybersécurité : coach pour étudiants chez Cybersup, professeur cybersécurité chez Jedha Bootcamp.
- **10** Certification ISC2 CISSP
- **+** Réserviste dans l'Armée de Terre

QUEL EST VOTRE POSTE ACTUEL ?

Je suis SOC Analyst, analyste en centre opérationnel de sécurité. On peut dire qu'on est les pompiers de la cybersécurité : on reçoit des alertes via nos systèmes de détection qui sont transformées en incidents, qui sont assignés à notre équipe. Au sein de mon organisation, nous sommes une vingtaine d'analystes répartis dans le monde.

Lorsqu'un incident nous est assigné, notre rôle est de l'analyser, le traiter dans un délai défini, identifier l'impact, les systèmes concernés, prendre des mesures afin de contenir la potentielle menace et documenter le tout.

On fait aussi du threat hunting (identification des menaces non identifiées), de la veille sur l'état de la menace (CTI), du retro-engineering, et de la rédaction de use case de détection. C'est un poste plus large que ce que le titre "SOC analyst" laisse entendre.

Il mêle technique, rigueur, analyse, mais aussi sens du collectif et réactivité.

QUELLES COMPÉTENCES SONT NÉCESSAIRES POUR FAIRE CE MÉTIER ?

Il faut être polyvalent : comprendre les réseaux, les systèmes, savoir coder, comprendre les vulnérabilités, les EDR.

Côté soft skills : il faut savoir gérer la pression, prendre des décisions rapidement et travailler avec un réel enjeu opérationnel derrière chaque action. Il faut aussi aimer apprendre en continu. C'est valable dans toute la cyber, mais particulièrement au SOC où les menaces peuvent prendre de grosses proportions rapidement.

Le métier de SOC nécessite de travailler 24h/24, donc on est en horaires décalés, on peut travailler les nuits, les week-ends et les jours fériés... J'ai passé mon dernier réveillon du Nouvel An au bureau. Il faut être flexible et polyvalent.

QUELLES ÉVOLUTIONS AVEZ-VOUS OBSERVÉES DANS LE SECTEUR DE LA CYBERSÉCURITÉ ?

La cyber est beaucoup plus visible qu'il y a 10 ans. On n'est plus juste des "geeks à capuche". Les entreprises, les gouvernements, le grand public prennent conscience de l'enjeu. Il y a plus d'attaques, mais aussi plus de moyens, plus de postes, plus de budget.

Le cyberespace est devenu un champ de bataille : ce n'est plus réservé aux services de renseignement. Les armées se structurent, les diplomaties aussi. On est dans une ère où la cybersécurité a un vrai poids géopolitique.

AVEZ-VOUS UN MEILLEUR SOUVENIR OU UNE ANECDOTE MARQUANTE À PARTAGER ?

Quand on vit des grosses alertes comme Log4Shell ou SolarWinds, on passe des nuits entières au bureau, toute l'équipe est mobilisée.

C'est intense, fatigant, mais on se sent utile. C'est ça aussi la cyber. Et une anecdote plus légère : dans les repas de famille, on me demande toujours de réparer les imprimantes, changer les claviers ou recommander une banque en ligne. Dès qu'on fait de la cyber, on est "l'interlocuteur SOS de la tech".

POURQUOI LE SUJET DE LA DIVERSITÉ EST-IL CRUCIAL DANS CE SECTEUR ?

Le secteur est encore très masculin, même si j'ai toujours travaillé avec des femmes dans mes équipes. Il y a une vraie volonté d'ouvrir le secteur, mais l'image reste un frein. L'image du hacker en sweat à capuche n'aide pas.

Pourtant, les femmes apportent une approche différente, parfois plus posée, plus méthodique, et c'est précieux en cybersécurité. Il faut plus de rôles modèles, et c'est grâce à des personnes comme elles que l'on change l'image du métier.

VOS CONSEILS POUR LES ÉTUDIANTS QUI VEULENT SE LANCER ?

Investissez-vous : allez à des conférences, participez à des CTF, lancez-vous dans des projets, même perso. La cyber ne se résume pas à un terminal, on peut la pratiquer partout.

Peu importe votre parcours, ce qui compte, c'est la motivation et la curiosité. Et surtout :
commencez tôt à acquérir de l'expérience, même bénévole. C'est ce qui fait la différence à l'embauche, partout dans le monde.

UN RÊVE DE CYBER-POUVOIR ?

" Donner de la cyber-vigilance à tout le monde. Si je pouvais, j'éduquerais tous les utilisateurs pour qu'ils arrêtent de cliquer sur n'importe quoi. Ça éviterait bien des incidents !

LA BOÎTE À OUTILS CYBER

Outils :

Shodan
CyberChef

Pour s'entraîner :

RootMe
TryHackMe
Hack The Box

Et surtout : **l'Institut SANS** pour la veille, les formations, les conférences et les CTF. Un incontournable pour monter en compétence.

Morgane NGUYEN

Adjointe RSSI

“Ce qui donne du sens à mon métier, c’est de protéger, d’anticiper, et de permettre à une organisation de tenir bon quand un incident de cybersécurité survient.”

PARCOURS

1. **Études supérieures :** Classe prépa scientifique - École d’ingénieur généraliste (Arts et Métiers).
2. **Premier poste chez Solucom** (devenu Wavestone) en tant que consultante en systèmes d’information.
3. **Très vite exposée à des projets en cybersécurité,** elle bascule totalement dans ce domaine au bout d’un an.
4. **Spécialisation progressive** sur les sujets de détection et gestion des incidents de sécurité.
5. **Rejoint l’Institut Pasteur comme adjointe RSSI,** avec un focus fort sur la détection, la réponse aux incidents, la gestion des vulnérabilités et les audits de sécurité.

EN QUOI CONSISTE VOTRE MÉTIER AUJOURD’HUI ?

Je suis adjointe au RSSI de l’Institut Pasteur. Mon périmètre est centré sur la sécurité opérationnelle : la détection et la réponse aux incidents, la gestion des vulnérabilités, et les audits de sécurité.

Je manage une équipe d’analystes cyber, et je garde volontairement deux journées par mois sur le traitement d’alertes, pour rester connectée au terrain. Cela me permet de comprendre les enjeux concrets auxquels font face mes équipes, d’ajuster notre feuille de route, et de rester à jour sur les outils et les pratiques.

QU’EST-CE QUI VOUS A ATTIRÉE DANS LA CYBERSÉCURITÉ ?

En arrivant chez Solucom, j’ai eu la chance de travailler très tôt sur des projets en cybersécurité à fort impact. Ce qui m’a tout de suite plu, c’est que l’enjeu va bien au-delà de la compréhension technique : il s’agit de protéger les systèmes, de prévenir les risques tout en accompagnant les évolutions des métiers, de réagir vite. J’ai aussi rencontré des personnes passionnées, expertes et engagées, qui m’ont donné envie d’aller plus loin. Très vite, j’ai su que c’était dans cette voie que je voulais m’investir.

Je suis entrée en cybersécurité, et je n’en suis jamais ressortie.

QUELLES SONT, SELON VOUS, LES COMPÉTENCES ESSENTIELLES POUR EXERCER CE MÉTIER ?

Sur le plan technique, il faut évidemment comprendre l’environnement : systèmes, réseaux, détection, vulnérabilités… Même si je ne vais pas aussi loin techniquement que mes équipes, je dois pouvoir les accompagner, les guider, et évaluer leurs besoins.

