CITALID, le GPS du risque cyber

Cartographier et quantifier les risques cyber des organisations requiert une expertise avancée dans de nombreux domaines de compétence, et une vision à 360° du contexte de l'organisation. *Maxime Cartan, co-fondateur & président de Citalid,* présente l'approche unique de la start-up à cet égard.

Maxime Cartan

Parlez-nous de la genèse de Citalid.
Mon associé et moi travaillions à l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) dans le domaine de la Cyber Threat Intelligence. À ce titre, nous avons participé à plusieurs opérations de cyber défense auprès de ministères ou d'entreprises sensibles françaises.
Nous avons été témoins, à travers ces missions, d'un manque de compréhension du risque cyber et d'implication des plus hauts niveaux décisionnels des entreprises. C'est la raison pour laquelle nous avons décidé de créer Citalid fin 2017, et notre équipe compte aujourd'hui une douzaine de collaborateurs.
En misant sur notre expertise dans le domaine de la connaissance des cybermenaces, nous avons été lauréats du Prix de l'Innovation 2018 des Assises de la Sécurité ainsi que du Prix du Public, et avons remporté le Prix Spécial du Jury de l'édition 2020 du Forum International de la Cybersécurité. Cela nous a permis de renforcer notre développement commercial et de réaliser une levée de fonds d'un montant de 1,2 M€ en juin dernier.

Citalid propose une plateforme logicielle de simulation du risque et des investissements cyber qui intègre une dimension financière. Pourquoi ce choix de positionnement ?
Au cours des dernières années, le métier de responsable de la sécurité des SI (RSSI) s'est considérablement complexifié.
Au-delà des menaces qui ne cessent de croître, notamment suite à la transformation numérique des entreprises, les décideurs doivent également intégrer une dimension budgétaire forte. Il n'est pas viable aujourd'hui d'espérer couvrir la totalité des scénarios de risque cyber. Les RSSI et Risk Managers doivent donc opter pour une logique d'arbitrage, et sélectionner les risques à accepter, à réduire, ou à transférer à un cyber assureur. Une telle réponse différenciée nécessite une connaissance et une vision à 360° de la menace et du niveau de défense de l'organisation. C'est à ce niveau que nous intervenons.

Concrètement, comment cela se traduit-il ?
Nous développons une solution logicielle qui agit comme un GPS du risque cyber à destination des décideurs : nos algorithmes évaluent leur positionnement par rapport à la menace, en prenant en compte leur niveau de maturité défensive et leur contexte ; puis la plateforme les aide à définir leurs objectifs de gestion du risque, et à quantifier leur exposition financière au risque cyber ; enfin, une fois la position et l'objectif définis, notre produit calcule automatiquement le chemin optimal, c'est-à-dire le plan d'action et les investissements prioritaires, et évalue le ROI associé.
Dans un domaine aussi technique que la cybersécurité, nous avons besoin de dépasser et de compléter les données techniques par un reporting dédié aux décideurs.
C'est pourquoi nous quantifions de manière économique chaque scénario de risque, en calculant les probabilités de fréquence et d'impact de chaque cybermenace pertinente dans le contexte de l'entreprise. Le risque peut être découpé en 3 composantes principales :
- La fréquence des attaques tentées ;
- Le taux de réussite de chaque attaque, en fonction du niveau de sophistication de l'attaquant et du niveau de défense de l'entreprise ;
- L'impact financier d'une attaque réussie.

Concrètement, cette méthode permettra aux entreprises de mieux comprendre leurs risques, et ainsi de rationaliser leurs investissements tout en impliquant le plus haut niveau décisionnel.

En ce qui concerne un sujet assez technique tel que la cybersécurité, comment engager les décideurs et les équipes de management au sein des entreprises?
Il est d'abord nécessaire de commencer à voir la cybersécurité non pas comme un centre de

coût, mais comme un centre d'investissement stratégique. Chaque grande vague de cyberattaques, comme celle de mai-juin 2017, contribue à sensibiliser les dirigeants à la criticité du risque cyber pour leurs entreprises. Afin de mieux les impliquer, il est donc nécessaire de dépasser la simple donnée technique et de raisonner en termes d'exposition financière pour l'organisation, à l'image de l'ensemble des risques historiques traités par l'entreprise.

