FIC

Forum International
de la Cybersécurité

2023

PANORAMA
de l'Innovation cyber

organised by Gendarmerie nationale ceis

with the support of Région Hauts-de-France

europe.forum-fic.com

#FIC2023 @FIC_EU

Farah RIGAL

LA PRÉSIDENTE DU JURY DU PRIX DE LA START-UP FIC REVIENT SUR L'ÉDITION 2023 DE CE CONCOURS QUI RÉCOMPENSE L'INNOVATION ET L'ENTREPRENARIAT DANS LA CYBERSÉCURITÉ.

Nous avons un devoir d'exigence envers les start-up

Farah Rigal était cette année la présidente du jury du prix de la start-up FIC 2023. Elle est vice-présidente et cheffe adjointe des services mondiaux de cybersécurité d'Atos. Ingénieure de formation, elle a accumulé les expériences au sein de groupes internationaux passant de la cryptographie, à l'ingénierie logicielle, la gestion des identités, la gouvernance ou encore les techniques de veille, de détection, d'analyse et de remédiation au sein des SOC.

Arrivée en 2014 chez Atos, elle a participé au développement de l'activité cybersécurité de la société qui fait aujourd'hui figure de champion européen.

Que retenez-vous de cette édition 2023 ?

C'était ma première édition dans ce rôle de présidente et j'ai été fortement impressionnée par la qualité, la maturité et la diversité des projets. J'ai aussi été frappée par le nombre de start-up européennes, puisque douze pays différents étaient représentés.

Que vous a apporté cette expérience ?

C'était très enrichissant d'un point de vue personnel. J'ai beaucoup aimé écouter les start-up faire leur pitch, sentir ce vent frais des débuts et se retrouver au centre de ce qui se fait de mieux en termes d'innovation. Mais j'ai eu autant de plaisir à participer aux débats avec les autres membres du jury et à écouter leurs interventions avec toute la connaissance des écueils et l'anticipation dont ils étaient capables. C'était aussi un honneur de faire partie de ce jury dont la composition était variée (investisseurs, prescripteurs, industriels, CTO) et dont tous les membres sont des références dans leur domaine.

Vous étiez-vous fixé un cap ?

Je voulais qu'il y ait un vrai devoir d'exigence vis-à-vis de ces start-up. Nous n'étions pas là simplement pour célébrer l'innovation et leurs atouts. Cela implique de leur faire un retour juste, critique et constructif. C'est le meilleur service que l'on puisse leur rendre.

Qu'est-ce qui distingue les lauréats des autres candidats ?

Toutes les start-up primées, Anozr Way, Astran, Dust Mobile, Onekey et Filigran, ont pour points communs la passion qu'elles ont réussi à communiquer mais combinée à une très bonne connaissance du terrain. Cela nécessite soit d'avoir une équipe qui a de l'expérience, que ce soit le cas du CTO ou encore que les start-up aient pu être accompagnées et conseillées stratégiquement par des gens ayant ces connaissances. Pour résumer, il ne suffit pas d'avoir une bonne idée techno et une bonne idée *business*. Il faut aussi de la maturité. On ne peut pas présenter un simple brouillon au client car ce dernier n'aura pas le temps et les ressources nécessaires pour faire mûrir en accompagnant le projet. Il faut déjà apporter de la satisfaction et de la valeur.

Quelles critiques d'ordre général pourriez-vous adresser aux candidats ?

Certains candidats ont peur de ne pas être suffisamment attractifs aux yeux du jury et ont la tentation de faire valoir une ambition sans mesure.

Or, ce que nous attendons, c'est que le plan de développement qu'ils présentent soit cohérent et réaliste. Nous avions donc davantage d'exigence face aux candidats qui montraient le plus d'ambition. Par exemple, si c'est un projet international qui est visé, il faut avoir été chercher les certifications, s'être renseigné sur la concurrence, etc. Même chose concernant les technologies, il ne suffit pas de prononcer le mot *deep learning* et de promettre un bénéfice miracle pour impressionner le jury. Non seulement, les candidats se doivent d'être transparents sur le fondement scientifique de leur projet, mais en plus il faut qu'ils sachent exactement où intégrer opérationnellement leur brique dans une solution déjà existante.

Comment voyez-vous l'avenir du prix FIC 2023 ?

Je pense que ce prix a beaucoup de potentiel et qu'il pourrait devenir incontournable au niveau européen et même mondial.

CYBERMENACES :
À QUOI FAUT-IL S'ATTENDRE POUR 2023 ?

ATTAQUES PROTÉIFORMES, CIBLAGE DES *SMARTPHONES* ET TENSIONS GÉOPOLITIQUES DEVRAIENT MARQUER LES MOIS À VENIR EN FRANCE ET À L'INTERNATIONAL, D'APRÈS LES ÉDITEURS ET LES EXPERTS EN CYBERSÉCURITÉ.

La menace informatique n'augmente pas mais elle se maintient à un niveau élevé depuis 2021, souligne l'Agence nationale de la sécurité des systèmes d'information dans son dernier rapport. De la vague de *malwares* en Ukraine au rançongiciel ciblant les serveurs ESXi, en passant par le vol du code source du jeu vidéo *League of Legends*, l'année 2023 semble partie pour reproduire la même litanie de cyberattaques qu'en 2022. On peut toutefois distinguer cinq nouvelles tendances à l'œuvre.

1. DES ATTAQUES PROTÉIFORMES

Les rançongiciels arrivent en tête des risques qui terrorisent les entreprises, même si leur nombre a marqué une certaine stabilisation en France en 2022, toujours d'après l'ANSSI. Toutefois, ils ont tendance à se transformer et à se combiner avec d'autres types d'attaques pour renforcer leur impact, rendant leur appréhension plus complexe.

