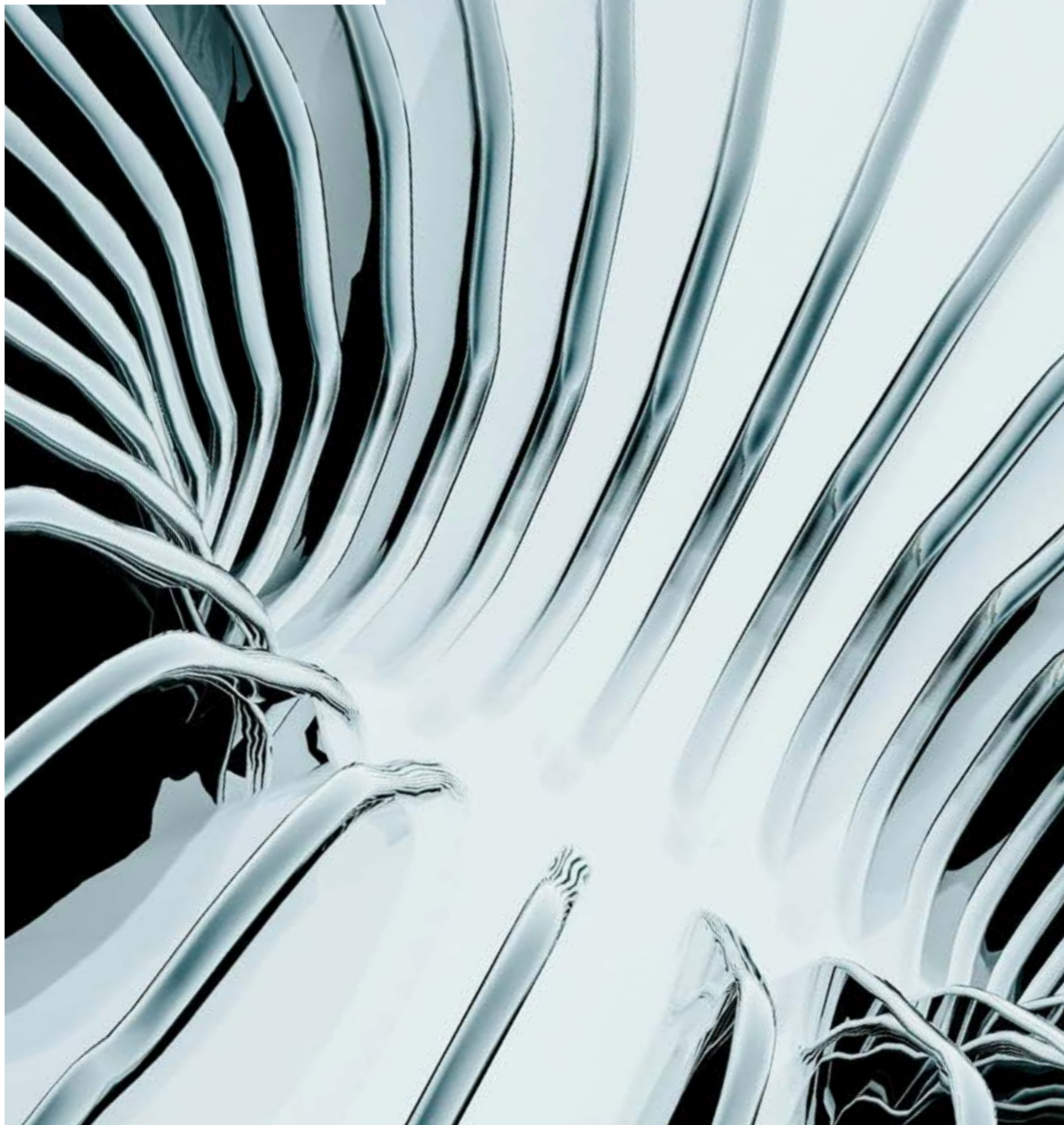


7^E ÉDITION – MARS 2026



TK TIKEHAU
CAPITAL

en partenariat avec

IN CYBER
FORUM

BAROMÈTRE

DE L'INVESTISSEMENT EUROPÉEN EN CYBERSÉCURITÉ

PRÉFACE

de Madame Despina SPANOU



Aujourd'hui, l'Europe et son voisinage font face à des menaces de plus en plus complexes et hybrides, combinant des cyberattaques visant nos infrastructures critiques avec des opérations de déstabilisation et d'influence menées sous le seuil de la conflictualité. Ces menaces prennent des formes multiples : violations de notre espace aérien par des incursions répétées de drones, tentatives de sabotage de câbles sous-marins, campagnes de désinformation ciblant nos concitoyens – souvent amplifiées par le recours massif à l'intelligence artificielle.

Les conflits récents confirment par ailleurs le recours à des activités offensives dans le cyberspace, en amont ou en accompagnement d'opérations militaires conventionnelles. Le cyber est désormais une composante à part entière de la guerre moderne.

Dans le même temps, les entreprises européennes, comme nos concitoyens, sont confrontés quotidiennement à une cybercriminalité devenue endémique. Selon le dernier rapport de l'Agence européenne pour la cybersécurité (ENISA), si les rançongiciels demeurent la cybermenace la plus impactante au sein l'Union, la cybercriminalité est aujourd'hui profondément transformée par l'intelligence artificielle, tant pour l'ingénierie sociale que pour le ciblage des chaînes d'approvisionnement numériques et des systèmes d'IA eux-mêmes¹

Face à ces menaces en constante évolution, l'Europe a un rôle central à jouer, non seulement dans la protection et la résilience de ses infrastructures critiques, mais aussi dans le développement de capacités opérationnelles pour y répondre. Dans une Europe interconnectée, la cybersécurité n'est jamais plus forte que son maillon le plus faible.

Notre vulnérabilité peut aujourd'hui aussi provenir de certaines dépendances au sein de nos chaînes d'approvisionnement des TIC.

L'exposition numérique de nos infrastructures critiques, la robustesse de leurs systèmes d'information et leurs dépendances digitales constituent autant de risques potentiels pour notre sécurité - qu'il s'agisse d'espionnage, d'influence ou encore de pré-positionnement stratégique. Ces dépendances numériques ne doivent en aucun cas devenir des vulnérabilités stratégiques.