Comment accompagnez-vous vos clients afin de mettre en place une démarche proactive des risques cyber ?

Les Responsables Cybersécurité utilisent notre logiciel afin de sélectionner et quantifier automatiquement les menaces les plus pertinentes. Ils disposent ainsi un tableau de bord qui leur donne un résumé complet des dangers auxquels ils font face, et leur propose la meilleure façon de les gérer à 360°.

Nous pouvons également les assister, ou les faire accompagner par un cabinet de conseil partenaire, pour identifier les « bons scénarios de risque » qu'il va falloir traiter selon leurs contextes métier.

Nous nous appuyons alors sur l'ensemble des données que nous collectons : des données techniques sur la menace et le niveau de défense, des données contextuelles ou géopolitiques, des données économiques, les statistiques de pertes financières, etc.

Quels sont les enjeux pour les produits de cyber assurance qui se développent sur le marché européen ? Comment appréhendez-vous ces challenges ?

Le marché de la cyber assurance est beaucoup plus développé aux États-Unis qu'en Europe. Cependant, les chiffres montrent une croissance accélérée à court et à moyen termes. L'enjeu principal est que le risque cyber est difficilement quantifiable par les assureurs.

En effet, l'approche actuarielle traditionnelle, fondée principalement sur les statistiques historiques des sinistres, n'est pas suffisante. En effet, le risque cyber est un risque nouveau, et il n'existe pas suffisamment de données historiques fiables pour avoir des résultats optimaux.

Afin de pallier les points faibles de cette démarche classique en assurance, il est nécessaire d'adopter une approche technique pour modéliser ce risque de manière complémentaire aux données statistiques. Ainsi, nous aidons nos clients à quantifier le risque en ajoutant notre expertise technique – modélisée dans notre solution logicielle – dans la balance.

Nous sommes également en capacité d'aider les assureurs à créer des produits d'assurance disruptif. En effet, nous pouvons modéliser des primes d'assurance dynamiques, qui reflètent l'exposition financière réelle de l'entreprise. Les assureurs pourraient de ce fait ajuster le prix et la couverture de leurs produits en fonction du contexte, de l'évolution de la menace, et des efforts de sécurité déployés par les assurés, dont nous pouvons calculer le ROI en termes de réduction du risque, et de l'évolution de la menace.

Qu'en est-il de vos perspectives ?

Aujourd'hui, nous sommes fiers d'être le choix de confiance de plusieurs grands comptes français dans des domaines critiques tels que le transport, l'énergie, ou les télécommunications. Nous cherchons donc à consolider notre position d'outil n°1 de gestion stratégique des risques et des investissements cyber.

En parallèle, nous travaillons de plus en plus activement avec le marché des cyber assurances, afin de faire bénéficier les assureurs et les courtiers de notre expertise technique. Enfin, 2020 sera l'année de l'internationalisation pour Citalid, avec notamment une ouverture déjà en cours dans certains pays européens.

Côté R&D, nous avons eu la chance de bénéficier en 2018 d'un partenariat avec l'école Polytechnique dans le cadre d'un Projet Scientifique Collectif.

Pendant un an, 5 brillants étudiants de l'X ont travaillé à nos côtés sur la modélisation du lien entre le contexte géopolitique international et les attaques cyber. Nous tenons ici à remercier Romain Cosson, Lorenzo Filippi, Antoine Guédon, Quentin Nicolas et Pierre Rizcallah pour leur implication et leur travail, qui continue encore aujourd'hui à porter ses fruits pour notre programme de R&D.

De quels profils avez-vous besoin afin de soutenir votre développement ?

Nous avons plusieurs postes à pourvoir, notamment pour des profils spécifiques tels que des data scientists, développeurs et analystes en Cyber Threat Intelligence.

En parallèle, nous avons aussi besoin de personnes intéressées par la géopolitique, l'intelligence économique et l'analyse des données issues de ces domaines.