The Positive Way

WAVESTONE

STARTUPS CYBERSECURITÉ EN FRANCE :

LE DÉBUT DE L'EMBELLIE ?

Cette année a montré l'amorçage d'une transformation de l'écosystème des cyber-startups françaises, le dynamisme des startups n'est plus à prouver et les entrepreneurs français brillent par leur capacité à innover sur différents sujets de la cybersécurité. Quelles actions concrètes permettraient à ces derniers d'intensifier le développement de leurs startups, d'acquérir une nouvelle envergure et, d'ainsi, confirmer le changement d'échelle amorcé ?

AUTEURS

GÉRÔME BILLOIS
gerome.billois@wavestone.com

JULES HADDAD
jules.haddad@wavestone.com

UN ÉCOSYSTÈME DE PLUS EN PLUS DYNAMIQUE

+18% de croissance en nombre de startups depuis janvier 2018

Notre radar recense désormais 134 startups cybersécurité, ce qui représente 25 startups de plus qu'en janvier 2018. Il est intéressant de remarquer que leur taille évolue également de manière positive : si les « très petites entreprises » restent majoritaires, le nombre de « petites entreprises » a augmenté de près de 56%. Au total, les startups représentent plus de 1200 emplois, soit 9% de plus que l'année précédente, et ce pour la 3ème année consécutive !

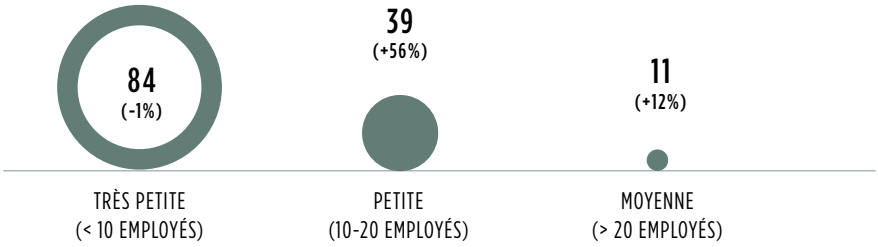
Concernant les sorties, 27 startups ont quitté notre radar, soit seulement 4 de plus que l'année dernière. Parmi ces dernières, 37% sortent du radar à cause de leur ancienneté (>7ans d'existence) et sans pour autant dépasser le critère de la taille limite (<35 employés), ce qui est un signe de difficultés de croissance ou bien simplement d'un manque de volonté de croissance et de prise de risque par les fondateurs. Ce manque de prise de risque est appuyé par un faible taux de liquidation (30%). Cependant nous constatons cette année que les cas de croissance rapide (dépassant les 35 employés avant d'atteindre les 7 ans d'existence) sont plus nombreux (18%) et observons même les premiers rachats (15%), ce qui témoigne d'une attractivité plus forte des ces acteurs.

Au niveau géographique, peu de surprises par rapport aux années précédentes, avec un centre névralgique positionné sur le bassin parisien. L'écosystème reste néanmoins bien réparti avec des présences régionales issues des différents incubateurs. En particulier le pôle Rennais gagne en importance avec les nombreux investissements réalisés par le ministère des armées qui souhaite y créer un véritable deuxième pôle d'expertise en France sur les sujets cybersécurité, comme le montre la présence de l'activité cybersécurité de la DGA sur son campus de Bruz.

Des signes particulièrement positifs pour la transformation de l'écosystème qui s'observent chez les clients ...

Identifié l'année dernière comme un axe essentiel au développement de l'écosystème, le financement des POC par les entreprises devient une pratique de plus en plus répandue puisqu'elle concerne 67% des startups que nous avons interrogées. Cette démocratisation est un signe particulièrement positif pour l'écosystème, car en plus de supprimer cet investissement initial pour les startups, cela montre que les grands groupes évoluent et font confiance à nos pépites françaises.

