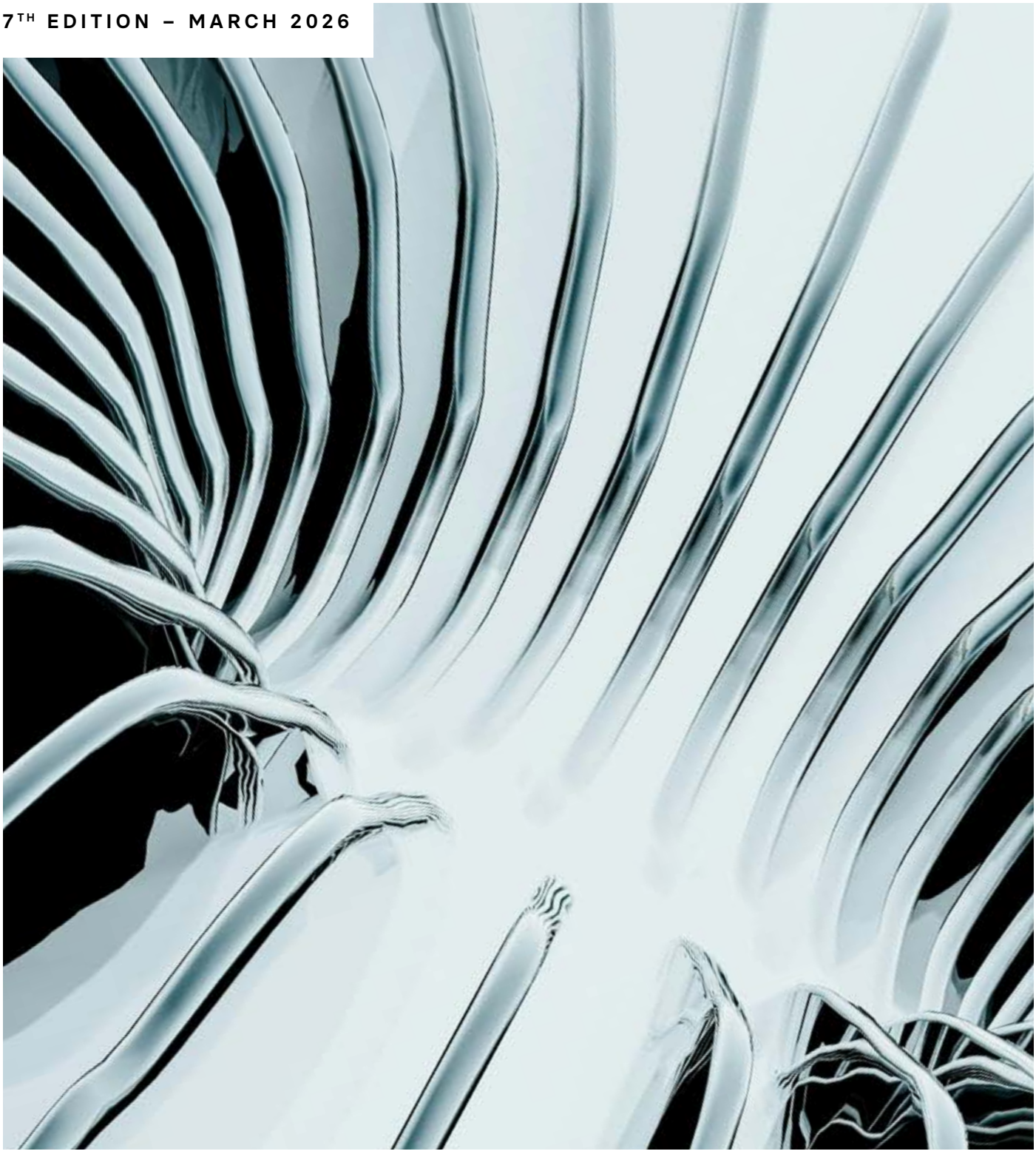
7TH EDITION – MARCH 2026



TIKEHAU CAPITAL

in partnership with

IN CYBER FORUM

BAROMETER

OF EUROPEAN INVESTMENT IN CYBERSECURITY

PRÉFACE

of Mrs. Despina SPANOU

Today, Europe and its neighborhood are facing increasingly complex and hybrid threats, combining cyberattacks targeting our critical infrastructure with destabilization and influence operations conducted below the threshold of open conflict. These threats take many forms: violations of our airspace through repeated drone incursions, attempts to sabotage undersea cables, disinformation campaigns targeting our citizens, often amplified by the widespread use of artificial intelligence.

