OCT 22

N°6

DigitalLovers

FOCUS

Confiance numérique et résilience : quels enjeux face aux nouvelles menaces ?

TRANSFORMATION

Le cloud de confiance au regard de la souveraineté et de la sécurité

ENGAGEMENT

Les rôles modèles du Groupe Sopra Steria en première ligne pour attirer toujours plus de talents féminins dans la tech

PAPIER 100% RECYCLÉ

MAGAZINE 100% RECYCLABLE

*Le monde est tel que nous le façonnons.

The world is how we shape it*

sopra steria

Dans un monde où la transformation digitale est une évidence pour beaucoup, et où la récente crise sanitaire a considérablement accéléré les usages du numérique, il est légitime d'éprouver une inquiétude croissante face aux risques cyber. C'est ce que révèle notre étude sur les Français et la cybersécurité, réalisée en avril 2022 en partenariat avec Ipsos : **82% de nos concitoyens expriment une crainte face aux risques d'une cyberattaque dans le monde et 79% en France.** En effet, au fil des transformations numériques, la cybersécurité est devenue un enjeu crucial permettant d'assurer la pérennité des activités, la souveraineté et l'indépendance des organisations publiques ou privées.

Alors, dans un contexte incertain qui fait à présent entrer la cyberguerre dans la réalité, **comment (re)donner confiance en la tech ? Comment assurer la protection et la résilience face aux cyberattaques de nos systèmes d'information, devenus indispensables à la bonne marche de notre société et notre économie ?**

En tant qu'acteur de la tech, notre engagement pour garantir cette confiance numérique prend de multiples formes. Celle de la création d'un écosystème de confiance avec le Campus Cyber France par exemple. Évidemment, celle de l'excellence déployée au quotidien par nos équipes d'experts en cybersécurité auprès de nos clients. Mais aussi en se tournant vers le futur, en formant les talents de demain sur des sujets de pointe, comme l'illustre le partenariat entre Sopra Steria Next et l'emlyon autour d'un cursus spécialisé en cybersécurité et défense.

Fabien Lecoq
Directeur Cybersécurité
chez Sopra Steria

Notre objectif ? **Ne pas faire de la sécurité un obstacle à l'innovation ou aux expérimentations mais bien un accélérateur de croissance et de confiance.**

Bonne lecture !

Impression éco-responsable

PAPIER 100% RECYCLÉ

MAGAZINE 100% RECYCLABLE

Le magazine DigitalLovers est imprimé sur un papier 100% recyclé, certifié FSC™ Recyclé et Écolabel Européen, issu à 100% de déchets de consommation. L'impression a été gérée par un imprimeur labellisé imprim'vert utilisant des encres végétales. Le papier utilisé ainsi que la reliure avec 2 piqûres métal permettent au magazine d'être 100% recyclable.

Crédits photos
Getty Images, Sopra Steria

Rédaction
Sopra Steria

Création et mise en page
Agence SMARTSON

Sommaire

4 **FOCUS**
Sopra Steria au coeur du Campus Cyber : ensemble, au service d'une grande nation cyber

10 **MÉTIER**
Les équipes Gouvernance Risques et Conformité, piliers de la cybersécurité

12 **TRANSFORMATION**
Le cloud de confiance au regard de la souveraineté et de la sécurité

19 **CONSEIL**
Retour sur le partenariat entre l'emlyon business school et Sopra Steria Next

25 **ENGAGEMENT**
Les rôles modèles du Groupe Sopra Steria en première ligne pour attirer toujours plus de talents féminins dans la tech

30 **ACTUALITÉS**
Quoi de neuf chez Sopra Steria ?

39 **BANDE DESSINÉE**

Sopra Steria au cœur du Campus Cyber : ensemble, au service d'une grande nation cyber

Engagés de longue date dans le développement de notre offre de cybersécurité et cyberdéfense, et soucieux de nous inscrire durablement parmi les leaders de la cyber en France, nous avons souhaité nous impliquer dans la création du Campus Cyber dès sa genèse en 2019.

Jean-Luc Gibernon
Représentant de Sopra Steria
au Conseil d'administration
du Campus Cyber

Qu'est-ce que le Campus Cyber ?

Projet initié par le Président de République, le Campus Cyber est le « lieu totem » de la cyber qui rassemble les principaux acteurs nationaux et internationaux du domaine. Il accueille sur un même site des entreprises (grands groupes, PME), des services de l'État, des organismes de formation, des acteurs de la recherche et des associations. Le Campus Cyber met en place des actions visant à fédérer la communauté cyber et à développer des synergies entre ces différents acteurs. À ce jour, ils sont plus de 160, issus d'une pluralité de secteurs d'activité, à s'y être engagés. Situé à la Défense, le Campus Cyber accueille 1 500 personnes dans une tour entièrement dédiée à ses activités, qui a ouvert ses portes au printemps 2022.

Quelles sont les 4 grandes missions du Campus Cyber ?

L'une des premières missions du Campus Cyber est de permettre un **partage d'informations** en temps réel entre les acteurs du secteur, sur un réseau de confiance ultra-sécurisé, dans un contexte de crise cyber majeur. Figurant parmi les tout premiers acteurs à avoir reçu la qualification Prestataire de Détection des Incidents de Sécurité (PDIS), Sopra Steria pourra apporter dans ce cadre son expérience en gestion de crise pour le compte de ses clients.

Puisqu'il importe d'innover pour mieux se protéger, le Campus Cyber a également pour mission de **favoriser l'innovation.** Pour cela, des synergies seront créées entre acteurs publics et privés et des programmes communs vont rassembler grandes entreprises, startups et centres de recherche.

Le **développement des formations** est également une mission du Campus Cyber : formations initiales et continues bénéficieront du cadre de travail qu'offre le Campus Cyber et des synergies qu'il permet, avec pour objectif de faire monter en puissance la filière française de la cyber en formant les talents de demain.

Enfin, le Campus Cyber est un lieu vivant et ouvert, dédié à la programmation d'événements et aux échanges, c'est ainsi qu'il assure pleinement sa mission d'**animation de l'écosystème.**

Pourquoi Sopra Steria participe au Campus Cyber ?

Dans un contexte international fortement marqué par l'augmentation du nombre de cyberattaques (+37 % en France entre 2020 et 2021) et une inquiétude grandissante (82 % des Français se disent inquiets face aux risques d'une cyberattaque dans le monde*), notre présence au Campus Cyber réaffirme notre engagement dans la construction d'un numérique de confiance et la lutte contre les menaces en Europe et dans le monde.

Cet engagement passe aussi par le partage et la collaboration des acteurs impliqués pour adresser les sujets d'innovation sensibles. C'est par exemple le cas de la voiture connectée, en associant sur un même plateau consommateurs, distributeurs et créateurs de solutions de cybersécurité.

Pour travailler au plus près de ces créateurs et contribuer ainsi à l'émergence de solutions technologiques de confiance à l'échelle nationale et européenne, Sopra Steria a décidé d'investir dans le fonds Brienne III piloté par Tikehau Ace Capital, premier fonds français entièrement dédié à la cyber, mais également en tissant des partenariats avec des centres de recherche tels que CEA Tech.

Rassembler les acteurs majeurs de la cybersécurité, publics et privés, c'est aussi créer les conditions pour former rapidement et collectivement les experts de demain. Dans ce contexte, nous apporterons notre pierre à l'édifice en capitalisant sur notre approche créative et immersive de la formation, développée depuis de nombreuses années en interne, à travers l'organisation régulière de bootcamps et de challenges cyber de type « Capture The Flag », qui donnent l'opportunité de s'affronter en équipe. La proximité avec des écoles partenaires de Sopra Steria, comme l'EPITA ou l'EFREI, présentes au Campus Cyber, est également une clé de réussite supplémentaire de cet écosystème d'excellence.

Les équipes de la BU Cyber, de l'agence Cyberdéfense, d'EvaBssi et de Galitt, marques du Groupe Sopra Steria, disposent au Campus Cyber d'un espace privatisé de 500 m², qui nous permet d'apporter notre contribution à ce grand projet et de tirer pleinement parti des opportunités qu'il apporte.

**Les Français et la cybersécurité, étude Ipsos pour Sopra Steria, avril 2022*

Équipes cyber recherchent talents énergiquement

Alexandra Jacobberger
DRH Adjointe Infrastructures and Security Services chez Sopra Steria

Consultants cyber, architectes, analystes… Notre activité cybersécurité recrute pour renforcer les équipes qui œuvrent au quotidien pour la protection des systèmes d'information de nos clients.

En 2023, nous prévoyons ainsi de recruter 360 profils de tous niveaux d'expérience : confirmé, jeune diplômé, stagiaire ou encore alternant, sur nos sites de Toulouse, Paris, Rennes, Toulon, Aix et Lyon.

Au programme: des missions passionnantes pour construire ensemble un numérique de confiance. Alors, rejoignez-nous!

- **250 CDI**
- **30 offres d'alternance**
- **80 stages à pourvoir**

Rejoignez nos équipes cyber !

Ransomwares et cybercriminalité : les nouvelles menaces

1. **Margaux Blandel-Coquet**
Chef de projet Cyberdéfense
chez Sopra Steria

2. **Guillaume Magniez**
Manager Cyberdéfense
chez Sopra Steria

3. **Antoine Vaillant**
Responsable technique
chez Sopra Steria

4. **Laurent Graff**
Ingénieur Cyberdéfense
chez Sopra Steria

Les ransomwares ?

Le 12 mai 2017, le monde découvre **Wannacry**. 150 pays touchés, 300 000 victimes, un correctif qui tarde à être mis à disposition, une panique mondiale : **il s'agit de la première campagne de ransomware (rançongiciel) médiatisée de l'histoire.** Cinq ans plus tard, pas une semaine ne passe sans un article de la presse généraliste sur le sujet : hôpitaux, administrations, entreprises, start-up sont les victimes quotidiennes de criminels d'un nouveau genre. Les suspects se font appeler Conti, Clop, Loki ou encore REvil.

Le ransomware est une famille de logiciels malveillants, divisée en deux catégories : la première vise à empêcher l'accès aux fonctionnalités de base des différents systèmes infectés (processus de démarrage, blocage de l'affichage, etc.). La seconde vise à chiffrer des données, empêchant ainsi leur consultation par leur propriétaire.

La quasi-totalité des opérations impliquant l'utilisation d'un ransomware sont effectuées dans une optique de gain financier significatif contre une promesse : celle d'un accès rétabli aux systèmes et aux données. Les ransomwares les plus récents ne sont généralement que la dernière étape d'une opération de cyberextorsion, faisant suite à l'exfiltration de données préalable à leur chiffrement, permettant aux acteurs malveillants de disposer de leviers envers leurs victimes les plus réfractaires.

L'industrialisation du ransomware

Véritable moteur financier de l'industrie cybercriminelle, les ransomwares ont beaucoup évolué au cours des 30 dernières années. Leur cible tout d'abord, qui est passée des particuliers aux grandes entreprises. Leurs moyens, en passant d'un système de diffusion manuel sur disquettes envoyées par courrier postal à une diffusion massive et mise à jour quotidiennement du logiciel malveillant par un botnet, exploitant des vulnérabilités non corrigées et 0-day. Leurs profils, du hacker surdoué à une structure agile organisée en pôles d'expertises pouvant sous-traiter certaines activités. Et enfin, leur modèle économique, d'une monétisation fiduciaire traditionnelle aux cryptomonnaies, permettant de dissimuler les paiements.

Autant de marqueurs d'une transformation de ces groupes en multinationales du crime, diffusant leurs logiciels malveillants à l'échelle mondiale. Cette évolution s'est opérée afin de faire face à une concurrence féroce et toujours plus innovante entre hackers, dans l'espoir de conserver ou d'augmenter leurs parts de marché. **Un marché estimé à plus d'un demi-milliard de dollars** sur les six premiers mois de l'année 2021, d'après le Trésor américain.

Coût de la remédiation

Malgré une volonté politique d'empêcher le paiement de la rançon, les victimes ont toujours tendance à le considérer comme une option viable, d'autant plus qu'il existe aujourd'hui des assurances cyber couvrant sous certaines conditions la rançon dans le cadre d'une cyberattaque. Ce n'est pas le cas ! En effet, **le coût de remédiation d'une attaque par ransomware est toujours plus important que la seule rançon.** Celui-ci prend en compte la perte de production associée, ainsi que des opérations techniques visant à éradiquer les logiciels malveillants déployés et à renforcer les défenses afin d'éviter une nouvelle infection.

Enfin, le rétablissement du système et des données n'est qu'une promesse: rien ne garantit la restauration rapide et complète des systèmes et des données chiffrées. Quelle confiance peut-on accorder à la parole d'une organisation criminelle ?

Réduire les risques

Quelques réflexes permettent de réduire les risques, et par extension l'impact, d'une infection par un ransomware :

Adopter la stratégie de sauvegarde dite « stratégie 3–2–1 » : 3 copies, réparties sur **2** supports physiques dont **1** support est déconnecté du réseau.