Côté soft skills, il faut être capable de vulgariser et d’adapter son discours, savoir animer une équipe, créer du lien et faire monter les collaborateurs en compétences.

Il faut aussi être curieux et avoir envie d'apprendre en continu. Sans oublier la capacité à rendre la cyber accessible. Travailler avec les utilisateurs, c'est essentiel, et ils doivent être en capacité de comprendre sans être noyés dans du jargon technique.

QU'EST-CE QUE VOUS PRÉFÉREZ DANS VOTRE MÉTIER AUJOURD'HUI ?

Ce que je préfère, c'est le côté vivant de la cyber qui évolue sans cesse. C'est exigeant, mais c'est ce qui rend le sujet fascinant. J'aime aussi côtoyer des personnes passionnées. Dès mes débuts, j'ai été marquée par cette culture de la passion dans la cyber. C'est contagieux, motivant et inspirant.

AVEZ-VOUS UN SOUVENIR MARQUANT À PARTAGER ?

Je suis intervenue sur une crise de ransomware chez un client, quand je travaillais chez Wavestone. L'entreprise était à l'arrêt complet, c'était très impressionnant de le vivre. C'est là que l'on réalise à quel point notre métier est concret, stratégique, utile. On ne se pose plus de questions : on agit, on aide, on est là pour remettre l'organisation sur pied. C'était intense et très formateur.

QUELS SONT LES GRANDS DÉFIS À VENIR, NOTAMMENT AVEC L'IA ?

L'IA va probablement faciliter les attaques. On le voit déjà : phishing mieux rédigés, escroqueries plus crédibles… Cela rend la détection plus difficile, surtout pour les utilisateurs non avertis. Mais je pense aussi que l'IA peut nous aider côté défense. Elle peut améliorer la détection, accélérer les réponses, nous faire gagner du temps sur certaines

VOS CONSEILS POUR LES ÉTUDIANTS QUI VEULENT SE LANCER ?

- Je leur dirais de se construire une veille le plus tôt possible. D'apprendre à suivre l'actualité, à identifier les bonnes sources, à rester curieux. C'est une habitude à prendre, et elle est indispensable.

- Je conseille aussi de découvrir plusieurs facettes de la cyber avant de se spécialiser. Cette vision globale est précieuse, même si on veut devenir analyste ou pentester.

UN RÊVE DE CYBER-POUVOIR ?

« J'aimerais, juste en clignant des yeux, pouvoir cartographier entièrement un système d'information et comprendre comment tout fonctionne.Connaître son environnement, c'est le point de départ de toute bonne stratégie de défense.

LA BOÎTE À OUTILS CYBER

Hack The Box, Root.me : pour comprendre les dessous techniques du hacking.

Le site de l'ANSSI : pour les bonnes pratiques et les alertes.

Le référentiel NIST : le standard international incontournable de la cybersécurité.

Des contenus plus accessibles de vulgarisation comme **le podcast Le Monde de la Cyber.**

Joséphine DELAS

AI Engineer

"L'IA et la cybersécurité ne sont pas des boîtes noires réservées aux experts. Ce sont des disciplines que l'on peut apprendre, comprendre, et rendre plus inclusives."

PARCOURS

1 **Études supérieures :** prépa scientifique - École polytechnique (formation généraliste avec focus sur l'informatique) - spécialisation en IA.

★ **Découverte de la cybersécurité :** grâce à un cours "capture the flag" à l'X.

2 **Master de recherche au Canada :** fiabilité des systèmes de détection d'intrusion basés sur l'IA, avec une approche théorique (apprentissage par renforcement).

3 **Retour en France & Harfanglab -** application concrète de l'IA en cybersécurité : détection de malwares, modèles embarqués, assistants analystes cyber.

EN QUOI CONSITE VOTRE MÉTIER CONCRÈTEMENT ?

Je travaille dans l'équipe IA chez Harfanglab. L'objectif principal, c'est d'utiliser l'intelligence artificielle pour améliorer notre produit, l'EDR, et aider l'utilisateur final, l'analyste cyber.

Il y a deux grands volets :

- Détection d'attaques/malwares via l'IA : on développe des modèles performants, mais aussi légers, pour qu'ils s'exécutent rapidement et avec peu de ressources.

- Assistant analyste cyber : on utilise des modèles de langage pour contextualiser les attaques, guider l'investigation, proposer des pistes. Le but, c'est d'aller au-delà du simple chatbot.

Cela implique aussi une vraie gestion de la donnée : collecter, nettoyer, structurer, et réentraîner régulièrement les modèles pour qu'ils restent pertinents face à des menaces en constante évolution.

QU'EST-CE QUI VOUS A ATTIRÉE DANS L'INFORMATIQUE ?

Je pense que c'est le côté très logique. J'aime bien les maths parce que c'est logique, et l'informatique pousse encore plus loin cet aspect. Tout peut s'expliquer. On sait qu'il y a une réponse, et qu'on peut l'atteindre étape par étape. Cela me rassure.

Je suis assez cartésienne, et je n'aime pas être face à une page blanche. L'informatique me convenait bien pour cela. Même au lycée, je m'amusais déjà un peu à coder sur les calculettes.

QUELLES SONT LES COMPÉTENCES TECHNIQUES CLÉS POUR EXERCER VOTRE MÉTIER ?

En IA, il est essentiel d'avoir un socle scientifique solide, notamment en mathématiques, probabilités et statistiques. Ce sont des compétences qui différencient l'IA d'autres disciplines informatiques.

Mais au-delà de la théorie, il faut aussi savoir vraiment coder, car la gestion des données, l'entraînement des modèles, leur déploiement, tout cela repose sur des compétences d'ingénierie logicielle.

L'IA n'est pas qu'une affaire de maths ou de R&D. Il faut être capable de transformer un modèle en un outil efficace, robuste, rapide, et qui fonctionne dans un environnement réel, avec des contraintes. Il faut donc aimer la complexité,mais aussi savoir la rendre utile.

QUELS SONT LES DÉFIS FUTURS DE L'IA ET DE LA CYBERSÉCURITÉ ?

Le rythme d'adoption est extrêmement rapide, parfois au détriment de la réflexion ou de la réglementation. L'IA explose depuis 2-3 ans, et la législation n'a pas encore suivi.

Ce qui me semble préoccupant, c'est le décalage entre la réalité et les normes. Il y a encore très peu de contrôle sur les modèles et les données d'entraînement. Il faut harmoniser, sécuriser, rendre l'IA plus compréhensible et éthique pour tous.

QUELLE EST VOTRE VISION DE LA DIVERSITÉ DANS LES MÉTIERS DE L'IA ET DE LA CYBER ?

Pendant longtemps, j'étais la seule femme dans mon équipe. Aujourd'hui, nous sommes deux.

C'est encore trop peu, mais c'est un début. Je ne vois pas d'évolution radicale ces dernières années, même si tout le monde dit que cela bouge. Pour moi, plus de mixité, c'est plus de points de vue, donc plus d'intelligence collective. Et en IA c'est crucial, car les biais sont présents partout.

VOS CONSEILS POUR LES ÉTUDIANTS QUI VEULENT SE LANCER ?

