

UN PURE PLAYER DE LA CYBERSÉCURITÉ

au service de ses clients

Laurent Charvériat, président du Groupe I-TRACING, détaille pour nous le positionnement de son entreprise. En plaçant ses clients et leurs besoins au cœur de sa stratégie, cette entreprise française couvre l'ensemble des problématiques cybersécurité et accompagne ses clients en France et dans leurs activités à l'international. Explications.



Laurent Charvériat

I-Tracing est un pure player de la cybersécurité. Qu'est-ce que ce positionnement implique ?

En effet, nous sommes des spécialistes de la cybersécurité. Nous ne sommes pas éditeurs de solutions de sécurité (firewall, antivirus, EDR, chiffrement, SIEM...), nous accompagnons les entreprises, essentiellement des grands comptes (entreprises du CAC40, SBF 120, grandes administrations, ETI...) dans l'intégration et l'exploitation des solutions de cybersécurité. Comparé à d'autres acteurs du métier, la

cybersécurité est véritablement notre cœur de métier. Nous ne faisons que cela et nous en couvrons toutes les dimensions : analyses de risques, audit et tests d'intrusions, conseil, ingénierie et intégration de solutions, SOC, services managés, réponses à incidents ...

Comment cela se traduit-il ?

En amont, nous identifions les besoins et les problématiques de nos clients en matière de cybersécurité et sécurisation de leurs données, leurs systèmes d'information, leurs infrastructures... L'idée est notamment de réaliser une classification des données et des actifs en fonction de leur criticité afin de mieux allouer les ressources financières et humaines.

Dans la continuité de cette phase de conseil et d'analyse, nous poursuivons sur nos métiers d'ingénierie et d'intégrateur. En partant toujours du besoin et de la problématique, mais également en prenant en compte la maturité de notre client, son infrastructure, son système d'information et ses compétences, nous lui proposons les solutions les plus pertinentes. Cette expertise technique combinée à la fine connaissance de l'écosystème des solutions de cybersécurité nous permet de faire des recommandations contextualisées et sur-mesure. En effet, il est essentiel de bien comprendre les éditeurs et leurs offres pour optimiser l'identification de la solution, son intégration, son exploitation, ainsi que son potentiel en termes d'évolution, car la cybersécurité est un sujet en perpétuelle

mutation. Une fois les solutions de sécurité intégrées et implémentées, il est aussi important d'assurer une surveillance permanente, car aucune entreprise n'est à l'abri d'une faille ou d'une erreur commise par un collaborateur. Depuis quelques années, cette activité de SOC se développe de plus en plus et s'impose comme un maillon indispensable de la chaîne de protection. I-Tracing dispose ainsi de plus d'une centaine d'analystes, des ingénieurs spécialistes de la sécurité, qui prennent en charge ce volet pour nos clients afin notamment de détecter les signaux faibles annonciateurs d'une attaque dans le but de la bloquer ou de limiter son impact.

En outre, nous avons aussi une capacité de réponse à incident. Nos équipes de spécialistes vont analyser les conditions de la survenue de l'incident ou de l'attaque, évaluer son impact puis accompagner notre client dans le rétablissement de son système d'information pour garantir un retour à un fonctionnement nominal.

Au travers de votre filiale IDENTO, vous capitalisez également sur une expertise pointue en matière d'Identity and Access Management (IAM). Qu'en est-il ?

L'IAM permet de gérer les identités et les accès. Il s'agit d'une expertise à part entière dans le domaine de la cybersécurité. Si nous disposons déjà de compétences en interne à ce niveau, nous avons fait le choix de renforcer nos expertises et notre positionnement sur ce sujet en rachetant l'entreprise

IDENTO, dont le cœur de métier est justement la gestion des identités et des accès. Nous avons une approche globale de cet enjeu au travers de missions de conseil et d'intégration de solutions. Nous accompagnons nos clients sur différents sujets : gestion des comptes, gestion des accès aux applications, sécurisation de l'accès aux données, gestion des droits d'accès aux données... tant pour leurs collaborateurs internes, que pour leurs partenaires ou leurs clients (CIAM, pour Customer IAM). L'ensemble de ces sujets nécessite, d'ailleurs, une réflexion en amont pour une stratégie efficace.