Disposer d'un processus et d'outils de mise à jour des systèmes permettant de réduire le risque d'exploitation des vulnérabilités connues par l'attaquant.

Sensibiliser l'ensemble des utilisateurs, le phishing étant aujourd'hui la première source d'infection.

Assurer la présence de logiciels de sécurité, aussi bien sur les systèmes que sur le réseau de l'organisme. La détection de signaux révélateurs d'une attaque en cours peut permettre d'y mettre fin avant le déploiement du ransomware.

Mettre en place un cloisonnement des systèmes au sein d'un réseau : ce cloisonnement limite la capacité de propagation d'un attaquant au sein d'un système d'information.

Enfin, **maîtriser les privilèges accordés aux utilisateurs et aux administrateurs**, ce qui permet de complexifier la tâche de l'attaquant, ne pouvant alors abuser de privilèges importants.

Le risque zéro n'existe pas, mais l'ensemble de ces mesures réduisent considérablement le risque d'infection par un ransomware. L'évolution constante des techniques utilisées par les attaquants ne sauront rendre cette liste durable. La protection, la formation, les mesures mises en œuvre doivent s'adapter au rythme et à l'inventivité des groupes criminels et de leurs nouvelles menaces.

Comment réagir en cas d'attaque ?

Rechercher les traces d'intrusion

Ces traces doivent permettre de répondre aux questions suivantes :

- Quelles actions ont été réalisées ?
- À quelle date et à quelle heure ?
- Quel est l'acteur impliqué ?

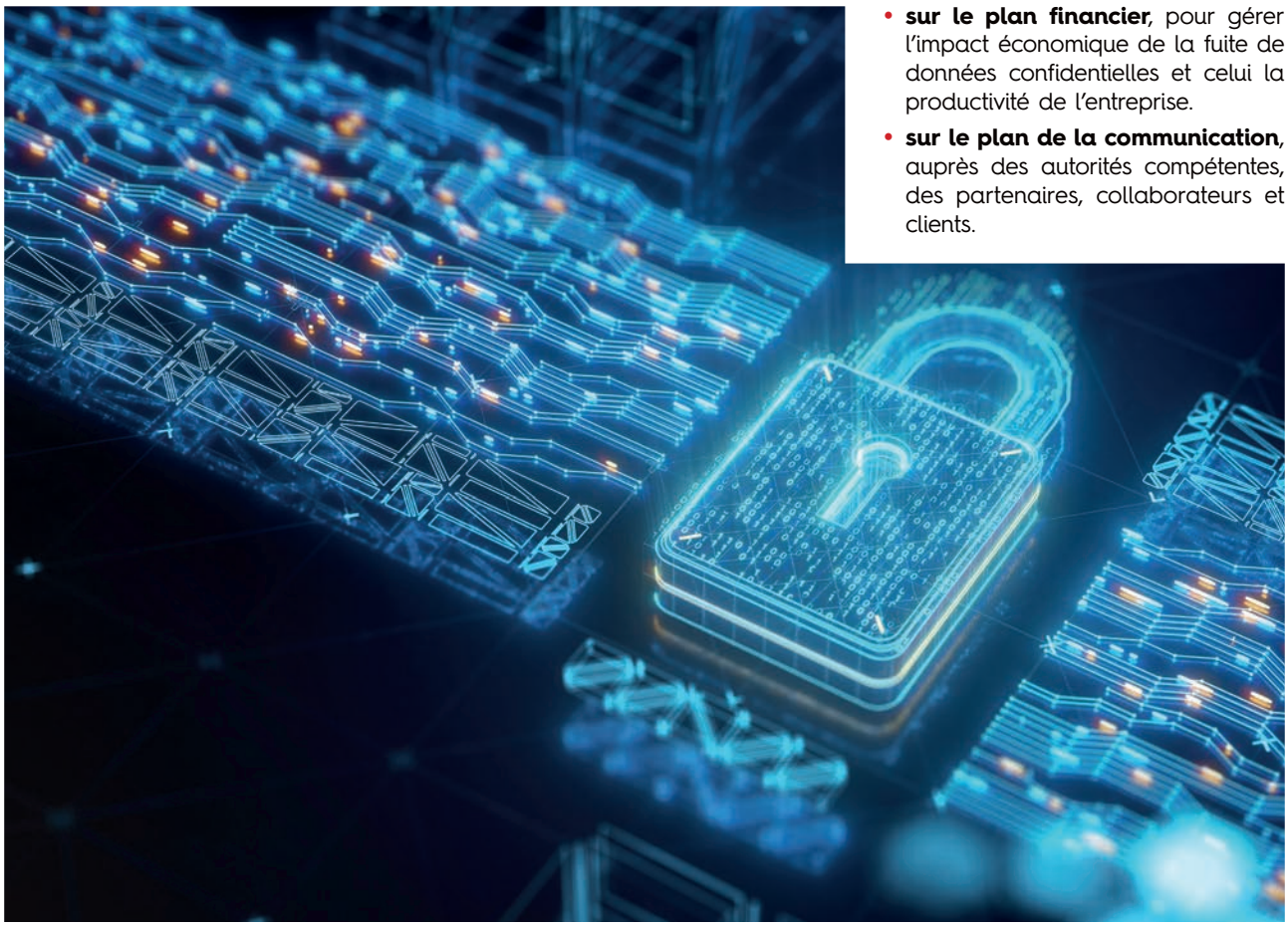
Mise en place d'une cellule de crise

Pour toute cyberattaque, il convient pour les organisations victimes de mettre en œuvre et piloter la réponse à l'incident au sein d'une cellule de crise, pour rétablir les données et systèmes compromis et maîtriser la communication autour de l'incident en cours.

Planifier et répéter

Dans le cadre d'exercices de crise simulés, les équipes métier et cyber s'exercent à apporter des réponses :

- **sur le plan judiciaire**, par le dépôt d'une plainte. Souvent nécessaire pour l'accompagnement financier via une assurance cyber.
- **sur le plan financier**, pour gérer l'impact économique de la fuite de données confidentielles et celui la productivité de l'entreprise.
- **sur le plan de la communication**, auprès des autorités compétentes, des partenaires, collaborateurs et clients.



L'OSINT : un atout majeur dans la maîtrise de l'identité numérique


1.


2.

1. **Clément Chesneau**
2. **Esteban Bouillard**
Ingénieurs Cyberdéfense et Intelligence chez Sopra Steria

L'OSINT, qu'est-ce que c'est ?

L'OSINT, ou Renseignement d'Origine Sources Ouvertes, est un ensemble de méthodologies et techniques utilisé dans le but de collecter et d'analyser de l'information en sources ouvertes (réseaux sociaux, journaux, archives...). Contrairement à l'ingénierie sociale, l'OSINT ne nécessite pas d'interactions actives (chat, demandes d'ami...). Dans un premier temps surtout exploité par les hackers dans la phase d'une attaque informatique ou par les services de renseignement, la mise en pratique de l'OSINT prend à présent de multiples formes.

Recrutement, guerre hybride, appui aux forces de l'ordre... des applications quasi-infinies

De nombreuses entreprises font aujourd'hui appel à des services de protection de leur identité numérique, au travers d'analyses d'e-réputation. Cette démarche consiste à recenser la présence d'une entité sur internet (exposition des serveurs, commentaires et avis...) dans le but de prévenir les attaques informatiques et les éventuels conflits.

En étudiant les communications des parties prenantes (clients, partenaires...), il est possible de déduire des éléments de stratégie sur leur développement et ainsi se positionner au plus proche de leurs besoins.

L'OSINT présente notamment un aspect très intéressant quant au recrutement des futurs collaborateurs. En effet, il devient aisé de trouver des profils qui n'apparaissent pas toujours sur des plateformes de grande ampleur comme LinkedIn, en utilisant par exemple le Dork, une technique liée aux requêtes Google qui permet de filtrer en profondeur les résultats de la recherche par le biais d'opérateurs spécifiques.

En dehors du contexte RH, et dans celui de la guerre hybride, on recense aussi de nombreuses initiatives.

Certaines sont par exemple liées à l'actualité comme le conflit entre l'Ukraine et la Russie où la communauté des « OSINTers » (passionnés d'OSINT) participe activement à la localisation des troupes russes ou du traitement des fake news. Par ailleurs, ces compétences nous servent également à aider les forces de l'ordre dans la recherche de personnes disparues ou encore à remonter la piste d'œuvres d'art volées.

Développer et transmettre les connaissances

Le périmètre du Renseignement d'Origine Sources Ouvertes est vaste et développer ses compétences sur ce domaine peut s'avérer fastidieux au vu du spectre de techniques et des outils existants, mais il existe aujourd'hui de nombreux moyens pour acquérir ces compétences de manière ludique.

Des communautés ont donc été créés sur des réseaux tels que Discord afin de permettre aux passionnés de se retrouver et d'échanger sur le sujet. La plus active à ce jour se nomme « OSINT FR », et les liens partagés sont un bon point d'entrée pour une première introduction.

Une autre méthode d'entraînement est la participation aux « Capture The Flag ». Les CTF dédiés à l'OSINT sont de plus en présents aujourd'hui. L'Association HEXA, sponsorisée par Sopra Steria, organise depuis 2021 la compétition « HEXA OSINT CTF » dont la nouvelle édition devrait par ailleurs se tenir courant décembre 2022.

Alors, prêts à rejoindre la communauté ?

1er L'équipe Sopra Steria #199 est arrivée première de l'European Cyber Cup 2022.

PLM + cybersécurité : une équation gagnante au service de la résilience des projets de transformation numérique

Simon Gary
Head of Innovation
chez CIMPA PLM Services

Avec la contribution de Michel Hoffman et Frédéric Lopez, experts Cybersécurité

Le PLM

Encore un acronyme ? Oui mais celui-ci est à retenir. Le PLM, pour Product Lifecycle Management concerne la gestion du cycle de vie du produit qui s'intègre dans tous les domaines industriels et notamment l'Aéronautique, le Transport ou encore l'Energie. Autant de domaines sensibles sur lesquels les enjeux cybers sont démultipliés. Chez CIMPA PLM Services, filiale du Groupe Sopra Steria secteur Aéroline, notre expertise se concentre sur cette approche qui se retrouve au cœur des stratégies de transformation digitale des industries.

Un exemple de solution PLM chez notre client Airbus est la solution « 3D as a portal ». Cette solution digitale PLM permet de transformer les méthodes de travail en améliorant la compréhension de tous les éléments constituant un avion avec les plus récentes mises à jour et leur représentation graphique en 3D, ceci tout au long de son cycle de vie. Dans une même application, toutes les informations sont collectées, structurées en fonction des configurations avion et mises à disposition à tous les contributeurs qu'ils soient à l'ingénierie, à la fabrication, à la qualité ou aux achats.

Le PLM poursuit donc plusieurs objectifs : rendre plus simple et agile la gestion globale du produit et tout son écosystème pour mieux le maitriser, mieux anticiper les changements, mieux interagir, mieux interopérer, et mieux déceler les aléas le plus en amont possible du cycle de vie.

Le PLM face aux menaces cyber

Pour les grands acteurs de l'industrie (Aéro, Spatial, Transport, Énergie, Défense, Militaire…), avoir un PLM au cœur d'une stratégie d'entreprise nécessite une cybersécurité forte adaptée aux spécificités complexes du PLM. Nous mettons donc en place plusieurs stratégies visant à renforcer la sécurité et la résilience de nos solutions, pour n'en citer que deux :

> **Le cloisonnement et la ségrégation des données** et des informations.

> **Des mécanismes dit « zéro confiance ».** Aujourd'hui, le mécanisme d'authentification classique ne suffit plus et chaque action utilisateur doit être confrontée à plusieurs moyens d'authentification (plusieurs clés de chiffrement, mot de passe, empreinte digitale, carte RSA…).

Le PLM Cloud, des risques supplémentaires ?

Avec le PLM Cloud, la question de la protection des données et des actifs critiques gérés dedans est certes basique, mais primordiale. À ce jour, si des données très sensibles, voire secret défense, sont dans un PLM, il est très difficile pour ne pas dire impossible de pouvoir les gérer dans un PLM hébergé dans le Cloud, les risques étant trop élevés.

Quoi qu'il en soit, le couple de solution « ségrégation » et mécanisme « zéro confiance » est un minima et d'autres contraintes de sécurité plus fortes viendront s'y ajouter pour garantir la protection de ces données.

Sur une solution PLM Cloud, nous limitons ainsi l'accès à l'ensemble des informations et des données. Chaque contributeur, qu'il soit interne ou partenaire, a uniquement accès aux données qu'il traite et utilise. En clair, ne sont disponibles que certaines données indispensables pour permettre la bonne exploitation de celles-ci.

D'autres moyens de protection dans les échanges de données existent :

> **Le chiffrement.** Il faut maîtriser qui va accéder à la donnée et permettre la lecture depuis une clé de déchiffrement.

> **La signature des échanges.** Cette solution nous permet de détecter rapidement une erreur humaine et de remonter plus efficacement à la source du problème avec la traçabilité des signatures. On se limite à ce que reçoit le destinataire et à ce que l'émetteur a envoyé.

