IN CYBER FORUM

EUROPE

2024

Panorama de L'INNOVATION

LAURÉATS 2024

Prix de la startup de l'année 2024 : **Snowpack**

Prix de la Recherche : **Idakto**

Prix de l'Impact Opérationnel : **Reversense**

Prix de la Croissance : **Duokey**

Prix Coup de Cœur : **Saporo**

organised by

Forward | ceis

with the support of

Région Hauts-de-France

#INCYBERFORUM

europe.forum-incyber.com

Farah RIGAL

LA PRÉSIDENTE DU JURY DU PRIX DE LA START-UP FORUM INCYBER REVIENT SUR L'ÉDITION 2024 DE CE CONCOURS QUI RÉCOMPENSE L'INNOVATION ET L'ENTREPRENARIAT DANS LA CYBERSÉCURITÉ.

Présidente du jury pour la deuxième année consécutive, Farah Rigal, Vice-President, Deputy Head of Global Cyber Security Services chez Eviden, nous livre son sentiment suite aux délibérations du jury et nous confie l'importance que revêt ce prix pour elle.

Quelle analyse faites-vous de cette édition du prix de la start-up 2024 ?

Si l'on se penche sur les candidatures, cette édition 2024 a résolument été marquée par le *Zero Trust*, qui consiste à accepter le risque et à le contourner par de nouveaux moyens. Les thématiques habituelles telles que la sécurité dans le *Cloud*, la protection de la donnée ou la sécurité industrielle ont bien été représentées, mais ce qui change, c'est le traitement. Par exemple, sur les problématiques d'authentification, les start-up mobilisent la *blockchain* ou la biométrie comportementale pour contrer les nouvelles vulnérabilités.

Et quand il s'agit de sécurité dans le *Cloud*, de nouveaux concepts tels que l'invisibilité apparaissent. L'objectif est alors de masquer les *assets* et de réduire la surface d'attaque, plutôt que de mettre en place des contrôles dont on connaît aujourd'hui le caractère faillible.

Pourquoi est-ce important pour Eviden d'accompagner ces start-ups innovantes ?

Nous faisons partie d'un écosystème. Il est d'un côté important pour nous d'accompagner ces start-up et, de l'autre, il est crucial pour nos clients de pouvoir accéder de bout en bout à un conseil qui intègre des technologies de niche, innovantes et émergentes, en complément des prestations de conseil traditionnelles.

Quel est l'impact du prix sur les lauréats ?

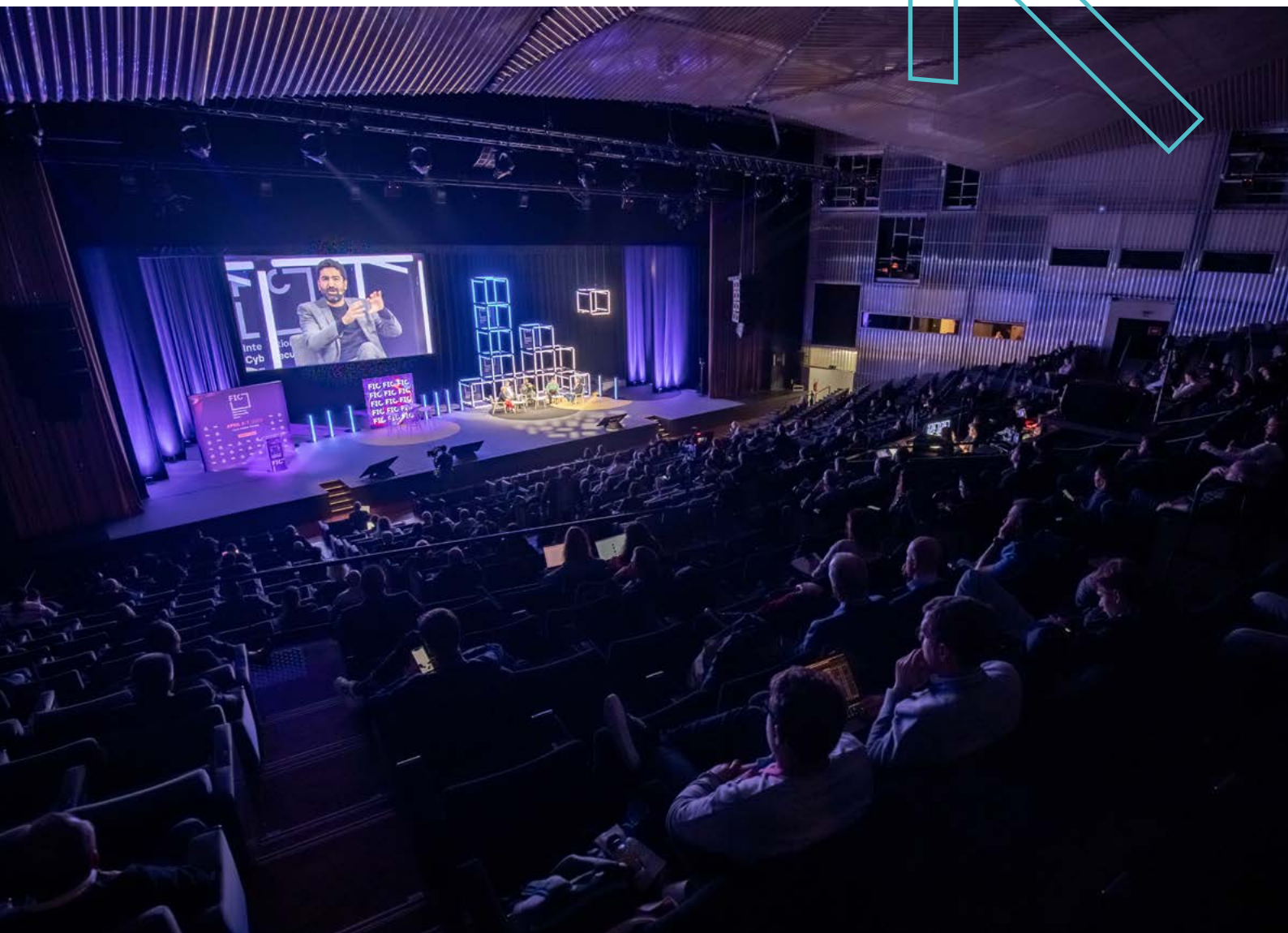
Si je regarde les start-up primées l'année dernière, je constate qu'elles ont toutes connu une formidable progression. Le prix leur apporte de la visibilité et une aide pour conquérir de nouveaux marchés, mais aussi recruter. Être choisi par un jury composé de personnalités très différentes (utilisateurs finaux, institutionnels, investisseurs…) est une validation à la fois de leur proposition de valeur et de leur *business model*. C'est un véritable sceau, une caution quant au sérieux de leur dossier.