Il est dès lors impératif de « dé-risquer » les secteurs devenus critiques pour notre économie et notre sécurité. La proposition de Règlement révisé sur la cybersécurité, présentée par la Commission européenne en janvier 2026, fournit à cet égard un cadre opérationnel permettant d'identifier ces secteurs critiques, les actifs numériques essentiels et les mesures de mitigation appropriées, sur la base de critères objectifs et une évaluation approfondie des risques et des potentielles incidences économiques sur le marché européen. Une fois adopté par les colégislateurs européens, ce cadre contribuera à réduire durablement nos vulnérabilités et à renforcer la résilience de nos infrastructures critiques.

Enfin, la montée en puissance des technologies émergentes dans le cyberspace impose un effort d'investissement résolu à l'échelle européenne dans l'innovation en cybersécurité. Cela implique de mobiliser pleinement le potentiel des technologies de rupture ainsi que les synergies avec le secteur de la défense afin d'améliorer nos capacités d'anticipation et de réponse aux menaces cyber. Le développement d'une industrie européenne de la cybersécurité robuste, dynamique et innovante constitue à cet égard un enjeu stratégique majeur, dont témoigne le Baromètre présenté cette année.

La cybersécurité est à la fois un facteur essentiel de résilience et un levier durable de création de valeur pour l'Europe. Il nous appartient désormais, collectivement - décideurs publics, gouvernements et acteurs industriels - de faire preuve d'ambition et de créativité pour renforcer notre sécurité collective. Deux atouts dont l'Europe, jusqu'à présent, n'a jamais manqué.

Madame Despina SPANOU

Directrice générale adjointe des réseaux de communication, du contenu et des technologies – Commission Européenne

À PROPOS DE TIKEHAU CAPITAL

Tikehau Capital est un groupe mondial de gestion d'actifs alternatifs qui gère 52,8 milliards d'euros d'actifs (au 31 décembre 2025).

Le Groupe a développé un large éventail d'expertises à travers quatre classes d'actifs : le crédit, les actifs réels, le private equity et les capital markets strategies. S'appuyant sur des fonds propres importants (3,1 milliards d'euros au 31 décembre 2025), Tikehau Capital investit son capital aux côtés de ses clients-investisseurs. Le Groupe est guidé par un esprit et un ADN entrepreneurial forts, partagés par ses 717 collaborateurs (au 31 décembre 2025) répartis dans ses 17 bureaux en Europe, en Asie et en Amérique du Nord.

Tikehau Capital est cotée sur le marché réglementé d'Euronext à Paris, Compartiment A
(code ISIN : FR0013230612 ; Ticker : TKO.FP).



Tikehau Capital compte en particulier en portefeuille les participations suivantes
dans les domaines cybersécurité et technologies de confiance :

TRUST IN SOFT

egerle

Quarkslab
Securing every bit of your data

jscrambler

VMRAY

EclecticIQ

<TEHTRIS>

GLIMPS

PROVENRUN

yogosha

build38

CHAPSVISION
DATA MAKE SENSE

trustpair

FTAPI

memory

Ekimetrics.

codrive

claranet

intersec

www.tikehaucapital.com/fr

MÉTHODOLOGIE

Pour réaliser ce baromètre, qui couvre les 10 dernières années de 2015 à 2025, Tikehau Capital a utilisé, croisé et analysé différentes sources d'information et en particulier les suivantes :

crunchbase.com

cbinsights.com/research-unicorn-companies

capitaliq.spglobal.com

returnonsecurity.com

momentumcyber.com

info.mergermarket.com

info.mergermarket.com

pitchbook.com

Sont comptabilisées dans la notion « d'investissement en capital » les opérations de pré-amorçage, d'amorçage et les Series A, B, C, D... (jusqu'à H) ; c'est-à-dire les tours de table *business angel*, *venture capital* et *growth* (mais ni les IPOs, ni les post IPOs, ni les financements en dette ou subvention ne sont inclus).

La définition de « cybersécurité » est assez large et inclut spécifiquement les activités suivantes :

- la sécurité des réseaux, du *cloud*, des postes de travail, des mobiles et des infrastructures
- la détection des menaces, des intrusions et des fraudes
- le management des accès, des identités et des risques cyber
- les tests de pénétration
- le filtrage de la messagerie et du web

Les zones géographiques couvertes par ce baromètre sont les Etats-Unis, Israël et l'Europe. La région « Europe » inclut les pays suivants : Allemagne, Autriche, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Norvège, Pays-Bas, Pologne, Portugal, République Tchèque, Roumanie, Royaume-Uni, Slovaquie, Slovénie, Suède et Suisse (soit les 27 membres de l'Union européenne plus le Royaume-Uni, la Norvège et la Suisse). Les chiffres historiques en montant ont été ramenés à une référence annuelle en Euros calculée sur la base du taux de change moyen constaté sur chacune des années concernées.

Étant essentiellement basé sur des informations communiquées publiquement par les sociétés qui ont réalisé des levées de fonds, ce baromètre ne prétend ni être exhaustif, ni avoir une précision exacte. Il n'engage en aucun cas la responsabilité de Tikehau Capital ou de l'un de ses affiliés. Si vous relevez des erreurs ou des omissions et si vous souhaitez proposer des améliorations pour les prochaines éditions, merci d'écrire à contact@tikehaucapital.com

Il est possible de reprendre ou de citer librement les analyses et les perspectives de ce baromètre à la condition de mentionner la source de ces informations avec le texte suivant :

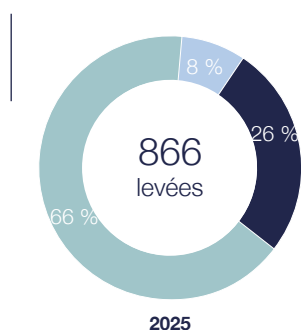
« Source : Tikehau Capital – Baromètre Tikehau Capital de l'investissement européen en cybersécurité – 7^e édition 2026 »