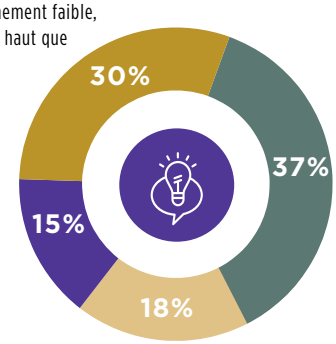
Nombre d'employés



27 startups ont quitté le radar

Liquidation

Un nombre étonnement faible, mais qui est plus haut que l'année dernière



> 7 années d'existence

Montre que la croissance n'est pas facile, ou pas un objectif

Rachat

Une nouvelle tendance: des solutions de cyber sécurité qui attirent de plus gros acteurs

madumbo SMARTMEUP

> 35 employés

Un nombre croissant de **fast risers**

CopSonic DIGITEMIS CybelAngel GATEWATCHER

... sur le marché ...

On ne peut que saluer l'ampleur prise par les levées de fonds cette année. Au niveau de notre radar, le total est 4 fois supérieur à celui de 2017 et pas moins de 7 startups ont levé des montants avoisinant les 10 millions d'euros. Il est également intéressant de mentionner la structure française Vade Secure qui a levé 70 millions d'euros via le fond américain General Catalyst, et la startup franco-américaine Dashlane qui a levé 110 millions de dollars. Il faut également noter que Vadesecure fera partie de Next40, ce programme d'accélération réservé aux 40 pépites de la French Tech et dévoilé récemment par le gouvernement. Cette ampleur est le résultat d'un début de démystification de l'écosystème qui permet aux investisseurs d'être moins frileux sur le sujet. Une autre preuve de cette confiance est la création d'un fonds d'investissement dédié, Brienne III. Cette structure qui a déjà réalisé un premier closing de 80 millions va permettre de continuer à rassurer les investisseurs et contribuer à l'évangélisation de l'écosystème.

Nous observons aussi les premiers **« exits »** des startups françaises. Ils concernent 4 startups de notre radar cette année, dont notamment Trustelem acquise en juillet par Wallix[1], Sentryo qui est en négociation avancée avec Cisco pour une intégration d'ici le premier trimestre 2020[2], et Madumbo[3] qui a été rachetée par l'éditeur franco-américain Datadog. Ils sont une preuve que ces startups françaises sont de plus en plus différenciantes, ce qui les rend plus attractives. En revanche, ces exits sont très souvent portés par des **structures étrangères** et dans la majorité des cas, ils entraînent **la délocalisation** des centres de décisions et de R&D de ces startups, ce qui reste dommageable pour l'entretien du dynamisme de l'écosystème et la souveraineté technologique en France.

Autre signe positif de l'évolution du marché, on observe également l'ouverture de la Défense, notamment avec la fondation de l'« *Innovation Défense Lab* » qui sera accueilli au sein du « *Starbust Accelerator* » et qui favorisera la collaboration des startups avec la DGA[4]. En parallèle, l'Etat a lancé un projet de campus de la cybersécurité. Cette entité aura pour vocation de créer des synergies entre les différents acteurs de l'écosystème en réunissant notamment des acteurs industriels, des startups, des universitaires, ainsi que certaines agences et ministères[5].

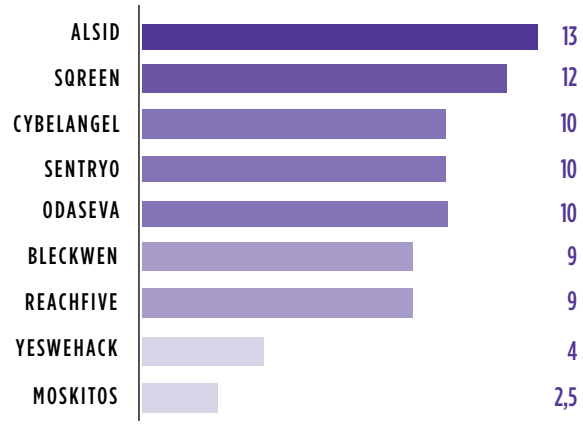
... et pour les startups

L'internationalisation des startups reste un gros levier de croissance, et les startups cybersécurité françaises l'ont compris. La moitié de celles que nous avons interrogées ont déjà des clients à l'étranger, et 15% sont en recherche d'opportunités à l'international : elles se donnent ainsi les moyens d'accéder à des marchés plus importants, plus stratégiques et potentiellement plus matures... et donc de trouver les leviers de croissances nécessaires à leur développement.