Ne vous laissez pas impressionner : "Cyber", "IA", ce sont des mots qui font peur. Mais en fait, c'est accessible. Il y a énormément de ressources gratuites et des gens passionnés prêts à aider. Il faut oser poser des questions.

Et surtout, ne vous comparez pas trop. Le domaine est vaste. On peut être expert sur un sujet et ignorer un domaine connexe. Il y a de la place pour tous les profils.

UN RÊVE DE CYBER-POUVOIR ?

" Un traducteur magique ! Quelque chose qui prend n'importe quelle techno ou jargon et l'explique simplement. Pour gagner du temps et apprendre efficacement, sans avoir l'impression d'être ignorant ou incompétent.

LA BOÎTE À OUTILS CYBER

En IA, on travaille surtout en Python. Il existe des bibliothèques open source optimisées pour l'entraînement et la manipulation de modèles : Scikit-Learn, PyTorch, mais aussi le traitement de données : Pandas.

Le livre "Deep Learning" disponible en ligne : deeplearningbook.org

En cyber, je recommande les **blogs spécialisés**, souvent très concrets : *itm4n.github.io ou thehacker.recipes*

Imane DAHOU

Manager Cybersecurity, Data Protection & IT Risks

"La cybersécurité, ce n'est pas que de la technique, c'est une lecture du monde, du pouvoir, de la société."

PARCOURS

Découverte de la cybersécurité : par les exercices de crise avec l'ANSSI - prise de conscience du caractère systémique du risque cyber.

1 **Études supérieures :** master Défense et Dynamiques Industrielles / MPA en stratégie militaire et politiques de défense.

2 **Stage de fin d'études :** journaliste - assistante rédacteur en chef au desk Moyen-Orient chez France 24.

3 **General Electric - Direction de la Sûreté :** project Risk Analyst - sécurisation de projets d'énergies renouvelables (Afrique, Moyen-Orient, Asie, Amériques) - analyste de risques pays - gestion de crise et continuité d'activité.

4 **Haut Comité français pour la défense civile - Déléguée générale adjointe :** participation aux exercices de crise nationaux et aux pressions médiatiques simulées associées (Vigipirate, Piranet, Piratair, etc.) - réflexion sur la doctrine et la politique sécuritaire de la France.

5 **Deloitte – Direction Risques et Sécurité :** premiers pas en GRC, implémentation et audit du SMSI en France, UK et dans 16 pays d'Afrique - passage de certifications (ISO 27001 LI, 27005 RM, EBIOS RM) - pilotage du TPRM (gestion des risques liés aux tiers) - data manager.

6 **Accenture :** conseil en cybersécurité et spécialisation en services financiers - premiers pas dans l'enseignement (IMT Lille, Polytechnique, UPC).

7 **Sia :** conseil en cybersécurité - enseignement à Université Paris Cité - engagements externes & rayonnement (GITEX, WAICF, OTAN, Europol, FIC).

QUELLES COMPÉTENCES TECHNIQUES ET NON-TECHNIQUES SONT ESSENTIELLES EN CYBERSÉCURITÉ ?

La première brique, c'est la compréhension des fondamentaux, à commencer par l'ISO 27001. Ce référentiel structure la gouvernance de la sécurité de l'information autour de trois piliers indissociables : la confidentialité, l'intégrité et la disponibilité. Son annexe A fournit une véritable cartographie des mesures techniques et organisationnelles à mettre en œuvre.

La technique ne suffit pas. En cybersécurité, les compétences humaines sont essentielles : maîtrise de l'anglais, posture professionnelle, lecture fine des enjeux. Comprendre les dynamiques géopolitiques et économiques est devenu indispensable.

La cybersécurité, c'est autant les systèmes que les rapports de pouvoir. Et s'il ne fallait en retenir qu'une : la curiosité, moteur d'agilité et de lucidité.

AUJOURD'HUI, QUE PRÉFÈREZ-VOUS DANS VOTRE MÉTIER ?

Le fait de travailler sur un sujet crucial. Oui, en cybersécurité, on sauve des vies, des économies, des pays. Cela donne du sens. J'adore aussi la diversité des profils dans mes équipes, l'émulation intellectuelle, l'exigence bienveillante. Et surtout, l'enseignement. Cela me pousse à rester à jour, à me remettre en question. Et les jeunes me challengent. Ils ont un regard frais, cela me nourrit.

QUELS SERONT LES GRANDS DÉFIS À VENIR, NOTAMMENT AVEC L'IA ?

Le principal défi, c'est la gouvernance. L'IA bouscule les silos traditionnels et impose une collaboration étroite entre cybersécurité, data, juridique, conformité et éthique. Le CISO y joue le rôle de chef d'orchestre, avec des politiques internes claires mais pragmatiques. Trop de rigidité pousse au contournement, trop de souplesse fragilise l'organisation. La formation est aussi essentielle pour bâtir une culture commune et que chacun comprenne le rôle des autres. Enfin, il faut rester vigilant face aux biais algorithmiques et à leurs impacts éthiques ou discriminatoires.

POURQUOI LA DIVERSITÉ EST-ELLE IMPORTANTE DANS CES MÉTIERS ?

La diversité est à la fois un impératif éthique et un gage d'efficacité. Dans le numérique, et surtout dans l'IA, son absence alimente les biais et fragilise la confiance. Des profils variés permettent d'anticiper les risques, d'innover et d'aborder les enjeux sous des angles inédits.

Je l'ai vécu : des parcours différents enrichissent l'analyse. Et il faut des rôles modèles pour montrer que la cybersécurité, ce n'est pas que de la technique - c'est aussi de l'humain.

UN SOUVENIR MARQUANT DANS VOTRE PARCOURS ?

Un audit au Tchad, sous escorte armée, a marqué un tournant. J'y ai compris que la cybersécurité dépasse les normes : elle prend tout son sens sur le terrain, là où la technique rencontre l'humain. Cette expérience m'a appris à sortir des cadres, à écouter, à m'adapter. Elle m'a rappelé que derrière chaque système, il y a un contexte, des vulnérabilités humaines, des rapports de force. Et que c'est là que notre métier prend toute sa valeur.

VOS CONSEILS POUR LES ÉTUDIANTS QUI VEULENT SE LANCER ?

Soyez curieux, entourez-vous et posez des questions. Rejoignez des associations étudiantes : vous y rencontrerez des pros, des institutionnels, des pairs. Et surtout : restez vous-mêmes. Il n'y a pas un seul profil type.

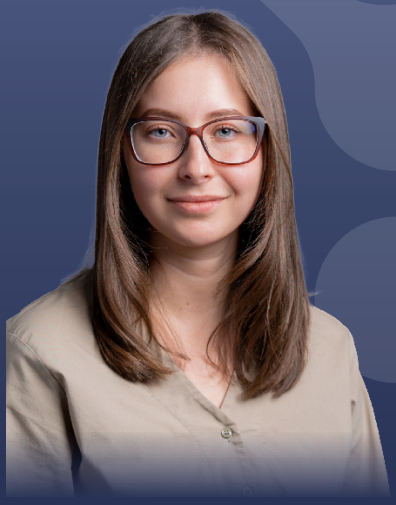
UN RÊVE DE CYBER-POUVOIR ?

« J'aimerais avoir les capacités de traitement d'un LLM pour anticiper les menaces, décoder les signaux faibles, prendre les bonnes décisions… avant même que les autres aient formulé les bonnes questions.