C'est l'un des phénomènes à surveiller pour Atos en 2023. *« Nous voyons émerger des attaques protéiformes. Elles vont, par exemple, commencer par du rançongiciel, puis se transformer en attaque DDos si la victime ne veut pas payer »*, relève Farah RIGAL, la vice-présidente et cheffe adjointe des services mondiaux de cybersécurité d'Atos.

On observe aussi désormais plusieurs niveaux de victimes ciblées. *« Les assaillants peuvent s'adresser dans un premier temps à l'entreprise, et ensuite directement aux victimes utilisatrices si de la donnée personnelle a été exfiltrée »*, remarque Farah Rigal. On connaissait la double extorsion, c'est-à-dire le fait de voler et de chiffrer des données, il va falloir maintenant s'habituer à la triple extorsion qui consiste à demander des rançons à des victimes collatérales.

2. NOS MOBILES DE PLUS EN PLUS CIBLÉS

Ils s'appellent Flubot ou Godfather. Ce sont des *malwares* Android conçus pour prendre le contrôle d'un téléphone à distance, aspirer ses données et se propager parmi les contacts de la victime. Ces Chevaux de Troie n'épargnent pas non plus les iPhone et peuvent être téléchargés malencontreusement par les utilisateurs depuis les magasins d'applications, via des messages texte, les réseaux sociaux et des appels vocaux.

Ils devraient prospérer encore davantage cette année. C'est en tous cas l'une des prédictions de l'éditeur Bitdefender. *« Ils sont très difficiles à contenir et peuvent facilement s'adapter à la situation sociale ou politique actuelle. Un SMS peut prévenir d'une livraison ratée ou inviter à baisser la facture d'électricité ou à voir la photo d'un ami »*, avertit la société dans ses prédictions pour 2023. L'un des derniers logiciels malveillants en date, Hook, est capable de faire des captures d'écran, d'envoyer des messages WhatsApp à votre place et d'intercepter des SMS de confirmation. Redoutable.

3. SE PRÉPARER AUX DEEPFAKES

En janvier 2020, un employé de banque basé aux Émirats arabes unis réalise un transfert de fonds de 35 millions de dollars conformément aux instructions laissées par un directeur d'entreprise dans un message audio. Mais sa voix a en fait été falsifiée par des criminels. On appelle cela un *deepfake*. Comme dans cet exemple, cette méthode consiste à imiter la voix ou même le visage de quelqu'un grâce à de l'intelligence artificielle, dans le but de pénétrer des systèmes informatiques, de dérober des fonds, de nuire à la réputation de quelqu'un ou d'une entité.

Les *deepfakes* ne concernent aujourd'hui les entreprises que de façon marginale car ils sont plutôt sophistiqués à mettre en place. Mais leur efficacité a de quoi inquiéter, d'autant que les progrès technologiques devraient rendre leur usage plus massif à l'avenir, comme le souligne l'Agence de l'Union européenne pour la cybersécurité (ENISA). Le phénomène n'épargne pas la France. C'est la raison pour laquelle les enquêteurs de la gendarmerie sont déjà en état d'alerte. « Les unités sont sensibilisées à cette forme de délinquance.

Le dispositif intégré de lutte contre les cybermenaces de la gendarmerie fort de ses 8 800 cyber gendarmes permet le recueil des plaintes et les investigations sur ce phénomène. *« Les enquêteurs de la division des opérations du ComCyberGend de ses antennes implantées à différents endroits du territoire national sont également en mesure d'appuyer les unités locales saisies de ces faits »*, nous indique le Général de division Marc Boget, commandant de la Gendarmerie dans le cyberspace.

4. LE DÉFI DE LA 5G

Si des services commerciaux 5G sont accessibles au grand public depuis fin 2020 dans notre pays, les opérateurs télécoms s'apprêtent seulement maintenant à déployer un vrai cœur de réseau 5G. Une bascule qui aura des implications en termes de sécurité, comme le fait observer le service NordVpn. *« La technologie a besoin d'une nouvelle infrastructure basée sur le Cloud pour fonctionner, ce qui crée davantage de points d'accès que les pirates peuvent exploiter »*. Ce n'est pas tout. Avec ce vrai cœur de réseau 5G, il va devenir possible de connecter un nombre incalculable d'objets connectés : voitures, usines ou drones. Autant d'appareils qui pourront être ciblés par des attaques. *« L'introduction de la 5G dans l'écosystème numérique signifie que presque tout peut être connecté à Internet. Elle intègre l'internet des objets dans son écosystème, aux côtés des technologies de l'information et des technologies d'exploitation, où le produit lui-même devient un point de vulnérabilité »*, confirme Capgemini pour 2023. Assurer la protection et la sécurité de la 5G sera donc l'un des défis à relever cette année.

5. ANTICIPER LES OFFENSIVES POLITIQUES

Cela fait plus d'un an maintenant que la Russie a attaqué l'Ukraine, doublant son assaut militaire sur le terrain d'une véritable cyberguerre destinée à entraver les capacités de réaction du pays assailli. Pour l'éditeur Kasperky, il faut s'attendre à ce que ce type de cyberattaques à visée politique se développe. Comment y faire face ?

La stratégie adoptée par l'Ukraine permet d'entrevoir quelques pistes. *« Elle a su renforcer ses capacités, que cela soit dans le domaine des télécommunications ou dans le domaine numérique, par des technologies de pointes venant bien souvent du monde civil et apportées par des acteurs non étatiques comme Comsat ou Starlink mais aussi les GAMAM (Google-Apple-Microsoft-Amazon-Microsoft) pour la redondance de l'hébergement de données et de services numériques, ainsi que la puissance de stockage mobile sur les zones de conflit »*, analyse Bertrand Blond, le directeur des systèmes d'information de Cyberdéfense. Miser à la fois sur le monde civil et militaire paraît aujourd'hui clef pour garantir la résilience des systèmes informatiques et des infrastructures critiques.