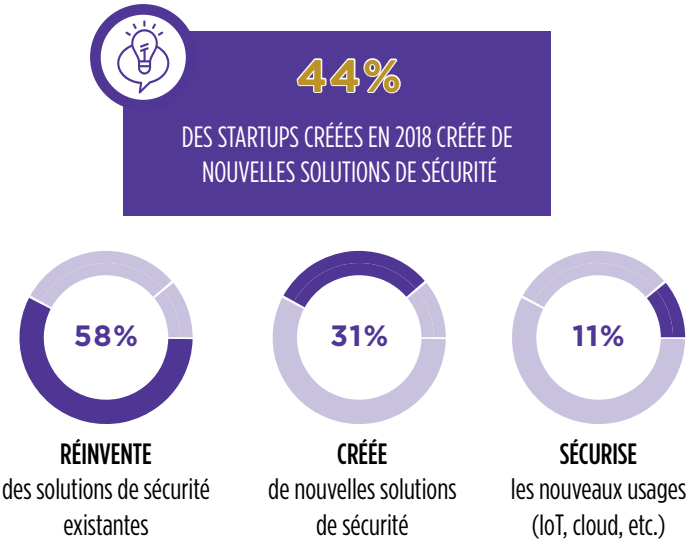
De plus, le positionnement de **l'innovation** change pour l'année 2019 grâce à une **augmentation de la proportion de startup innovantes parmi les nouvelles créations.** En effet, 44% des startups créées cette année proposent des solutions disruptives n'existant pas auparavant sur le marché.

Cela porte à 31% le nombre total de startup de notre radar appartenant à cette catégorie alors qu'il n'était que de 19% l'année dernière.

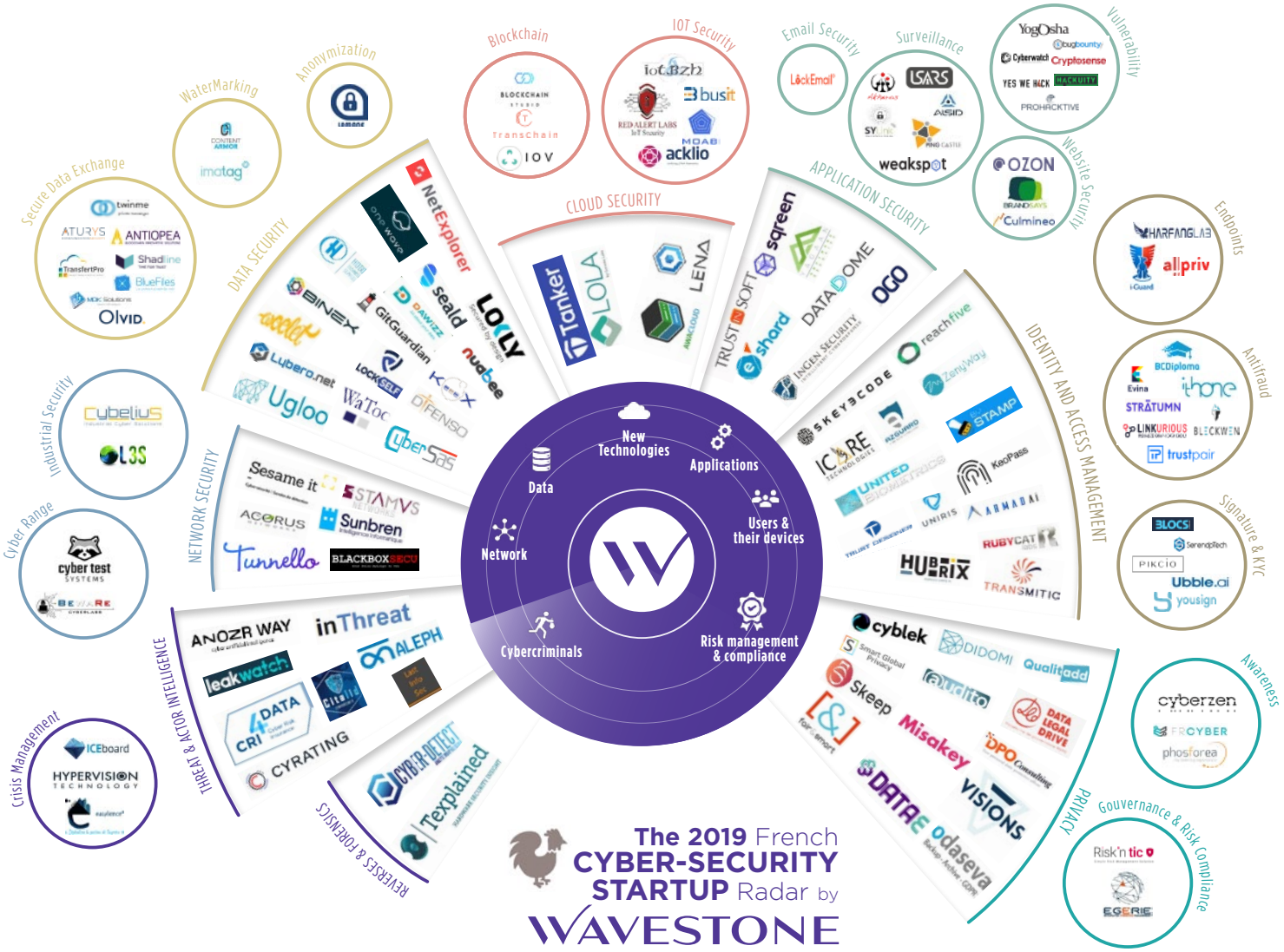
Levées de fonds (en Millions d'euros)