Comment avez-vous vécu cette nouvelle expérience de présidente du jury ?

J'ai vécu cette « deuxième fois » avec beaucoup de plaisir et d'intérêt. Comme l'an dernier, une belle dynamique s'est installée avec le jury, remplie d'échanges très instructifs entre pairs. Les complémentarités qui existent entre les membres du jury permettent à chacun d'affiner son propre jugement et de faire maturer ses décisions. Je suis par ailleurs très satisfaite du consensus qui s'est créé autour des lauréats cette année. En résumé, c'est une formidable expérience.

Un mot sur Snowpack, la start-up ayant remporté le grand prix 2024 ?

Snowpack conjugue à la fois l'idée géniale et la simplicité de mise en œuvre. Cette start-up illustre parfaitement les principes du *Zero Trust* avec un réseau de nœuds sur lequel des clients peuvent opérer un certain nombre de nœuds. Plus le réseau augmente et plus la résilience globale s'accroît, ce qui constitue la boucle vertueuse que l'on enseigne dans les écoles comme étant garante de la longévité et de la réussite.



Laurence Thomazeau

Air Liquide

PARTICIPANT POUR LA DEUXIÈME FOIS CONSÉCUTIVE AU JURY DU GRAND PRIX DE LA START-UP, LAURENCE THOMAZEAU, RSSI GROUPE ET DPO D'AIR LIQUIDE, NOUS LIVRE SON RESSENTI SUR LES DOSSIERS ÉTUDIÉS ET SUR CERTAINES START-UP LAURÉATES.

Quelles sont vos impressions après votre deuxième participation au jury du Grand Prix de la start-up ?

J'ai trouvé que les discussions au sein du jury ont été plus fluides que l'an dernier. Je les avais en effet trouvées plus âpres l'année dernière durant les délibérations. Cette année, il y a eu plus de consensus sur les lauréats, ces derniers sont arrivés dans un mouchoir de poche en tête des votes.

Les entreprises qui composent le palmarès de cette édition sont par ailleurs moins concentrées dans un domaine précis que l'année dernière. Les sociétés lauréates viennent en effet d'horizons très diversifiés : défensif, détection, *forensic*, sécurisation de la donnée dans le cloud, analyse de code sur les mobiles...

Quels ont été vos critères de choix ?

En tant que jurée, quand j'ai réalisé ma présélection sur la base des 78 dossiers que j'avais entre les mains, j'ai veillé à ne pas biaiser mes choix par rapport aux métiers de mon entreprise, Air Liquide. J'ai veillé à rester neutre quant à l'appréciation de l'originalité, de la créativité et de l'impact opérationnel des start-up en lice.

Je me souviens par exemple de dossiers qui ne pouvaient avoir aucune application chez Air Liquide, mais qui pouvaient rendre de grands services aux PME / PMI, celles-ci constituant un écosystème potentiellement plus vulnérable que celui des grands groupes.

En tant que RSSI, qu'est-ce qui a orienté vos décisions ?

D'un point de vue strictement métier, j'ai privilégié l'originalité et l'impact opérationnel. Par exemple, j'ai trouvé l'activité de Snowpack (Grand Prix 2024) très intéressante. Snowpack propose une technologie de VIPN (Virtual & Invisible Private Network) qui permet à une entreprise ayant une très grande surface d'exposition sur Internet d'être davantage protégée en rendant « invisibles » ses utilisateurs, équipements et données sur les réseaux.

Quant à Saporo, qui a reçu le Prix « Coup de cœur du jury », j'ai également trouvé sa démarche originale. Saporo aide les entreprises à anticiper la façon dont les attaquants peuvent exploiter les failles liées aux identités. Identifier les chemins les plus exposés à des scénarios d'attaque me semble tout à fait pertinent pour de très nombreuses organisations.

Citons également le Grand Prix de la recherche, décerné à Idakto, qui a déjà déposé un certain nombre de brevets et acquis une forte maturité sur son marché. Idakto facilite l'établissement de relations de confiance entre des fournisseurs de services publics ou privés et leurs utilisateurs. Sa solution, iDCluster, permet aux gouvernements et aux entreprises de proposer une identification conforme au règlement eIDAS.

Cette deuxième participation au jury a été à nouveau une très belle expérience. C'est beaucoup de travail et d'implication. Les questions posées sont très précises, parfois même piquantes, mais toujours dans la bienveillance. Et tout s'est déroulé dans une ambiance très sympathique.