> **Le Social Engineering**, qui permet une analyse comportementale capable de déceler des comportements suspects d'utilisateurs. Couplé à du Machine Learning et de l'intelligence artificielle, ce moyen de protection est d'une efficacité redoutable.

En conclusion, les solutions pour une cybersécurité de haut niveau dans une gestion du cycle de vie d'un produit étendu à tout son écosystème existent. Mais il est essentiel que le modèle économique les prenne en compte dès le lancement du projet. Ainsi, grâce à l'alliance de toutes ces solutions et expertises, nous permettons aux industries de décupler leur résilience.

Les équipes Gouvernance Risques et Conformité, piliers de la cybersécurité

Chloé Ricous
Responsable Adjointe offre GRC-P (Gouvernance, Risque, Conformité – Projets) chez EvaBssi

Raconte-nous ton parcours au sein de EvaBssi, marque du Groupe Sopra Steria

« Je travaille depuis 7 ans déjà dans le conseil des SI et de la cybersécurité. J'ai suivi un cursus d'ingénieur au sein de l'école Télécom Sudparis. Au cours de mes études, j'ai également eu l'opportunité de partir étudier aux États-Unis, à Georgia Tech, où j'ai obtenu le Master of Science « Electrical and Computer Engineering ».

Après avoir débuté ma carrière chez Devoteam Management Consulting, j'ai rapidement décidé de rejoindre EvaBssi, marque du Groupe Sopra Steria, pour la diversité des missions proposées et sa forte empreinte internationale. J'ai d'abord intégré l'équipe « intervenant », ce qui m'a permis de découvrir un large panel de clients (Secteurs Privé / Public, Luxe, Industrie et Énergie), d'activités (Consultations, Audits, Homologation, Formation) et de domaines technologiques (Infrastructures, Cloud, Communications Unifiées).

Au bout de trois ans j'ai entamé un virage vers la cybersécurité, notamment au travers de la formation ISO 27005. J'ai par exemple pu accompagner un organisme d'importance vitale dans son homologation à la Loi de Programmation Militaire.

Aujourd'hui je suis multi-casquettes. La première d'entre-elles est celle de Responsable Adjointe des activités GRC-P (Gouvernance, Risque, Conformité – Projets) avec pour mission de faire vivre une équipe d'environ 40 collaborateurs. Nous faisons notre maximum pour fédérer, stimuler et accroître le sentiment d'appartenance de nos collaborateurs qui sont à temps plein en prestation chez nos clients.

Depuis février 2020, je travaille aussi en régie chez un leader mondial de l'énergie en tant que cheffe de projet sur un programme de sécurisation des sites industriels.

Et enfin, au-delà de tous ces aspects opérationnels, je suis également Manager de plusieurs collaborateurs au sein de l'équipe GRC-P. Je les accompagne ainsi dans leurs carrières au sein de l'entreprise et dans la poursuite de leur évolution. »

Quels sont tes projets du moment ?

« Dans mon rôle de consultante cheffe de projet, j'ai pour objectif de sécuriser les systèmes IT critiques afin de traiter en premier lieu les risques humains. Dans le service où j'interviens, nous avions l'ambition de sécuriser plus d'une centaine de sites à travers le monde avant la fin de l'année 2021, pour faire face aux nouvelles menaces et cyberattaques. Et pour la petite anecdote, le défi a été relevé le 31 décembre au soir ! Le projet ayant été un succès, il est en cours de déploiement sur d'autres sites.

Avant d'en arriver là, je suis d'abord intervenue seule pendant un an, puis deux collaborateurs m'ont rejoint à temps plein. Les solutions techniques de sécurisation avaient été définies en amont par le Groupe afin d'appliquer des standards et pratiques homogènes, mais pour le reste, nous étions autonomes aux côtés du B-iCSO (Business Industrial Chief Security Officer) de la branche. Il a fallu faire preuve de pédagogie et de persévérance pour embarquer plus de 5 000 personnes sur un sujet encore émergeant. En effet, la sécurité des systèmes OT ne peut pas être calquée sur celle que l'on maîtrise en environnement IT : les enjeux, les fournisseurs, les cycles de vie, les contraintes opérationnelles et les programmes sont différents.»

Un mot sur EvaBssi et ses engagements ?

« Depuis mon intégration chez EvaBssi, je suis consciente de la chance que j'ai d'être dans un Groupe où l'engagement est bien réel et non une vitrine.

Le premier engagement dont je bénéficie moi-même est celui de l'égalité femmes/hommes. EvaBssi a ainsi accompagné ma trajectoire de carrière tout en garantissant un équilibre vie pro/vie perso.

Outre cela, il y a un véritable esprit de solidarité qui s'est manifesté par exemple au travers d'une initiative de mécénat de compétences que j'ai portée au sein de l'entreprise. Nous avons ainsi mis nos connaissances à profit d'un groupe de 15 jeunes en situation de désinsertion sociale, suivis par l'association Aurore qui accompagne les personnes en situation de précarité ou d'exclusion vers une insertion sociale et professionnelle. »

Expertise Galitt
Cybersécurité des paiements

galitt
a Sopra Steria company
Passion for payments

Un accompagnement dans l'amélioration continue de la sécurité des Systèmes d'Information des clients par une approche globale couvrant les aspects :

Conseil et Accompagnement

- Gouvernance
- Conformité
- Risques
- AMOA Solutions

Audits et Evaluation

- PCI DSS & Swift
- ISO27001, GDPR & LPM

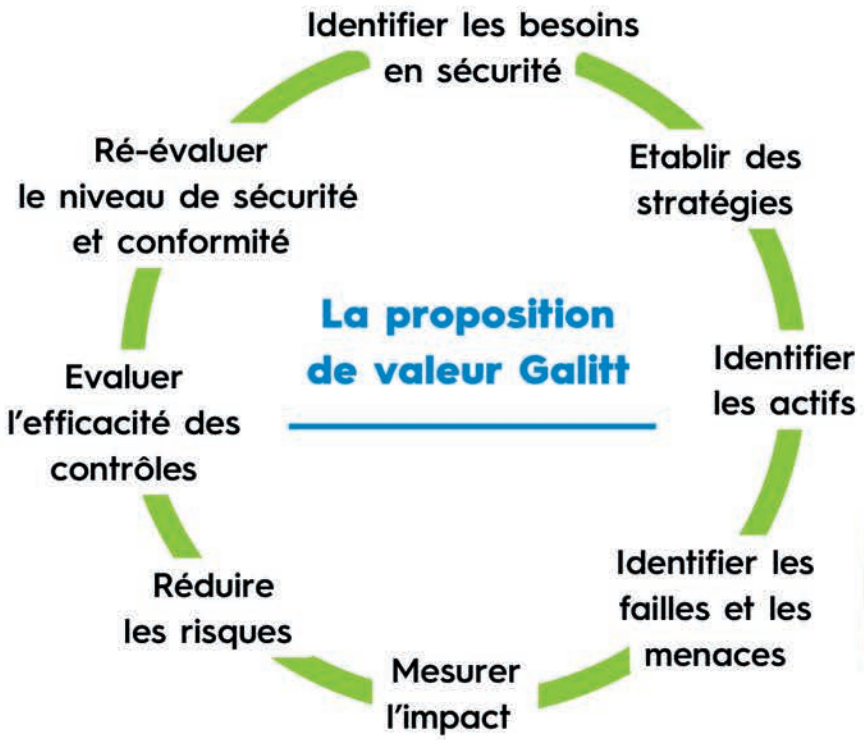
Sécurité opérationnelle

- CERT/CSIRT
- Pentest
- SOC & SIEM

Etapes pour atteindre la certification et maintenir son niveau de sécurité

1. Définition du périmètre
2. Réduction
3. Analyses
4. Remédiation
5. Certification
6. Suivi et maintien

La proposition de valeur Galitt



Pssst ! Vous voulez en savoir plus ? C'est par ici !

www.galitt.com

Le cloud de confiance au regard de la souveraineté et de la sécurité

Hugues Valentin
Directeur Centre d'Excellence Cloud/
Digital Factory Plateforme
chez Sopra Steria

Avec la contribution de Renaud Fleury, Directeur Technique chez Sopra Steria.

La souveraineté numérique : un enjeu pour tous

Dans l'ère du numérique, existe-t-il encore des frontières pour les données ? En effet, si un appareil législatif existe au niveau européen (RGPD) force est de constater que la maîtrise et l'exploitation des données font intervenir des acteurs aux stratégies différentes. Pour les États, **elles représentent un enjeu de sécurité et de souveraineté** tandis que pour les entreprises, il s'agit également et avant tout d'une source de création de valeur fondamentale. Dans ce contexte, s'ajoute un autre élément-clé : **la massification de notre recours au cloud.** Avec la numérisation de nos sociétés, le cloud a investi tous les pans de notre économie. Hier, seuls les géants du numérique y avaient recours ; aujourd'hui dans tous les domaines de l'industrie, du secteur public et de l'éducation, nous avons recours au cloud pour héberger et traiter toujours plus de données. Sans cloud, pas de voiture autonome, de chaînes de production automatisées, de robots dans les blocs opératoires ni de réseau électrique adapté aux énergies renouvelables, etc.

Ce constat fait intervenir une notion de plus en plus d'actualité : celle de **la souveraineté numérique.** Il s'agit de notre capacité à maîtriser nos dépendances aux solutions technologiques extra-européennes, à garantir l'autonomie stratégique des États et de leurs entreprises. Mais c'est aussi notre capacité à ne pas se laisser imposer une certaine vision du numérique et à garder notre propre pouvoir d'influence politique dans le monde qui se dessine sous nos yeux.

Le « cloud de confiance » : une première solution pour garantir la souveraineté numérique

C'est pourquoi la notion de « **cloud de confiance** » s'est hissée au cœur des préoccupations – tant dans le domaine privé, public, qu'étatique. En

effet, un fournisseur de cloud proposant des solutions souveraines assure que son infrastructure et les traitements effectués sont réalisés dans le strict respect des règles en vigueur, ceci afin de protéger la liberté de choix de ses utilisateurs, ainsi que la confidentialité et la souveraineté des données. Ces règles sont celles du ou des pays dans lesquels il opère et propose ses services. **Être acteur d'un cloud de confiance, c'est faire en sorte qu'aucun droit extraterritorial ne s'applique aux données et qu'elles ne soient pas utilisées par des tiers**; que ce soit pour alimenter des algorithmes d'intelligence artificielle (IA) ou pour contribuer à l'enrichissement de plateformes monolithiques, voire par utilisation de logiciels éditeurs. La question n'est pas « Faut-il aller sur le cloud ? » mais « Comment, et dans quelles conditions ? ».

Des partenaires de confiance

Pour accompagner cette transformation, nous nous sommes adossés à un écosystème de confiance en capacité de fournir des services cloud au plus près des besoins métiers de nos clients. Nous avons ainsi bâti des partenariats avec des acteurs français et européens tel qu'OVHCloud, Outscale, Clever-Cloud. Nous bénéficions à travers cet écosystème du label de l'État Secnumcloud, label favorisé par les acteurs du secteur public dans le cadre de leur transition vers le cloud et de sa doctrine « cloud au centre » encadrant cette transformation. Ces partenaires « cloud de confiance » nous ont permis de proposer des solutions à nos clients construites en particulier autour de notre offre « Trusted Digital Platform ».

Des expertises de pointe

Par ailleurs, le fait d'avoir les bonnes solutions techniques n'est pas une fin en soi pour un projet de migration vers le cloud. Il est également indispensable d'avoir les bonnes expertises et compétences pour accompagner ces démarches de transformation. **L'accompagnement doit pouvoir se faire sur toutes les étapes du chemin vers le cloud, en partant de la définition de la bonne stratégie de « move-to-cloud », puis sa mise en œuvre et enfin jusqu'à la phase d'exploitation.**

À l'instar du label de confiance des cloud Provider, nous avons mis en place un **Centre d'Excellence « cloud de confiance »** qui rassemble toutes les expertises techniques et projets autour de l'écosystème « cloud de confiance » et en capacité d'accompagner nos clients dans toutes leurs étapes de transformation. Par ailleurs, les compétences requises pour développer un écosystème « cloud de confiance » concernent aussi la gestion de projet, le modèle Agile étant favorisé via l'approche DevOps permettant d'accélérer les mises en production des applications.

Un Centre d'Excellence Cloud Défense & Sécurité pour accompagner les talents de Sopra Steria

Les exigences de la doctrine « cloud au centre », spécifique à la sphère publique, engendre une transformation en profondeur des activités numériques de nos clients et de nos équipes fortement mobilisées sur les activités Secteur Public, Défense & Sécurité, et Santé Social Emploi. C'est pourquoi un **Centre d'Excellence Cloud Défense & Sécurité a été créé pour accompagner les talents de Sopra Steria** et participer à leur montée en valeur des équipes via des parcours spécifiques (formation, coaching, certification...). Ces initiatives contribuent activement **à la stratégie de souveraineté numérique de notre écosystème public et, in fine, à la confiance des citoyens** dans l'ère du numérique.