Les startups sont de plus en plus innovantes



1. Wallix (2019), « *Wallix signe la première acquisition de son plan ambition 21* », Communiqué de presse.
2. CERTES Nicolas (2019), « *Cisco prêt à mettre la main sur Sentryo* », Le Monde Informatique.
3. CROCHET-DAMAIS Antoine (2019). « *Datadog rachète la start-up parisienne MAdumbo et se renforce dans l'IA* », Journal du Net.
4. Ministère des armées (2018). « *Le ministère des armées lance l'Innovation Défense Lab* », Actualité de la DGA sur le Site internet du ministère des armées
5. Services du Premier Ministre (2019). « *Un campus cybersécurité pour renforcer l'écosystème français* », Communiqué de presse du service de communication des services du premier ministre.



Radar des startups françaises en cybersécurité (- 35 employés, -7 ans d'existence) septembre 2019

Les entrepreneurs cybersécurité innovent dans les domaines matures de la cybersécurité

On pourrait s'attendre à ce que ces domaines bien établis où la concurrence est rude soient moins attractifs. Cependant les entrepreneurs n'hésitent pas à les aborder sous un angle nouveau afin de gagner des parts de marché.

La sécurité de la donnée comporte ainsi son lot d'innovations. Les startups Binex et Ugloo ont par exemple conçu des solutions de stockage « décentralisé » en faisant la promesse aux entreprises de pouvoir récupérer le contrôle de leurs données aujourd'hui sauvegardées dans des Cloud de fournisseurs différents.

La gestion des identités et des accès, éternel casse-tête des entreprises, est un terrain où l'innovation est possible, comme le prouve ArmadAI qui optimise les habilitations des utilisateurs via l'utilisation de l'intelligence artificielle. La start-up Reachfive se positionne elle sur le CIAM (*Customer Identity and Access Management*) en fournissant une plateforme d'identité client répondant aux enjeux de sécurité et d'expérience utilisateur. Enfin des acteurs comme RubycatLabs n'hésitent pas à bousculer les segments où les parts de marché sont rares, ici la gestion des comptes à privilèges, en se différenciant non pas par la technologie mais par une simplicité d'utilisation et des modèles tarifaires attractifs.