J’ai privilégié l’originalité et l’impact opérationnel des start-up en lice

4 cybermenaces émergentes à surveiller de près

POUR LA TROISIÈME ANNÉE CONSÉCUTIVE, LES INCIDENTS DE CYBERSÉCURITÉ ARRIVENT EN PREMIÈRE PLACE DU BAROMÈTRE DES RISQUES ALLIANZ 2024[1], QUE CE SOIT SUR LE PÉRIMÈTRE FRANÇAIS, EUROPÉEN OU MONDIAL. EN FRANCE, CETTE POLE POSITION A ÉTÉ CHOISIE PAR 44 % DES RÉPONDANTS (SOIT 4 POINTS DE PLUS QUE L'AN DERNIER), DEVANT LES RISQUES D'INTERRUPTION D'ACTIVITÉ (40 %) ET LES CATASTROPHES NATURELLES (25 %).

Dans le même temps, le coût annuel de la cybercriminalité est aujourd'hui estimé à 119 milliards d'euros dans notre pays, alors qu'il n'était « que » de 87 milliards d'euros un an plus tôt et de 4,7 milliards d'euros seulement en 2016, selon les estimations issues des *Technology Market Insights* de Statista[2].

Afin d'illustrer plus précisément ces chiffres, nous avons choisi de rentrer dans le détail des principaux enjeux de cybersécurité auxquels les entreprises sont confrontées au quotidien, à travers quatre cybermenaces qui montent en puissance.

Cyber-extorsion : « toujours plus haut, plus fort »

Quel que soit le levier utilisé (chiffrement des données, divulgation d'informations confidentielles, blocage des accès…), les faits de cyber-extorsion ont augmenté l'an dernier de 46 % dans le monde, selon le rapport de recherche en sécurité d'Orange Cyberdefense, intitulé *Security Navigator 2024*[3].

Face à cette menace, ce sont les grandes entreprises qui paient le plus lourd tribut (40 % des attaques), avec une hausse régulière pour celles dont le nombre de collaborateurs dépasse les 10 000. Cette tendance a été exacerbée par l'acteur malveillant Cl0p, qui a exploité deux vulnérabilités majeures en 2023. Les petites entreprises représentent un quart (25 %) des victimes, suivies de près par les moyennes entreprises (23 %).

Cette progression fulgurante des cyber-extorsions repose notamment sur un vecteur bien précis : les *ransomwares*. Selon le rapport *Cyber Attacks : The Apex of Crime-as-a-Service* de l'agence européenne Europol[4], publié en septembre 2023, « les groupes de ransomware sont restés la menace la plus importante et ont établi une approche claire pour attaquer les entreprises internationales, les organisations publiques, les infrastructures critiques et les services essentiels ».

Intelligence artificielle : les *deep fake* en embuscade

Jusqu'à présent, les progrès récents réalisés dans le domaine de l'IA générative ne représentaient qu'une menace relative. Dans des articles de blog, Microsoft et OpenAI ont récemment communiqué sur le fait que certains acteurs de la menace utilisaient leurs technologies de LLM comme des outils de productivité parmi d'autres. « Nos conclusions montrent que nos modèles n'offrent que des capacités limitées et supplémentaires pour les tâches de cybersécurité malveillantes », a déclaré OpenAI sur son blog[5] en février dernier.

Mais quand les progrès de l'IA servent à monter une arnaque au président de grande envergure (plus de 25 millions de dollars), les directeurs financiers et dirigeants du monde entier se mettent à trembler. La police de Hong Kong a en effet rela-

1 https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2024-Appendix.pdf

2 https://fr.statista.com/infographie/31783/cout-annuel-cybercriminalite-cyberattaques-en-france/

3 https://www.orangecyberdefense.com/fr/insights/security-navigator

4 https://www.europol.europa.eu/cms/sites/default/files/documents/Spotlight%20Report%20-%20Cyber-attacks%20the%20apex%20of%20crime-as-a-service.pdf

5 https://openai.com/blog/disrupting-malicious-uses-of-ai-by-state-affiliated-threat-actors

té en février dernier le cas d'un salarié ayant été dupé par des pirates très expérimentés.

Après avoir reçu un e-mail lui demandant de réaliser des virements pour plus de 25 millions de dollars, le collaborateur – méfiant – a participé à une visioconférence au cours de laquelle son responsable hiérarchique était présent, ainsi que d'autres collègues. Il n'a cependant pas prêté attention au fait que les vidéos – pré-enregistrées – étaient des *deep fake*. Une fois les virements effectués, il s'est aperçu de son erreur, mais il était trop tard.

Les campagnes de désinformation dans le viseur des autorités européennes

Alors que les élections européennes auront lieu en juin prochain et qu'elles seront suivies, quelques semaines plus tard, par l'organisation des JO de Paris 2024, la protection de notre environnement informationnel est plus que jamais d'actualité. Selon Samuel Hassine, CEO et cofondateur de la start-up Filigran (lauréate en 2023 du Prix du Jury InCyber), « l'utilisation massive des campagnes de désinformation à travers le monde souligne la capacité des cyberattaquants à perturber les communications et à créer de la confusion, mettant en lumière les défis croissants en matière de sécurité de l'information ».

