MAÎTRISER TOUTE LA CHAÎNE DE PROTECTION un vrai plus dans le marché de la cybersécurité

Allentis est une entreprise française en forte croissance dans le domaine de la cybersécurité. Elle déploie ses activités sur plusieurs secteurs, hardware et software, et fournit des services variés sur toute la chaîne des flux de données. ***Son président et fondateur, Éric Fries, nous explique son approche.***

Éric Fries

Bio express
Ingénieur diplômé de Télécom SudParis (1984), il a travaillé chez Alcatel, créé plusieurs PME. Il a fondé Allentis en 2011 et il en est le président.

“L’ANSSI effectue un travail extraordinaire depuis dix ans pour dynamiser l’écosystème cyber français.”

Pouvez-vous nous présenter vos activités ?
Nous sommes une PME française qui existe depuis dix ans maintenant, basée sur trois sites, Paris, Tours et Nîmes. Nous avons trois métiers, en fait trois savoir faire : la fabrication de systèmes de réplication de trafic, c’est-à-dire un hardware qui permet d’extraire du trafic pour l’envoyer à des systèmes d’analyse. Le deuxième, dans le logiciel, concerne les solutions de détection de menaces cyber en ligne. Notre troisième métier correspond aux systèmes d’analyse de la performance des flux de données (voix, images, data), la volumétrie, les comportements, etc. Ces trois domaines se complètent. Nos clients sont en général des grandes entreprises qui disposent de leur data center ou bien qui confient tout ou partie de leur système informatique à des sous-traitants divers.

Vous avez développé vous-même vos propres solutions ?
Nous avons entièrement développé nous-mêmes nos systèmes logiciels de détection. Sur l’aspect matériel également, nous avons développé de l’électronique et de l’optique pour pouvoir fabriquer des systèmes de réplication de trafic.

Quelles sont les compétences demandées par l’expertise qui est la vôtre ?
Faire des logiciels de détection de menace demande des compétences variées. En dehors de savoir développer des logiciels, il est nécessaire d’avoir une connaissance très pointue du décodage protocolaire. Ensuite, il faut avoir une connaissance étendue des architectures réseau, c’est-à-dire comment vont et viennent les données dans un data center et sur les réseaux étendus, et il faut comprendre le comportement normal des utilisateurs. En résumé, nous avons des compétences pour décoder, analyser les data, comprendre la circulation normale des flux, mais aussi comprendre le comportement type d’un utilisateur. Notre métier a aussi une autre exigence : pour faire des systèmes robustes, il faut avoir des compétences en architecture logicielle, faire les bons choix, ce qui n’est pas toujours le cas dans ce secteur où finalement les clients ne voient pas « ce qu’il y a sous le capot ».
Nos systèmes sont des serveurs dans lesquels sont injectés du trafic en temps réel. Il faut donc faire de la programmation sur des systèmes qui fonctionnent en temps réel : cela demande des compétences qui s’acquièrent progressivement.
Il y a des pièges dans la construction de ces systèmes, et l’expérience R&D est donc un point important.
Notre caractéristique, c’est que technologiquement nous maîtrisons l’ensemble du processus ; comme nous produisons des systèmes de réplication, nous pouvons fournir au client toute la chaîne de protection périmétrique, y compris les équipements qui vont lui permettre d’extraire les données de son réseau et les envoyer à des systèmes d’analyse que nous aurons aussi

fournis. Nos confrères généralement ne s'occupent que de détection. Nos systèmes de détection sont aussi particulièrement performants : et il faut souligner que tous ne se valent pas, surtout dans la capacité à présenter les données de manière simple et rapidement exploitable. Le risque numéro un du client et de son SOC (Security operation center), c'est la noyade dans une masse de données complexes à traiter. C'est justement ici que nous faisons la différence.

Qu'est-ce qui, pour vous, dynamise le marché aujourd'hui ?

Aujourd'hui, très clairement, c'est la mise en conformité des organisations avec le volet cyber de la loi de programmation militaire. Dans la dernière loi, il y a un volet cyber très important dont l'exécution, en termes réglementaires, est portée par l'ANSSI. Et ce volet cyber oblige les opérateurs d'importance vitale (OIV) à s'équiper de systèmes de défense dans un certain délai. Les opérateurs de services essentiels (OSE) doivent quant à eux initier une démarche de cyber-protection. C'est ce marché que nous visons, sur la partie détection de menaces.