Une note d'espoir alors que la conjoncture économique complique un peu la tâche des entreprises pour affronter toutes ces menaces. *« Nous sommes dans un marché de l'emploi difficile et nous manquons cruellement d'experts pour gérer et monitorer l'ajout de nouvelles solutions dans nos systèmes d'information. Cela pousse à l'émergence de solutions répondant à ce besoin avec le moins de ressources humaines nécessaires et une prise en main/mise en œuvre rapide »*, prévient Marine Martin, la responsable de l'équipe de réactions aux incidents informatiques d'AG2R La Mondiale.

PANORAMA
de l'Innovation cyber

Les informations présentées dans ce panorama ont été collectées auprès des 81 sociétés candidates à ce prix. Organisé en partenariat avec Atos et avec le soutien d'ECSO, il récompense chaque année les entreprises les plus innovantes dans le domaine de la cybersécurité.

ECS Atos

FIC

BAROMÈTRE
Innovation

LES LAURÉATS 2023

LES GRANDES TENDANCES

65 % de primo-candidats

88 % de hausse de la participation depuis 2019

78 % des postulants ont eu une croissance de plus de 20% en 2022

71 % d'entre elles ont déjà réalisé au moins un tour de table

57 % envisagent de lever des fonds dans les six mois

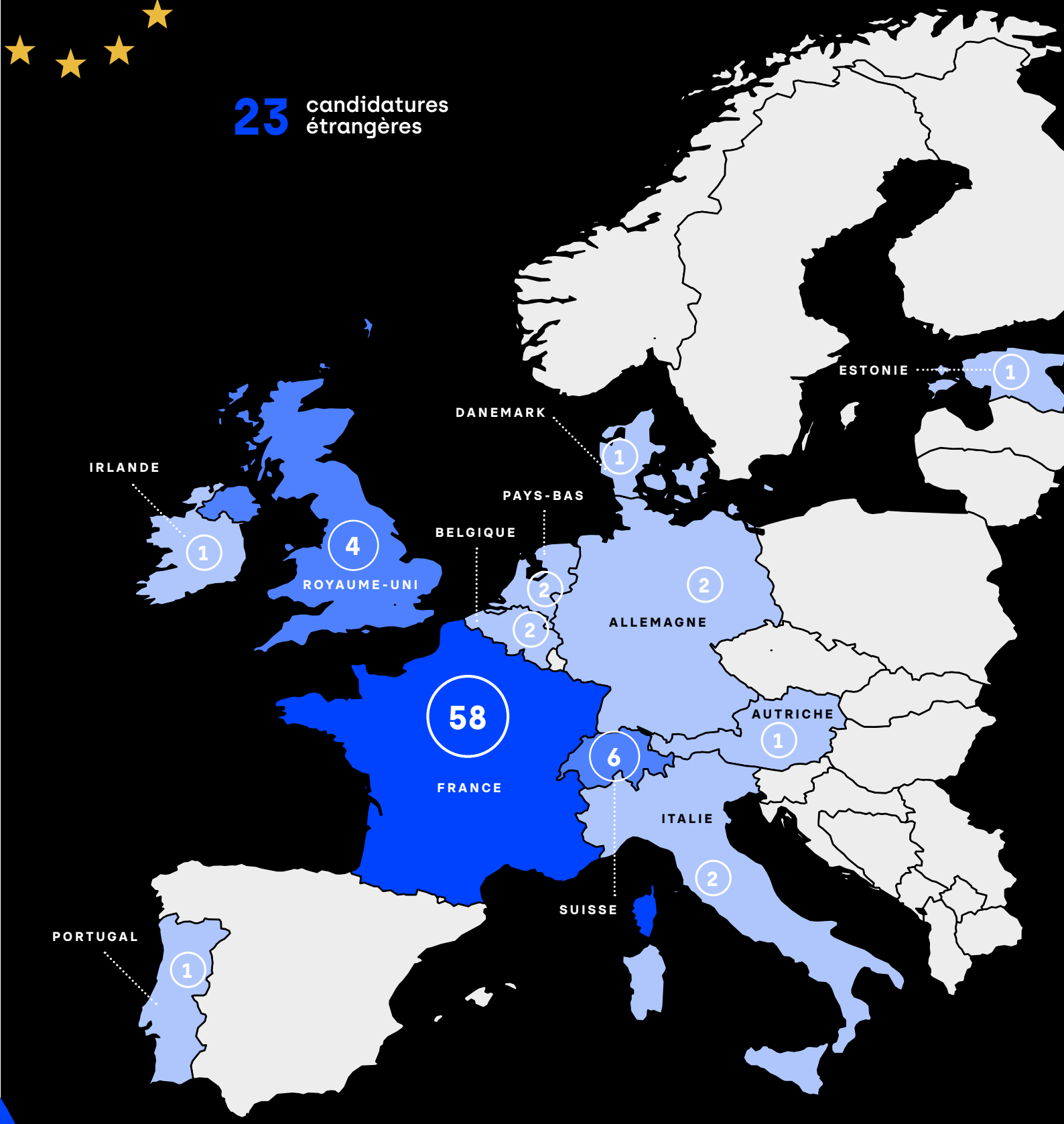
1/4 des entreprises ont entre 5 et 10 salariés

83 % des solutions proposées sont *SaaS/Cloud* compatibles

Un prix européen

12 PAYS DIFFÉRENTS

23 candidatures étrangères



Cette édition a compté 23 candidatures étrangères, soit 28% du total. Elles provenaient de 12 pays différents. C'est la première fois qu'ils sont si nombreux : Irlande, Royaume-Uni, Portugal, Belgique, Pays-Bas, Danemark, Allemagne, Autriche, Italie, Suisse, Estonie et bien sûr, la France qui concentre 72 % des participations.