ÉTATS-UNIS, EUROPE & ISRAËL

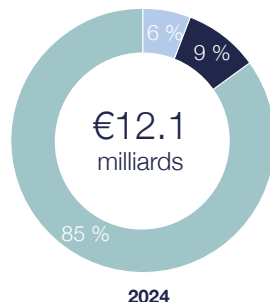
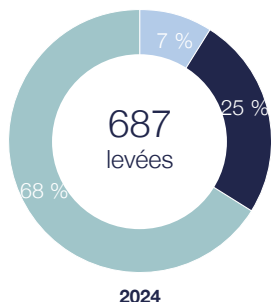
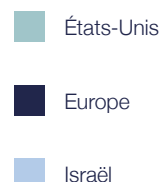
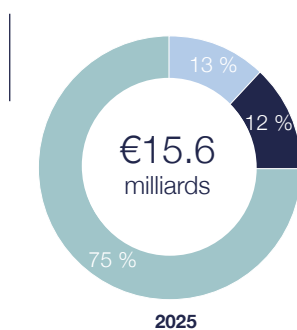
BILAN 2025

En 2025, les start-ups spécialisées en cybersécurité ont levé un total de 15.6 milliards d'euros, répartis sur 866 transactions. Comme les années précédentes, les États-Unis dominent à la fois en volume et en montant total levé. L'Europe maintient sa contribution en nombre d'opérations par rapport à 2024 et renforce sa part en montants levés, reflet d'un marché davantage orienté vers des tours avancés.

Nombre de levées cyber



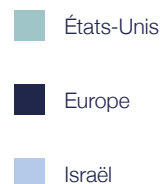
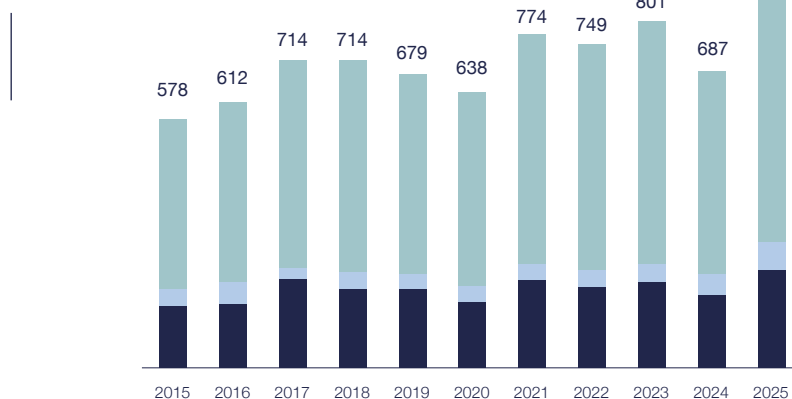
Montants levés cyber



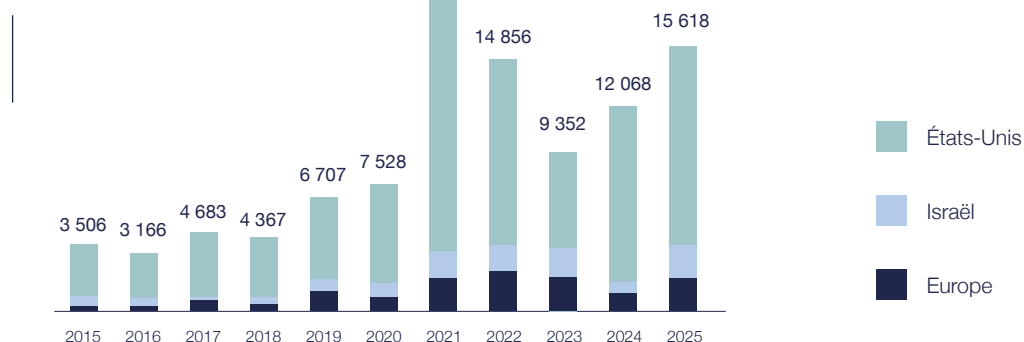
TENDANCES 2015 - 2025

Par rapport à 2024, le nombre de levées a progressé de 27 % et les montants totaux ont augmenté de 32 %, confirmant un rebond global et des besoins de financement en hausse. Sur la décennie, le nombre de transactions a crû de 50 % et les capitaux levés ont été multipliés par 4,5.

Nombre de levées

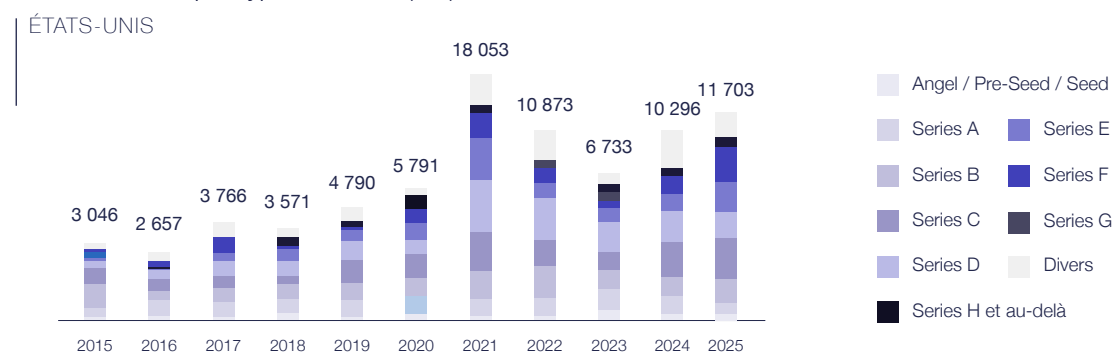


Montants levés (M€)



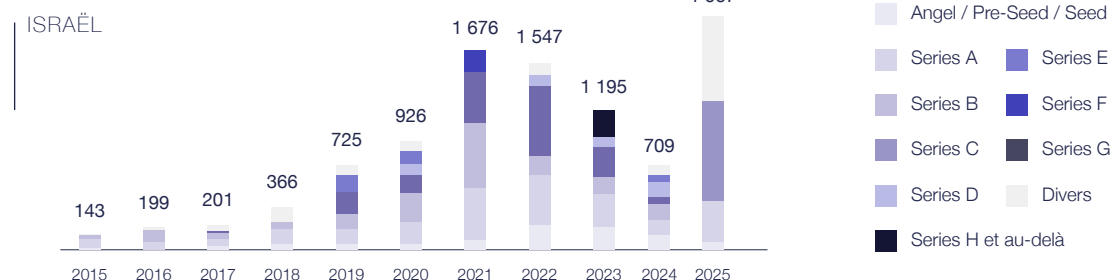
En 2025, le montant levé par les entreprises américaines de cybersécurité a été principalement porté par des tours de levées de Serie C, D et E (46 % du montant total levé). La croissance des montants atteint 14 % sur un an, portée par des tours significatifs réalisés par des scaleups, témoignant de la préférence pour des modèles éprouvés et la concentration des capitaux sur le *laterstage*.