Recent conflicts have further confirmed the use of offensive activities in cyberspace, either preceding or accompanying conventional military operations. Cyber is now a fully-fledged component of modern warfare.

At the same time, European companies, like our citizens, are confronted daily with cybercrime that has become endemic. According to the latest report from the European Union Agency for Cybersecurity (ENISA), while ransomware remains the most impactful cyber threat within the Union, cybercrime is now profoundly transformed by artificial intelligence, both in social engineering and in targeting digital supply chains and AI systems themselves[1].

Faced with these constantly evolving threats, Europe has a central role to play, not only in protecting and strengthening the resilience of its critical infrastructure, but also in developing operational capabilities to respond. In an interconnected Europe, cybersecurity is never stronger than its weakest link.

Our vulnerability today can also stem from certain dependencies within our IT supply chains. The digital exposure of our critical infrastructure, the robustness of their information systems, and their digital dependencies all represent potential risks to our security, whether in terms of espionage, influence, or strategic pre-positioning. These digital dependencies must never become strategic vulnerabilities.

It is therefore imperative to "de-risk" sectors that have become critical for our economy and security. The revised Cybersecurity Regulation proposal, presented by the European Commission in January 2026, provides an operational framework for identifying these critical sectors, essential digital assets, and appropriate mitigation measures, based on objective criteria and a thorough assessment of risks and potential economic impacts on the European market. Once adopted by the European co-legislators, this framework will help to sustainably reduce our vulnerabilities and strengthen the resilience of our critical infrastructure.

Finally, the rise of emerging technologies in cyberspace requires a determined investment effort at the European level in cybersecurity innovation. This means fully leveraging the potential of breakthrough technologies and synergies with the defense sector to improve our ability to anticipate and respond to cyber threats. The development of a robust, dynamic, and innovative European cybersecurity industry is, in this respect, a major strategic challenge, as highlighted by the Barometer presented this year.

Cybersecurity is both an essential factor of resilience and a lasting lever for value creation in Europe. It is now up to us, public decision-makers, governments, and industry players, to demonstrate ambition and creativity to strengthen our collective security. Two assets that Europe has never lacked.

Mrs. Despina SPANOU

Deputy Director General for Networks and Technology Cybersecurity coordination
European Commission

1 ENISA Threat Landscape 2025 (ENISA Threat Landscape 2025_v1.2.pdf)

ABOUT

TIKEHAU CAPITAL

Tikehau Capital is a global alternative asset management group managing €52.8 billion of assets (as of 31 December 2025).

The Group has developed a wide range of expertise across four asset classes: Credit, Real Assets, Private Equity, and Capital Markets Strategies. Capitalizing on its strong equity base (€3.1 billion as of 31 December 2025), Tikehau Capital invests its own capital alongside its investor-clients. The Group is guided by a strong entrepreneurial spirit and DNA, shared by its 717 employees (as of 31 December 2025) across 17 offices in Europe, Asia, and North America.

Tikehau Capital is listed on the regulated market of Euronext Paris,
Compartment A (ISIN code: FR0013230612; Ticker: TKO.FP).