FIC

BAROMÈTRE Innovation

SEGMENTS DES SOLUTIONS

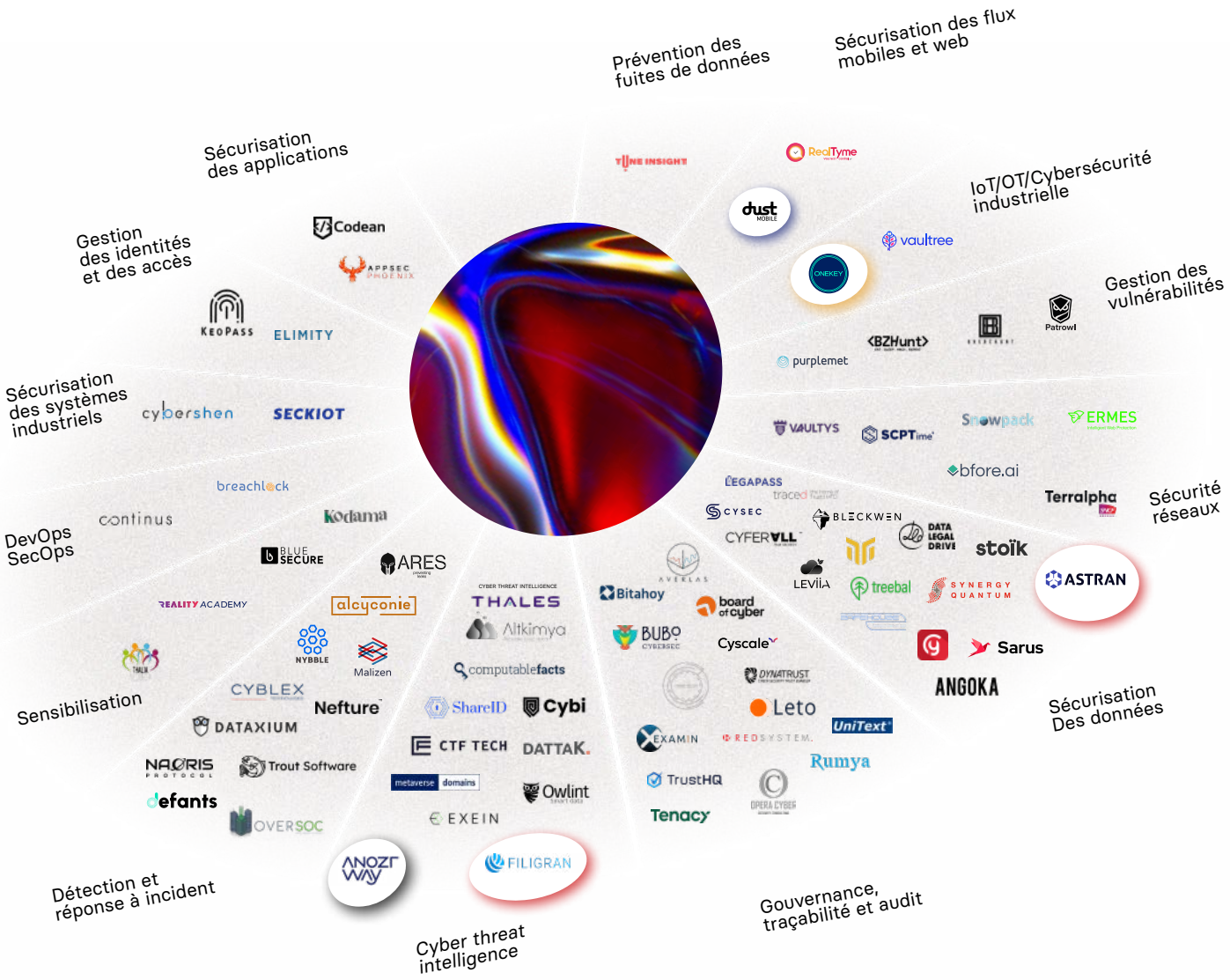
Sécurisation des données **16** (+3)	Détection et réponse à incident **11** (+7)	Sécurité réseaux **6** (NEW)	Sensibilisation **4** (NEW)
Gouvernance, traçabilité et audit **15** (+2)	Cyber Threat Intelligence **12** (+7)	IOT / OT / Sécurisation des systèmes industriels **4** (-9)	Vulnérabilité **4** (NEW)
DevOps / SecOps **2** (NEW)	Sécurisation des flux mobile et web **2** (+1)	Sécurisation des applications **2** (-5)	Gestion des identités et des accès **2** (-1)
Prévention des fuites de données **1** (-7)			

On note une hausse de 7% des solutions de « Détection et réponse à incident » et de « *Cyber Threat Intelligence* », les deux étant liés. Une augmentation qui s'explique probablement par le bénéfice tiré de l'intelligence artificielle pour améliorer la détection des menaces et dont tout le potentiel n'a pas fini d'être exploré.

Mais ce sont toujours les segments « Sécurisation des données » et « Gouvernance, traçabilité et audit » qui sont les plus représentés avec respectivement 16 et 15% du total. La « Sécurisation des données » fournit un vivier historique avec un profil de start-up très technologique qui s'est retrouvé dopé en 2022 par la standardisation des premiers algorithmes de cryptographie. La « Gouvernance, traçabilité et audit » est composée d'entreprises de services venues du conseil et qui valorisent aujourd'hui leur savoir-faire pour gérer et quantifier le risque.