IA, cyberrésistance et cloud hybride : trois leviers d'innovation pour la banque d'aujourd'hui et de demain

Samuel Durand
Mainframe and IT transformation expert
chez Sopra Banking Software

Dans un monde en constante évolution, les institutions financières doivent répondre à des défis qui se multiplient : amélioration de l'expérience client, émergence de nouveaux besoins, lutte contre une cybercriminalité multiforme, transition numérique, migration des services et applications sur le cloud... Pour fonctionner efficacement et répondre au plus près des attentes de nos clients, le secteur bancaire doit disposer de systèmes d'information toujours plus modernes et solides, en intégrant de nouvelles briques technologiques. Pour la structure industrielle et traditionnelle du secteur bancaire, ces solutions numériques représentent des atouts majeurs qui lui permet de gagner en compétitivité et de se démarquer de la concurrence.

Parmi ces solutions, trois méritent une attention particulière : **l'intelligence artificielle (IA), la cyberrésistance et l'hybridation du cloud.** Elles constituent de véritables leviers pour les équipes de Sopra Banking Software, qui apportent aux institutions financières des outils pour s'adapter à de nouveaux besoins, de nouvelles régulations et de nouvelles menaces.

L'intelligence artificielle (IA)

L'IA et ses technologies d'apprentissage automatique (machine learning) permettent au système bancaire de traiter plus rapidement des volumes de données conséquents, de raccourcir les processus et d'augmenter la productivité.

Au-delà d'un gain de temps évident, on peut identifier trois axes d'amélioration qu'offrent aux institutions bancaires les plateformes d'IA polyvalentes :

L'IA permet une adaptation rapide aux exigences de conformité et aux réglementations changeantes qui peuvent parfois bouleverser tout un pan du système financier, comme ce fut le cas avec les réformes* encadrant l'Open Banking et l'ouverture des données bancaires à des applications externes.

L'IA améliore aussi l'expérience du client final des institutions financières (vous et moi !). Cela passe notamment par les tests de conformité qui empêchent la prise de contrôle des comptes et l'usurpation d'identité, l'octroi de récompenses, l'accès à des services de gestion de patrimoine avec des modèles prédictifs, la prévision des taux d'intérêts ou encore le traitement plus rapide et l'évaluation des prêts.

L'IA permet enfin d'optimiser les processus métiers bancaires, de les automatiser et de les numériser. Ceux-ci s'appuyant sur une multitude d'individus, d'applications et d'équipes, l'automatisation du suivi permet, en les modélisant, de leur faire gagner en efficacité.

La cyberrésistance

La capacité de résistance du secteur bancaire est plus importante que jamais à une époque où les risques qui pèsent sur ses acteurs se multiplient. **Le défi consiste à protéger à la fois les données et les systèmes d'information** au fur et à mesure que de nouveaux usages numériques (comme la généralisation des paiements sans contact ou l'usage de banques en ligne) engendrent de nouveaux risques. Vous l'aurez compris, la cybercriminalité ne cesse d'innover et de se développer, entraînant les entreprises dans une course à la régulation et à l'innovation pour trouver des moyens de parer ces attaques. Si la protection passe par un ensemble de règles et de bonnes pratiques dans les usages, elle passe donc aussi par

une recherche constante de nouveaux outils numériques.

L'autre versant de la cyberrésistance recouvre **la conformité réglementaire**: il est crucial que le secteur bancaire puisse être suffisamment résilient pour s'adapter aux évolutions des usages en continuant à garantir la conformité réglementaire à chaque étape du processus de transformation.

L'hybridation du cloud

La majorité des établissements bancaires utilisent déjà les technologies du cloud. Mais pour favoriser la transformation digitale et bénéficier des avantages des outils cloud sans créer de latence entre les systèmes, **il est désormais possible d'utiliser un modèle hybride, entre cloud privé et cloud public, ou entre cloud et écosystèmes préexistants.**

De cette manière, depuis le cloud, les acteurs peuvent interagir, maîtriser et contrôler les systèmes en place, tout en leur ajoutant des applications plus modernes qui répondent aux besoins des régulateurs ou des clients. Cela permet aux banques d'optimiser les données en temps réel, de limiter les coûts et d'améliorer les capacités de résilience en cas de panne, le tout en assurant la continuité et l'uniformité des services.

Le cloud hybride permet la « scalabilité » : les banques peuvent optimiser les données dont elles ont besoin, évitant ainsi des coûts de stockage numérique inutiles tout en gagnant en efficacité. En même temps, ce cloud permet d'assurer la continuité des fonctionnalités et des performances quel que soit le volume de la demande. Cette flexibilité face à la charge participe de l'amélioration de l'expérience client.

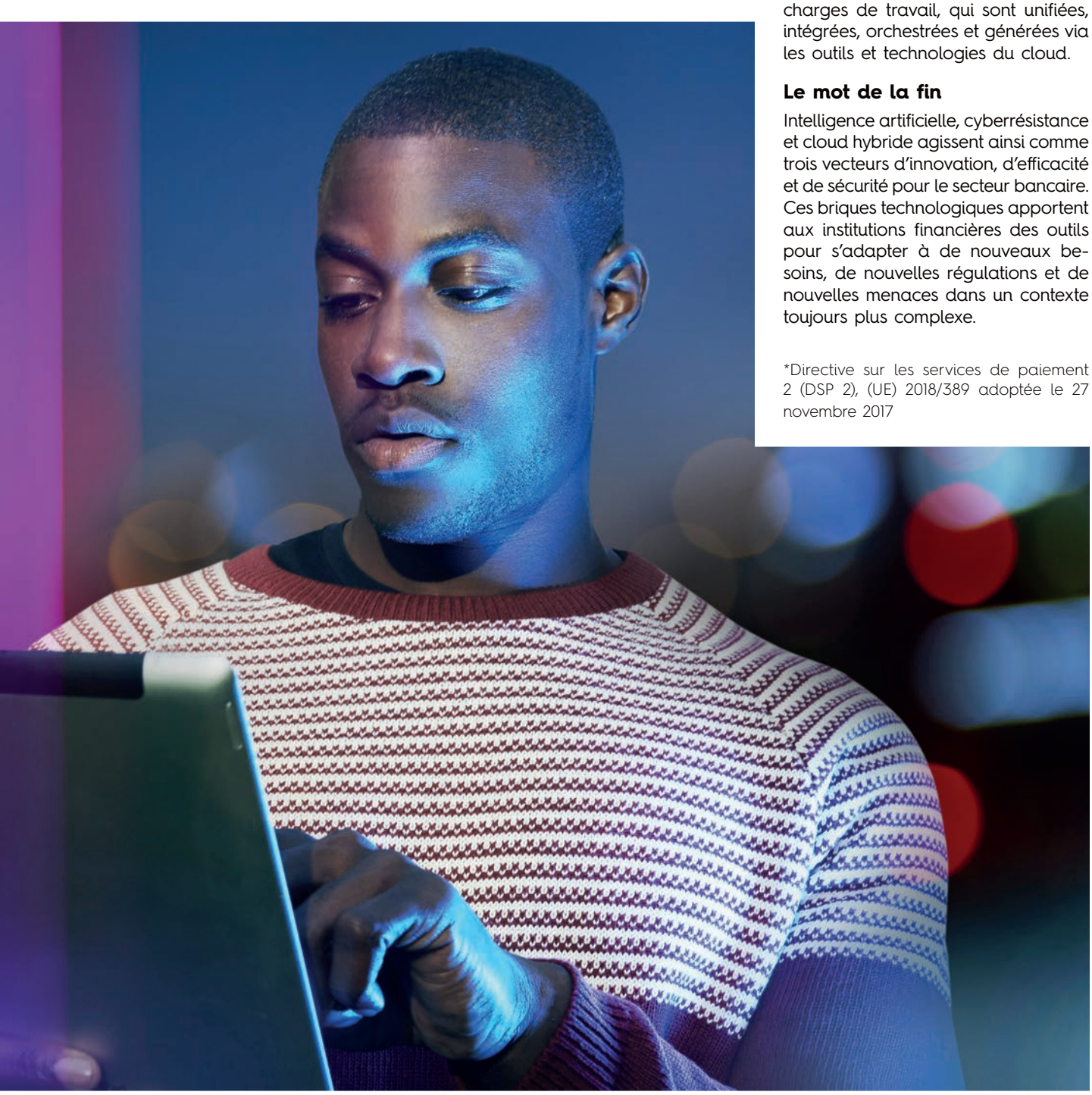
Le cloud hybride est vecteur d'innovation et renforce les capacités de gestion des risques financiers et la lutte contre la cybercriminalité, en n'étant pas circonscrit à un lieu géographique.

Enfin, il favorise la portabilité des charges de travail, qui sont unifiées, intégrées, orchestrées et générées via les outils et technologies du cloud.

Le mot de la fin

Intelligence artificielle, cyberrésistance et cloud hybride agissent ainsi comme trois vecteurs d'innovation, d'efficacité et de sécurité pour le secteur bancaire. Ces briques technologiques apportent aux institutions financières des outils pour s'adapter à de nouveaux besoins, de nouvelles régulations et de nouvelles menaces dans un contexte toujours plus complexe.

*Directive sur les services de paiement 2 (DSP 2), (UE) 2018/389 adoptée le 27 novembre 2017



Renforcer la cybersécurité et la cyberrésilience dans les solutions RH

Guillaume Le Bozec
Responsable sécurité Cloud
chez Sopra HR Software

Sopra HR Software est un des leaders des solutions Ressources Humaines avec plus de 900 clients implantés dans une cinquantaine de pays. Ce parc client représente environ 12 millions de salariés. Avec 1 million de bulletins de paie dans le cloud de Sopra HR, la sécurité est un enjeu majeur, c'est pourquoi nous la plaçons au cœur de notre stratégie.

Quels enjeux pour les solutions RH ?

Faut-il encore le rappeler ? Le contexte que nous connaissons actuellement (crises internationales, télétravail, etc.) est accompagné d'une recrudescence des risques de cybersécurité. De plus, la règlementation sur les sujets de la cybersécurité est devenue de plus en plus contraignante et exigeante. On peut notamment citer le cas du RGPD mais aussi de la future NIS 2 (directives européennes imposant aux ESN, entreprises de services numériques, des règles à respecter en matière de cybersécurité) en cours d'élaboration par l'UE.

C'est pourquoi chez Sopra HR, nous avons augmenté considérablement notre niveau de maîtrise du risque cyber. Les équipes Sopra HR travaillent également sur l'amélioration de la résilience des solutions hébergées sur notre cloud afin de pouvoir réagir efficacement à tout incident de type cyber.

Quelles solutions déployées pour y faire face ?

L'une de nos priorités a été de préserver la confiance numérique de nos clients, et de la renforcer en apportant des éléments de preuve, à l'aide des certifications obtenues et des audits de sécurité menés par nos clients. On peut notamment citer la signature des BCR (Binding Corporate Rules, une politique de protection des données qui s'applique pour les transferts de données hors de l'Union Européenne) avec la CNIL, l'obtention de la certification ISO 27001 en 2021 (norme délivrée par l'AFNOR qui définit la mise en œuvre d'un système de management de la sécurité de l'information) et l'audit annuel de nos processus via l'ISAE 3402 sur le périmètre France et Espagne (standard permettant de s'assurer de la qualité des contrôles internes que met en œuvre Sopra HR dans le cadre des prestations des offres cloud).

La sécurité étant l'affaire de tous, nos collaborateurs sont particulièrement sensibilisés aux enjeux de sécurité grâce à des formations internes.

Enfin, pour assurer une cyberrésilience, Sopra HR effectue un test annuel de son plan de continuité d'activité (PCA) afin de tester l'organisation du pilotage de crise, faire monter en compétences les collaborateurs participant au PCA et améliorer la solution technique.

Quel impact et bénéfice pour le collaborateur et les clients ?

Maintenir nos certifications ainsi qu'un haut niveau de sécurité permet de rassurer nos clients et d'établir un lien de confiance en leur garantissant que les données qu'ils nous confient soient en sécurité dans nos infrastructures.

Lorsqu'un client choisit une de nos offres cloud, nous nous engageons contractuellement à maintenir les conditions de sécurité en appliquant tout un ensemble de mesures de sécurité pendant toute la durée de la prestation.

Ma mission au quotidien ?

Je suis fier d'apporter mon expertise chaque jour pour garantir la sécurité de nos systèmes et protéger les data RH de nos clients. Je me sens utile et au cœur d'un dispositif industriel performant. C'est un métier qui me permet aussi d'innover et d'utiliser le meilleurs des technologies notamment l'IA pour être le partenaire de confiance de nos clients.