Dans la même optique, la startup Sqreen propose de révolutionner le domaine de la **sécurité applicative** en déployant son micro-agent au sein des applications, permettant ainsi de les monitorer et protéger. D'autres startups ont choisi des problématiques de niche dans ce domaine, comme Datadome avec sa solution qui empêche les « mauvais » robots (Scraping, DDoS, vol de compte ...) de nuire aux applications des entreprises, tout en autorisant les robots légitimes (Googlebot...) à y accéder.

Que dire de **la gestion des vulnérabilités** où les quelques leaders du marché se partagent les parts du gâteau. Le constat est simple aujourd'hui : les entreprises sont très compétentes quand il s'agit de trouver des vulnérabilités, mais beaucoup moins quand il s'agit de les corriger, à cause des problèmes de criticité (d'un point de vue disponibilité) des ressources concernées. On observe ainsi deux approches intéressantes visant à modifier ce constat : celle de Cyberwatch qui propose d'évaluer les vulnérabilités dans un contexte métier afin de prioriser celles qu'il faut corriger ; et l'approche d'Hackuity qui suggère de centraliser et de normaliser les résultats des différents tests d'intrusion sur une même plateforme et d'implémenter une fonctionnalité de « rejeu » de la vulnérabilité afin de pouvoir suivre la résolution de cette dernière de façon automatique.

Les entreprises françaises, en particulier celle ayant le statut d'opérateur d'importance vitale (OIV), sont toujours à la recherche de souveraineté, et cela s'applique également à **la sécurité réseau**, où les entreprises étrangères comme Darktrace ou Vectra sont les leaders du marché. C'est ce qui explique, entre autres, la réussite de la startup Gatewatcher dont les sondes de détection d'intrusions ont été récemment qualifiées par l'ANSSI. C'est également le cas de **la sécurité endpoint**, où des EDR à la française voient le jour comme la jeune pousse Harfanglab et son EDR Hurukai.

Pour finir, la connaissance de la menace est devenue un atout stratégique pour les entreprises, faisant la part belle au domaine de la **Threat Intelligence.** Dans ce domaine, l'acteur français Citalid innove en commercialisant une plateforme d'anticipation des cybermenaces et de quantification des risques reposant sur l'utilisation de la méthodologie FAIR.

Les startups comprennent les enjeux du marché et se positionnent sur les sujets « porteurs ».

Le domaine de la **vie privée** a fait parler de lui ces derniers mois en raison de la multiplication des fuites de données à caractère personnel et des premières sanctions vis-à-vis du RGPD. Les entrepreneurs cybersécurité l'ont bien en tête car c'est aujourd'hui une petite quinzaine de startups qui adressent ce sujet, comme la startup Smart Global Privacy dont la solution smart GDPR optimise la gestion des traitements de données à caractère personnel en automatisant certaines actions et en fournissant des templates préconstruit en fonction des métiers de l'entreprise.

Dans le même temps, le besoin de pouvoir **collaborer de façon sécurisée** est plus présent que jamais. Cependant, les solutions actuelles pâtissent d'un manque de simplicité de déploiement et d'ergonomie d'utilisation. C'est ce qui explique la multitude de solutions qui apparaissent sur le marché, et qui promettent à la fois un niveau de sécurité élevé et une expérience utilisateur acceptable. La messagerie mobile élaborée par la startup Olvid est un parfait alliage entre un modèle de sécurité cryptographique extrêmement robuste et les fonctionnalités standards d'une messagerie. Shadline et Twinlife proposent également des outils collaboratifs sécurisés. Mais il sera dur de se faire une place sur un marché déjà très concurrentiel.

La thématique de **la gestion de crise** fait son apparition sur le radar 2019. La startup Easylience a notamment conçu une solution permettant d'assister les entreprises dans la gestion des crises de grande ampleur.

Avec l'avènement de **la digitalisation des parcours client**, le besoin de pouvoir identifier et authentifier ces derniers sans avoir besoin de les rencontrer physiquement a émergé. Ubble et Serendptech adressent cette problématique, d'ailleurs encadrée

par le règlement européen eIDAS, en distribuant une technologie de vérification d'identité basée sur des algorithmes de reconnaissance vidéo pour les premiers, et une application mobile qui aide à garantir l'authenticité d'un titre d'identité pour les seconds.