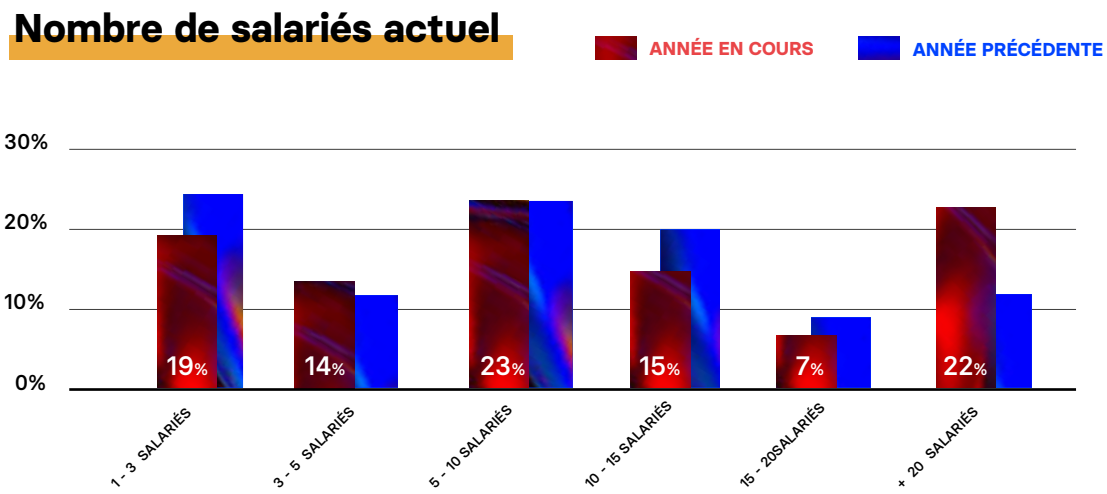
POSITIONNEMENT DES **CANDIDATS PAR SEGMENT**

FIC PRIX Startup · PRIX du Jury · PRIX Coup de cœur · CFI Cybersecurity For Industry



ENTREPRISES

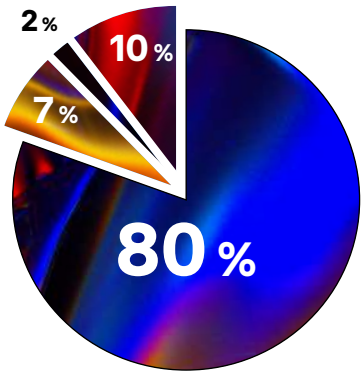
Nombre de salariés actuel



22% DES ENTREPRISES EMPLOIENT PLUS DE 20 SALARIÉS, **UNE AUGMENTATION DE 10 POINTS DE POURCENTAGE PAR RAPPORT À L'ANNÉE PRÉCÉDENTE.**

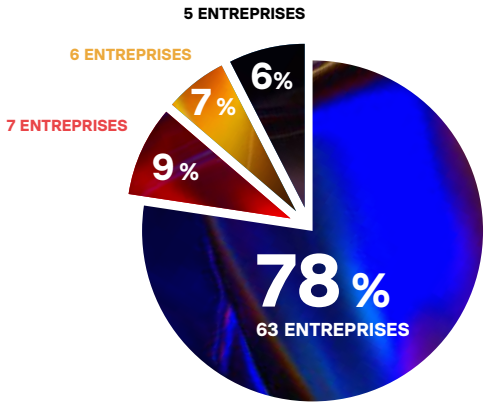
+10

% du CA investi en R&D



- + DE 20 %
- ENTRE 10 % ET 20 %
- ENTRE 5 % ET 10 %
- - DE 5 %

Croissance en 2022



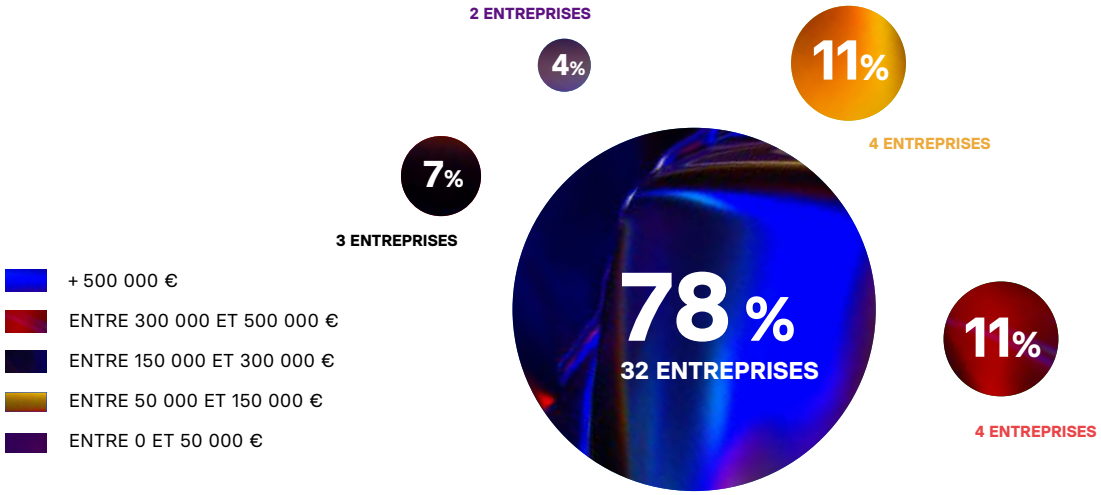
- + DE 20 %
- ENTRE 10 % ET 20 %
- ENTRE 5 % ET 10 %
- - DE 5 %

DES ENTREPRISES EN FORTE CROISSANCE : **78 % ONT EU UNE CROISSANCE DE PLUS DE 20% EN 2022.**

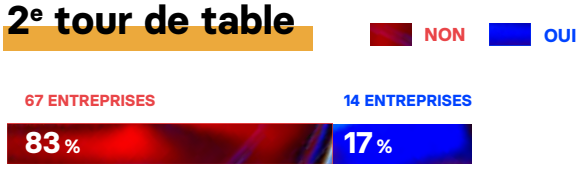
Investir plus de 20% de son chiffre d'affaires dans la recherche et le développement marque la volonté très forte d'innovation de ces sociétés dont la masse salariale est réduite. C'est le même niveau que des géants de la tech.