TIKEHAU CAPITAL

Tikehau Capital's portfolio includes the following investments in the fields of cybersecurity and trusted technologies:

TRUST IN SOFT · egerie · Quarkslab (Securing every bit of your data) · jscrambler · VMRAY

EclecticIQ · <TEHTRIS> · GLIMPS · PROVENRUN · yogosha

build38 · CHAPSVISION DATA MAKE SENSE · trustpair · FTAPI · memority

Ekimetrics. · odrive · claranet · intersec

www.tikehaucapital.com/en

METHODOLOGY

In the preparation of this barometer, which covers the last 10 years from 2015 to 2025, Tikehau Capital used, cross-referenced and analysed various sources of information, including:

crunchbase.com | cbinsights.com/research-unicorn-companies | capitaliq.spglobal.com | returnonsecurity.com | momentumcyber.com | info.mergermarket.com | info.mergermarket.com | pitchbook.com

The concept of "private equity" includes pre-seed, seed, and Series A through to H operations, i.e. business angel, venture capital and growth fundraisings (but not IPOs, post-IPO investments, debt financing or subsidies).

The definition used for "cybersecurity" is quite broad and specifically includes the following activities:

- → the security of networks, the cloud, work stations, mobile devices and infrastructure
- → the detection of threats, intrusion and fraud; the management of access, identities and cyber risks
- → penetration tests
- → mail and web filtering

The regions covered by this barometer are the United States, Israel and Europe. "Europe" includes the following countries: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom, (the 27 EU member states plus the United Kingdom, Norway and Switzerland).

Past amounts have been adjusted to create an annual reference in euro, calculated on the basis of the average exchange rate observed in each of the years concerned.

Being essentially derived from information published by the companies that raised the funds, this barometer does not claim to be exhaustive or completely accurate. Neither Tikehau Capital nor any of its affiliates accept any liability with regard to the barometer. Please contact us if you note any errors or omissions or would like to suggest improvements for subsequent issues: **contact@tikehaucapital.com**

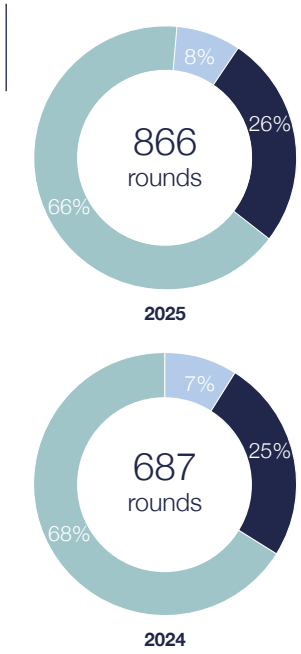
You may reproduce or quote the analyses and forecasts shown in this barometer provided you mention the source of this information by including the following text:

"Source: Tikehau Capital – Tikehau Capital Barometer of European Investment in Cybersecurity – 7th edition 2026"

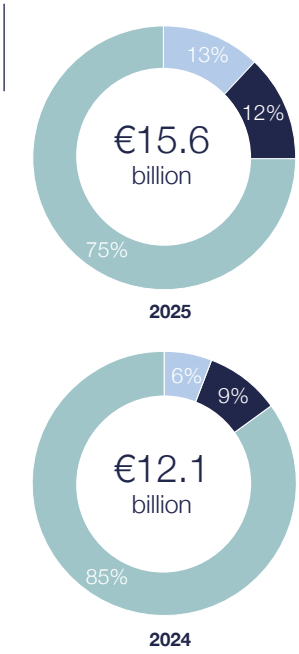
UNITED STATES, ISRAEL & EUROPE
2025 SUMMARY

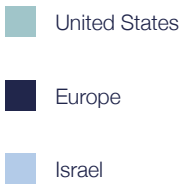
In 2025, start-ups specialising in cybersecurity raised a total of €15.6 billion across 866 transactions. As in prior years, the United States leads both in volume and in total amounts raised. Europe maintained its contribution to the number of deals relative to 2024 and increased its share of amounts raised, reflecting a market increasingly oriented toward later-stage rounds.