À plus long terme, comment voyez-vous l'évolution du marché ?

Je prendrais la question d'un peu plus loin. Dans la cybersécurité telle que nous l'abordons, il y a deux problématiques. En premier lieu, la protection périmétrique : par exemple construire une ligne de défense qui surveille ce qui entre et ce qui sort d'un data center ou d'une partie d'un système d'information.

Il y a un deuxième besoin : la protection des end points (ordinateur portable, smartphone, tablette, serveur, composant IOT, etc.), c'est-à-dire des équipements aux mains des utilisateurs ou accédés par eux. Ce sont les deux grands lieux de protection. Allentis s'intéresse à la première problématique : la protection périmétrique, au travers des équipements de type NDR (Networks detection and response) qui sont branchés au niveau des réseaux et non dans les end points.

L'évolution du marché, c'est peut-être une intégration et une automatisation de ces deux types d'équipements, même si cela est complexe à réaliser. Nos systèmes de détection peuvent repérer un comportement anormal en périphérie ou dans le data center. À l'autre extrémité, les logiciels EDR auront pu détecter des événements anormaux ou agressifs sur les end points.

L'objectif, c'est se protéger de cette menace ; par de bonnes pratiques d'urbanisme et de configuration, puis en mettant en place des règles dans les équipements de contrôle d'accès et de flux (comme les pare-feu) afin de diminuer la surface d'attaque, ce qui revient à ôter aux attaquants des possibilités d'entrer dans le périmètre, et en troisième lieu par l'éducation des utilisateurs et la restriction des usages. Les équipements tels que nous les fabriquons, et ceux que produisent ceux de nos confrères qui font des logiciels de protection des end point, peuvent – cela se pratique déjà mais de manière limitée – piloter des équipements de type pare-feu pour modifier, enrichir leurs règles et ainsi optimiser en quasi temps réel les niveaux de protection. C'est une évolution possible, même si elle met en jeu des automatisations dont on peut craindre les effets de bord.

À quels types d'attaques est-on confronté le plus souvent aujourd'hui et comment y répondre ?

Toute organisation présente une surface d'attaque : elle laisse ouvertes des opportunités d'être attaquée. Un des objectifs de la protection cyber, c'est évidemment de détecter les tentatives d'attaque, et de les parer, mais au-delà de cet aspect, c'est aussi de réfléchir à ce qui a permis à l'assaillant de rentrer chez vous et de prendre des mesures pour réduire la surface d'attaque, en somme fermer des portes. Aujourd'hui la très grande majorité des attaques arrivent par les mails avec deux stratégies : le phishing, l'objectif étant de chiffrer ou de soutirer vos données, soit directement sur votre poste, soit en se propageant dans votre organisation. La deuxième famille d'attaques, c'est le social engineering, plus orienté vers l'extraction d'informations.

Quelle est votre projection à l'international ? Est-ce que le marché français est dynamique ?

Nous travaillons au niveau international, à petite échelle. Nous avons 250 clients, et 10 % de notre chiffre d'affaires se fait à l'étranger. Mais le marché français est très porteur, pour deux raisons. D'abord, grâce à l'ANSSI qui effectue un travail extraordinaire depuis dix ans pour dynamiser l'écosystème cyber français. Pour parler clairement, nous avons triplé de taille sur les quatre dernières années grâce à l'impulsion de l'ANSSI, grâce à la labellisation, et à la dynamisation du marché qu'ils ont provoquée. Le deuxième point, c'est le problème de la menace cyber en tant que telle, qui est un phénomène massif et très médiatisé.

Les techniques d'attaque ne sont pas vraiment nouvelles, mais l'extension du numérique au niveau de la société, et donc des entreprises et organisations, augmente fortement la surface d'attaque globale, qui devient colossale : tout le monde communique par mails, et souvent de façon imprudente. Cette surface d'attaque ayant considérablement augmenté, la criminalité organisée y a vu une opportunité.

EN BREF

- *Société fondée en 2011 fournissant des solutions de sécurité et de performance des systèmes*
- *19 employés répartis sur trois sites : Paris, Tours et Nîmes. ALLENTIS fournit aux grandes entreprises et administrations des solutions d'analyse des flux de données à des fins de sécurité, d'activité ou de performance.*