FINANCEMENT

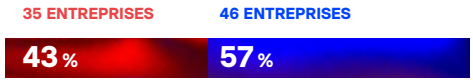
Montant 1er tour de table



2e tour de table



Levée de fonds envisagée dans 6 mois

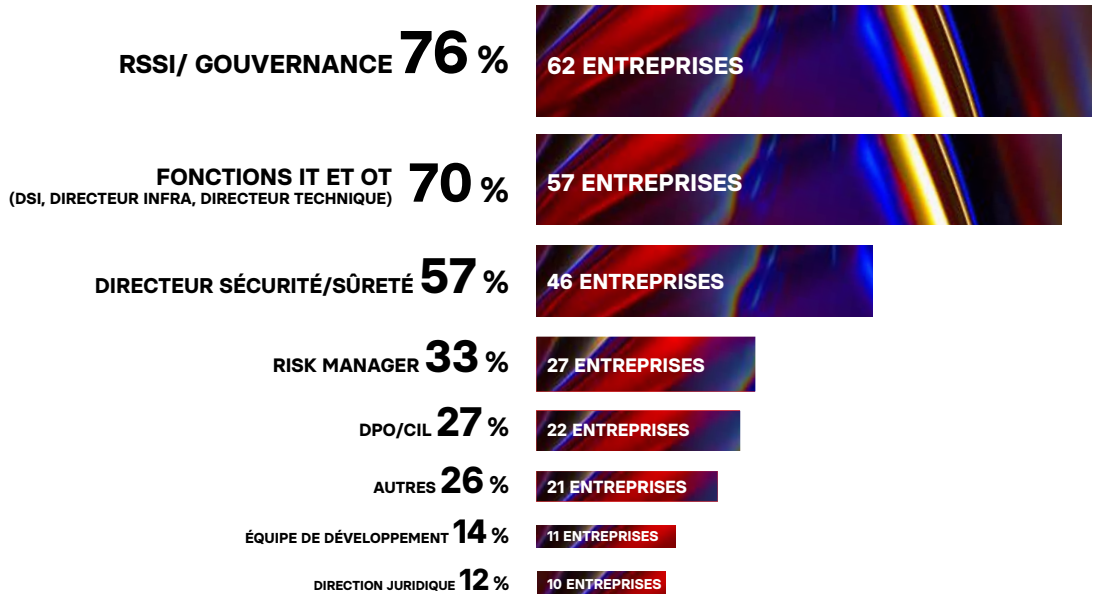


Les entreprises candidates sont majoritairement encore au début de leur aventure avec un seul tour de table réalisé mais à plus de 500 000 € tout de même pour amorcer la première version de leur produit ou service. Cependant, une majorité d'entre elles envisage de lever des fonds pour trouver de nouveaux financements dans les six mois. **Cela confirme la rapidité de leur croissance.**