Montants levés par type de series (M€)



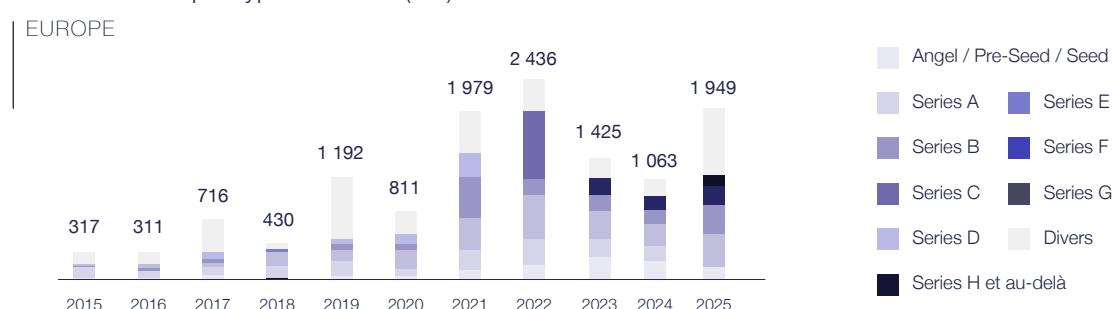
Le marché israélien enregistre un rattrapage marqué après la contraction de 2024 (et de 2023). Plusieurs opérations de grande taille, notamment chez Cato Networks et EON, totalisant 659 M\$ (environ un tiers du total 2025), ont porté la dynamique, entraînant une hausse de 178 % des montants par rapport à 2024.

Montants levés par type de series (M€)



En 2025, les entreprises européennes de cybersécurité ont principalement financé leurs activités à travers des tours de table de maturité supérieur aux années précédentes (supérieur à des Serie C). Comme en 2024, l'année 2025 est marquée par des montants conséquents levés en Serie F et plus (5 % en 2025). Au global nous constatons une croissance des montants levés de 83 % comparé à 2024.

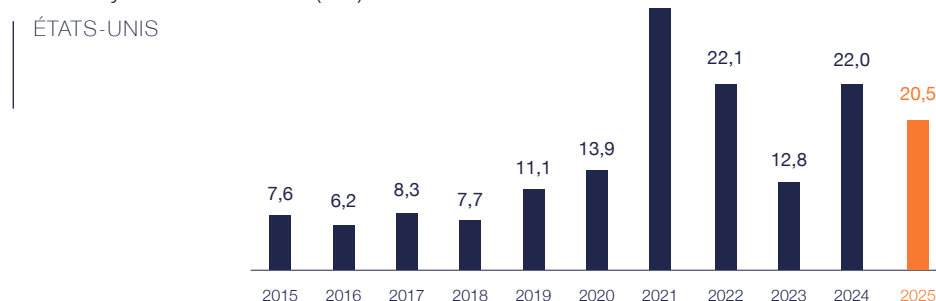
Montants levés par type de series (M€)



TAILLE MOYENNE DES LEVÉES 2015 - 2025

L'année 2025 se caractérise par une stagnation des montants moyens levés aux États-Unis. En revanche, c'est l'inverse pour l'Europe et Israël avec des hausses respectives de 38 % et 101 %. En 2024, nous avons constaté une tendance inverse avec une stagnation en Europe et en Israël.

Taille moyenne des levées (M€)



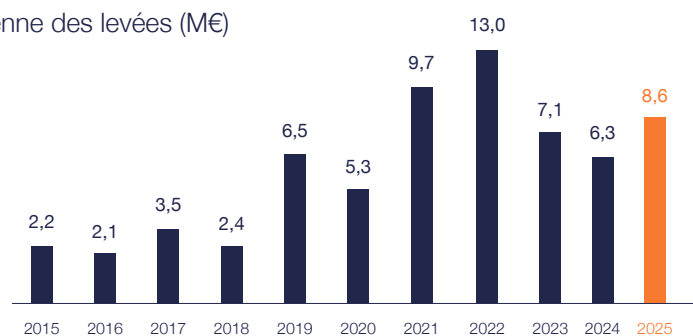
Taille moyenne des levées (M€)

ISRAËL



Taille moyenne des levées (M€)

EUROPE

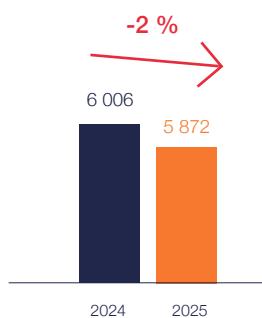


EUROPE

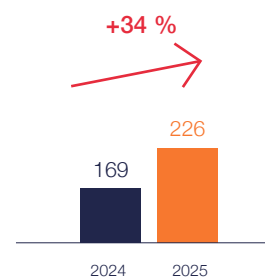
TENDANCES 2025 VS. 2024

Toutes industries confondues, le nombre de levées en Europe recule légèrement en 2025 (-2 %, après -20 % en 2024). La cybersécurité s'inscrit à contre-courant avec une hausse de 34 % du nombre d'opérations. Corrélativement, les montants cumulés toutes industries diminuent de 5 %, tandis que les montants levés en cybersécurité progressent de 83 %, confirmant l'attractivité du segment.