LA BOÎTE À OUTILS CYBER

Le site **EUR-Lex** : *eur-lex.europa.eu* Pour lire les textes réglementaires de l'UE. C'est là que se joue l'avenir.

Lire les **livres blancs** de l'ANSSI, de l'OTAN, du CESIN, d'Interpol. Des cas d'usage concrets et inspirants.



Livia TIBIRNA

Analyste Cyber Threat Intelligence

“Le cyberespace n’est plus un domaine technique isolé, mais un théâtre d’affrontement géopolitique à part entière.”

PARCOURS

1. **Formation :** master en Relations Internationales, spécialisation Europe de l’Est et espace post-soviétique.
2. **Stage de fin d’études :** cabinet d’intelligence économique : investigations numériques appliquées à des enjeux économiques internationaux.
3. **Première expérience en Cyber Threat Intelligence (CTI) :** découverte de la CTI chez Intrinsec.
4. **Analyste en Cyber Threat Intelligence Stratégique** depuis plus de 4 ans chez Sekoia : analyse de menaces, contextualisation géopolitique, spécialisation sur les menaces russophones.

EN QUOI CONSISTE VOTRE MÉTIER ET QUEL EST LE RÔLE DE VOTRE ÉQUIPE ?

Je suis analyste en Cyber Threat Intelligence chez Sekoia, un éditeur de logiciels spécialisé dans la détection et la réponse aux menaces. Je travaille au sein d’une équipe d’une vingtaine d’analystes. Ma mission est d’analyser et d’anticiper les attaques, en identifiant les groupes d’attaquants, leurs tactiques, leurs motivations, et en contextualisant les campagnes pour nos clients.

Mon travail alimente directement notre solution logicielle : les clients consultent les résultats de nos investigations, accèdent à des fiches détaillées, et peuvent connecter notre veille à leur environnement pour mieux détecter les menaces, les comprendre et réagir rapidement.

CONCRÈTEMENT, COMMENT EST-CE POSSIBLE D’ANTICIPER DE FUTURES ATTAQUES ?

Les attaquants ont des ressources limitées et des schémas d’attaque souvent cohérents dans le temps. Il est possible de repérer ces patterns, de suivre les évolutions, et ainsi d’anticiper les prochaines campagnes en fonction de leur logique passée.

Nous plaçons des capteurs sur différents réseaux pour détecter les signaux faibles. Et lorsque de nouveaux indicateurs émergent, nous les corrélons à des groupes connus ou nouveaux. Cela permet à nos clients de réagir plus vite, tout en ayant une vision claire du contexte et des actions à mener.

QUELLES COMPÉTENCES SONT INDISPENSABLES POUR EXERCER VOTRE MÉTIER ?

Ce métier requiert une excellente capacité d’analyse, de la rigueur, une bonne culture générale, de la curiosité, et un vrai sens de l’observation.
Il faut savoir contextualiser les faits techniques, marier des indicateurs de compromission avec des dynamiques politiques ou géopolitiques : c’est un métier pluridisciplinaire, à la croisée du technique, du stratégique, du législatif et du comportemental.

Les compétences linguistiques sont aussi essentielles : comprendre une langue étrangère permet de suivre diverses publications sur le Dark Web, Telegram, ou autres réseaux exploités par les cybercriminels, lire et interpréter leurs conversations, identifier des comportements culturels, autant d'éléments clés dans l'analyse ou l'attribution.

QU'EST-CE QUI VOUS PASSIONNE LE PLUS DANS VOTRE MÉTIER AUJOURD'HUI ?

Le fait d'être à la croisée de plusieurs mondes : technique, stratégie, géopolitique. C'est une discipline en mouvement constant, avec une richesse humaine et intellectuelle immense. J'apprends tous les jours, je collabore avec des spécialistes aux parcours variés, et je contribue à protéger le monde du numérique, un espace qui nous concerne tous aujourd'hui : particuliers, entreprises, organisations ou États.

COMMENT VOYEZ-VOUS L'AVENIR DE LA CYBERSÉCURITÉ ?

Je m'attends à une massification des menaces, à des attaques plus rapides, plus automatisées, plus sophistiquées. Je vois aussi une porosité grandissante entre cybercriminalité, cyberactivisme et attaques étatiques, ce qui rend l'analyse et l'attribution de plus en plus complexes. Enfin, un des défis sera organisationnel : savoir coopérer efficacement entre acteurs publics et privés va devenir indispensable pour faire face à une menace qui ne cesse de se professionnaliser.

QUEL ÉVÉNEMENT CYBER A MARQUÉ VOTRE PARCOURS ?

La résurgence des groupes activistes en 2022, dans le contexte de la guerre en Ukraine : on a assisté à une explosion d'activités, des coalitions informelles, des campagnes d'influence parfois mêlées à des actes de sabotage. Certains groupes étaient liés à des intérêts étatiques, d'autres non, et cette effervescence a rendu le suivi analytique très complexe. Cela a rendu la frontière entre criminalité, activisme et opérations étatiques encore plus floue. C'est à ce moment-là que l'on a mesuré à quel point le cyberespace n'était plus un domaine technique isolé, mais un théâtre d'affrontement géopolitique à part entière.

VOS CONSEILS POUR LES ÉTUDIANTS QUI VEULENT SE LANCER ?

- Travaillez votre culture générale et développez votre esprit critique. Soyez curieux, rigoureux, apprenez à faire des ponts entre différents domaines. Ne cloisonnez pas compétences techniques et non-techniques : les deux sont étroitement liées.
- Ne vous limitez pas à votre formation d'origine. Dans la cyber, ce sont votre motivation et vos compétences qui comptent.
- Entourez-vous, posez des questions, allez sur le terrain. Le monde de la cyber est ouvert à ceux qui s'y engagent vraiment.

UN RÊVE DE CYBER-POUVOIR ?

« J'aimerais pouvoir faire coopérer tous les décideurs au-delà des conflits géopolitiques, pour contrer les cybermenaces sans être bloqués par des limites politiques ou territoriales. Trop souvent, des attaques pourraient être stoppées si la coopération internationale était possible dans l'immédiat.

LA BOÎTE À OUTILS CYBER

VirusTotal : analyse d'URLs, fichiers et indicateurs malveillants

Shodan, Censys, etc. : outils de recherche pour cartographier les surfaces d'attaque

Raindrop : Outil de veille collaboratif

Romain MARCOUX

Expert en cybersécurité transverse, consultant indépendant

“Si vous souhaitez devenir indépendant, travaillez aussi vos compétences sociales, votre rigueur, et votre présence sur LinkedIn ! Rien ne remplace la confiance que vous inspirez par vos échanges”

PARCOURS

1. **Études supérieures :** DUT Réseaux et Télécoms et Master 2 en école d’ingénieurs spécialisée en télécoms et réseaux.
2. **Premier poste :** ingénieur systèmes et réseaux (gestion de pare-feu, premières expériences en cybersécurité).
3. **Spécialisation cyber :** CDI dans une entreprise pure-player - une immersion complète dans l’univers technique de la cybersécurité pendant 9 ans.
4. **Depuis 2021 : Consultant indépendant :** missions techniques, accompagnement de PME/ETI, conseil stratégique et gouvernance cyber.

EN QUOI CONSISTE VOTRE MÉTIER AUJOURD’HUI ?