DÉVELOPPEMENT

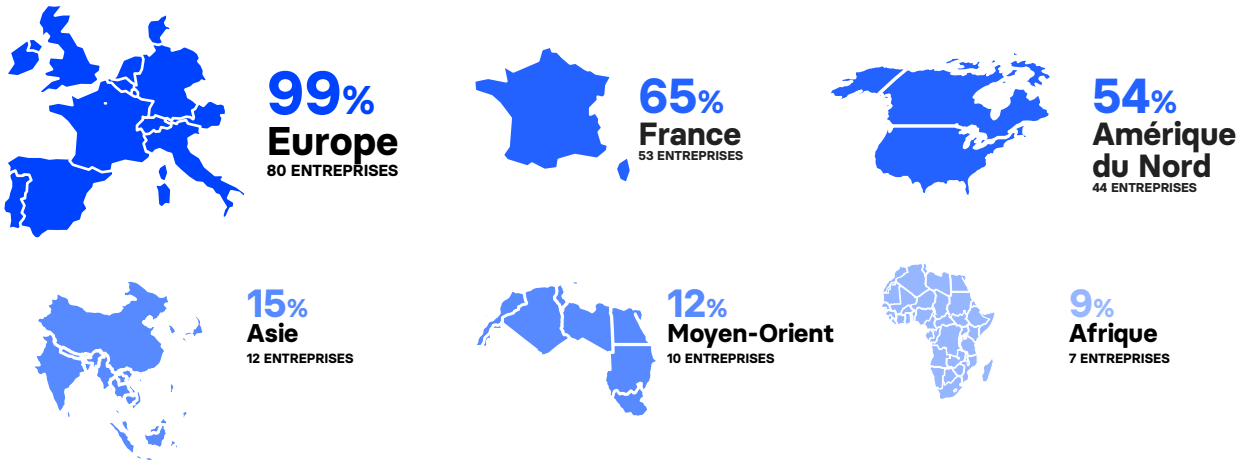
Cibles en termes de fonction*

**Les start-up sondées pouvaient choisir plusieurs cibles*



Priorités business de développement*

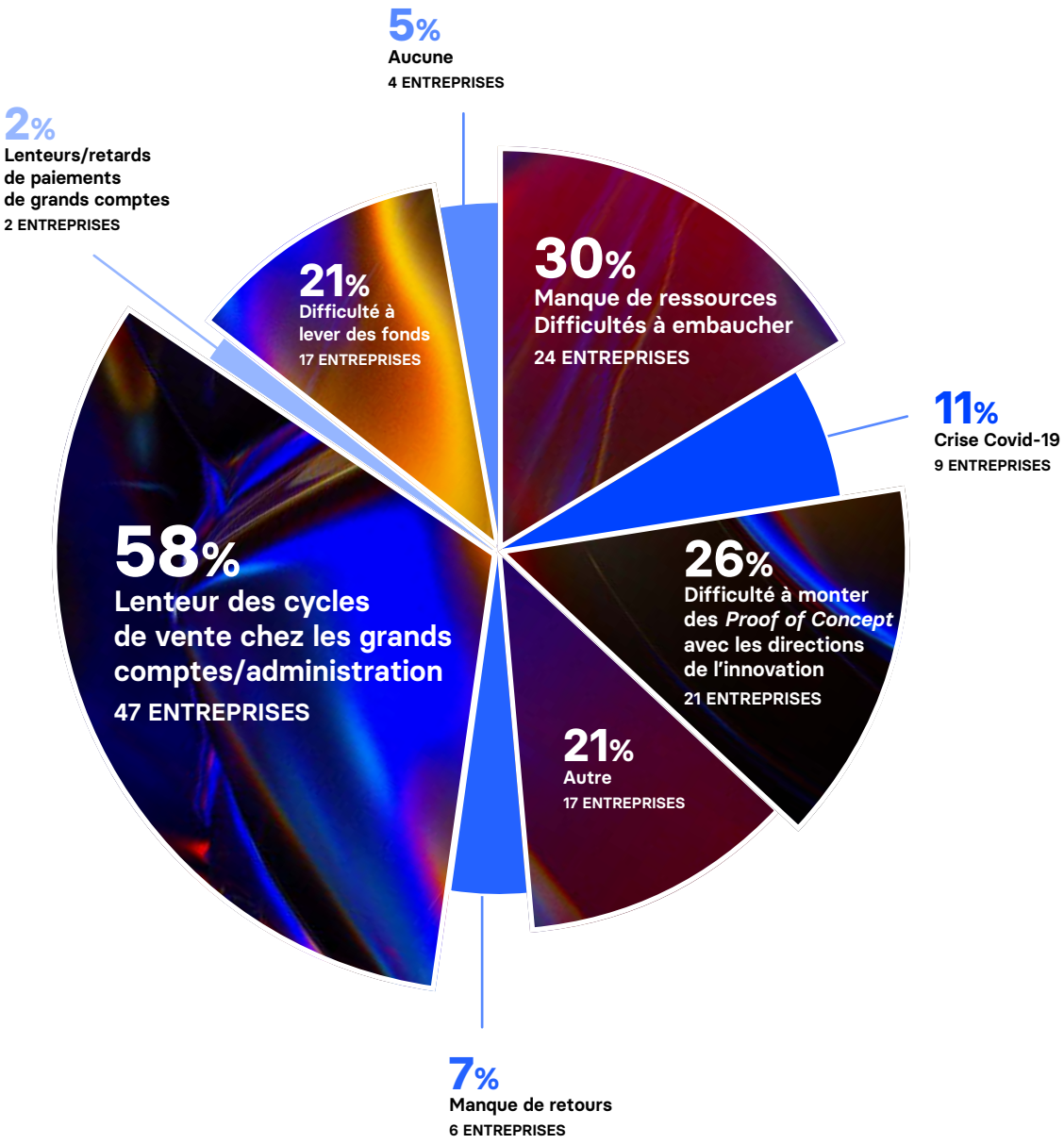
**Les start-up sondées pouvaient choisir plusieurs régions comme axe de développement*



Convaincre les responsables de la sécurité des systèmes d'information est plus que jamais une priorité pour les start-up pour gagner des clients. C'est également le cas, dans une moindre mesure des directeurs techniques, infrastructures et des directeurs des systèmes d'information.

L'Europe et la France restent le périmètre d'action majoritaire, avec des ambitions sur le sol américain bien que ce marché soit très compétitif et difficile à pénétrer. On remarquera que l'Asie ou l'Afrique sont sous-représentés, alors qu'ils sont très dynamiques.

DIFFICULTÉS RENCONTRÉES



L'obstacle au développement le plus cité par les start-up, est la lenteur des cycles de vente chez les grands comptes et administrations. Les start-up essayent de croître rapidement, tandis que les grandes entreprises sont engagées dans des cycles plus longs. Un *Proof of Concept* mobilisant une partie de leurs ressources humaines et financières, cela n'est pas forcément leur priorité.

Cela montre bien que ces jeunes pousses doivent constamment composer avec des clients qui n'ont pas la même temporalité.

QUE SONT-ILS DEVENUS ?

Les réponses de la start-up Datadome
PRIX FIC 2019

DATADOME

1. **SALARIÉS AU MOMENT DU PRIX VS SALARIÉS ACTUELS**
   21 vs. 180

2. **NOMBRE DE LEVÉES DE FONDS SI RÉALISÉES**
   Seed funding en 2017
   Série A en 2018 de 2,5 M d'euros
   Série B en 2021 de 35 M de dollars

3. **ÉVOLUTION DE L'ENTREPRISE EN 2 CHIFFRES-CLÉS**
   DEPUIS SA PARTICIPATION JUSQU'À AUJOURD'HUI
   Plus de 300 clients dans le monde
   Les revenus de l'entreprise ont été **multipliés par 10** depuis le prix.

4. **ÉVOLUTION DE L'ENTREPRISE**
   DEPUIS SA PARTICIPATION JUSQU'À AUJOURD'HUI
   Croissance fulgurante : d'un acteur français à un leader global qui protège les plus grandes marques digitales dans le monde.

