

# LES MENACES DE DEMAIN, DÉFI MAJEUR DE LA CYBERSÉCURITÉ

Les nouvelles tendances technologiques, les transformations de l'écosystème numérique et la multiplication des attaques malveillantes, poussent les acteurs du marché de la cybersécurité à développer et déployer des outils de plus en plus innovants.

Rencontre avec Jean-Luc Gibernon (91), Directeur Défense & Sécurité chez **Sopra Steria**.



Jean-Luc Gibernon (91)

## BIO EXPRESS

Après avoir quitté les bancs de l'École polytechnique en 1994, Jean-Luc Gibernon (91) a entamé sa carrière professionnelle à la Direction Générale de l'Armement, dans le domaine des systèmes de renseignement et des systèmes d'information opérationnels. En 2013, il rejoint la Business Unit Défense & Sécurité du groupe Sopra Steria.

## Pourriez-vous nous présenter Sopra Steria ? Vos activités ?

Sopra Steria est l'un des leaders européens de la transformation numérique. Nous figurons dans le top 10 des services IT en Europe et dans le top 5 en France.

tion face aux attaques informatiques, et, comme celles-ci sont parfois très furtives, ils ignorent s'ils subissent des attaques. Bref ils sont vis-à-vis de la menace informatique, en plein brouillard... Nos interventions permettent de lever le brouillard et de mieux affronter la menace.

INNOVER EST UN MOYEN INDISPENSABLE POUR LUTTER, POUR RENFORCER SES DÉFENSES ET *IN FINE* ÉVITER DES SCÉNARIOS DRAMATIQUES.

Nous proposons un des panels de services les plus complets du marché : du conseil à l'intégration de systèmes en passant par l'édition de solutions métier et les business process services. Nous apportons une réponse globale aux enjeux de développement et de compétitivité de nos clients, en combinant valeur ajoutée et innovation dans les solutions que nous offrons. Nous comptons 37.000 collaborateurs dans plus de 20 pays et nous affichons un chiffre d'affaires de 3.4 milliards d'euros (2014).

Nous couvrons, à travers notre offre de services, trois volets primordiaux et complémentaires : prévention, protection et détection-réaction. Le volet **prévention** recouvre l'ensemble des mesures techniques et/ou organisationnelles à prendre sur le moyen-long terme. Dans le volet **protection**, nous définissons des architectures sécurisées et intégrons les meilleures solutions de sécurité disponibles sur le marché. Quant à la **détection-réaction**, elle se concrétise par la mise en place d'un service de veille active permanente sur les réseaux les plus critiques de nos clients, ainsi que les capacités de gestion de crise associées.

## Sopra Steria a également développé une large activité en cybersécurité. Pouvez-vous nous en dire davantage ?

Notre communauté cybersécurité compte environ 750 personnes, dont 250 en France. Nous proposons une large panoplie de services complétée par une offre de développement de solutions de sécurité. En général, nos clients ne savent pas quel est leur niveau réel de protec-

## Vous portez une considération particulière à l'innovation. Pouvez-vous nous expliquer comment l'innovation se décline chez Sopra Steria ?

Les cyberattaquants font preuve de beaucoup d'imagination et de ténacité, chaque année



Vue d'un « Security Operations Center » de Sopra Steria.

nous mesurons leur progression. Les attaques deviennent ainsi de plus en plus complexes et sophistiquées. Innover est un moyen indispensable pour lutter, pour renforcer ses défenses et *in fine* éviter des scénarios dramatiques.

Par ailleurs, l'évolution ultrarapide du monde numérique nous impose d'être constamment à la recherche de nouvelles solutions pour parvenir à les protéger.

Pour ce faire, chez Sopra Steria, nous disposons d'équipes dédiées à la R&D, situées à Toulouse et Rennes, qui apportent cette capacité d'innovation.

Nous sommes, par ailleurs, en mesure de fournir des technologies innovantes grâce aux partenariats de transfert technologique que nous avons noués avec différents instituts de recherche technologique. A titre d'exemple, nous avons conclu un accord de partenariat avec le CEA Tech, qui vise à transférer les technologies génériques issues du CEA au sein du « Laboratoire d'Innovation » de notre Centre de Cybersécurité.

