L'APPROCHE STRATÉGIQUE, globale et intégrée de la dimension cyber

Société française spécialisée en intelligence et contre-intelligence stratégique, Corexalys accompagne les directions des grands groupes ainsi que les industries sensibles dans la connaissance et l'anticipation des cybermenaces. ***Le point avec son Associé et Directeur e-tech, Pierre-Mayeul Badaire (96).***

Pierre-Mayeul Badaire (96)

Bio express
Pierre-Mayeul Badaire (96), ingénieur en chef du corps des Mines, est diplômé de l'École Polytechnique et de Télécom parisTech. Il a complété sa formation académique par un DEA en cryptographie à l'ENS. Pierre-Mayeul Badaire a commencé sa carrière comme ingénieur en cryptographie au ministère des Armées. Après avoir occupé divers postes d'encadrement, il a été conseiller en charge des technologies d'une haute autorité du ministère puis a rejoint l'industrie en 2012. Il a notamment été directeur général de la société Suneris Solution (groupe Ercom, depuis acquis par Thales) entre 2015 et 2018. Au travers de son parcours, il a développé une solide connaissance des technologies cyber, du big data et de l'industrie du numérique. Il est associé et directeur e-tech de Corexalys depuis 2018.

"C'est l'Humain qui doit maîtriser la technologie et non l'inverse !"

Corexalys est spécialisée en intelligence et contre-intelligence stratégique. Dites-nous-en plus sur votre cœur de métier.
Corexalys a pour objectif la protection des actifs critiques des entreprises et l'identification de ceux qui les convoitent. L'une des premières problématiques d'une entreprise est d'identifier ses actifs critiques qui sont souvent sous-estimés ou mal définis. Au delà des brevets, des codes sources des produits et des bases clients, il existe d'autres actifs critiques parfois plus difficilement appréhendables comme la réputation, sans parler évidement des personnes-clés.

Plus particulièrement, quelle est la différence entre ces deux notions ?
L'intelligence stratégique est une activité consistant à bien comprendre l'environnement externe de l'entreprise pour optimiser la performance de cette dernière, voire à l'influencer et le façonner. La contre-intelligence stratégique est l'approche duale qui consiste à évaluer la vulnérabilité et éprouver les mécanismes de protection de l'entreprise face à des actions hostiles à l'encontre des actifs critiques.

Qu'est-ce que cela sous-entend en termes de positionnement ?
Aujourd'hui, nous employons une vingtaine de collaborateurs et commercialisons nos services auprès de deux grandes typologies de clients.
Nous répondons d'une part aux besoins de grands groupes français qui souhaitent être accompagnés sur des missions ponctuelles ou sur le plus long terme sur une approche globale de contre-intelligence stratégique.
D'autre part, nous accompagnons des ETI, des PME, des start-up ayant une problématique spécifique ou des fonds d'investissement, typiquement dans le cadre d'une opération d'acquisition ou de revente de l'un de leurs actifs. En effet, la valeur d'actif nette d'une entreprise est fortement impactée par son niveau de risque sur les actifs critiques (y compris dans le domaine de la cybersécurité), et les fonds souhaitent aujourd'hui intégrer beaucoup mieux cela dans les processus de due-diligence.
Sur ces sujets et bien d'autres, nous misons sur notre comité stratégique qui a pour but de nous accompagner dans notre réflexion et notre développement.

Concrètement, quels sont les principaux services que vous proposez aux entreprises à ce niveau ? À quels besoins répondez-vous ?
Nous nous distinguons à travers notre approche holistique qui intègre de manière équilibrée les dimensions techniques et humaines. Nous aidons nos clients à connaître leurs vulnérabilités et à maîtriser leurs expositions dans le

cyberespace face à des menaces en perpétuelle évolution. De manière duale, nous accompagnons aussi nos clients dans l'utilisation innovante et proactive de l'internet dans une approche plus globale de l'intelligence stratégique, à travers :

- la réalisation de Cyber Empreintes ;
- la mise en place de veille stratégique et d'opérations de contre-ingérence ;
- les interventions en cyber due diligence ;
- la conduite d'audit Red Team (attaque ciblée de haut niveau par moyens humains, opérationnels et techniques sur l'entreprise) ;
- des missions d'investigation numériques ou de Cyber Threat Intelligence par l'intermédiaire de notre laboratoire d'étude de comportement des virus informatiques (CXS Lab).

N'oublions pas qu'une cyberattaque est avant tout un groupe d'individus face à un clavier. C'est pourquoi avant de s'intéresser à la correction des failles techniques, il s'agit de comprendre les motivations des attaquants, et d'identifier leurs capacités à employer l'arsenal cyber pour collecter de l'information ou nuire au bon fonctionnement de l'entreprise.

La technologie et l'innovation jouent un rôle considérable dans ce domaine en perpétuelle évolution. Comment appréhendez-vous cette dimension ?

Nous nous appuyons sur la combinaison d'une connaissance approfondie des attaquants et de leurs commanditaires et d'une technologie innovante développée par nos soins. Concernant les technologies, en préambule, je souhaite souligner que nos algorithmes n'ont de la valeur que parce qu'ils intègrent le savoir-faire de nos équipes et de notre réseau. Nous utilisons, bien évidemment, des technologies de traitement et d'analyse massifs de l'information. Par exemple, nous suivons par exemple l'activité du darknet et des réseaux sociaux, en nous focalisant sur les communautés d'intérêts qui ne sont paradoxalement pas si nombreuses. Dans le cadre de cette approche, nous mettons un accent particulier sur le traitement de l'information, en cherchant à la structurer correctement pour notre contexte. Ainsi, les couches métiers sont co-développées avec nos analystes pour coller au mieux aux besoins de nos clients et être le plus pertinent pour leurs missions.

En parallèle, nous bénéficions d'un environnement technologique très favorable : l'essor du logiciel libre permet aujourd'hui de réaliser très rapidement la plupart des fonctions complexes à moindre coût. Par exemple, en ce qui concerne le traitement de l'information, l'écosystème très dynamique en Python sur des sujets comme le crawling ou la classification ouvre de nouvelles possibilités.

Ainsi, des acteurs en forte croissance comme notre entreprise peuvent créer très rapidement de la valeur pour leurs clients sur les couches informationnelles et sémantiques : en agençant correctement ces briques, guidés par notre savoir-faire et nos expertises, nous pouvons obtenir des résultats pertinents pour nos clients en quelques semaines, voire quelques jours.

De manière plus générale, quel regard portez-vous sur l'écosystème dans lequel vous évoluez ?

Le niveau de maturité des comités exécutifs des entreprises sur les questions de souveraineté numérique et de guerre de l'information a fait un saut quantique depuis quatre ans.

La communication percutante de l'ANSSI, le RGPD européen, les fuites massives de données, et l'affaire Snowden, ont très largement contribué à cette prise de conscience globale. De manière plus générale, notre société perçoit avec beaucoup plus d'acuité les enjeux liés au renseignement économique. La question est donc plutôt maintenant pour les entreprises d'optimiser leurs investissements cyber dans un cadre reconfiguré, plus global et cohérent, de la protection de leurs actifs et d'adaptation à leurs marchés. Je suis convaincu — et c'est peut-être à contre-courant des croyances ambiantes — qu'il y a un mouvement de fond de relocalisation à l'échelle nationale et européenne dans le numérique. Le poids relatif des acteurs globaux va diminuer et la pertinence d'acteurs de confiance verticalisés, ancrés dans leurs marchés, sera plus importante. Conscients de ces évolutions, nous souhaitons accompagner la souveraineté numérique du tissu industriel français.