Entre 2000 et 2023, la base de données du European Repository of Cyber Incidents (EuRepoC[6]) a recensé 2 506 cyberattaques à caractère politique dans le monde, perpétrées par 679 acteurs ou groupes connus. 11,9 % de ces cyberattaques à dimension politique détectées depuis le début du siècle ont été lancées depuis la Chine. La Russie s'adjuge, elle, 11,6 % des cyberincidents, suivie par l'Iran (5,3 %) et la Corée du Nord (4,7 %). Il faut préciser que 45 % de ces actes malveillants ne sont pas attribués, faute d'identification du pays d'origine.

Rappelons également que la Commission européenne a ouvert fin 2023 des « enquêtes formelles » contre X (ex-Twitter) pour manquement présumé aux règles édictées par le DSA (*Digital Service Act*). La Commission enquête sur des manquements présumés aux obligations de lutte contre les contenus illicites et de désinformation et aux obligations de transparence. Le réseau social, propriété d'Elon Musk, risque une amende pouvant atteindre 6 % de son chiffre d'affaires mondial.

Menace mobile : la confirmation

Enfin, la cybermenace se déroule aussi sur le front des mobiles. L'année 2023 a été marquée par la publication d'une enquête, menée par l'European Investigative Collaborations (regroupement de neuf médias européens), sur le logiciel espion Predator. Celui-ci aurait été déployé dans plus de 25 pays pour espionner des hommes politiques, membres de la société civile, journalistes, activistes et autres universitaires… Cela fait d'ailleurs dire à Agnès Callamard, secrétaire générale d'Amnesty International, que « des produits de surveillance hautement invasifs sont commercialisés à une échelle quasi industrielle et sont libres d'opérer dans l'ombre sans contrôle ni véritable responsabilité ».

L'année 2023 a également vu l'opération « Triangulation » être mise au jour. Au début de l'été 2023, Kaspersky a en effet découvert une attaque ciblant les appareils iOS. Cette campagne a employé une méthode sophistiquée pour distribuer des exploits zéro-clic via iMessage. L'objectif était de prendre le contrôle complet de l'appareil et des données de l'utilisateur. Un millier de téléphones appartenant à des personnalités (des diplomates, par exemple…) et à des salariés de la société Kaspersky, auraient été visés.

Et pour Robin Liso Y Claret, Sales Manager chez Dust (start-up lauréate en 2023 du Prix Coup de cœur du Jury InCyber), l'enjeu se situe aussi du côté des réseaux mobiles : « Les réseaux mobiles, de la 2G à la 5G, nécessitent des mesures de sécurité supplémentaires pour protéger les données des utilisateurs et prévenir les attaques de type interception d'appel, de SMS ou de données, de géolocalisation malveillante et d'usurpation d'identité mobile. Les opérateurs de téléphonie mobile doivent mettre en place des mécanismes de sécurité robustes pour protéger les communications et les données transitant sur le réseau ».

> [En France], le coût annuel de la cybercriminalité est aujourd'hui estimé à 119 milliards d'euros.

6 https://eurepoc.eu/

IN CYBER FORUM

EUROPE

Panorama de L'INNOVATION

Les informations présentées dans ce panorama ont été collectées auprès des 78 entreprises candidates. Organisé en partenariat avec Eviden, ce prix récompense chaque année les sociétés les plus innovantes dans le domaine de la cybersécurité.

PARIS 2024

EVIDEN

SUPPORTEUR OFFICIEL
DES JEUX OLYMPIQUES
ET PARALYMPIQUES DE PARIS 2024

PARIS 2024

Panorama de
L'INNOVATION

LES LAURÉATS 2024

GRAND PRIZE — snowpack

PRIX RECHERCHE — iDAKTO	PRIX CROISSANCE — duokey
PRIX IMPACT OPÉRATIONNEL — </ReverSense>	PRIX COUP DE CŒUR — SAPORO ORDER IN CHAOS

LES GRANDES TENDANCES

80% des candidats proposent une solution *full Cloud* ou hybride

20,5% des entreprises ont déjà déposé un ou des brevets

63% ont eu une croissance de plus de 20% sur l'année 2023

25% des candidats ont déjà contractualisé avec au moins une entreprise du CAC 40

45% des candidats ont déjà fait un tour de table

18,4% de leur CA est réalisé par le secteur public

81,6% de leur CA est réalisé avec le secteur privé

Un prix européen

Provenance

59 françaises

19 candidatures étrangères

comprenant :