Tech'Me UP : le collectif qui incarne les ambitions d'excellence technique du Groupe Sopra Steria

1. **Matthieu Vincent**
2. **Guillaume Le Dain**
Animateurs du collectif Tech'Me UP chez Sopra Steria

Pour développer une culture d'excellence tech reconnue de tous et au service de nos clients, quoi de mieux que de jouer collectif ? C'est l'ambition de « Tech'Me UP », né en juin 2021 sous l'impulsion de Gregory Wintrebert, CEO Sopra Steria France, et de la volonté de fédérer l'ensemble des initiatives techniques de différentes entités.

Pour répondre à cet enjeu, le collectif s'est construit autour de collaborateurs aux expertises complémentaires qui s'assurent de porter une vision commune et de travailler sur trois axes principaux :

- **Opérationnel :** assurer que l'environnement de travail des techs répondent aux attentes en termes de matériel, logiciel et méthodologie de travail.
- **RH :** accompagner les trajectoires de carrière et définir des parcours de formation pertinents et en adéquation avec les enjeux et ambitions technologiques du Groupe.
- **Communication :** promouvoir en interne et en externe le savoir-faire, les experts et les initiatives du collectif.

Un an après, des premières réalisations concrètes

Les premiers chantiers ont porté sur l'accompagnement de carrière, la construction et l'animation de la communauté Tech'Me UP. Cela a permis de mettre en évidence les trajectoires de carrière possible en tant qu'expert technique et architecte au sein de Sopra Steria. Pour centraliser tous les contenus créés en interne (webinar, articles...), les équipes ont déployé un portail accessible par tous. Il permet de recenser tous les contenus existants, d'en faciliter la consultation et de s'en inspirer pour la résolution de challenges ou pour la publication de futurs contenus.

Enfin, point d'orgue de l'année 2021, le collectif a lancé l'événement « tech_assembly » : deux jours avec quinze interventions animées principalement par des collaborateurs de Sopra Steria pour partager les savoirs-faire et valoriser l'expertise technique du Groupe. Fort de ce succès, une seconde édition a été organisée en juillet 2022 sur le même format mais complétée par la mise en place de hub de rassemblement sur les principaux sites Sopra Steria en France.

Que réserve la suite ?

De très beaux projets sont prévus sur 2023 : continuer la programmation des rendez-vous communautaires, compléter les cursus de formation et les élargir à un maximum d'expertises techniques. De nouveaux sujets viennent progressivement s'ajouter :

- **Tech'Women UP**, un programme d'accompagnement des femmes dans la Tech.
- **La sensibilisation** des collaborateurs autour du Software Craftsmanship.
- **L'ouverture d'un blog technique** qui a l'ambition de promouvoir les savoir-faire et de s'imposer en tant que communauté d'experts techniques à l'externe.

Pour encourager les collaborateurs qui s'investissent au sein de la communauté, la création de « Pix3ls », plateforme de valorisation des savoir-faire, a été lancée. Chaque intervention, article ou certification que les contributeurs réaliseront, permettra de collecter des Pix3ls, l'équivalent de jeton d'échange. Ils pourront ensuite transformer ces Pix3ls en récompense : places pour des événements techniques, du temps pour assurer de la veille technologique...

160 collaborateurs Sopra Steria, représentant la communauté Tech'Me Up, étaient présents pour la 10ème édition du Devoxx France.

« Aeroline Zero Emission » : un programme ambitieux à destination du secteur aéronautique

Ayedin Manzari
Directeur du Programme « Aeroline Zero Emission »
chez Sopra Steria

Convaincus que le digital joue un rôle clé pour accélérer la décarbonation de l'aviation, Aeroline, le vertical de Sopra Steria dédié au secteur de l'aéronautique, a conçu un programme sur-mesure destiné à transformer les organisations et à participer à la conception d'un futur durable pour l'aviation. Ce programme, à la croisée des chemins entre innovation et engagement environnemental, "Aeroline Zero Emission" est conçu pour accompagner les acteurs de l'aéronautique dans leur transition environnementale.

Intégrer la dimension environnementale sur l'ensemble de la chaîne de valeur

Dans la lignée des directives de l'Organisation des Nations unies (ONU) et de l'Union Européenne (UE), enjoignant tous les acteurs de l'aéronautique à atteindre la neutralité carbone à l'horizon 2050, le programme est destiné à accompagner les industriels du secteur dans l'atteinte de leurs propres objectifs et couvre toute la chaîne de valeur, depuis les métiers de conception avion aux opérations aéroportuaires et aériennes. La connaissance de ces métiers, couplée à la maîtrise des processus et technologies associées, est une de nos forces pour accompagner cette transformation majeure.

Le digital comme facteur d'accélération de l'aviation décarbonée

Parce que le digital permet de mesurer, de modéliser et de simuler les impacts environnementaux, il constitue un potentiel considérable pour prendre les meilleures décisions dans un environnement complexe à la recherche de plus de sobriété.

« Aeroline Zero Emission » se concentre sur **5 leviers** de transformation pour l'aviation décarbonée :

- **La mesure, la simulation et le pilotage de la performance environnementale** pour prendre des décisions opérationnelles éclairées.
- **Le cadrage de la transition vers des organisations plus durables** pour réduire l'impact sur l'ensemble des scopes 1, 2 et 3 (émissions directes, émissions indirectes liées à l'énergie et autres émissions indirectes) tels que définis par le GHG (GreenHouse Gas) Protocol. tout en trouvant l'équilibre entre expériences client, collaborateur et performance opérationnelle. Par exemple, comment décarboner une zone industrielle et impulser un changement chez tous les acteurs.
- **Le déploiement de plateformes digitales et de gouvernance collaboratives** pour une meilleure collaboration multi-acteurs grâce à un tiers digital, sécurisé et souverain permettant de meilleures synergies sur les flux de ressources, matériel et personnes.
- **Le développement de produits et services « Sustainable by Design »** pour des solutions durables sur l'ensemble de leur cycle de vie. Cela implique de trouver les meilleures hypothèses dès les premiers pas de conception grâce à des outils de modélisation et de simulation qui favorisent la collaboration cross-disciplines et permettent de minimiser l'impact environnemental d'un produit.
- **La préparation du passage à l'échelle de l'aviation décarbonée** sur toute la chaîne de valeur et permettre un déploiement rapide. Par exemple, comment réduire la probabilité de formation de trainée de condensations.

Le lancement de « Aeroline Zero Emission » pour notre secteur aéronautique, sous les feux des projecteurs dans le contexte de la crise climatique actuelle, est le résultat d'un engagement fort de nos collaborateurs envers nos clients. Sous l'impulsion de ce programme, nos équipes sont désormais mobilisées pour contribuer à l'émergence d'une aviation décarbonée et pour relever les challenges de demain.

Retour sur le partenariat entre l'emlyon business school et Sopra Steria Next

1. **Mélanie Nedelec**
Consultante Senior, alumni de l'emlyon (Mastère Spécialisé Transformation Digitale, Marketing & Stratégie - 2019)
2. **Hichem Dhrif**
Managing Partner, Division Conseil Défense & Sécurité

Pour quelles raisons ce partenariat a-t-il été lancé en début 2022 ?

M.N. « Le partenariat, d'une durée de trois ans, repose sur trois piliers. Le premier est de contribuer à la mission première d'une école : le développement des savoirs et compétences des élèves avec un apport pédagogique de Sopra Steria Next. Le second est de permettre aux élèves de se projeter sereinement dans le monde du travail avec l'accompagnement de nos consultants. Enfin, il est important pour nous de valoriser l'image et les activités de Sopra Steria Next, qui est un débouché naturel pour les élèves du Master MSc « Cybersecurity & Defense Management ».

Quelles formes prennent les interventions menées auprès des élèves ?

M.N. «L'idée est de prévoir un accompagnement des élèves de bout en bout. Tout d'abord, nous participons à leur cursus pédagogique en donnant des cours, notamment sur la stratégie appliquée aux entreprises numériques ou en intervenant lors des conférences organisées par l'emlyon. Puis nous les préparons à leur sortie d'école avec des coaching RH (préparation aux entretiens, aides à la rédaction de CV). Enfin, et c'est un élément distinctif de ce partenariat, nous proposons de les former en-dehors des murs de l'école, en immersion dans nos missions. Les étudiants sont ainsi au contact des consultants et consultantes afin d'apprendre ce qu'est leur métier.

Ces immersions sont pensées en cohérence avec le contenu de leur formation avec de forts enjeux cyber : le programme France Identité numérique, l'Observatoire national interministériel de la sécurité routière ou encore la digitalisation de la procédure pénale au niveau européen. »

H.D. « Cet accompagnement se prolonge au-delà du champ strict du partenariat, car plusieurs étudiants nous ont rejoint en CDI ou pour leur stage de fin d'année. »

Si le partenariat apporte des bénéfices pédagogiques pour les étudiants, il a également un fort intérêt pour Sopra Steria Next. Comment cela s'incarne-t-il ?

H.D. «Le programme a pour objectif de former des talents mais aussi de contribuer à la Recherche. Le milieu académique a une longueur d'avance sur les sujets de demain, qui, à moyen terme, se traduiront dans les pratiques du Conseil. Ce partenariat permet de réduire l'écart entre la matrice conceptuelle, l'école, et la matrice empirique, le Conseil. C'est toutefois une intention qu'il reste à opérationnaliser après ces premiers mois de découverte réciproque et j'ambitionne qu'à terme, notre partenariat irrigue d'autres thématiques que la cyber. »

M.N. « Intervenir dans l'école est aussi une expérience enrichissante pour les consultants. S'ils présentent des sujets qu'ils maîtrisent au quotidien, le dialogue avec les étudiants les pousse à les penser différemment, à porter un regard critique sur leur expertise. Les étudiants sont eux-aussi demandeurs de sujets sortant du cadre de leur programme cybersécurité. Nous avions ainsi proposé une étude de cas lors d'un consulting challenge : « Comment réduire l'impact environnemental du numérique au sein d'une entreprise du CAC40 ? ». Ce sont des sujets dont ils se sentent particulièrement concernés. »

Mélanie, ton statut d'alumni apporte-il quelque chose au partenariat ?

M.N. « En complément de mon rôle de Consultante, je suis campus manager pour l'emlyon, c'est-à-dire que je suis chargée de faire vivre la relation école/entreprise pour Sopra Steria Next. Le fait que je sois une alumni facilite grandement le partenariat, car je connais les acteurs des deux côtés. Au sein de l'emlyon, il y a un fort esprit de communauté et de partage : quand on contacte d'autres alumni au sein de Sopra Steria Next pour contribuer, elles et ils sont tout de suite volontaires. »

À quoi faut-il s'attendre pour la rentrée ?

M.N. « Nous allons participer à plus d'évènements de recrutement dans l'année et accentuer l'apport pédagogique en augmentant le nombre de participations en cours. »

H.D. « Ce n'est peut-être pas du court terme, mais nous allons étudier les possibilités d'étendre le partenariat à d'autres formations au sein de l'emlyon. Les étudiants d'aujourd'hui sont les leaders de demain. Nous les retrouverons bientôt dans nos comités de direction et dans ceux de nos clients, c'est pourquoi il faut continuer à nouer des liens. »

Quels enseignements de la crise COVID 19 pour la place de la cybersécurité ?

Philippe Muller
Partner Stratégie et nouveaux modèles d'entreprise, Centre d'Expertise digitale

Dans quel contexte avez-vous amorcé cette réflexion sur la « résilience des SI » ?

«Elle s'est enclenchée au sortir du premier confinement en mai 2020. La situation était extraordinaire pour les entreprises : les effectifs étaient dispersés sur le territoire et l'activité ne tenait plus que par un fil «numérique». Le COVID a montré à quel point la définition du «mode de fonctionnement normal» pouvait varier. Par exemple, en confinement, les logiciels de paye sont devenus l'une des fonctions les plus importantes d'un SI, soutenant une économie nationale à l'arrêt. En mode normal, la paye est loin d'être considérée comme un SI critique. C'est donc la résilience de l'ensemble du système d'information et des processus qu'il faut penser : réduire des coûts de fonctionnement pour limiter le poids du SI dans le bilan de l'entreprise, modulariser son architecture pour qu'elle soit aisément réorientable vers les processus critiques, agiliser ses équipes, et internaliser les composants critiques. Ainsi analyser sa gestion de crise du point de vue IT révèle la résilience du SI, et donc de l'entreprise. »

Deux ans après, quel regard portes-tu sur la place de la cybersécurité en entreprise ?

«La vision d'un outil IT résiliant, capable de supporter l'adaptation rapide d'une organisation, pose la question de la maîtrise du risque dans les choix de transformation, alors que les décisions doivent se prendre de plus en plus vite. Par exemple, alors que les entreprises vont vers le cloud, comment sécuriser les données avec un hébergement externalisé ? Comment maîtriser la reconfiguration de sa chaîne de production, digitalisée et automatisée, en évitant les risques de cyberattaque ?

Cette approche par les risques me paraît toutefois limitée. Si les dirigeants ont pris conscience que le rôle du DSI dépasse la simple fonction support, il n'est pas encore devenu un véritable business partner. Un parallèle peut être tracé avec l'évolution du réglementaire dans le secteur bancaire. Initialement, les banques travaillaient la connaissance de leurs clients par ce prisme (maîtrise de la solvabilité, etc.). Puis elles se sont rendues compte que cette connaissance client était un enjeu d'économie et de performance.