Je suis consultant indépendant en cybersécurité, avec une approche transverse. J’accompagne tous types d’organisations :

- Des PME dans l’évaluation et l’amélioration de leur niveau de protection face aux cyberattaques, parfois jusqu’à l’implémentation technique ;
- Des ETI, pour lesquelles j’interviens de manière plus globale : remédiation, choix de solutions, configuration, conseil ;
- De grandes organisations (ministères, groupes CAC 40), sur des missions d’expertise ciblées et critiques, comme des migrations d’architectures ou des audits complexes.

Je suis également spécialisé sur les solutions Fortinet, notamment les pare-feu FortiGate, qui représentent une part significative de mon activité.

QUELLES COMPÉTENCES SONT ESSENTIELLES POUR RÉUSSIR DANS VOTRE DOMAINE ?

Une base technique solide est indispensable : connaître les architectures, comprendre les flux, maîtriser les outils. Il faut aussi savoir s’adapter aux contextes, dialoguer avec les clients, proposer des solutions réalistes et pragmatiques. C’est un métier d’équilibre : entre expertise et vulgarisation, entre autonomie et coopération.

COMMENT EN ÊTES-VOUS VENU À VOUS SPÉCIALISER DANS LES SOLUTIONS FORTINET ?

Lors de mes premières missions, j’ai souvent travaillé sur des environnements FortiGate. J’ai vite compris que cet écosystème, à la fois riche et souvent sous-exploité, offrait un vrai levier d’efficacité à condition d’en maîtriser les subtilités.

J’ai approfondi le sujet, partagé des connaissances et des bonnes pratiques, avec une approche pédagogique adaptée à différents profils. Aujourd’hui, j’interviens sur des configurations sensibles ou complexes, avec pour objectif de rendre la technologie plus claire et accessible.

QU’EST-CE QUI VOUS PLAÎT LE PLUS DANS VOTRE MÉTIER ?

Sans hésiter : l’échange et la transmission. J’aime faire progresser mes clients, les utilisateurs de mes outils, ou mes pairs dans la communauté cyber.

Et j'apprends autant d'eux que je leur transmets. Ce qui me stimule, c'est cette boucle d'enrichissement mutuel, souvent amplifiée par des outils comme LinkedIn, sans lesquels je ne serais peut-être jamais devenu freelance.

QUEL EST LE PROJET LE PLUS ORIGINAL, AMBITIEUX OU INATTENDU QUE VOUS AYEZ MENÉ ?

J'ai conçu et je maintiens une liste d'IP malveillantes agrégées à partir de plusieurs sources communautaires. L'idée m'est venue d'un client qui m'a demandé de scinder une liste trop longue pour certains pare-feux. Je l'ai publiée sur GitHub, et elle est aujourd'hui utilisée par des milliers de personnes dans le monde, y compris des intégrateurs reconnus. C'est un projet né d'un besoin terrain, devenu une ressource libre et vivante, à la croisée de la technique, du partage, et de l'utilité directe.

POUVEZ-VOUS PARTAGER UNE ANECDOTE MARQUANTE DE VOTRE PARCOURS ?

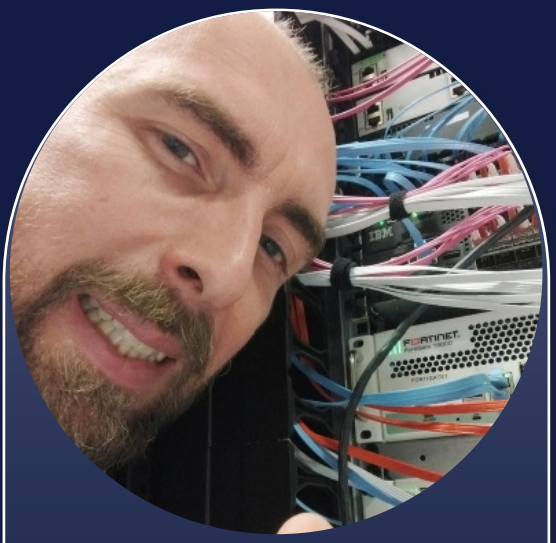
Lors d'une mission pour un groupe du CAC 40, j'ai été chargé de la migration d'une triple barrière de pare-feux, comptant chacun près de 4 000 règles de filtrage, destinée à protéger des systèmes particulièrement sensibles. Validation de passeports biométriques, transactions bancaires sans contact, activation de cartes SIM, entre autres. L'intervention s'est déroulée dans un data center ultra-sécurisé, sur un site dont l'emplacement est tenu "top secret". Les conditions d'accès physiques y étaient d'une rigueur extrême. Pour garantir qu'aucun matériel ne soit exfiltré, nous étions pesé à l'entrée et nous devions faire le même poids à la sortie. Ce type de projet à haute responsabilité vous rappelle à quel point la cybersécurité est essentielle au fonctionnement de services quotidiens.

QUELLE EST LA FAILLE OU L'INCIDENT QUI VOUS A LE PLUS MARQUÉ ?

L'attaque WannaCry en 2017. Elle exploitait une vulnérabilité connue de Microsoft, déjà corrigée deux mois avant sa diffusion. Malgré cela, elle a paralysé des géants comme Renault, Saint-Gobain, Maersk. C'est l'un des premiers événements où l'on a pu chiffrer précisément l'impact : plus de 300 millions de dollars pour certaines entreprises. Cette attaque a mis en lumière un fait fondamental : ne pas mettre à jour ses systèmes et le manque de cloisonnement peut coûter très, très cher.

QUELS SONT LES GRANDS DÉFIS À VENIR SELON VOUS ?

Tout est de plus en plus interconnecté, donc la surface d'attaque ne cesse de croître. Le contexte géopolitique rend aussi les cyberattaques plus nombreuses et plus variées. Face à cela, il faut former plus de professionnels, renforcer la collaboration entre acteurs, et ne pas négliger l'éducation des petites structures, qui restent très vulnérables. La cybersécurité reste, plus que jamais, un enjeu collectif.



UN RÊVE DE CYBER-POUVOIR ?

" Être ce super-héros de la cyber qui arrive au tout début d'une attaque, avant qu'elle ne fasse des dégâts, et qui aide les entreprises à colmater leurs failles avant qu'il ne soit trop tard. Être ce "Super Cyber Héros" qui intervient à temps et forme les équipes à prendre le relais.

LA BOÎTE À OUTILS CYBER

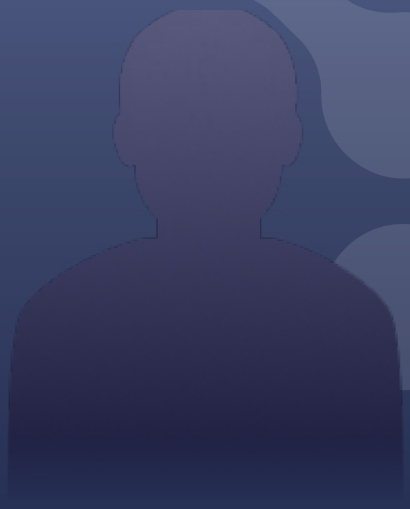
Ma liste d'IP malveillantes en open source : *https://github.com/romainmarcoux*

L'onglet «Outils» de mon site internet : *https://sekio.fr/outils.php*

Les outils que j'utilise le plus : **Notepad++ et Excel.**

Cygwin qui vous permet d'avoir un shell Linux sur votre poste Windows.