5. **APPORT DU PRIX POUR L'ENTREPRISE**
   (VISIBILITÉ, PARTENARIATS/CRÉDIBILITÉ SUR LE MARCHÉ, ETC.)
   Le prix nous a crédibilisé dans le domaine de la cybersécurité et a donné confiance à de grandes marques d'essayer notre solution - et ensuite ils sont convaincus !

Les réponses de la start-up Pradeo
PRIX FIC 2015

pradeo

1. SALARIÉS AU MOMENT DU PRIX VS SALARIÉS ACTUELS

10 salariés au moment du prix / 60 à date

2. NOMBRE DE LEVÉES DE FONDS SI RÉALISÉES

1 en 2012

3. ÉVOLUTION DE L'ENTREPRISE EN 2 CHIFFRES-CLÉS
DEPUIS SA PARTICIPATION JUSQU'À AUJOURD'HUI

1 acquisition

2 filiales (San Francisco et Londres)

4. ÉVOLUTION DE L'ENTREPRISE
DEPUIS SA PARTICIPATION JUSQU'À AUJOURD'HUI

Pradeo est reconnue par les plus grands cabinets d'analystes (Gartner, Frost & Sullivan, IDC) et s'est imposée dans le top 3 mondial dans le domaine de la sécurité mobile en étant la seule entreprise européenne.

5. APPORT DU PRIX POUR L'ENTREPRISE
(VISIBILITÉ, PARTENARIATS/CRÉDIBILITÉ SUR LE MARCHÉ, ETC.)

Reconnaissance des professionnels de la cybersécurité (RSSI, CISO) et Visibilité

FIC PRIX Startup

FIC

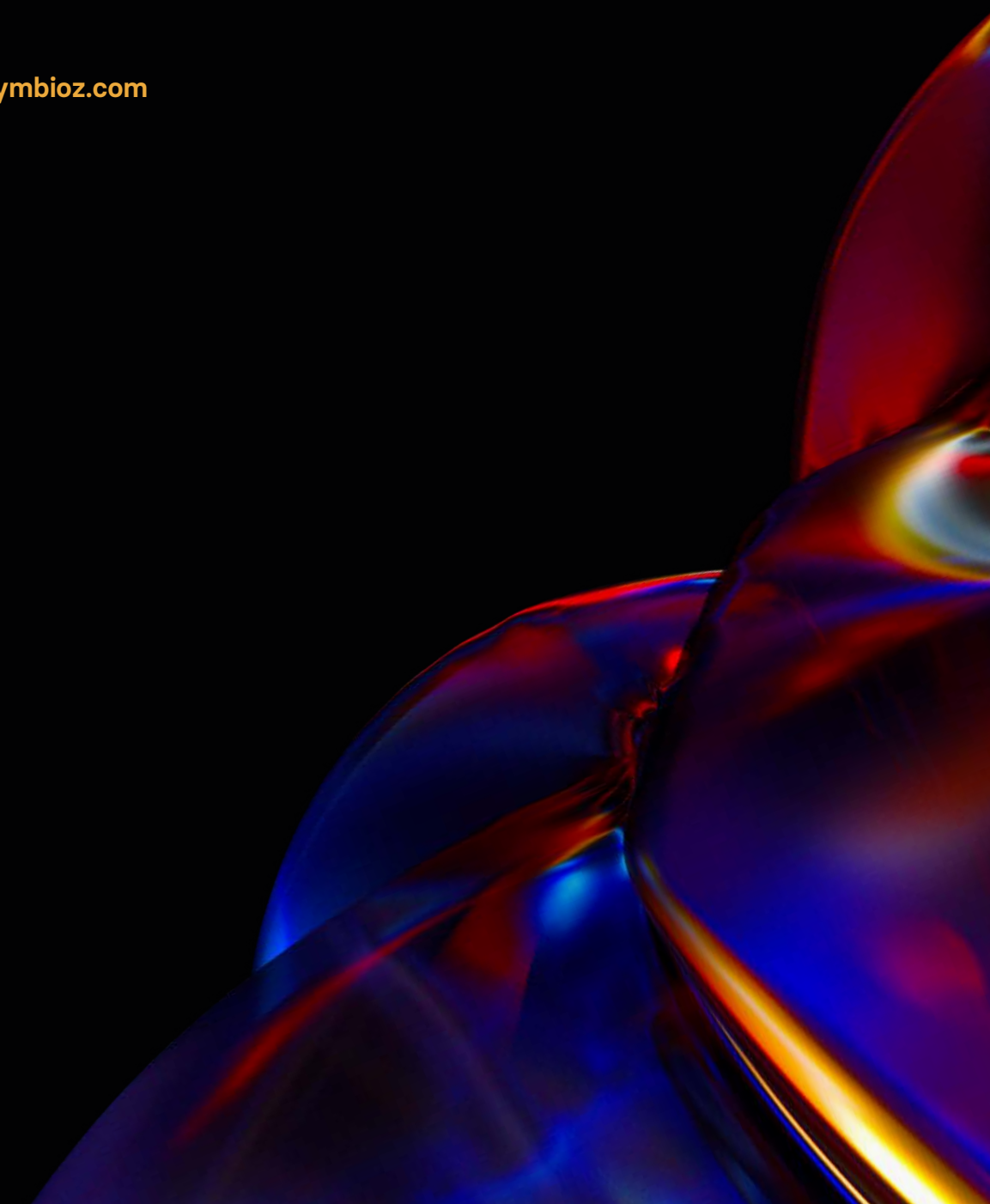
Forum International de la Cybersécurité

organisé par Gendarmerie nationale, ceis

avec le soutien de Région Hauts-de-France

Contact presse

Laëtitia BERCHÉ
laetitia.berche@cymbioz.com



europe.forum-fic.com