Enfin, le domaine de **la sécurité de l'IoT** n'a rien à envier à ceux mentionnés précédemment quand on considère l'avènement des objets connectés, pour les particuliers mais également pour les entreprises. La startup Acklio contribue à sécuriser les objets connectés en rendant compatibles les réseaux LPWAN (réseaux à longue portée et basse consommation comme Lora ou Sigfox) nécessaires au bon fonctionnement de ces objets et le protocole IP. Sa solution permet de comprimer les messages internet et d'ainsi assurer la communication native entre l'objet et les applications métier. La startup Moabi elle se positionne sur l'évaluation de la sécurité des firmwares intégrés dans ces objets, en utilisant notamment les technologies d'exécution symbolique.

En revanche, **la sécurité par déception** est encore trop peu adressée par les startups, bien qu'elle ait fait son apparition avec des startups comme SesameIT et Anozrway qui commencent à implémenter des fonctionnalités de ce type.

IA ET CYBERSÉCURITÉ : COMMENT LA FRANCE SE POSITIONNE ?

L'intelligence artificielle, désignant souvent l'utilisation du ***Machine Learning*** sous toutes ses formes, est un sujet en vogue parmi les start-ups françaises en cybersécurité. En effet, sur les **134 startups** recensées dans notre radar, **70%** déclarent vouloir développer l'usage de la technologie dans les années à venir et **19%** proposent déjà des solutions basées sur l'IA principalement afin d'améliorer leurs performances en matière de **rapidité** et **fiabilité**.

Il est à noter que l'utilisation du *Machine Learning* varie de manière importante d'une thématique du radar à l'autre car son utilisation nécessite certaines conditions réunies plus facilement dans certains thèmes et cas d'usages. En effet, pour entrainer correctement un tel algorithme, il faut des **données** en nombre **suffisant, pertinentes, variées et représentatives** c'est-à-dire à jour et n'introduisant pas de biais. Les secteurs « *Application Security* », « *Endpoint* », « *Industrial Security* » et « *Web Security* » sont particulièrement concernés, même si on peut noter quelques cas d'usages particuliers dans d'autres thèmes du radar tel DPO Consulting utilisant du Machine Learning pour aider à la prise de décisions dans le cas d'une évaluation des risques.

Enfin, même si le *Machine Learning* offre de nouvelles possibilités permettant d'améliorer les capacités des produits, **cette technologie n'est pas une solution miracle**. Il est donc important de bien lire au-delà du discours marketing pour cerner la plus-value d'une telle solution et garder en tête qu'une solution basée du *Machine Learning*, comme n'importe quelle solution, répond à **un cas d'usage précis**. Cette mise en garde nous semble nécessaire même si nous constatons bien souvent **une utilisation pertinente et justifiée de ces technologies par les start-ups françaises en cybersécurité.**

Startups françaises qui utilisent de l'IA dans leur solution de cybersécurité

DES CHALLENGES QUI FREINENT LA PROGRESSION DES STARTUPS

Les échanges réalisés avec les équipes de startups présentes dans le radar permettent d'identifier des challenges concrets qui pour certains sont ambitieux à relever.

Les startups ont du mal à recruter des profils adéquats

A l'instar de l'ensemble du marché, les startups cyber sont confrontées à une pénurie de main d'œuvre spécialisée. Les jeunes diplômés ne sont pas suffisamment formés à la cybersécurité dans les écoles françaises pour alimenter les effectifs ou être à l'initiative de création de startups. Cet état de fait, partagé par l'intégralité du marché en cybersécurité, est encore plus prégnant pour les startups qui ne peuvent pas souvent suivre la course salariale qui s'en suit.

Des fondateurs de startups peu enclins à la prise de risque

66% des fondateurs ont déjà expérimenté une création d'entreprise, mais rarement plusieurs alors que la moyenne d'âge de ces entrepreneurs dépasse les 40 ans. Le profil des fondateurs révèle plutôt des experts que des serial entrepreneurs audacieux. Si on peut saluer la ténacité de certaines startups, il faut souligner la peur de l'échec qui est un problème récurrent en France et qui n'a pas lieu d'être à l'échelle international. Par exemple, un entrepreneur de la Silicon Valley ou israélien ne sera vraiment considéré qu'après plusieurs échecs de création d'entreprise.