8 suisses

4 néerlandaises

2 belges

2 anglaises

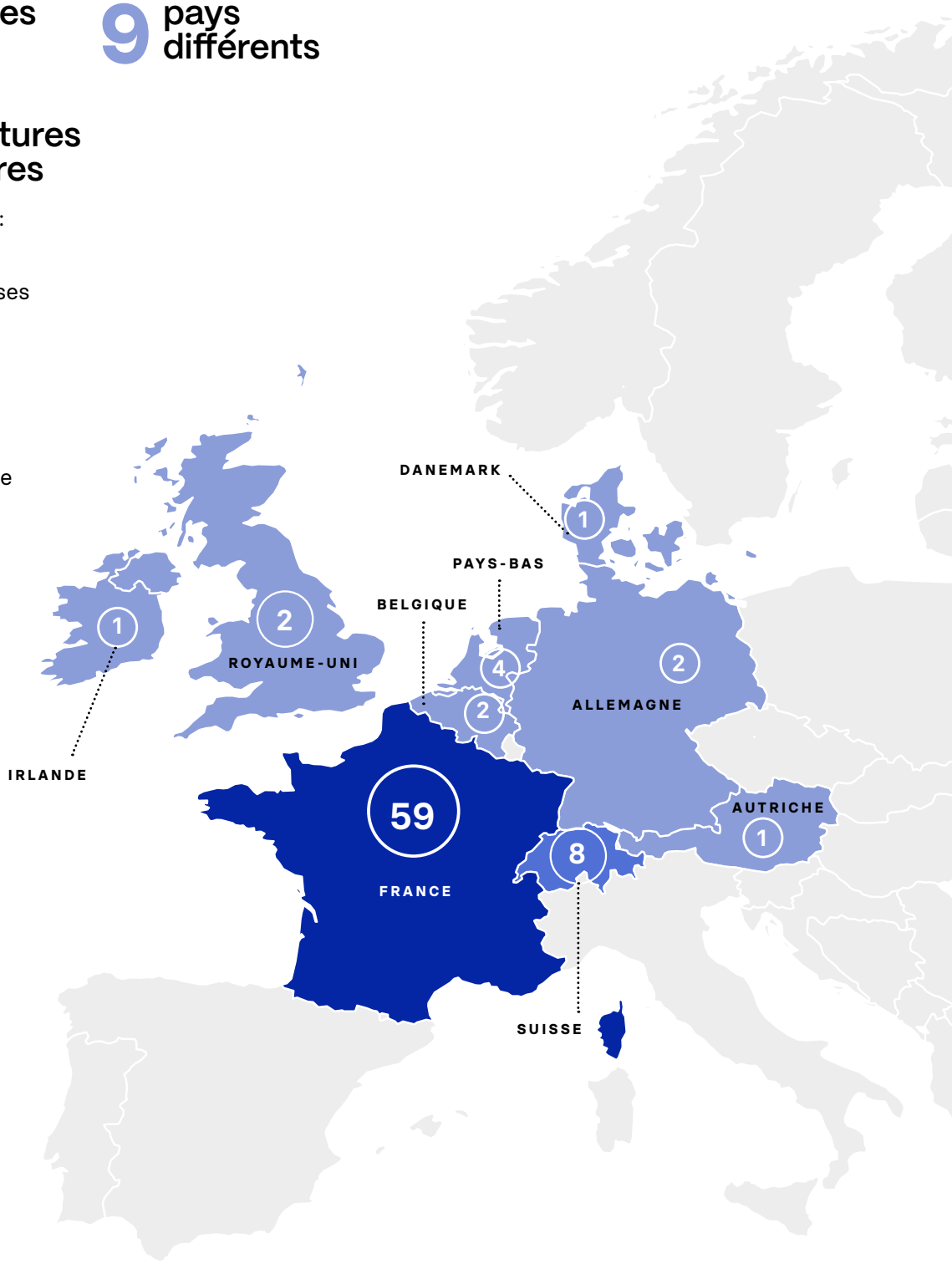
1 danoise

1 irlandaise

1 autrichienne

Répartitions des candidats par pays

9 pays différents



Panorama de
L'INNOVATION

SEGMENTS

Sécurisation des données
13 (-3)

Détection et réponse à incident
11 (+7)

IOT/OT/Cyber-sécurité industrielle
7 (+3)

Sécurisation des applications
5 (+3)

Gouvernance, traçabilité et audit
12 (-3)

Gestion des identités et des accès
9 (+7)

Cyber Threat intelligence
6 (-6)

Sensibilisation
5 (+1)

Prévention des fuites de données
2 (+1)

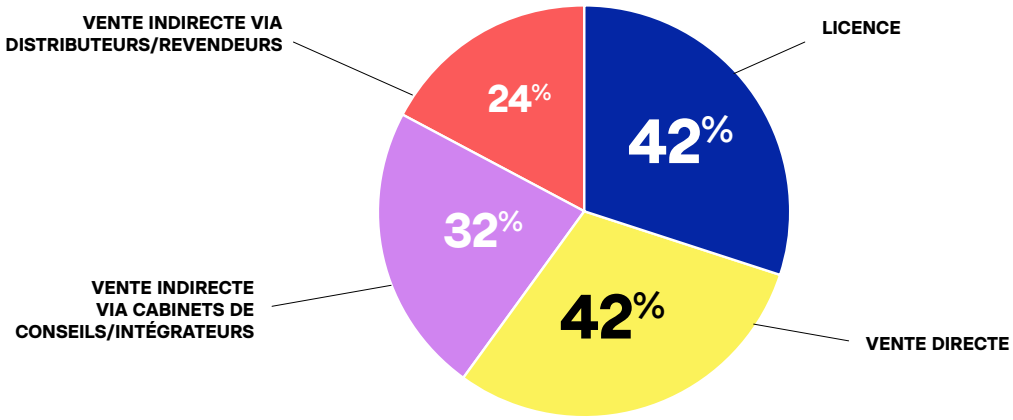
Sécurité réseaux
3 -(3)

Vulnérabilité
5 (+1)

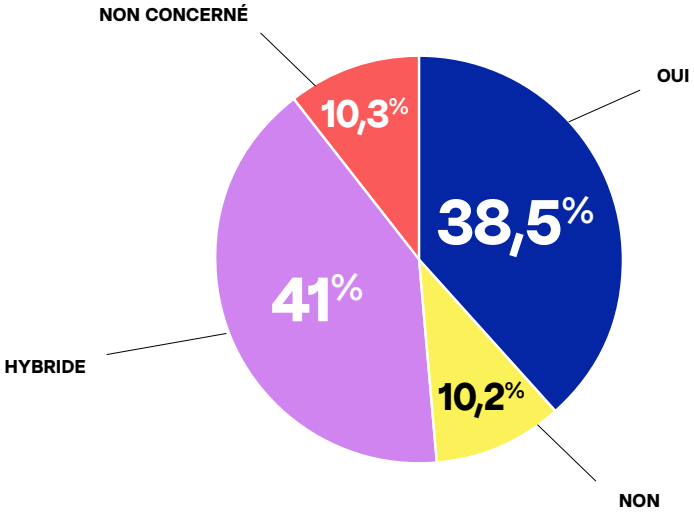
La sécurisation des données (13 solutions) occupe, comme l'an dernier, la première place devant le segment « Gouvernance, traçabilité et audit » (12 solutions), avec respectivement 16,6% et 15,4% des dossiers enregistrés. Ces deux activités sont en recul de 3 candidatures, alors que le segment « Gestion des identités et des accès » enregistre une forte progression, avec 7 solutions de plus. La gestion des identités et des accès (*Identity and Access Management*) reste un des piliers fondamentaux de la gestion de la sécurité des Systèmes d'Information, avec comme enjeu principal la bascule vers le *Cloud* et les apports de l'IA.