Cyber Fundraising - Number of rounds



Cyber Fundraising - Amount

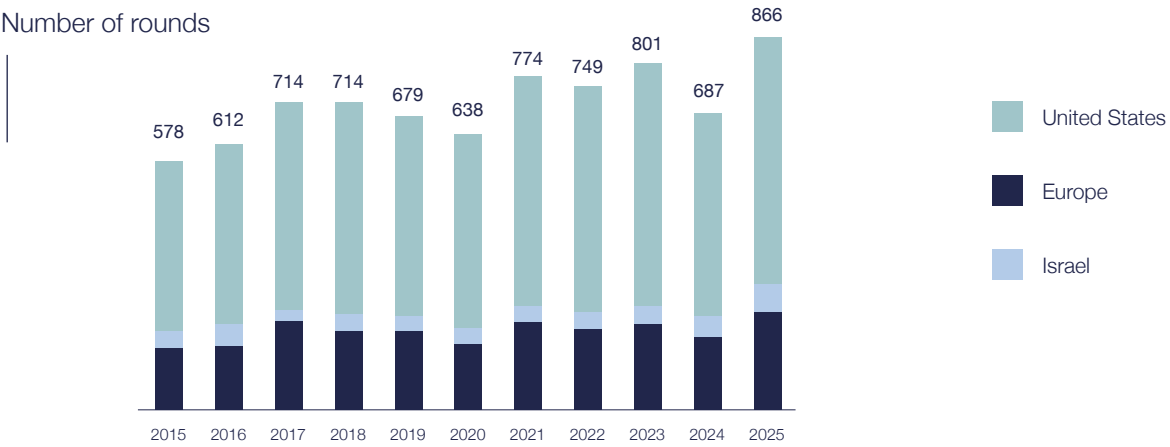


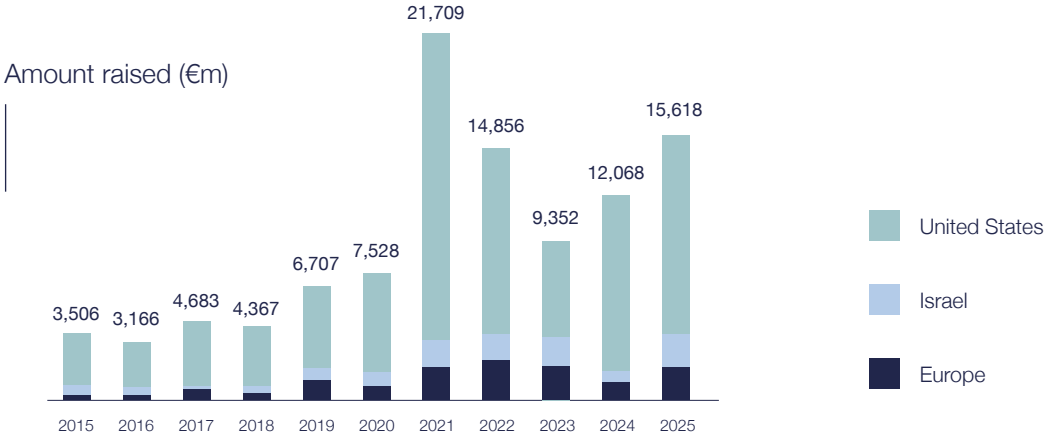


TRENDS 2015-2025

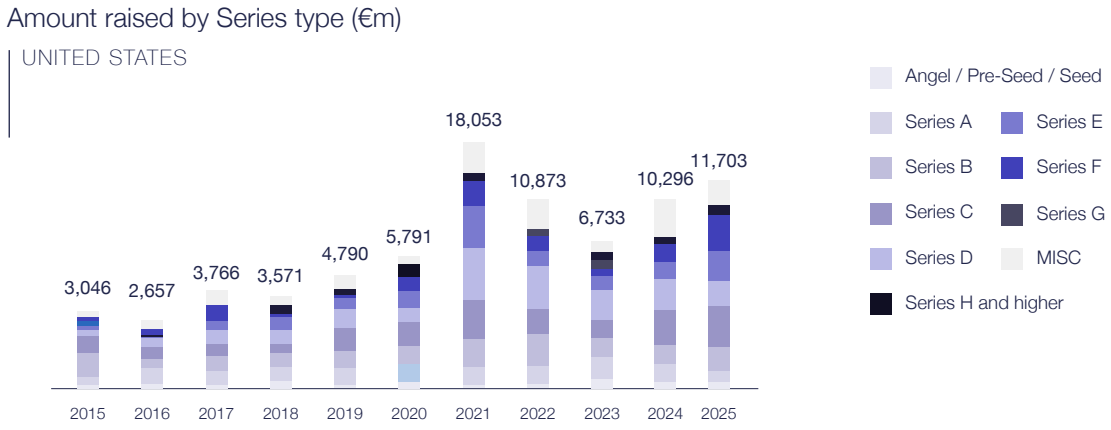
Compared with 2024, the number of fundraisings rose by 27% and total amounts by 32%, confirming an overall rebound and growing financing needs. Over the decade, the number of transactions grew by 50% and capital raised by a factor of 4.5.