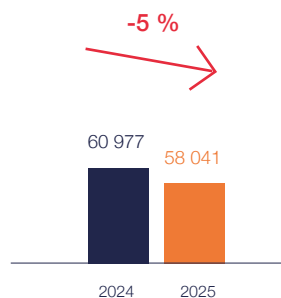
Nombre de levées
tous secteurs



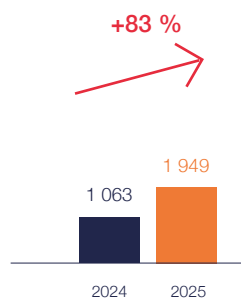
Nombre de levées
cybersécurité



Montants levés (M€)
tous secteurs



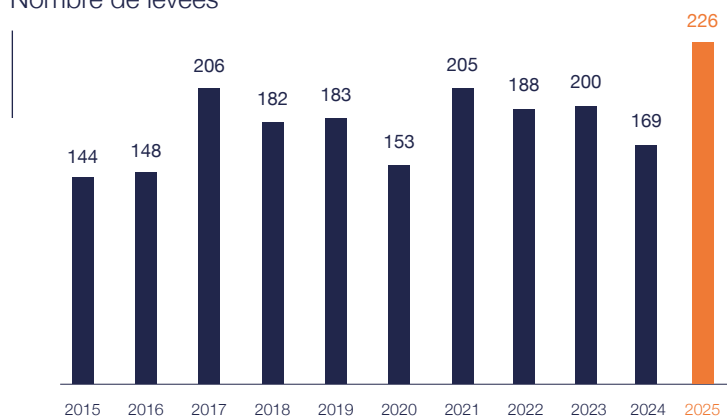
Montants levés (M€)
cybersécurité



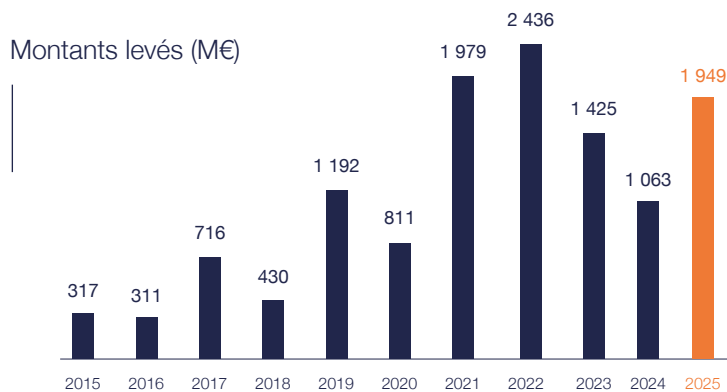
TENDANCES 2015 - 2025

Sur dix ans, le marché européen de la cybersécurité s'est nettement structuré : le nombre de transactions a été multiplié par 1,6 et les montants levés par 6,2. Cette progression reflète la montée en maturité des acteurs et l'approfondissement de la base d'investisseurs.

Nombre de levées



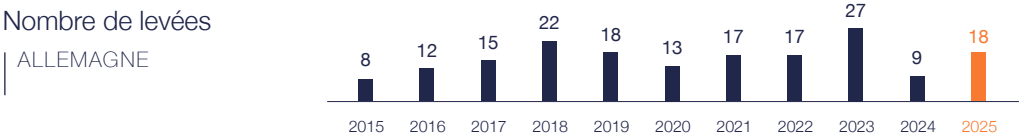
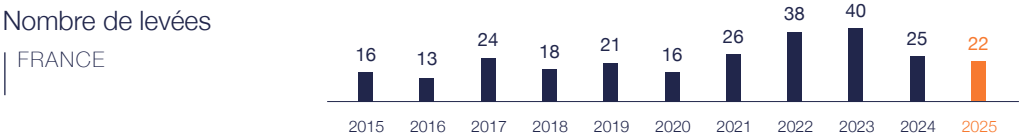
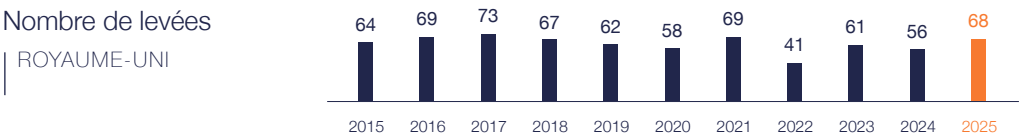
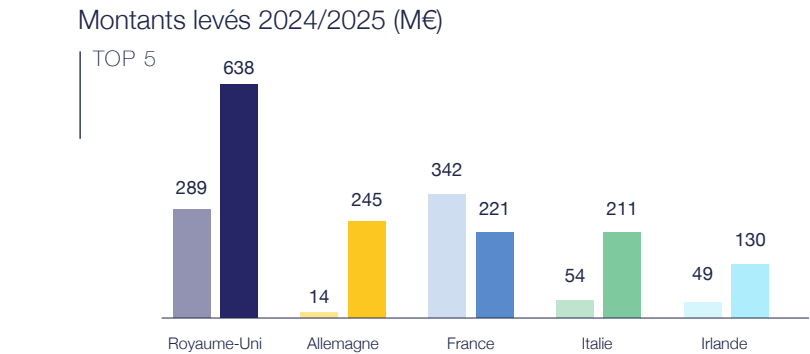
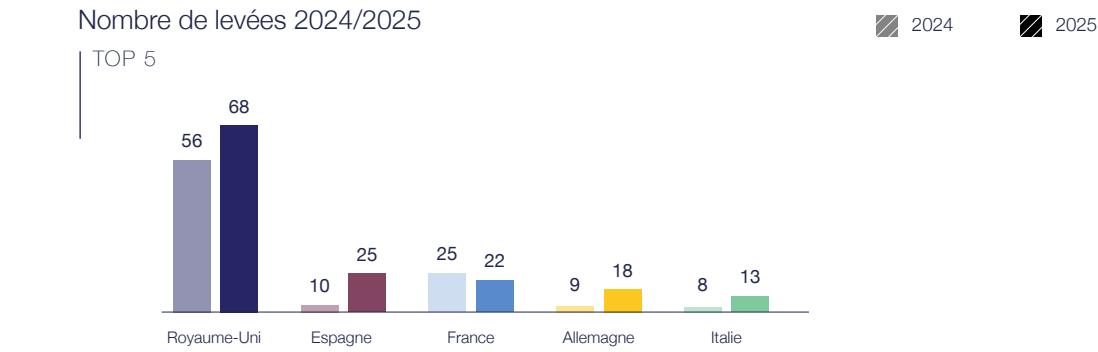
Montants levés (M€)



FOCUS 2025

La France s'affirme comme un acteur majeur du financement de la cybersécurité en Europe, se classant troisième en montants levés et en nombre d'opérations.