Le modèle de vente*

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



Dotation *full-Cloud* des solutions



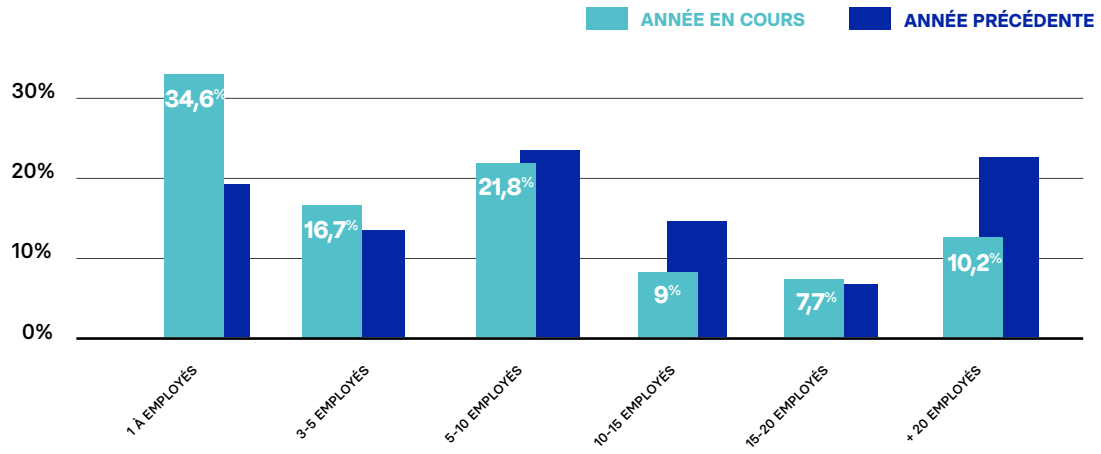
Dépôt de brevet

20,5% des entreprises ont déjà déposé un ou des brevets

41% des répondants privilégient un modèle hybride de dotation de leurs solutions. Le mode *full-Cloud* séduit cependant près d'un éditeur sur 4.

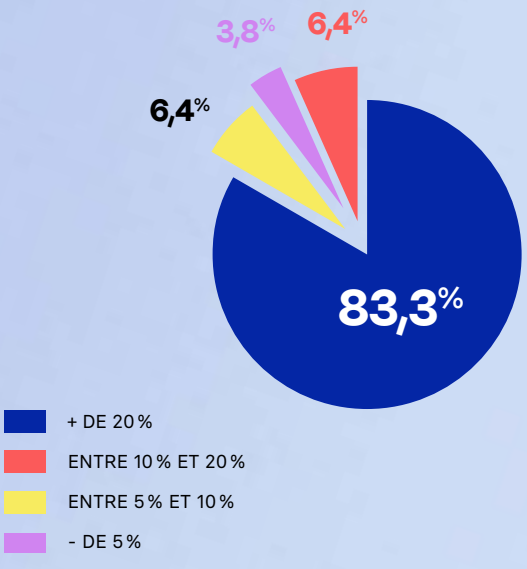
Entreprises

Nombre de salariés actuel

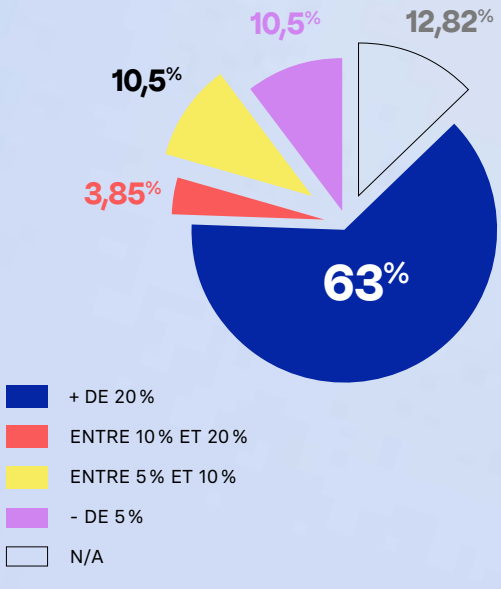


Près des trois quarts des entreprises candidates (73%) emploient moins de 10 salariés. Celles qui dépassent la barre des 20 collaborateurs représentent 10,2% des start-up ayant concouru cette année pour le prix.