Number of rounds

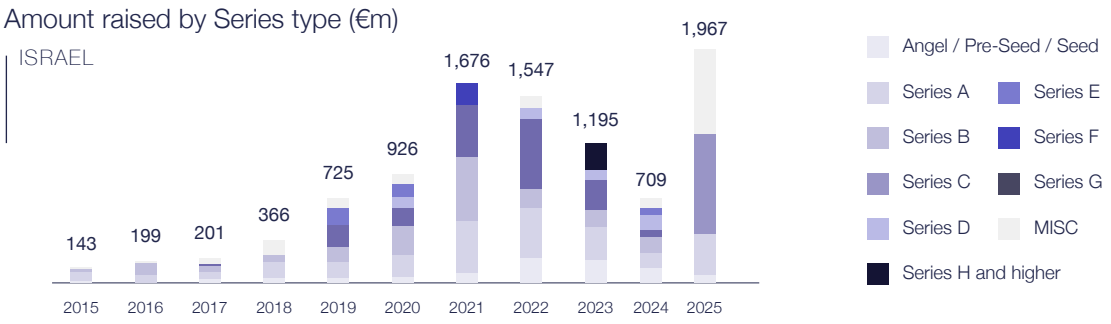




In 2025, amounts raised by US cybersecurity companies were driven primarily by Series C, D, and E rounds (46% of total amounts). Year-on-year growth reached 14%, propelled by significant rounds among scale-ups — a sign of investor preference for proven models and the concentration of capital on later-stage opportunities.

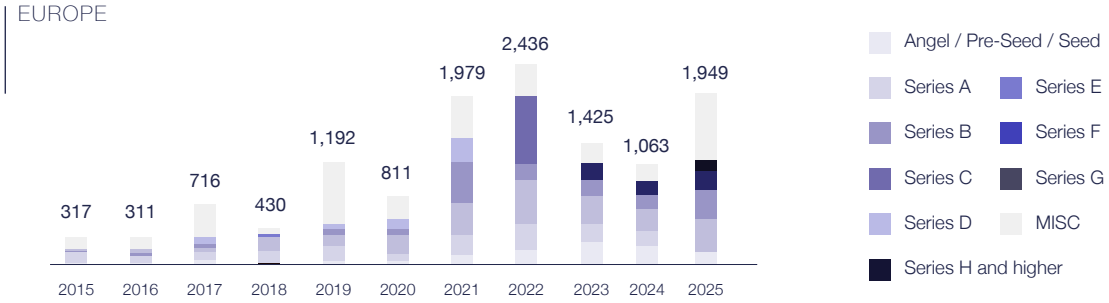


The Israeli market posted a marked catch-up after the contraction of 2024 (and 2023). Several large transactions — notably at Cato Networks and EON, totalling $659 million (around one-third of the 2025 total) — buoyed momentum, leading to a 178% increase in amounts versus 2024.



In 2025, European cybersecurity companies primarily financed their activities through rounds of greater maturity than in prior years (beyond Series C). As in 2024, 2025 was marked by substantial amounts raised in Series F and later (5% in 2025). Overall, we observe an 83% increase in amounts raised compared with 2024.