Une stratégie marketing carencée...

Les équipes des startups sont davantage composées de profils techniques et spécialisés sécurité que commerciaux. Il en résulte une difficulté des startuppers à rendre leur offre commerciale attirante auprès des prospects. Des efforts sont à faire sur le volet marketing, aussi bien au niveau du produit que du discours. A titre d'exemple, les incubateurs anglo-saxons déploient des programmes d'accélération business élaborés, comme l'incubateur londonien Cylon dédié à la cybersécurité qui forme à « pitcher » efficacement sa startup auprès de potentiels investisseurs, clients et partenaires. Les startups en récoltent les fruits et sont réputées pour leur force commerciale outre-Manche et outre-Atlantique.

...qui se répercute sur les ventes

Les startups françaises ne rencontrent pas de problèmes liés à leur phase de création, mais ont en revanche du mal à faire connaître leurs solutions et à vendre à court et moyen terme. Seul 15% des startups contactées nous a confirmé faire plus de 500 000 euros de chiffre d'affaires. Parmi ces startups, deux tiers ont déjà entre 4 et 7 années d'existence sur le marché de la cybersécurité.

COMMENT CONCRÉTISER CETTE TRANSFORMATION ?

Pour les startups, apprendre à se vendre

Les startups doivent proposer des solutions sur étagère et ainsi atteindre un plus grand nombre de clients avec des coûts optimums. Pour ce faire, il est nécessaire que les fondateurs identifient et valorisent une proposition unique de vente plutôt qu'un segment de marché.

Un axe clé pour eux serait de se positionner sur des problématiques non résolues par les solutions traditionnelles. En effet, les grands groupes sont plus enclins à collaborer avec les startups lorsqu'elles adressent des problèmes pour lesquels aucune solution n'existe sur le marché. La startup Alsid, qui se distingue par son premier rang dans notre classement des levées de fonds, est un bel exemple puisqu'elle traite une problématique pour laquelle aucune solution n'existait auparavant : le monitoring de la sécurité d'Active Directory.

Savoir présenter un pitch clair et attirant se concentrant sur les différentiateurs est un axe d'amélioration clé du développement des start-ups. En effet, c'est une étape cruciale dans la relation avec les investisseurs, les partenaires et les clients afin de les convaincre de la valeur ajoutée de la solution.

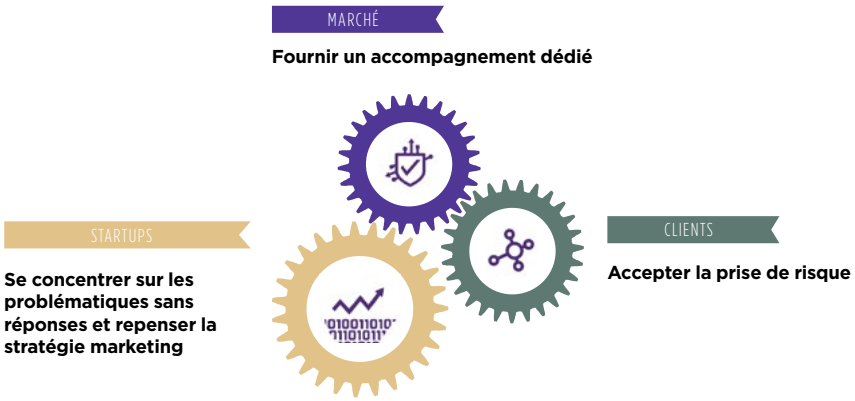
Un autre élément à envisager est de penser au design et à l'expérience utilisateur dès la création de la solution. Dans un marché où ces critères ne sont pas forcément pris en compte par les concurrents, cela peut représenter un vrai atout. Exemple singulier sur le marché, la startup israélienne Cybereason l'a bien compris et a engagé un VP Créative & Head of Design pour imaginer le design de ses produits parallèlement à la construction des fonctionnalités.