% du CA investi en R&D



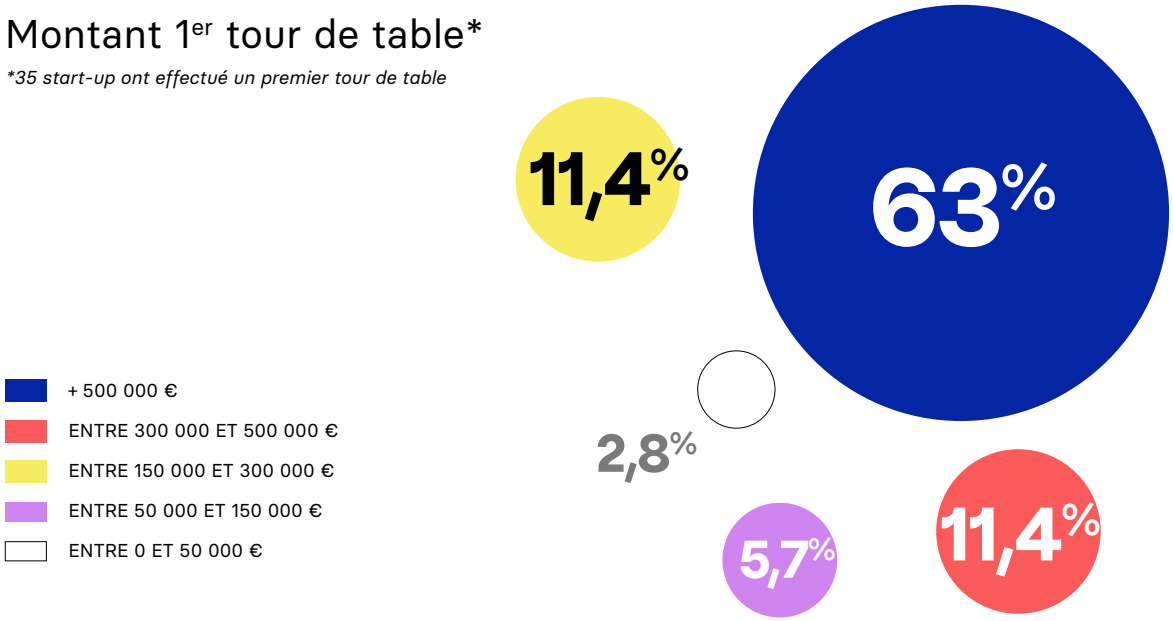
Croissance en 2023



Financements

Montant 1er tour de table*

**35 start-up ont effectué un premier tour de table*



Montant 2e tour de table*

7 start-up ont effectué un second tour de table, toutes à plus de 500 000 euros

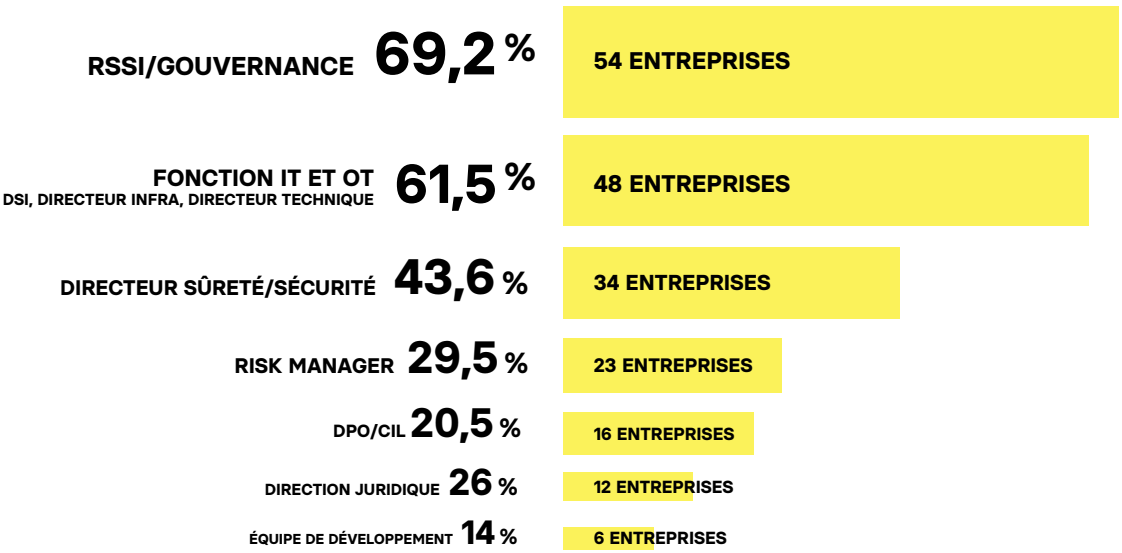
Levée de fond envisagée dans les 6 mois

Presque 45% des entreprises candidates ont réalisé un premier tour de table en 2023. Pour près des deux tiers d'entre elles (63%), le montant levé est supérieur à 500 000 euros. Les 500 000 euros ont également été atteints pour les 7 start-up ayant effectué un second tour de table l'an dernier. La proportion d'entreprises ayant l'intention de lever des fonds dans les 6 prochains mois est beaucoup plus élevée que l'an dernier : 71,8% contre 57%.