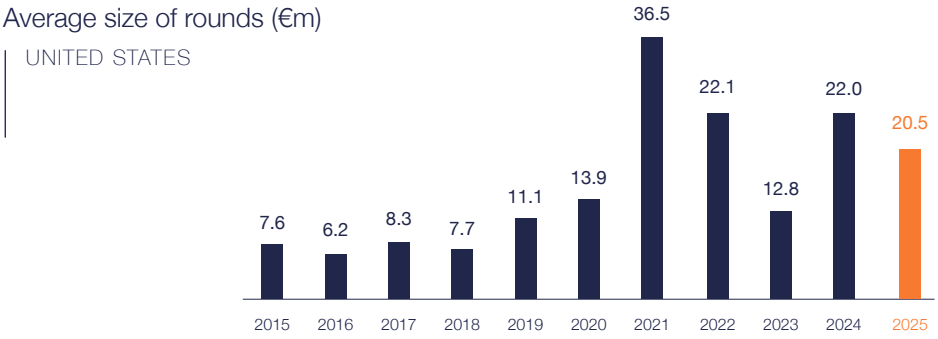
Amount raised by Series type (€m)

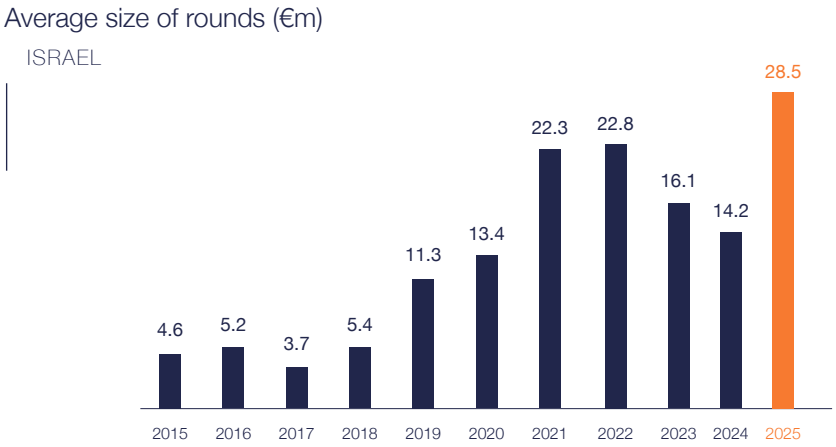


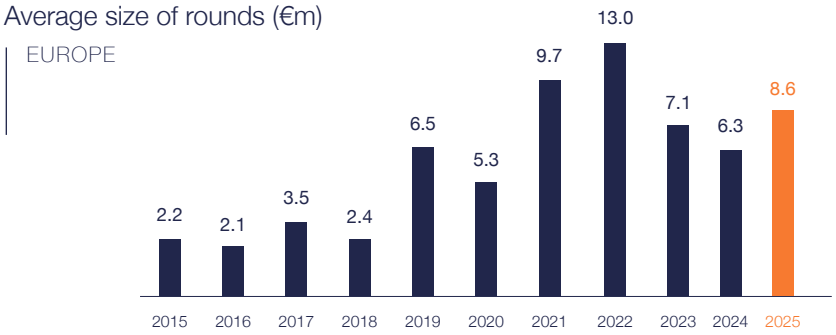
AVERAGE FUNDRAISING SIZE

The year 2025 was characterised by stagnation in average amounts raised in the United States. By contrast, Europe and Israel moved the other way, with respective increases of 38% and 101%. In 2024, we had observed the opposite trend, with stagnation in Europe and Israel.

Average size of rounds (€m)