Les solutions de sécurité, une fois déployées, doivent être opérées, gérées et exploitées. Que proposez-vous à ce niveau ?

En effet ! Dans ce cadre, nous avons un pôle dédié qui s'articule autour de deux activités :

- le support : nous formons les équipes internes de nos clients en charge de l'exploitation et de la gestion de la solution. Et ces dernières peuvent bien évidemment nous solliciter en cas d'incident. Même si nous intégrons des solutions d'éditeurs tiers, nous sommes le point d'entrée pour toutes demandes d'assistance ;
- les services managés : nos clients nous font aussi confiance pour gérer et exploiter les solutions que nous intégrons et déployons pour eux.

Sur l'ensemble de ces sujets et problématiques, quelles sont vos forces ?

Nous sommes à la fois un généraliste et un pure player de la cybersécurité. Ce positionnement nous permet d'accompagner nos clients en amont, sur la réflexion ; au niveau de l'intégration des solutions ; en aval, dans l'exploitation et le support des solutions.

L'interaction de ces différents métiers et expertises garantit également une montée

“Nous sommes à la fois un généraliste et un pure player de la cybersécurité. Ce positionnement nous permet d'accompagner nos clients en amont, sur la réflexion ; au niveau de l'intégration des solutions ; en aval, dans l'exploitation et le support des solutions.”

en compétences de nos ingénieurs et un enrichissement mutuel qui nous permettent de proposer des services toujours plus performants et pertinents. En effet, nous faisons de la sécurité pour répondre aux besoins de nos clients. Dans nos recrutements, nous sensibilisons nos futurs collaborateurs à ce mindset. Cela nous permet d'être toujours en adéquation avec la problématique et la réalité des entreprises, mais aussi à l'écoute de leurs besoins.

D'ailleurs, nous recherchons des compétences passionnées par la cybersécurité qui ont avant tout la volonté de mettre leurs expertises et savoir-faire au service des clients.

Qu'en est-il de vos enjeux et de vos perspectives ?

I-Tracing a vu le jour il y a bientôt 17 ans. Après avoir été longtemps détenue par quatre associés, nous avons ouvert en 2017 le capital de la société. Accompagné alors par le fonds Keensight Capital, nous avons développé notre activité pendant trois ans et demi. En 2021, Keensight a cédé ses parts à Eurazeo et Sagard NewGen qui nous soutiennent dans notre développement en France et à l'international. D'ailleurs, nous disposons de filiales en Angleterre, au Canada et à HongKong. Cette couverture des différents fuseaux horaires nous permet de garantir une activité de surveillance de la sécurité (SOC) et des services managés en 24/24 et 7/7. C'est un véritable atout, car une attaque peut survenir à n'importe

quel moment. Au moindre signal faible, un ingénieur peut intervenir pour analyser et évaluer la menace.

Dans le cadre de notre croissance organique, notre enjeu principal est le recrutement sur un marché en tension où il y a une pénurie avérée de compétences et de talents. Nous sommes passés de deux personnes à nos débuts à plus de 350 aujourd'hui. Sur les prochaines années, nous avons un objectif de 100 à 120 recrutements par an. Portés par une dynamique de croissance avérée, nous pouvons proposer à nos collaborateurs une carrière évolutive avec une prise de responsabilités et des opportunités de mobilité à l'international.

Dans le cadre de notre développement à l'international, nous accordons une importance particulière à la Chine continentale pour accompagner des entreprises européennes présentes en Chine et qui ont besoin d'un partenaire de confiance expert en cybersécurité pour leurs filiales chinoises. Nous sommes dans ce cadre en train de créer notre filiale à Shanghai. ×