La cybersécurité suit le même chemin : elle est aujourd'hui beaucoup appréhendée sous un angle risque alors qu'elle est devenue un véritable enjeu de performance et de développement commercial. Le jeune diplômé qui veut faire de la cybersécurité sera probablement le business partner de demain : il mettra sa connaissance et son savoir-faire au service de la promesse de l'entreprise. Or, on ne peut pas dire que les DSI aient finalisé leur mutation pour devenir plus adaptatives. »

Toutes les fonctions support n'ont-elles pas vécu ce retour en grâce avec la crise ? La cybersécurité fait-elle exception ?

«Aujourd'hui les métiers de cybersécurité sont qualifiés de métiers d'expertise. Mais le jour où cette expertise sera automatisée, que restera-t-il ? La valeur de l'individu, sa capacité à porter des innovations qui nourrissent le produit ou le service proposés, en améliorant le parcours client et la promesse de l'entreprise.

C'est vrai pour toutes les fonctions supports, mais les spécialistes de la cybersécurité ont probablement un impératif d'innovation – et d'alignement - encore plus fort.»

Les réseaux sociaux échappent-ils à la souveraineté des États ?

Florence G'sell
est agrégée et professeur de droit privé à l'Université de Lorraine.
Enseignante à Sciences Po

Partout dans le monde, les populations recourent aux réseaux sociaux pour s'informer, communiquer, débattre, s'instruire, se divertir, acheter ou vendre. La force de frappe de ces immenses plateformes transnationales tient au nombre impressionnant de leurs utilisateurs : Facebook comporte, à l'heure actuelle, 2,94 milliards d'utilisateurs actifs par mois et 1,96 milliards d'utilisateurs actifs par jour, à comparer avec le milliard d'utilisateurs actifs mensuel (sur 1,39 milliards d'utilisateurs) de la plateforme TikTok. **Le gigantisme des plateformes, leur omniprésence dans la vie quotidienne, le pouvoir qu'elles exercent désormais dans l'information des citoyens et le débat public conduisent insensiblement à comparer leur puissance à celle des États.** Cette puissance s'exerce toutefois sans les garanties démocratiques propres aux États de droit. Bien au contraire, les réseaux sociaux sont administrés par des entreprises privées à but lucratif, qui agissent dans l'intérêt de leurs actionnaires et sont pilotées de manière verticale par des dirigeants souvent très médiatisés qui détiennent la majorité du pouvoir de décision de l'entreprise.

Dans le même temps, le fonctionnement des réseaux sociaux présente des risques aigus pour la société, la vie démocratique et la sécurité des personnes. Les contenus haineux, violents ou incitant à la violence sont aujourd'hui monnaie courante. Les fake news et les contenus à caractère complotiste prolifèrent en ligne et constituent autant de moyens de manipuler les opinions, parfois sous l'influence de puissances étrangères. Surtout, le modèle d'affaires lui-même des plateformes est en soi générateur de risques. Tirant leurs revenus de la publicité et de la collecte de masse des données de leurs utilisateurs, les plateformes ont intérêt à augmenter leur fréquentation et la durée de connexion des utilisateurs. Or leurs algorithmes, conçus pour maximiser le temps passé en ligne, sont fréquemment accusés d'exacerber la propagation de la désinformation, d'accentuer la polarisation politique, voire de privilégier le racisme, l'extrémisme et la violence.

Dans un tel contexte, les États ont adopté des approches différentes. Aux États-Unis prévaut le modèle de l'auto-régulation : les plateformes sont sans réel contrepouvoir, n'engagent pas leur responsabilité et ne se voient généralement appliquer que des réglementations limitées. Si les démocrates espèrent, pour beaucoup, l'adoption d'une réglementation incitant les réseaux sociaux à modérer davantage les contenus les plus toxiques, les républicains se plaignent des pratiques de modération actuelles des plateformes, qu'ils jugent biaisées à l'encontre des plus conservateurs, et veulent précisément légiférer pour empêcher ce qu'ils perçoivent comme une censure. De son côté, l'Union Européenne a récemment décidé, avec l'adoption du Digital Services Act , d'encadrer davantage l'activité des plateformes afin de les obliger à lutter effectivement contre les contenus illégaux, à modérer les contenus dans le respect des droits des utilisateurs et à faire preuve d'une réelle transparence dans leurs pratiques.

Ces deux approches ont chacune leurs avantages et leurs limites. Aucune ne paraît, toutefois, permettre de régler des questions fondamentales. Les plateformes peuvent-elles modérer à leur guise et choisir, sur le fondement de leurs conditions d'utilisation, d'interdire des contenus par ailleurs licites ? Ou faut-il leur imposer de limiter leurs activités de modération à la censure des contenus illégaux ?

> **Comment, par ailleurs, articuler la politique de modération menée par les plateformes avec des droits nationaux pouvant largement diverger quant à la définition des contenus illicites ?**

Peut-on, enfin, véritablement estimer que c'est par le droit que se régleront des difficultés finalement suscitées par des modèles d'affaires peu vertueux ?

Toutes ces questions mènent à se demander si une meilleure option ne consisterait pas à modifier l'organisation et la gouvernance des plateformes de manière à mieux répartir le pouvoir entre leurs propriétaires, leurs utilisateurs et la puissance publique. La création d'instances indépendantes chargées de déterminer la stratégie de la plateforme dans l'intérêt du plus grand nombre et dans le respect des droits fondamentaux pourrait être envisagée. L'adoption de protocoles décentralisés pourrait également permettre de réduire le pouvoir excessif des plateformes tout en conférant davantage d'autonomie aux utilisateurs.

Le cloud hydride : être autonome dans ses choix

Benjamin Chossat
Responsable de la Tribu Cloud Design
au Centre d'Expertise digitale
chez Sopra Steria Next

Qu'est-ce que le cloud ? En quoi peut-il devenir « hybride » ?

Il existe plusieurs modèles de cloud. Le cloud public est le plus courant : les ressources sont proposées à tout le monde par une société spécialisée qui prend en charge toute la dimension physique : les serveurs, les disques durs et mutualise ces ressources physiques auprès de ses clients pour proposer des ressources cloud à utiliser simplement. C'est le modèle d'AWS ou de Microsoft Azure. Le cloud privé, lui, est réservé à une seule organisation qui sera seule à accéder aux ressources mutualisées. Moins courant, le cloud communautaire est partagé entre plusieurs organisations. Chacune de ces approches comporte avantages et inconvénients. Le cloud public permet d'augmenter très facilement les capacités de stockage, de se décharger facilement de la maintenance auprès du fournisseur cloud mais inclut aussi des services à plus haute valeur ajoutée comme l'analyse de données. En retour, il délègue de nombreux choix et responsabilités au cloud provider qui est décideur des possibilités et des usages. Le cloud privé, plus cher et complexe à mettre en œuvre, permet de s'affranchir de cette délégation à un tiers.

Le cloud hydride a la particularité d'être composé d'au moins deux infrastructures cloud distinctes mais connectées. Le plus souvent il encapsule des capacités cloud public, flexibles et peu chères, avec une composante cloud privé qui héberge les données et services les plus critiques. On peut parfois lire qu'il rassemble « le meilleur des deux mondes (public et privé) ».

Pourquoi une entreprise va-t-elle sur le cloud hydride ?

L'une des principales raisons c'est la souveraineté permise par l'hybridation du cloud qui protège les activités et données sans se couper des apports du cloud public. Elles le font aussi par souci de performance. La dématérialisation a tendance à nous le faire oublier, mais pour certaines actions il faut conserver une proximité géographique entre le serveur et l'usage. Les robots d'usines nécessitent un haut niveau de sécurité et de performance. Leur serveur gagne donc à être colocalisé avec ces robots. L'hybridation est un des moyens permettant d'obtenir cette proximité tout en se préservant l'utilisation des apports du cloud public partout où cela est possible. D'autres approches technologiques, notamment la 5G, permettent de couvrir les mêmes objectifs et restent totalement compatibles avec la notion de cloud hybride.

Qu'implique le choix de type de cloud, ou de niveau d'hybridation pour une entreprise ?

Ce choix est éminemment stratégique, même s'il s'adosse à des contraintes techniques. Pour pouvoir l'effectuer en toute connaissance de cause, une entreprise doit avoir une bonne connaissance de son patrimoine : qu'est-ce qui fait la valeur de mon entreprise ? Qu'est-ce que je dois protéger le plus possible ? Quel est l'impact du non-fonctionnement d'un logiciel ? Mais elle doit également prioriser ses objectifs et les moyens nécessaires pour les atteindre : quel niveau de performance ? De robustesse ? Pour quelle activité ? Parmi les centaines de solutions possibles, il faut déterminer celle qui apporte le plus de valeur.

Le cloud public offre une gamme de solution et de services dont la complexité est très largement prise en charge par l'opérateur. Cela permet d'utiliser les technologies les plus avancées avec un investissement minimal, d'aller toujours dans une logique de progrès en supprimant une part de la complexité inhérente à ces nouvelles technologies : IA, Big Data en sont de bons exemples. Adosser un cloud public à une composante privée, et donc hybrider, c'est gagner en capacité d'innovation, et maîtriser son investissement. Un levier fort au service de la stratégie de l'entreprise.

Identifier au sein d'une entreprise ce qui peut être traité dans le cloud public, ce qui doit rester sous contrôle souverain est parfois difficile. Les paramètres à prendre en compte sont complexes et pour faire un choix adéquat, il faut parfois se faire accompagner par des experts. Ce regard externe n'apporte pas qu'une dimension technique, mais permet aussi de questionner comment un client priorise ses activités.

Le cloud hydride ne concerne-t-il que les entreprises hébergeant les données et activités les plus sensibles ? Est-il l'instrument principal de la souveraineté numérique ?

Des obligations réglementaires s'imposent à certains acteurs (énergie, santé, transport, etc.). Ils doivent prendre des mesures de sécurité spécifiques, qui passent parfois par l'hybridation. Mais la question de la souveraineté, ou de l'indépendance, ne doit pas se réduire au contrôle de sa donnée. C'est la capacité de décider et de faire dans un cadre incertain, en adaptant son infrastructure aux enjeux. En cela, le cloud hydride est un outil au service d'une stratégie d'entreprise.

C'est de l'action que naît l'inspiration.

Une vision ne vaut que si elle est réellement actionnable. Chez Sopra Steria Next, nous concevons des stratégies ancrées dans la réalité de votre entreprise qui produisent des résultats concrets, durables et bénéfiques pour tous.

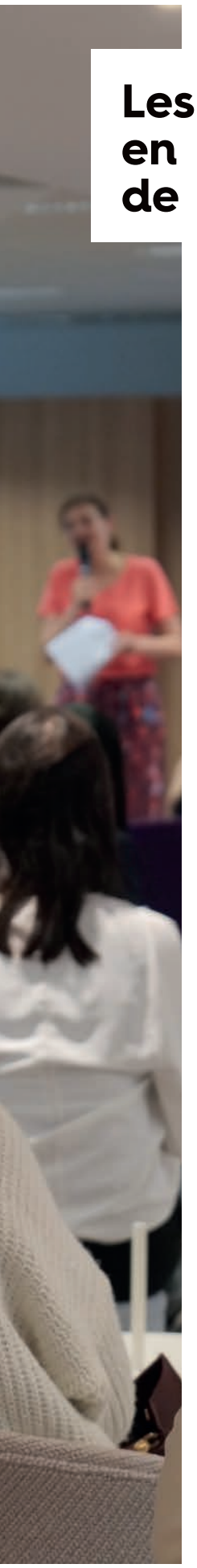
Sopra Steria Next,
le conseil en transformation digitale.

* Le monde est tel que nous le façonnons.

The world is how we shape it*

sopra steria next


sopra steria
Afterwork
Inspiring Women
@ Sopra Steria
Nos opportunités de carrière sont multiples
avec plus de 30 familles de métiers, autant de passerelles à imaginer ensemble.



Les rôles modèles du Groupe Sopra Steria en première ligne pour attirer toujours plus de talents féminins dans la tech

Dans le secteur de la tech, **la féminisation des métiers du numérique** reste un enjeu majeur sur lequel le Groupe Sopra Steria poursuit son engagement. C'est pour cela que nous avons déployé cette année **le programme « Femmes Inspirantes »**, venant soutenir la volonté du Groupe d'attirer plus de femmes vers les métiers du numérique et à les accompagner dans leur évolution. Témoignages, partage d'expertise, afterworks et networking, nous poursuivons l'effort au quotidien pour inciter les femmes à s'intéresser au monde de la tech et à nous rejoindre.

Une campagne de témoignages sur Brut.

Sopra Steria a lancé avec le média Brut une campagne vidéo donnant la parole à deux collaboratrices, Karen Heitzmann, Directrice des opérations Energy & Utilities, et Aïcha Diaw, Consultante Senior de Sopra Steria Next, spécialisée dans le secteur de l'énergie et de la transition énergétique. Karen et Aïcha ont chacune des parcours uniques et incarnent des modèles inspirants pour des jeunes filles et femmes qui souhaiteraient s'impliquer dans les projets de transformation numérique majeurs.