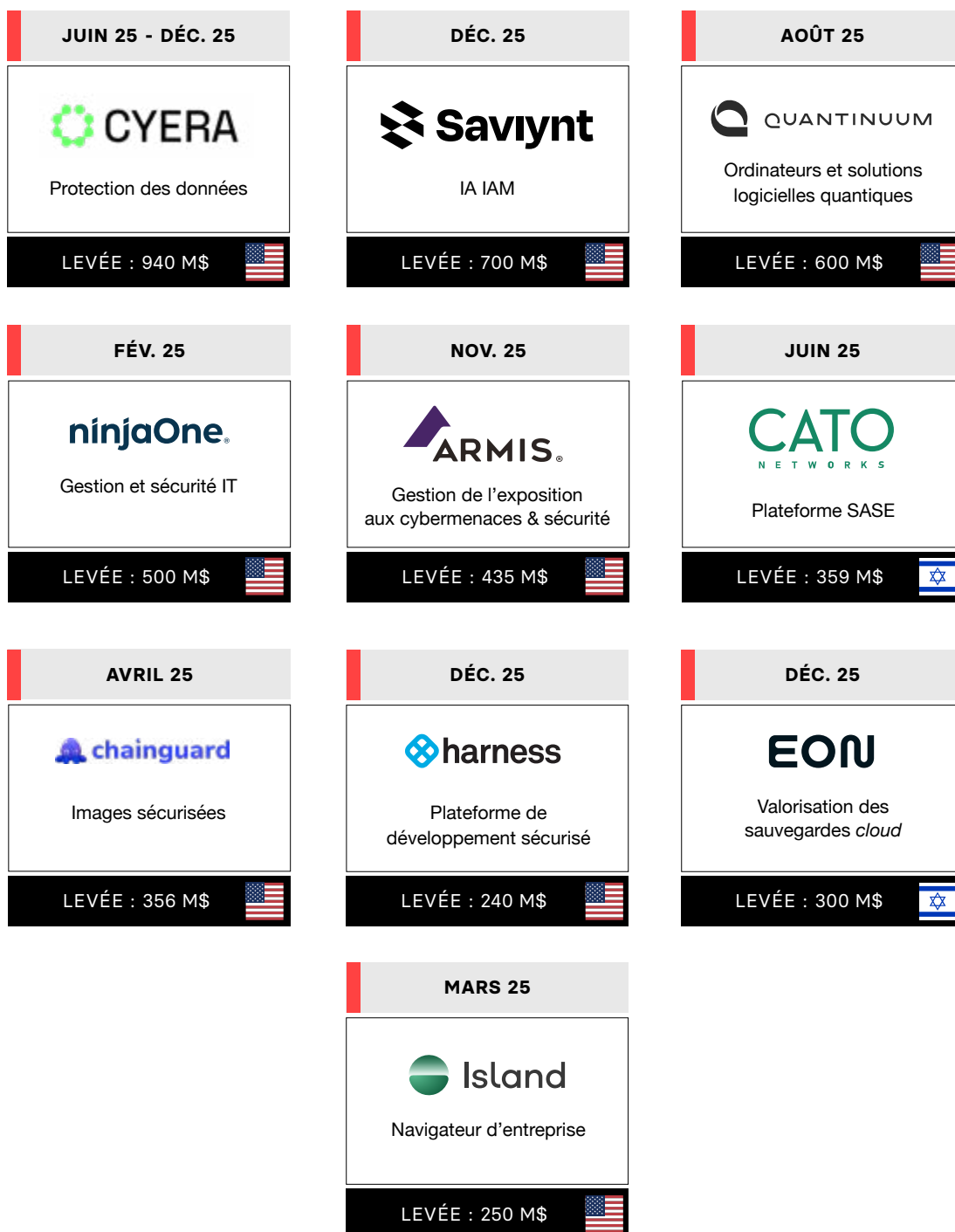
Le Royaume-Uni continue de dominer le marché Européen et retrouve une dynamique positive après une année 2024 de repli, en volumes et en valeurs.



2025

LES 10 PLUS IMPORTANTES LEVÉES CYBERSÉCURITÉ MONDIALES

En 2025, les dix plus importantes levées mondiales totalisent 4,7 Md€ et concernent majoritairement des entreprises américaines. La moitié des sociétés figurait déjà au classement 2024 (Cyera, Quantinuum, NinjaOne, Armis, Island), signe de la concentration des capitaux sur un noyau de leaders.



 Reste du monde  Europe

2025

LES NOUVELLES LICORNES CYBERSÉCURITÉ MONDIALES

Le nombre de nouvelles entreprises de cybersécurité atteignant le statut de licorne dans le monde (avec une valorisation supérieure à 1 milliard de dollars) avait été divisé par 7 entre 2022 et 2023. En 2025, le nombre de nouvelles licornes a été divisé par deux par rapport à 2024, avec seulement 4 nouvelles entreprises. Cette évolution traduit une discipline accrue des investisseurs et des critères de valorisation plus exigeants.