Entreprises

Cibles en termes de fonction*

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



Priorités business de développement*

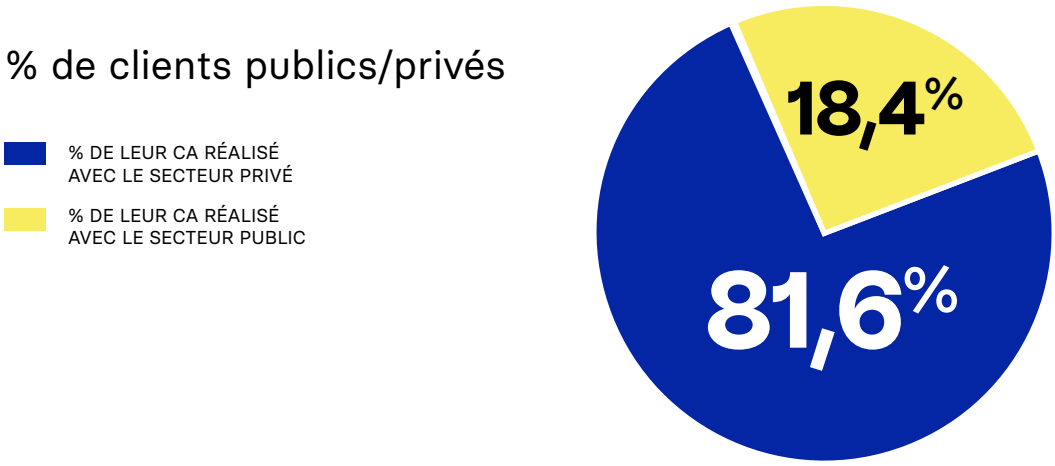
**Les start-up sondées pouvaient choisir plusieurs régions comme axe de développement*

99%
Europe

82%
France

71,8%
Amérique du Nord

% de clients publics/privés



Entreprises ayant contractualisé avec une ou des entreprises du CAC40

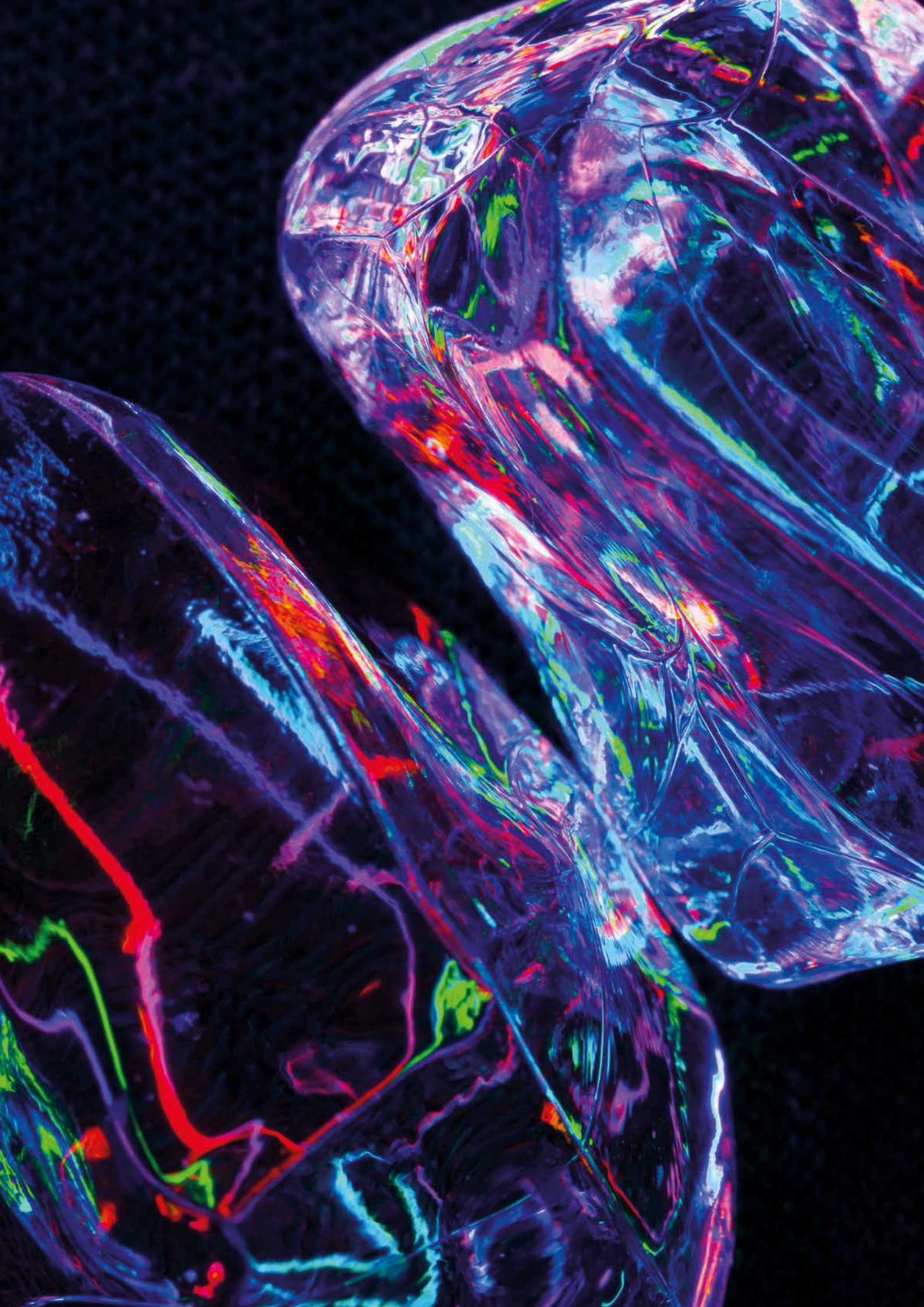
20 ENTREPRISES **58 ENTREPRISES**

17,9% Afrique

16,6% Moyen-Orient

10,2% Asie

2% Amérique du Sud



IN CYBER
NEWS

LE MÉDIA DE LA CONFIANCE NUMÉRIQUE

Retrouvez toute l'actualité cyber sur
incyber.org

IN CYBER FORUM

EUROPE

Contact presse

Laëtitia BERCHÉ
laetitia.berche@cymbioz.com