Deux live sur LinkedIn pour faire rayonner l'expertise de nos femmes inspirantes à l'international

Dans la continuité des actions menées, deux webinars ont été organisés pour donner la parole à des expertes techniques du Groupe pour partager avec notre audience à l'international la réalité de leurs métiers, de leurs secteurs d'activité et de leurs expertises techniques.

Consuelo Bénicourt
Directrice Responsabilité Sociale chez Sopra Steria

Scannez les QR code et retrouvez les replays des deux conférences :

Cloud et IA avec Kritika Saraswat, et Béatrice Rollet.

Défense et finance inclusive avec Sue-Elle Wright et Nelly Kambiwa.

Se rencontrer pour partager avec les talents féminins

Dans la continuité de ces actions, il ne nous manquait plus que de franchir la barrière du réel, et d'organiser des événements physiques pour permettre à des étudiantes et des candidates de pouvoir directement interagir avec les femmes inspirantes du Groupe. **Des afterworks dédiés aux talents féminins ont été organisés aux quatre coins de la France pour permettre à des jeunes femmes de bénéficier d'une expérience de recrutement inédite.** À Paris, c'est plus d'une centaine de femmes qui se sont rendues dans nos locaux pour participer à des conférences sur nos métiers, nos parcours de carrières, des sessions de coaching… Tout était organisé pour accompagner au mieux ces candidates à entrer sereinement dans le monde du numérique et même à les inciter à y faire carrière.

Rendez-vous pour les prochaines éditions ?

Comment la tech peut-elle nous aider à réduire l'impact environnemental des activités humaines ?

Catherine Royer
membre du Conseil d'administration
de la Fondation Sopra Steria – Institut de France et
directrice du développement humain
du vertical Défense & Sécurité
chez Sopra Steria

Le 30 juin 2022, la Fondation Sopra Steria-Institut de France décernait son 19e Prix Entreprendre pour demain. Le thème de cette année : « Quelles solutions la tech peut-elle apporter pour réduire l'impact environnemental des activités humaines ? ». Une question plus que centrale, à la fois pour nos métiers mais aussi pour notre quotidien, à laquelle ont répondu les deux lauréats de cette édition : Osiris Agriculture et INSECTA accompagnés de la marraine du Prix, Inès Leonarduzzi.

Le constat est sans appel : **l'empreinte du numérique ne cesse de croître, avec une projection à +60% d'ici 2040*.** Il y a donc urgence de faire du numérique un levier d'action environnementale positif, en faisant preuve de sobriété dans la conception des produits (green IT) d'une part et en facilitant le développement de solutions plus durables d'autre part, c'est-à-dire en mettant l'IT au service du green.

Et parce que les jeunes générations ont besoin de tout notre soutien pour faire naître leurs idées, la Fondation Sopra Steria-Institut de France récompense au travers du Prix Entreprendre pour demain les projets des étudiants et les jeunes entrepreneurs engagés pour mettre la Tech au service de l'humain et de la planète.

Cette année encore la sélection s'est avérée particulièrement riche. **Au total, l'édition 2022 a mobilisé une centaine d'équipes, vu près de 50 dossiers examinés par le jury de sélection,** retenu six équipes finalistes et récompensé deux lauréats: INSECTA dans la catégorie Étudiants et Osiris Agriculture pour les Jeunes entrepreneurs.

**Sénat, Rapport d'information de la mission d'information sur l'empreinte environnementale du numérique, juin 2020*

Ouvrir des portes grâce au réseau

Au-delà du soutien financier et de la visibilité que leur apporte le Prix Entreprendre pour demain, les lauréats bénéficient également de l'accompagnement de deux de nos partenaires, Planetic Lab, incubateur solidaire, et Vianeo, spécialiste du développement des startups innovantes. Mais aussi et surtout de l'accès à notre réseau, avec des conseils d'expert des collaborateurs bénévoles de Sopra Steria et de la marraine de cette édition, Inès Leonarduzzi, fondatrice et présidente de Digital For The Planet, autrice de « Réparer le futur, du numérique à l'écologie » et directrice générale de MTArt Agency.

Et après ?

Le Prix Entreprendre pour demain a vocation à accompagner les porteurs de projet dans la durée. C'est pourquoi nous avons créé une véritable communauté d'entrepreneurs, réunissant toutes les personnes impliquées dans l'aventure : les lauréats des différentes éditions, les experts, les parrains-marraines... Objectif : constituer un lieu d'échanges entre acteurs de la Tech pour construire ensemble un avenir plus durable.

La nouvelle édition du Prix Entreprendre pour demain sera lancée à l'automne. Rendez-vous sur notre site internet : https://www.fondationsoprasteria.org/

Créé par quatre étudiants de l'ECE Paris, INSECTA accompagne les acteurs de l'entomoculture pour améliorer la production d'insectes, grâce à l'intelligence artificielle, afin de réduire considérablement l'empreinte carbone de l'industrie agroalimentaire.

Côté jeunes entrepreneurs, Osiris Agriculture met la robotique au service de la transition agroécologique de l'agriculture européenne, en révolutionnant la gestion de l'eau et des fertilisants.

Lutter contre les violences faites aux femmes passe aussi par leur sécurité numérique

Dominique Lambert
Déléguée générale
de la Fondation Sopra Steria-Institut de France

Les femmes tentant d'échapper à des partenaires violents sont souvent victimes de logiciels espions ou traquées via les réseaux sociaux. Leurs données sont sensibles et pour mieux les protéger, la Fédération nationale solidarité femmes (FNSF) a opéré une grande refonte de la sécurité de ses sites et de ses outils avec l'accompagnement des bénévoles de la Fondation Sopra Steria-Institut de France.

> **Il y a eu une prise de conscience des acteurs sociaux sur l'utilité des outils numériques. Cela a donné naissance à beaucoup de bonnes pratiques ou les a renforcées.**

Les sites de la Fédération nationale solidarité femmes (FNSF) ont déjà été hackés, et comme nous l'a dit Françoise Brié, sa directrice générale, il était urgent d'améliorer leur sécurité et les protéger d'actions malveillantes entravant leur réseau ou bien exposant des données privées.

Depuis trois ans, la Fondation Sopra Steria-Institut de France travaille ainsi avec la FNSF France pour revoir de fond en comble sa présence numérique. Cette refonte s'est matérialisée par des formations pour les équipes de la FNSF et les différentes associations de leur écosystème.

Protection numérique

Via les réseaux sociaux, les auteurs de violences peuvent surveiller tous les faits et gestes de leurs compagnes, mesurer leurs déplacements et même les retrouver lorsqu'elles sont hébergées dans des lieux sécurisés, entraînant un risque d'agression à proximité des centres d'hébergement. Parce que des logiciels espions sont fréquemment installés sur les téléphones portables des victimes, il est essentiel de savoir comment les repérer et les désactiver. Il faut également faire attention aux enfants, dont le téléphone peut être utilisé par les agresseurs pour se renseigner sur les faits et gestes de leur mère.

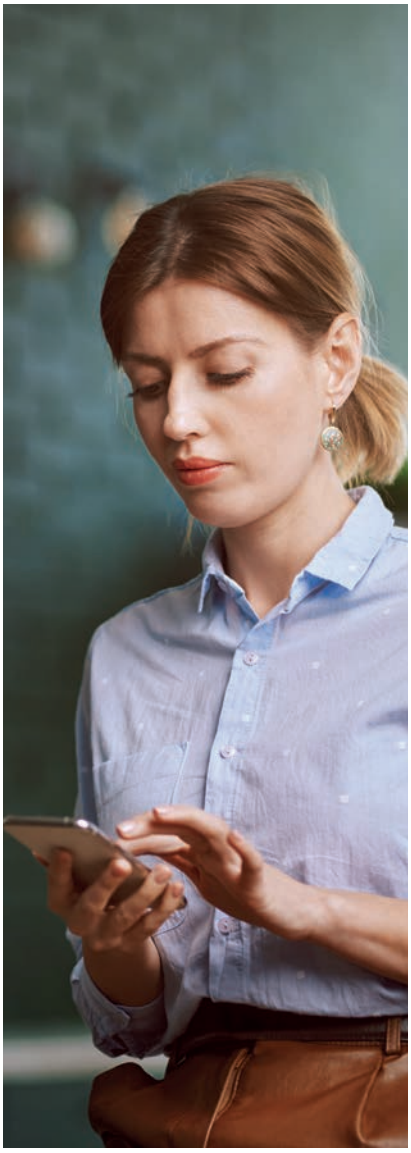
La sécurité des données que la FNSF traite pour accompagner les femmes victimes de violences est donc primordiale, et demande de se poser sans cesse la question : comment éviter les failles ?

Des outils rapides et adaptés

La fiche d'appel, récapitulant les informations recueillies par les écoutantes de la FNSF, est un outil essentiel qui a fait l'objet d'une refonte complète - tant sur la nature de certaines données que sur sa présentation ou sa facilité d'utilisation, et cette nouvelle version sera bientôt mise en ligne. À l'instar d'Agnès, collaboratrice de Groupe Sopra Steria et engagée dans la Fondation Sopra Steria-Institut de France, les bénévoles ont travaillé sur une application modernisée, flexible, actualisée et capable de gérer le fait que le 3919, le numéro d'appel de la FNSF, reste joignable 24h/24h.

Un outil plus simple et, surtout, plus rapide à utiliser car, dans l'action que mène la FNSF, il faut pouvoir agir vite et être efficace. Le numérique permet cela, et cela ne passe pas forcément par des solutions complexes. Dans certains cas la réponse à un besoin passe simplement par la construction d'un groupe de conversation sur Whatsapp.

Avec les associations de son réseau, et avec l'aide de la Fondation Sopra Steria-Institut de France, la FNSF compte donc continuer d'innover et de traquer les failles de ses systèmes pour pouvoir garantir la sécurité des femmes qui font appel à ses services.



Comment sensibiliser et former les plus jeunes à l'usage du numérique ?

Olivier Jacquot
Senior Manager Défense & Sécurité
chez Sopra Steria
et parrain bénévole pour « La main à la pâte », un projet accompagné par la Fondation Sopra Steria-Institut de France

L'accès aux sciences du numérique dès le plus jeune âge est un sujet central tant la technologie est désormais omniprésente dans la société et dans la vie des citoyens, y compris les plus jeunes. Au-delà des problématiques d'accès aux infrastructures et aux outils, c'est bien l'usage même du numérique qui pose question.

Deux enfants sur trois dans le monde n'ont toujours pas accès à internet chez eux. **Une fracture numérique qui ne fait qu'accroître les inégalités tout au long de la vie : 57 % des offres d'emploi sont en effet inaccessibles aux personnes dépourvues de compétences numériques.** C'est pourquoi il est essentiel de former aux outils numériques et à leurs usages dès le plus jeune âge.

S'engager au plus près du terrain

Au sein de cette société du « tout numérique », l'illectronisme constitue un frein fondamental dans les aspects les plus essentiels de sa vie. Un paradoxe certain, tant le numérique porte en lui des valeurs républicaines et égalitaires. C'est pourquoi l'éducation dès le plus jeune âge s'impose comme le meilleur rempart face aux inégalités grandissantes. Avec un enjeu majeur : donner des clés de citoyenneté aux nouvelles générations. C'est à peu de choses près l'objectif que s'est fixé l'Éducation Nationale dans son plan « sciences et technologies à l'école primaire » qui entrera en vigueur à la rentrée 2022.

La Fondation Sopra Steria-Institut de France s'est impliquée dans la formation continue des professeurs des écoles aux côtés de la Fondation « La main à la pâte » pour garantir cette transmission des connaissances aux jeunes générations, y compris dans les zones rurales et réseaux d'éducation prioritaire (REP). Le numérique devient ici un levier d'intégration, au service de publics fragilisés ce qui est en accord total avec notre raison d'être.

Professeurs et professionnels du numérique : un duo gagnant

Pour accompagner la Fondation « La main à la pâte » dans sa mission de former plus de 12 000 enseignants en sciences, la Fondation Sopra Steria-Institut de France s'est mobilisée pour la deuxième année consécutive en ce qui fait notre force : les sciences du numérique.

Parmi les projets menés : un défi robotique, réalisé dans dix classes de primaire avec l'aide de sept bénévoles Sopra Steria. Le principe consistait à faire suivre à un petit robot un parcours très simple, présélectionné. Mais le véritable but était de donner aux professeurs et à leurs élèves les bases de la programmation. Nos collaborateurs bénévoles sont également intervenus dans les classes pour faire prendre conscience aux enfants du rôle et de la place du numérique dans leur quotidien, et ouvrir les portes d'une sensibilisation, en expliquant en termes simples leur métier.