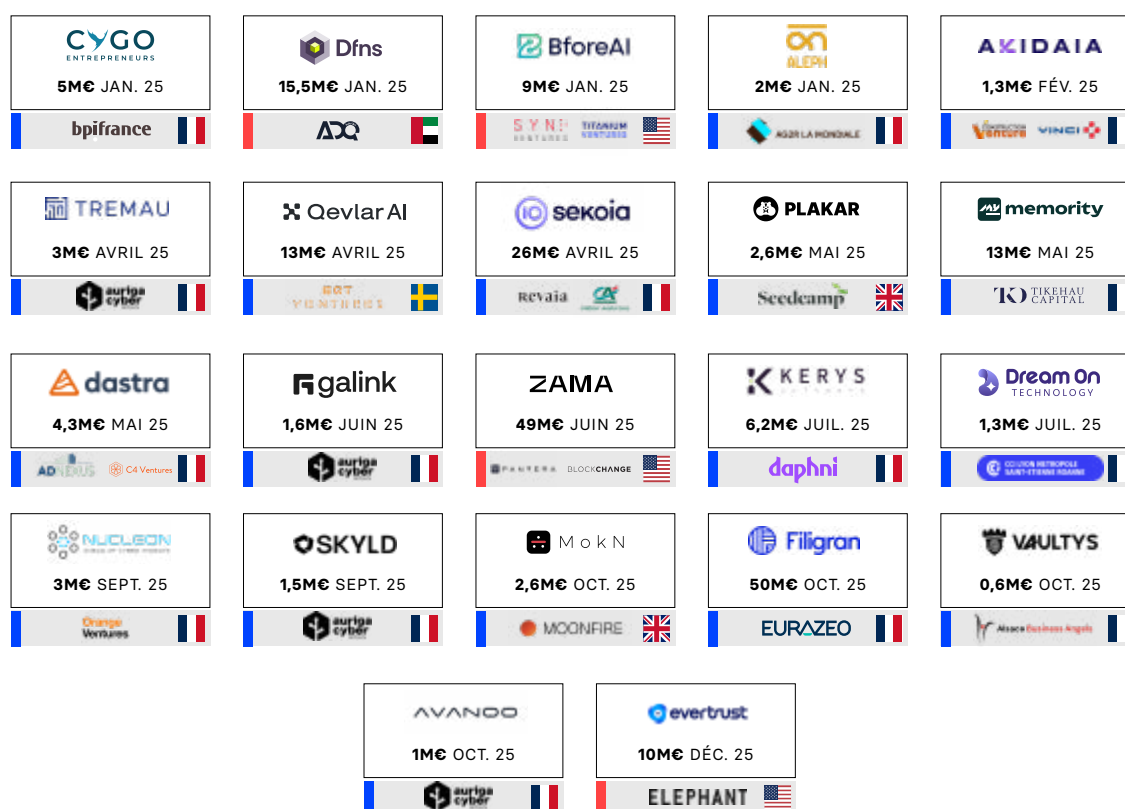
 Reste du monde  Europe

2024 & 2025

LES LEVÉES CYBERSÉCURITÉ EN FRANCE

22 LEVÉES FRANÇAISES EN CYBERSECURITÉ ANNONCÉES EN 2025

L'écosystème français demeure dynamique. En 2025, 22 levées de fonds ont été annoncées pour un total de 221,6 M€, soit un ticket moyen d'environ 10,1 M€. L'activité est portée par quelques tours significatifs et un tissu soutenu d'opérations *mid-market*. En 2024, 25 levées avaient été recensées, confirmant la résilience du marché malgré la normalisation en cours.



Reste du monde Europe

2024

LES LEVÉES CYBERSÉCURITÉ EN FRANCE

25 LEVÉES FRANÇAISES EN CYBERSECURITÉ ANNONCÉES EN 2024

EDAMAME TECHNOLOGIES 0,4M€ JAN. 24 BA	Tenacy 6M€ JAN. 24 kreaxi	alcyonnie Normale management capital 1,4M€ JAN. 24 bpifrance	Filigran 15M€ & 32,3M€ FÉV. & OCT. 24 Accel	Look Up! BNECC N/A FÉV. 24 N/A
ZAMA 67M€ MARS 24 Accel	mindflow 5M€ MARS 24 auriga cyber	nijta 2,1M€ MARS 24 elaia	ANOZT WAY 6M€ MARS 24 	Kamaé aplan logo 1,4M€ MARS 24 SUPER CAPITAL
BforeAI 14,4M€ & 9,6M€ AVRIL & DÉC. 24 SYN TITANUM FORTUNE	ipeeo 1,8M€ MAI 24 	Finovox 3,9M€ JUIN 24 shapventures	YesWeHack 26M€ JUIN 24 Adelie	soteria 0,8M€ JUIL. 24 bpifrance
alphaguard 0,2M€ AOÛT 24 NTLER	Patrowl 11M€ SEPT. 24 SWEN CAPITAL PARTNERS	:probabl. 5,5M€ SEPT. 24 bpifrance	dotfile 6M€ SEPT. 24 SEAYA	stoik 25M€ OCT. 24 alven
	CHAPSVISION DATA MAKE SENSE 85M€ NOV. 24 bpifrance Qualium Q CNEO	Daspren 1M€ NOV. 24 N/A	Dfns 15M€ DÉC. 24 FURTHER	