#### **En plus de l'innovation, sur quoi vous basez-vous pour consolider votre positionnement sur le marché de la cybersécurité ?**

En plus de notre capacité à apporter une réponse évolutive, nous nous distinguons sur le marché par notre double positionnement : nous sommes à la fois un offreur global en cybersécurité et une Entreprise de Service Numérique capable de mener à bien des projets technologiques hautement complexes de grande ampleur.

#### **Comment accompagnez-vous vos clients ?**

Notre objectif est d'accompagner nos clients dans leurs programmes de transformation, aussi com-

plexes soient-ils, et les aider à faire un meilleur usage du numérique en toute confiance.

Nous sommes donc présents sur l'ensemble de la chaîne de valeur. Cela signifie que nous proposons à nos clients des prestations de conseil, de développement de solutions, d'intégration de systèmes et d'évaluation de la sécurité. Pour finir, nous avons également la capacité à opérer la sécurité des systèmes d'information de nos clients depuis notre Centre de Cybersécurité de nouvelle génération situé à Toulouse.

#### **Le marché de la cybersécurité connaît une forte dynamique. Qu'en pensez-vous ?**

D'une manière globale, le marché est en forte expansion en raison de trois facteurs : les évolutions technologiques apportées par le secteur du numérique (il faut les sécuriser), les nouvelles solutions de sécurité du marché (il faut en tirer parti) et les nouvelles menaces informatiques (contre lesquelles il faut se protéger).

Par ailleurs, les systèmes d'information que nous protégeons sont de plus en plus ouverts et interconnectés, ils présentent par conséquent une surface d'attaque de plus en plus grande.

Cette situation nous conduit à une remise en cause systématique et permanente de nos acquis. Nous sommes en recherche perpétuelle d'avancées technologiques et nous faisons de l'anticipation sur la menace de demain pour mieux être en mesure d'y faire face.

#### **Ce marché arrive-t-il à maturité ?**

L'évolution du marché est indéniable mais on ne peut le qualifier de mature. Dans l'écosystème français, on peut observer la constitution de deux grands pôles, avec d'une part des grands acteurs économiques du secteur, qui consolident

encore leurs positions, et d'autre part un large tissu de PME innovantes, capables d'émerger sans nécessiter de gros investissements, et qui sont très soutenues par les pouvoirs publics.

#### **Comment envisagez-vous votre développement à l'échelle internationale ?**

Nous avons pour ambition de devenir un acteur global de premier plan dans le domaine. Le développement à l'international est donc un axe de développement de niveau stratégique. Après avoir ouvert un Centre de Cybersécurité en Angleterre, nous venons d'inaugurer un Centre de Cybersécurité de dernière génération à Singapour. Et nous ne nous arrêtons pas là, puisque deux nouveaux Centres de Cybersécurité sont prévus, en Allemagne et en Belgique.

#### **Un petit mot aux élèves de Polytechnique ?**

La cybersécurité, c'est tout un univers... non pas un métier, mais un large spectre de métiers bien différents. Le secteur est en pleine expansion et offre de très belles opportunités.

La cybersécurité, c'est aussi une communauté de passionnés qui relèvent, tous les jours, des défis technologiques dans un contexte d'enjeux stratégiques. Malgré tout, le domaine conserve un aspect parfois très ludique, comme en témoignent les « hacking challenges » que nous organisons et qui attirent nombre d'étudiants, venant se confronter, pour le plaisir, aux épreuves techniques de Cybersécurité que nous leur préparons... ■

#### **EN BREF**

- Un réseau mondial de plus de 750 experts dédiés à la cybersécurité
- Plus de 300 références dans des projets complexes en cybersécurité
- Une offre globale de services couvrant l'ensemble du cycle de vie
- Des Centres de Cybersécurité de référence en Europe et dans le monde
- Un modèle de service unique sur le marché
- Une expertise reconnue dans la gestion des identités numériques et la cyberdéfense