La plus belle récompense est venue d'une jeune élève qui nous a expliqué que ce qu'elle avait préféré dans ce défi, c'était la réflexion et le travail menés ensemble pour trouver des solutions aux difficultés rencontrées. Finalement, c'est exactement ce que l'on attend de l'éducation et c'est aussi ce qui donne du sens à notre engagement sur le terrain.

sopra hr
SOFTWARE

OSEZ INVENTER LES RH DE DEMAIN

Nous guidons les entreprises
dans la transformation digitale & positive des RH.

Ensemble conjuguons nos talents. #futureofwork

www.soprahr.com

Quoi de neuf chez Sopra Steria ?

Sopra Steria fait son road show !

En mai dernier, les équipes Sopra Steria étaient présentes au pied de l'Arche de la Défense pour la première date du road show Sopra Steria. Cette opération à destination de nos écoles partenaires vise à promouvoir nos métiers sur une dizaine de campus en France à partir de la rentrée. Lors de cette première date à la Défense, les étudiants ont pu découvrir les dernières innovations Sopra Steria, échanger avec nos équipes et découvrir l'univers du Groupe.

Course croisière EDHEC : Sopra Steria prend le large

Une nouvelle fois, Sopra Steria était partenaire de cette 54ème édition de la Course Croisière EDHEC. Pendant une semaine, nos équipes étaient présentes pour accompagner les équipages sponsorisés par Sopra Steria et échanger avec les étudiants. De nombreuses animations étaient prévues sur le stand Sopra Steria : une journée Mission Handicap, challenge OSINT, concours de winch, ou encore initiation à la réalité augmentée.

Encore félicitations aux équipages des écoles Centrale Marseille, Centrale Nantes, UTT, INSA Rennes, Mines de Nancy, ENSEIRB, CentraleSupélec et l'EDHEC pour leur participation à la régate et aux différents challenges inter-équipages organisés tout au long de la semaine.

Handitour : tour de France et sensibilisation pour la Mission Handicap

De mai à juillet, la Mission Handicap Sopra Steria a fait le tour des sites Sopra Steria pour le Handitour 2022. C'était l'occasion pour nos collaborateurs d'être sensibilisés à la prise en compte du handicap en entreprise et de participer à de nombreuses animations.

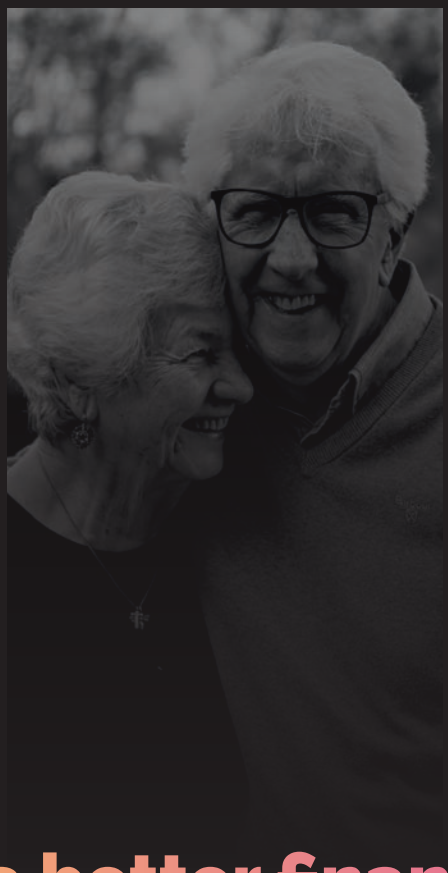
Le programme était riche tout au long du tour : mise en situation de handicap sur des activités ludiques comme du tir laser, initiation aux jeux vidéo adaptés, une conférence sur "Le métavers, une chance pour l'accessibilité ?", organisation d'une journée thématique lors de l'Open Sopra Steria à Lyon, découverte de l'handisport avec de nombreux athlètes et champions paralympiques: Nantenin Keita, Dimitri Pavadé, Fabien Lamirault ou encore des joueurs du Stade Toulousain.

Pour sa campagne d'alternance, Sopra Steria ouvre ses portes aux étudiants

Lors d'une journée dédiée aux étudiants du CFA Afia, centre de formation d'apprentis de plusieurs établissements parisiens partenaires du Groupe, les équipes Sopra Steria ont partagé leur passion du numérique dans les locaux flambants neufs du site de Latitude, à la Défense.

À cette occasion, de nombreux étudiants ont pu échanger avec des collaborateurs et recruteurs lors d'ateliers, jeux de pistes, et speed-recruiting. Sopra Steria s'engage chaque année à soutenir les formations en alternance en recrutant plus de 500 jeunes en contrat d'apprentissage ou professionnalisation.

Coding **Colorful** Banking


Building a better financial World

for each of us, everywhere, anytime

#financialinclusion
#corporateresponsability



Sopra Banking Software

Intégrez un environnement stimulant animé par l'envie de réussir ensemble

Chez CIMPA, nous sommes des passionnés, animés par l'envie de donner le meilleur de nous-mêmes, partageant le goût du défi et de l'innovation.
Nous aimons donner chaque jour du sens à notre action, en valorisant une offre et un savoir-faire uniques autour du PLM (Product Lifecycle Management) de produits de haute technologie.

Pour répondre aux besoins de nos clients, nous aimons nous doter de multiples talents qui pensent différemment et s'engagent dans un collectif fort et dynamique.

Découvrez notre univers sur www.cimpa.com

The world is how we shape it*

CIMPA
PLM Services
a Sopra Steria company

(*) Le monde est tel que nous le façonnons.

Découvrez les secteurs où se joue la transformation digitale

Sopra Steria, l'un des leaders européens du conseil, des services numériques et de l'édition de logiciels, aide ses clients à mener leur transformation digitale. Fort de 47 000 collaborateurs dans 30 pays, le Groupe place l'humain au centre de son action pour construire un avenir positif.

Assurance & protection sociale

Apporter une solution de gestion globale de la complémentaire santé et prévoyance, en individuel et en collectif.

Telecom, media & entertainment

Accompagner nos clients dans la course à l'innovation technologique pour qu'ils gardent leur avantage dans un contexte ultra concurrentiel.

Banque

Refondre les systèmes d'information en mode agile avec des équipes internationales.

Secteur public

Accompagner ministères et collectivités locales dans la mise en œuvre des réformes du quinquennat et du programme Action Publique 2022.

Automotive

Travailler étroitement avec le secteur automobile sur ses nouveaux défis technologiques : véhicule autonome ou électrique, voiture connectée.

Nos marques et filiales

sopra steria next

Le conseil en transformation digitale de Sopra Steria. Nos 3400 consultants en Europe conçoivent des stratégies visionnaires et réellement actionnables aux résultats tangibles et aux bénéfices durables.

Sopra Banking Software

Développer et déployer les technologies permettant aux Banques et Institutions Financières de donner accès aux services financiers à des millions de personnes dans le monde.

sopra hr SOFTWARE

Offrir des solutions RH complètes, parfaitement adaptées aux besoins des directions des ressources humaines.

sopra steria

Santé, social, emploi

Permettre les transformations liées aux réformes dans les domaines emploi, formation professionnelle, santé, retraite, recouvrement et famille.

Défense & Sécurité

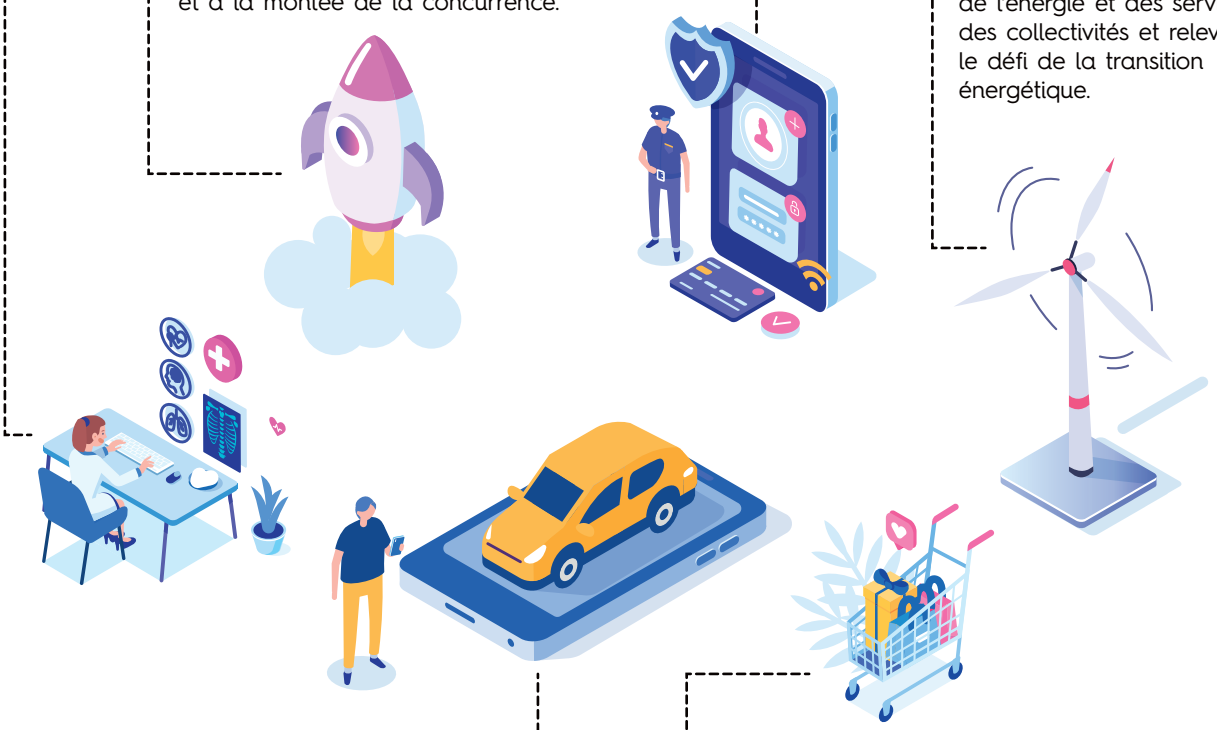
Construire et déployer les meilleurs outils digitaux au profit des armées, de la gendarmerie, de la police et de la justice.

Aérospatial & Aéronautique

Aider les entreprises du secteur Aéronautique & Spatial à faire face à la croissance du trafic voyageurs et à la montée de la concurrence.

Énergie & Utilities

S'adapter aux mutations de l'énergie et des services des collectivités et relever le défi de la transition énergétique.



Transport

Construire la mobilité intelligente et durable de demain au travers de solutions multimodales.

Retail

Accompagner nos clients retailers sur l'optimisation de toute leur chaîne de valeur, du process d'approvisionnement à l'influence client.

sopra real estate SOFTWARE

Libérer le potentiel du patrimoine immobilier de nos clients avec une plateforme de services digitaux dédiée.

CIMPA PLM Services a Sopra Steria company

Accroître la productivité des entreprises en améliorant les processus, les cycles de production, la gestion et la traçabilité documentaire.

galitt a Sopra Steria company

Accompagner les établissements financiers, les commerçants et les acteurs de l'industrie du paiement dans la transformation de leurs services de paiement, afin de les rendre simples, efficaces et sûrs, dans la vie de tous les jours.

Abonnez-vous à notre newsletter carrière

#DigitalLovers

sopra steria

Nos implantations

En France

Et à l'international dans 30 pays

ALLEMAGNE	EMIRATS ARABES UNIS	MONACO
AUTRICHE	ÉTATS-UNIS	NORVÈGE
BELGIQUE	FRANCE	PAYS-BAS
BRÉSIL	GABON	POLOGNE
BULGARIE	INDE	ROYAUME-UNI
CAMEROUN	ITALIE	SÉNÉGAL
CHINE	LIBAN	SINGAPOUR
CÔTE D'IVOIRE	LUXEMBOURG	SUÈDE
DANEMARK	MAROC	SUISSE
ESPAGNE		TUNISIE

Le Groupe en chiffres

+ de 47000
collaborateurs

présence dans
30 pays

+ de 50 ans
d'expertise

4,7 Mds
d'euros de CA en 2021

+ de 50
métiers

11
secteurs d'activité


sopra real estate
SOFTWARE
REJOIGNEZ L'ÉDITEUR LEADER
DU MARCHÉ DE L'IMMOBILIER
FRANÇAIS
Participez à la **transformation du secteur de l'immobilier** au côté de nos 800 experts.

BD

DigitalLovers

Nous rejoindre

Retrouvez l'ensemble de nos offres d'emploi sur notre site carrières :

soprasteriarecrute.fr

Suivez-nous sur les réseaux sociaux : actualités, échanges en direct, etc.

Sopra Steria
6, avenue Kléber
75116 PARIS

www.soprasteria.fr

Œuvrons pour un digital au service de la souveraineté

Chez Sopra Steria, nous contribuons à créer des clouds souverains pour le secteur public.
Rejoignez Sopra Steria, l'un des leaders européens du conseil, des services numériques et de l'édition de logiciels.

www.soprasteriarecrute.fr

(*) Le monde est tel que nous le façonnons.

The world is how we shape it*

sopra steria