Les commandes **Linux** incontournables à maîtriser: **grep, awk, sed, sort, uniq**



Maksym ZAITSEV

Consultant indépendant en cybersécurité, formateur et développeur open source

"Ce n'est pas la compétence qui fait la différence. C'est la passion et la rigueur que l'on met dans ce que l'on fait."

PARCOURS

1. **Autodidacte précoce :** premier ordinateur à 5 ans - Premier site web codé à 10 ans - Rétro-ingénierie de jeux vidéo pendant l'adolescence, première approche concrète du hacking.
2. **Formation universitaire :** début en faculté, jugée trop théorique. éorientation vers une école d'ingénieur puis intégration d'une école spécialisée en cybersécurité (bac+3 puis bac+5).
3. **Stages et premières expériences** en startup, PME, banque et R&D : découverte d'environnements variés, de l'audit à la défense.
4. **Indépendant depuis plusieurs années :** formateur en cybersécurité (écoles, secteur public et privé) - Interventions sur des sujets offensifs, défensifs, sécurité logicielle, sécurité réseau, etc. - Missions d'audit, R&D et développement d'outils open source.

EN QUOI CONSISTE VOTRE MÉTIER AUJOURD'HUI ?

Je suis consultant indépendant en cybersécurité. J'interviens sur plusieurs volet : audit de code, tests d'intrusion, R&D, mais surtout formation, qui représente aujourd'hui près de 80 % de mon activité.

Je forme aussi bien des étudiants que des professionnels, dans des écoles comme Cybersup ou au sein de grandes entreprises, publiques comme privées. Je couvre des sujets variés : pentest, sécurité réseau, sécurité logicielle ou matérielle. Mon approche est toujours très concrète, orientée compétences et savoir-faire technique.

QUELLES SONT LES COMPÉTENCES ESSENTIELLES DANS VOTRE MÉTIER ?

Il faut évidemment de solides bases techniques, mais ce n'est pas suffisant. Il faut aussi être rigoureux, fiable, capable de vulgariser. Les compétences humaines, la pédagogie, la gestion du temps : tout cela est essentiel.

QUEL EST LE PROJET LE PLUS AMBITIEUX SUR LEQUEL VOUS AVEZ EU L'OCCASION DE TRAVAILLER ?

J'ai développé un outil open source appelé MorphAES, qui permet de générer du shellcode polymorphique en assembleur, c'est-à-dire du code capable de changer de forme à chaque génération tout en conservant la même fonction.

Cela permet de simuler des attaques plus réalistes lors de tests d'intrusion, notamment en contournant certaines détections antivirus souvent trop rigides, et de repérer des failles.

Ce projet, très technique, m'a permis d'intervenir en conférence, d'échanger avec des éditeurs de solutions de sécurité et de contribuer à faire évoluer les pratiques de défense.

Ce qui me motive c'est de créer un outil qui questionne les limites actuelles, tout en restant dans une démarche responsable : exposer des failles pour aider et non pour attaquer.

QUELLE EST LA FAILLE LA PLUS IMPROBABLE QUE VOUS AYEZ DÉCOUVERTE ?

Lors d'un audit dans une grande banque française, je me suis penché sur l'architecture cryptographique en place, et notamment sur un HSM, un boîtier matériel censé sécuriser des opérations critiques comme la génération ou le stockage de clés.

En l'analysant de près, j'ai découvert une porte dérobée : une fonctionnalité ni documentée, ni annoncée, mais qui permettait une prise de contrôle à distance, en contournant toutes les protections normales. Ce genre de cas rappelle que même les produits de sécurité peuvent avoir des failles, voire des fonctions cachées. La confiance dans un produit ne doit jamais être aveugle : il faut toujours auditer, vérifier, tester.

UN EXEMPLE DE MISSION PARTICULIÈREMENT CRITIQUE ?

J'ai été sollicité en urgence par une entreprise de luxe, victime d'un piratage ciblé : un attaquant avait discrètement modifié leur site e-commerce afin d'intercepter les coordonnées bancaires des clients au moment du paiement.

L'attaque était active depuis plusieurs jours lorsque je suis intervenu. L'origine du problème était tristement classique : le site reposait sur un CMS non mis à jour, contenant une faille connue et documentée depuis plusieurs mois. Un correctif existait, mais n'avait jamais été appliqué. Cette négligence avait suffi à exposer toute leur chaîne de paiement.

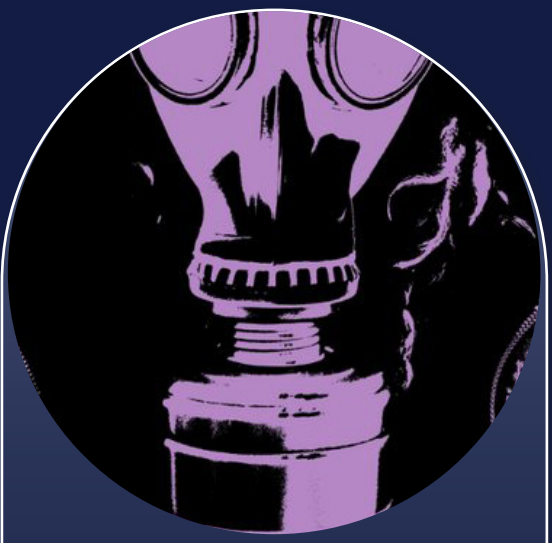
UN PROJET PARTICULIÈREMENT EXIGEANT ?

En 2017, j'ai contribué à l'analyse du leak de la NSA publié par le groupe Shadow Brokers. Ce dernier avait divulgué un ensemble d'outils d'exploitation très avancés, utilisés par l'agence pour infiltrer des systèmes à grande échelle.

Parmi eux figurait notamment EternalBlue, une vulnérabilité de type zero-day qui sera ensuite exploitée dans des attaques majeures comme WannaCry ou NotPetya. Mon rôle a consisté à analyser en profondeur ces outils, à comprendre leur logique, et à documenter leur fonctionnement pour permettre à la communauté de se défendre. C'était un travail exigeant qui m'a permis de contribuer à la correction de failles critiques ensuite.

VOS CONSEILS POUR LES ÉTUDIANTS QUI VEULENT SE LANCER ?

Soyez curieux, discipliné, et surtout : passionné. Ce n'est pas la meilleure école ou la plus grande entreprise qui fait tout. Ce qui compte, c'est votre implication personnelle. L'école est un point de départ. Ensuite, il faut lire, expérimenter, pratiquer.



UN RÊVE DE CYBER-POUVOIR ?

« Pouvoir me connecter instantanément à n'importe quelle machine au monde. Pas seulement pour attaquer mais pour patcher aussi vite que l'on peut compromettre, pour agir en temps réel, en attaque comme en défense.

LA BOÎTE À OUTILS CYBER

- **BlackArch Linux :** distribution ultra-complète pour l'offensif et le défensif
- **Security Engineering, Ross Anderson :** un classique technique et fonctionnel
- **GitHub MorphAES :** générateur de shellcode en assembleu
- **Environnement Linux + outils bas niveau :** assembleur, debuggers, scripts custom

Cécile DEGRUGILLIER

Lead CTI & Senior Incident Handler

"Dans mon métier ce qui m'anime, n'est pas uniquement de réagir, mais surtout d'anticiper et cela va au-delà de la technique : c'est comprendre les enjeux business, les tensions géopolitiques, et détecter et qualifier les signaux les plus faibles."