Pour finir, les startups ne doivent pas hésiter à réfléchir international dès leur lancement (langue de travail, documentation des codes sources, rédaction des documents produits...) afin de ne pas alourdir inutilement l'effort, déjà conséquent à fournir sur le plan commercial, pour accéder à des marchés plus matures et pouvoir ainsi accélérer le passage à l'échelle.

Pour le marché

Les avantages liés à l'incubation sont nombreux pour les startups (regard extérieur, service à prix réduit, proximité avec d'autres...), mais en même temps la cybersécurité est un domaine avec des besoins spécifiques (confidentialité, expertise scientifique, protection physique...). Ces raisons font que peu de startups en cyber trouvent leur place efficacement dans un incubateur standard. Cela exacerbe le besoin d'un incubateur spécialisé cybersécurité. De plus cet incubateur pourrait devenir un totem de l'innovation cyber « à la française » et un lieu d'accueil des investisseurs et des grands clients. La France réfléchit à se doter d'un hub dédié à la cybersécurité et les premières propositions seront remises à Matignon d'ici la fin du mois de novembre. Il faut espérer que ce lieu proposera

Les axes d'améliorations



réellement un environnement propice au développement des startups, ainsi que des services d'accompagnement qui ne soient pas seulement liés à de l'aide à la recherche.

Enfin, il serait pertinent de favoriser la création de startups par d'anciens membres de la cyberdéfense des Armées ou de l'ANSSI. En effet, leur réseau et leur expertise professionnelle acquis en début de carrière sont des facteurs de succès dans l'écosystème cyber, comme l'ont prouvé les ex-collaborateurs de l'ANSSI et désormais fondateurs des startups Alsid et Citalid.

Pour les clients

Afin de permettre le développement de l'écosystème, les clients doivent accepter la prise de risque. Ils ont pour l'instant des difficultés à faire confiance et à contractualiser rapidement avec de jeunes structures innovantes. Pour un quart des startups interrogées, le temps de signature du contrat après la réalisation du POC est supérieur à 6 mois, et cette observation est particulièrement prégnante chez les grands groupes. Ces derniers peuvent s'inspirer des grandes entreprises israéliennes qui se tournent très vite vers les startups lorsqu'elles identifient des problèmes pour lesquels le marché traditionnel n'offre pas de solutions en acceptant les risques mais en négociant également des tarifs très attractifs pour le futur.

On pourrait également envisager la création d'un accompagnement à la prise de risque de la part de l'Etat afin d'encourager la collaboration des grands groupes avec les startups. En restant sur l'exemple israélien, l'Etat a créé une agence indépendante qui sélectionne des projets innovants pour lesquels à chaque Shekel investi par le secteur privé, l'Etat investit un Shekel sans contrepartie[6].

MOBILISONS-NOUS POUR CONCRÉTISER LA TRANSFORMATION

2019 a montré une vraie embellie dans l'innovation cybersécurité en France. Pour que l'écosystème continue sur sa lancée et concrétise son passage à l'échelle, les axes d'améliorations évoqués se doivent d'être accompagnés par un changement d'état d'esprit de l'écosystème, qui demeure pour l'instant trop fermé. Avec la collaboration des différents acteurs, il n'y a nul doute que la dynamique amorcée se confirmera. Les grands projets entamés à l'échelle de l'état, en particulier le Campus cyber, sont une opportunité unique pour transformer notre écosystème. Mobilisons-nous tous pour que cela devienne une réalité !

Nous pouvons aussi nous réjouir des annonces récentes faites par le gouvernement, sur la création de fond de financement «late stage», qui pourront régler une partie des problèmes rencontrés sur le sujet, en particulier pour garder nos pépites en France ou à minima en Europe. Nous espérons observer l'an prochain les effets de ces annonces sur la croissance des startups et les levées de fonds.

6. *The Israeli Innovation Authority* (2019), "About us", page internet du site officiel de The Isreali Innovation Authority

The Positive Way
WAVESTONE