Reste du monde

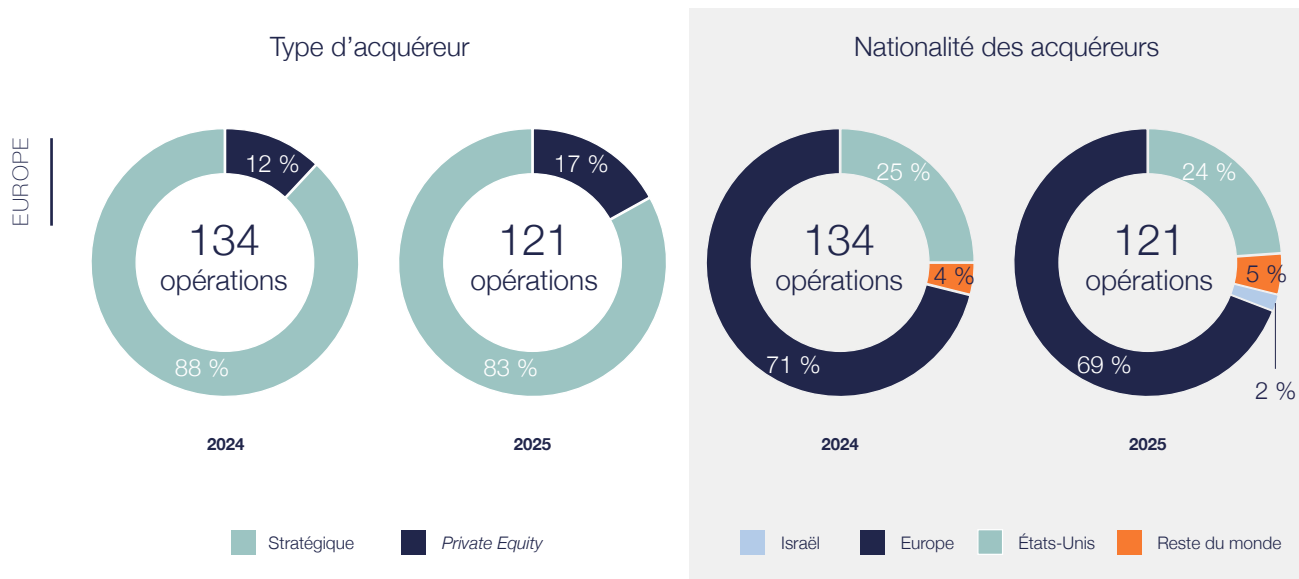


Europe

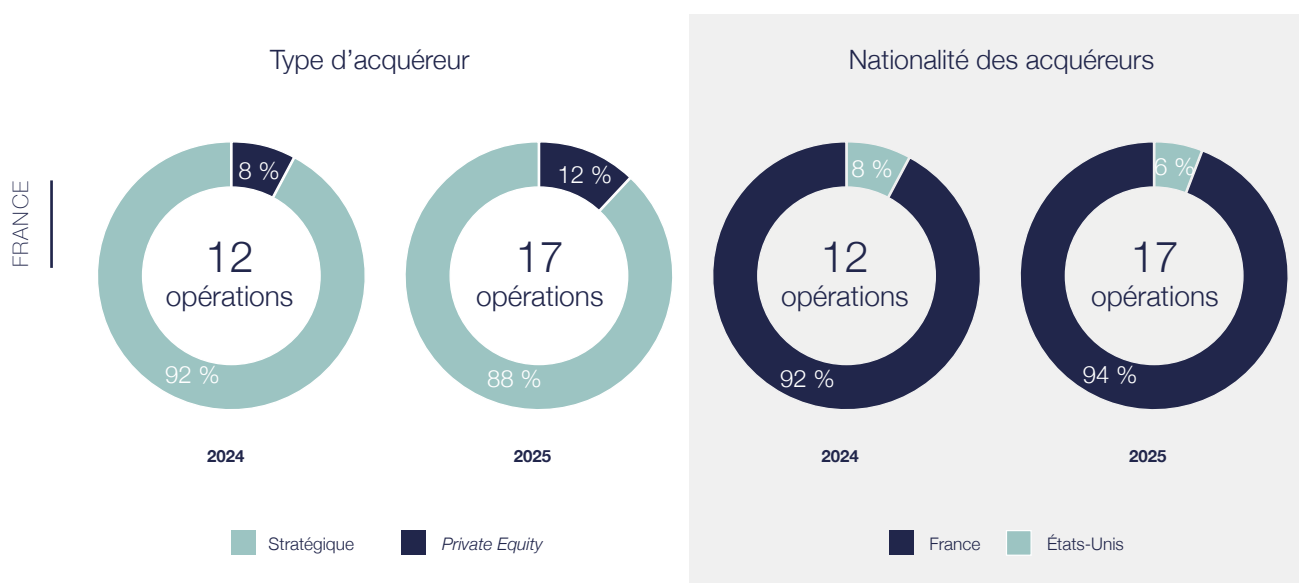
ACQUISITIONS & CONSOLIDATION EN 2025

FOCUS SUR L'EUROPE ET LA FRANCE

En Europe, 121 sociétés de cybersécurité ont été acquises en 2025, soit un recul d'environ 9 % par rapport à 2024. La majorité des transactions (83 %) relève de stratégies de consolidation, et 69 % des acquisitions ont été réalisées par des acteurs européens, preuve d'une intégration progressive au sein du continent.



En France, 17 acquisitions ont été enregistrées (+40 % par rapport à 2024), dont 88 % menées par des acquéreurs stratégiques ; 94 % des opérations ont été réalisées par des sociétés françaises, indiquant une dynamique largement domestique.



CONCLUSION

Après un point bas en 2024, 2025 consacre un rebond net du financement de la cybersécurité, avec 15.6 Md€ levés et 866 opérations.

La dynamique reste menée par les États-Unis, où la majorité des montants se concentre sur des tours avancés (C/D/E), traduisant une préférence pour des modèles éprouvés. Israël enregistre un rattrapage marqué, bien que largement tiré par quelques opérations de taille. L'Europe surperforme clairement son marché technologique : malgré un léger recul des levées tous secteurs, la cybersécurité bondit de 87 % en montants et de 32 % en volumes, portée par des tours plus matures (jusqu'aux Series F et ultérieures) et par une consolidation principalement intra-européenne.

En France, l'activité se maintient à un niveau élevé avec 22 levées et un ticket moyen autour de 10,1 M€, tandis que le Royaume-Uni retrouve sa vigueur. La hausse des tickets moyens en Europe et en Israël suggère un retour de la confiance des investisseurs, une normalisation des valorisations et un besoin accru de capital pour accélérer la mise à l'échelle. Les opérations de M&A, en hausse en France et majoritairement locales, attestent d'une stratégie de construction de champions régionaux.

Pour 2026, plusieurs facteurs devraient soutenir la trajectoire: la montée en puissance des exigences réglementaires (NIS2/DORA) et des enjeux de souveraineté (*cloud* de confiance), la pression croissante sur la protection des chaînes de valeur industrielles, et l'émergence de ruptures technologiques (ex. : quantique) qui créeront de nouveaux vecteurs de risque et d'investissement. Dans ce contexte, nous anticipons la poursuite d'une allocation sélective, focalisée sur :

- des plateformes en phase d'expansion, capables d'industrialiser la distribution et le support multi-géographies.
- des solutions natives *cloud*, IA, *datadriven* et intégrables dans des environnements hybrides.
- des consolidations créatrices de valeur, combinant extension de portefeuille, couverture sectorielle et capillarité commerciale.

Pour les investisseurs, la combinaison d'un marché adressable en croissance, d'un environnement réglementaire structurant et d'un pipeline d'assets plus matures offre un couple rendement/risque attractif. Le cycle 2026 devrait ainsi confirmer l'ancrage de la cybersécurité comme pilier durable de l'innovation européenne.

À PROPOS DU FORUM INCYBER



Organisé depuis 2013 par Forward Global, le Forum INCYBER s'est imposé comme l'événement de référence en Europe en matière de sécurité et de confiance numérique.

Événement hybride, associant un salon professionnel (près de 700 partenaires exposants, 20 000 m²), un sommet international et un forum de haut niveau (550 intervenants), il réunit durant trois jours l'ensemble des décideurs européens du domaine : grands clients finaux privés, dirigeants d'entreprises et politiques, fond d'investissement et innovateurs, hautes autorités civiles et militaires, représentants diplomatiques, chercheurs académiques et hackers éthiques.

CONTACTS PRESSE



Valérie SUEUR

press@tikehaucapital.com

Tél. : 01 53 59 03 64



Charles CITROËN

charles.citroen@forwardglobal.com

Tél. : 01 40 17 91 28

7^E ÉDITION – MARS 2026



TIKEHAU CAPITAL

en partenariat avec

IN CYBER
FORUM