PARCOURS

Études supérieures : master 2 en géopolitique, géoéconomie et intelligence stratégique puis MBA Management des Risques, Sûreté Internationale et Cybersécurité à l'Ecole de Guerre Economique.

1

Découverte de la cybersécurité : sur le terrain, au cœur du CERT-FR, dans le traitement des opérations majeures de cyberdéfense françaises, aux côtés de profils variés. Une montée en compétence intensive grâce à un environnement technique stimulant des enjeux de souveraineté nationale et une équipe inclusive.

2

Plusieurs stages : dans le secteur de la défense.

3

ANSSI - Centre opérationnel (CERT-FR) : analyste au Bureau Situation et Analyse Participation à la cyberdéfense nationale pendant 4 ans ; contextualisation et vulgarisation des opérations pour les décideurs de haut niveau ; analyse des groupes d'attaquants et de leurs modes opératoires.

4

Société Générale - CERT : réponse aux incidents, veille stratégique, analyse de la menace cyber, astreintes. Référente CTI (Cyber Threat Intelligence) : pilotage de la connaissance de la menace, anticipation, partage d'informations (InterCERT France, communautés bancaires), rédaction d'analyses opérationnelles et stratégiques.

EN QUOI CONSISTE VOTRE MÉTIER AUJOURD'HUI ?

Je travaille au sein du CERT (Computer Emergency Response Team) du Groupe Société Générale qui est chargé de la détection, de l'analyse et de la réponse aux incidents de cybersécurité.

Mon rôle, en tant que Lead Analyst en Cyber Threat Intelligence, est d'analyser la menace, de suivre l'évolution des modes opératoires des attaquants, et d'anticiper et de détecter des attaques.

Cela passe par de la veille, du partage d'information entre pairs, et un travail de vulgarisation, pour s'adresser aussi bien aux équipes techniques qu'aux décideurs. tant au niveau opérationnel que stratégique. Nous intervenons pour l'ensemble des entités du Groupe, en France comme à l'international.

QUELLES SONT LES COMPÉTENCES ESSENTIELLES POUR EXERCER VOTRE MÉTIER ?

La curiosité : le secteur de la cybersécurité évolue vite, il faut constamment apprendre, rester au fait tant au niveau de l'évolution des technologies que des modes opératoires des attaquants.

La rédaction et la vulgarisation : il faut savoir rendre intelligible et contextualiser des informations techniques notamment sur le plan géopolitique pour des profils variés, parfois éloignés du monde cyber.

Une bonne culture technique : même si je ne code pas au quotidien, je dois comprendre une ligne de commande, les détails d'une attaque ou d'un incident.

COMMENT AVEZ-VOUS VU LE SECTEUR ÉVOLUER DEPUIS VOS DÉBUTS ?

À mon arrivée à l'ANSSI, les attaques relevaient surtout de l'espionnage. En 2015, celle de TV5Monde a marqué un tournant car il s'agissait d'un acte de sabotage.

L'année 2017 a été marquée par WannaCry, NotPetya. Ensuite, l'explosion des ransomwares a révélé l'ampleur systémique du risque cyber et la montée en puissance des cybercriminels.

Aujourd'hui, l'impunité recule : les forces de l'ordre multiplient les opérations coordonnées contre les groupes criminels. En parallèle, la culture du partage s'est renforcée : elle est désormais structurée, portée notamment par l'ANSSI et l'InterCERT France.

C'est un pilier essentiel de la défense collective. Enfin, le niveau de cybersécurité progresse en France, sous l'effet des régulateurs et d'échéances majeures comme les JOP Paris 2024.

QUELS SONT LES GRANDS DÉFIS ACTUELS ET À VENIR ?

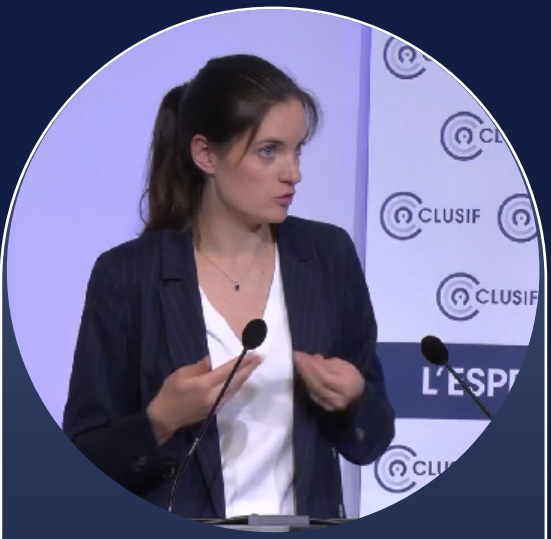
L'IA est déjà utilisée par les attaquants et cela va s'accentuer dans les différentes étapes de la kill chain : de la reconnaissance au traitement des données exfiltrées, par exemple. Le quantique représente également une rupture majeure à venir. Les attaquants se professionnalisent et adaptent rapidement leurs méthodes aux nouveaux usages et ces évolutions exigent une veille constante, de la curiosité, et une capacité à se préparer à l'inconnu.

POURQUOI LA DIVERSITÉ EN CYBERSÉCURITÉ EST-ELLE ESSENTIELLE ?

Les femmes sont peu nombreuses dans le domaine : elles représentent 14 à 16 % des effectifs dans le cyber, c'est très faible. Et pourtant, c'est un sujet stratégique, où les femmes ont évidemment leur place et permettent de réduire les biais. Il faut oser, ne pas se censurer. La diversité, ce n'est pas seulement une question de parité : elle renforce l'efficacité collective.

QUELS CONSEILS DONNERIEZ-VOUS À DES ÉTUDIANTS OU JEUNES DIPLÔMÉS QUI VEULENT SE LANCER ?

Osez. Même si vous ne cochez pas toutes les cases, allez-y. Posez des questions, demandez de l'aide. J'ai travaillé avec des experts de très haut niveau technique qui étaient incroyablement humbles et disponibles pour partager leurs connaissances. La communauté cyber, c'est une communauté de partage. Il ne faut pas hésiter à demander.



UN RÊVE DE CYBER-POUVOIR ?

"Avoir une coopération poussée à son paroxysme, entre les pairs, les forces de l'ordre, au niveau national et international et ancrer la culture cyber dans chaque esprit.

LA BOÎTE À OUTILS CYBER

Le site de l'ANSSI (informations, MOOC, CTF), suivre les flux d'actu (CERT-FR)

InterCERT France, éditeurs,..)

Podcasts : Le Monde de la Cyber, Le comptoir de la Secu

Certaines **plateformes** proposent des labs ou des contenus de qualité comme **ImmersiveLabs, Rangeforce, LetsDefend**

Le magazine MISC

Sophie THÉNOT

Head of Group CISO Office

''Je pense qu'il est temps de voir la cybersécurité non comme une contrainte, mais comme un partenaire stratégique et un accélérateur de confiance"

PARCOURS

1. **Formation initiale :** école de management Institut Mines-Télécom Business School.
2. **Première expérience professionnelle :** chargée de marketing digital dans une PME spécialisée en cybersécurité.
3. **Reconversion en cybersécurité :** transition vers le conseil en cybersécurité à l'occasion du rachat de la PME par Solucom (devenu Wavestone).
4. **Wavestone (2015–2021) :** missions de conseil en cybersécurité (sensibilisation, gestion de crise, gouvernance, pilotage de projet, création d'un benchmark cybersécurité national).
5. **FDJ United (depuis 2021) :** d'abord BISO (Business Information Security Officer) pour les activités digitales, puis responsable de la stratégie et de la gouvernance cybersécurité à l'échelle du groupe, dans un contexte international.

EN QUOI CONSISTE VOTRE MÉTIER AUJOURD'HUI ?

Je dirige une équipe de dix personnes, réparties entre profils internes et externes. Nous avons trois missions principales :

- Définir le cadre de gouvernance cybersécurité du groupe (politiques, plan de contrôle, cartographie des risques),
- Piloter la stratégie cybersécurité à l'échelle du groupe,
- Superviser le budget et les feuilles de route associées.

Nous contribuons également à des sujets techniques tels que l'accompagnement cybersécurité de la migration vers le Cloud ou les enjeux post-quantiques. Ce rôle exige une vision d'ensemble et une capacité à vulgariser les enjeux avec les membres du COMEX.

QUELLES COMPÉTENCES SONT NÉCESSAIRES POUR EXERCER VOS FONCTIONS ?

Dans mon métier, il faut être capable de prendre de la hauteur, pour comprendre les enjeux dans leur globalité, et les rendre intelligibles aux décideurs : la vulgarisation est une compétence clé.

Comme je ne suis pas issue d'un parcours technique, j'ai appris à aller chercher l'expertise dont j'ai besoin, et je m'entoure des bons profils. Ce qui compte, c'est de pouvoir piloter une stratégie claire et cohérente, et non de tout savoir faire soi-même.

UN MOMENT MARQUANT DANS VOTRE PARCOURS ?

Je repense à mes premières missions chez Wavestone, lorsque le client me demandait d'intervenir sur des projets très techniques alors que je devais initialement intervenir sur de la gouvernance...!

Je me suis retrouvée face à des profils techniques, dans des réunions où le niveau d'expertise rendait parfois difficile la compréhension immédiate des enjeux ou des attentes. Chaque matin, j'allais au travail sans savoir comment la journée allait se dérouler.... C'était vertigineux. Et en même temps, et à la fois extrêmement formateur : en 6 ans, j'ai l'impression d'avoir fait un bond de 10 ans en expérience.

UN PROJET PARTICULIÈREMENT ORIGINAL ?

Chez Wavestone, j'ai eu l'opportunité de piloter la création d'un baromètre sur la maturité cyber des entreprises. On était partis de zéro, avec l'idée de s'appuyer sur les référentiels connus sur le marché comme l'ISO ou le NIST. On a développé un questionnaire de 150 points couvrant les aspects gouvernance et outillage. Cet outil a été utilisé par plus de 150 entreprises et relayé dans les médias. Grâce à une dynamique d'équipe, une idée s'est transformée en un outil structurant au service de tout un écosystème.

CE QUE VOUS AIMEZ LE PLUS DANS VOTRE MÉTIER ?

La diversité des sujets : un jour je travaille sur l'IA, le lendemain sur la cyber-résilience, puis sur l'optimisation budgétaire ou la structuration d'une roadmap. J'ai l'impression de faire dix métiers en un avec une vraie mission de fond : protéger un système complexe en constante évolution.

COMMENT LE SECTEUR A-T-IL ÉVOLUÉ DEPUIS VOS DÉBUTS ?

Quand j'ai commencé, les profils comme le mien, femme issue du marketing ou du management, étaient très peu présents. Le secteur s'est ouvert progressivement. Aujourd'hui, les parcours hybrides sont mieux reconnus, et la place des femmes progresse. Mon équipe à la FDJ est d'ailleurs majoritairement féminine : impensable il y a quelques années à peine !

VOS CONSEILS POUR LES JEUNES QUI VEULENT SE LANCER ?

Ne laissez pas l'aspect technique vous intimider. La motivation, la curiosité et la rigueur comptent plus que le diplôme. Et surtout, faites-vous confiance. Vous n'avez pas besoin de tout savoir tout de suite. L'important, c'est d'apprendre, de savoir s'entourer, et de rester en mouvement.

UN RÊVE DE CYBER-POUVOIR ?

« J'aimerais que la cybersécurité s'impose naturellement dès l'initiation de tout projet et qu'elle soit spontanément considérée comme un partenaire stratégique, et non comme un frein ou une obligation.

LA BOÎTE À OUTILS CYBER

OpenClassrooms : ressources gratuites de qualité, en particulier pour les bases techniques

ANSSI : documentation officielle (gestion de crise, bonnes pratiques)

LinkedIn & podcasts : pour la veille et la vulgarisation

CYBERSUP, PARTENAIRE DES ACTEURS QUI FONT LE NUMÉRIQUE.

Cybersup développe des **partenariats** pédagogiques techniques d'**excellence** pour offrir à ses étudiants des formations alignées sur les standards des entreprises et les **évolutions du numérique.**

"Nos partenariats pédagogiques avec des acteurs de référence comme AWS, Cisco, Microsoft, Huawei, Red Hat et bien d'autres, sont au cœur de notre approche.
Ils permettent à nos étudiants de travailler sur les mêmes outils et environnements que dans les entreprises, de passer des certifications reconnues et de se confronter à des cas concrets dès leur formation.
Pour les entreprises qui recrutent nos étudiants en alternance ou en CDI, c'est une garantie : elles accueillent des jeunes déjà opérationnels, motivés et capables de contribuer rapidement à leurs projets."

Laurent Biagiotti, Directeur pédagogique Cybersup

Cybersup permet aux entreprises de recruter des alternants **opérationnels et employables, confiants** et agiles dans un monde du travail en **constante mutation.**

Ils nous font déjà **confiance** pour renforcer leurs équipes **IT, cybersécurité et data.**

LIVRET ÉDITÉ PAR
CYBERSUP

Cybersup est l'**École de la Protection Numérique,** fruit de l'alliance entre le groupe FROJAL (Lefebvre Dalloz) et l'école du numérique La Plateforme. Grâce à ce partenariat exclusif, Cybersup forme des profils incontournables de la **cybersécurité** à la croisée de l'informatique et du réglementaire.

Elle combine ainsi l'excellence de la **pédagogie projet** active développée par La Plateforme depuis 2019 avec l'**expertise** reconnue de Lefebvre Dalloz (marque française du groupe Lefebvre) dans le domaine réglementaire, en particulier dans le droit du numérique. Cybersup propose des **formations** de Bac+3 à Bac+5 (Bachelor et MSc., titres RNCP de niveau 6 et 7), en Cybersécurité, IA & Data, DPO & Digital Compliance.

CONCEPTION ET RÉALISATION

Directeur de Publication : Société FROJAL EDUCATION, Présidente de Cybersup représentée par la société FROJAL.
Directeurs de Création : Steve DANINO, Manon PELLAT, Amandine FLAMENT
Chef de Rédaction : Leslie FORNERO

CYBERSUP

ÉCOLE SUPÉRIEURE DE CYBERSÉCURITÉ ET IA

RENDEZ-VOUS SUR NOTRE SITE INTERNET

www.cybersup.ai

et sur nos réseaux sociaux