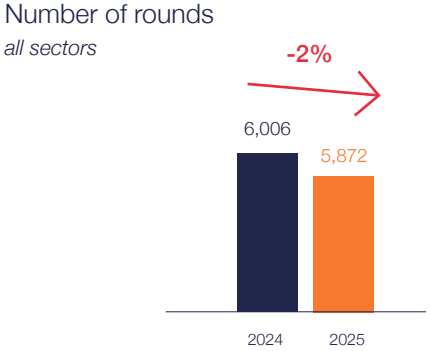


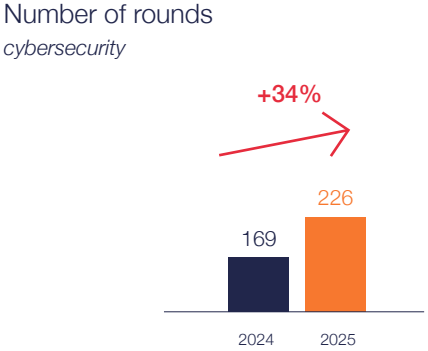


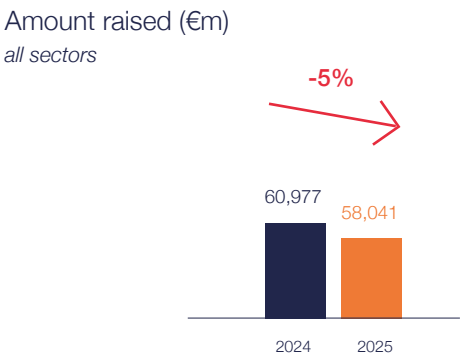


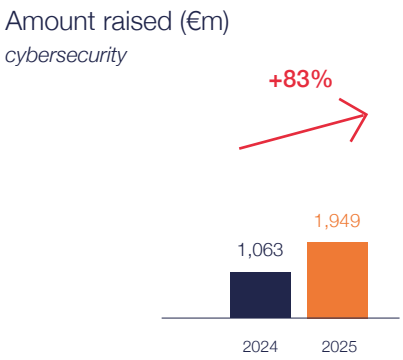
EUROPE
TRENDS 2025 VS. 2024

Across all industries, the number of raises in Europe edged down in 2025 (–2%, after –20% in 2024). Cybersecurity ran counter to the trend, with a 34% increase in the number of transactions. Accordingly, cumulative amounts across all industries decreased by 5%, while amounts raised in cybersecurity rose by 83%, confirming the segment's appeal.



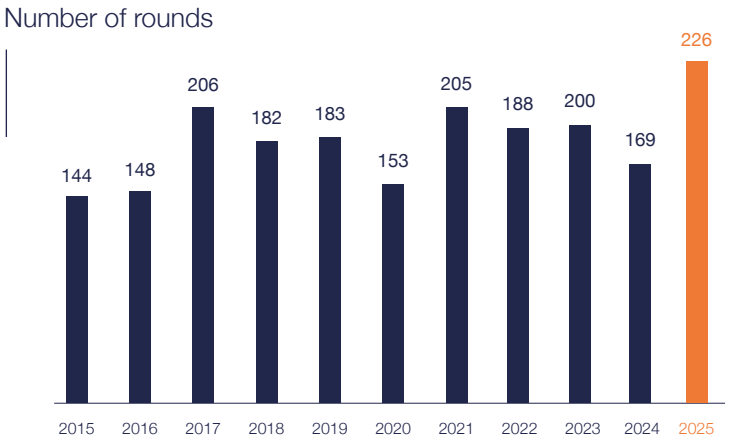


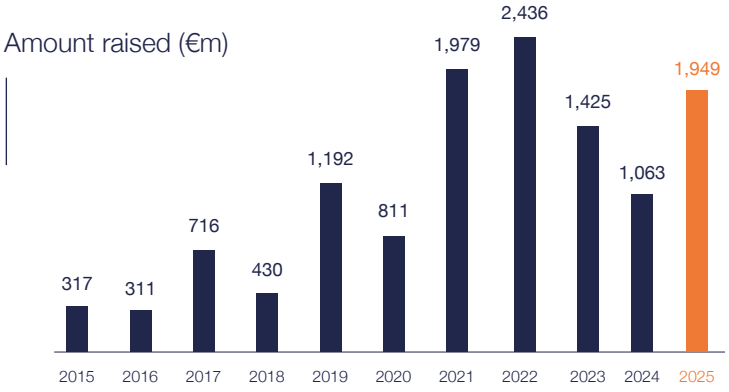




TRENDS 2015-2025

Over ten years, the European cybersecurity market has clearly matured: the number of transactions has multiplied by 1.6 and amounts raised by 6.2. This progression reflects the growing maturity of players and the deepening of the investor base.

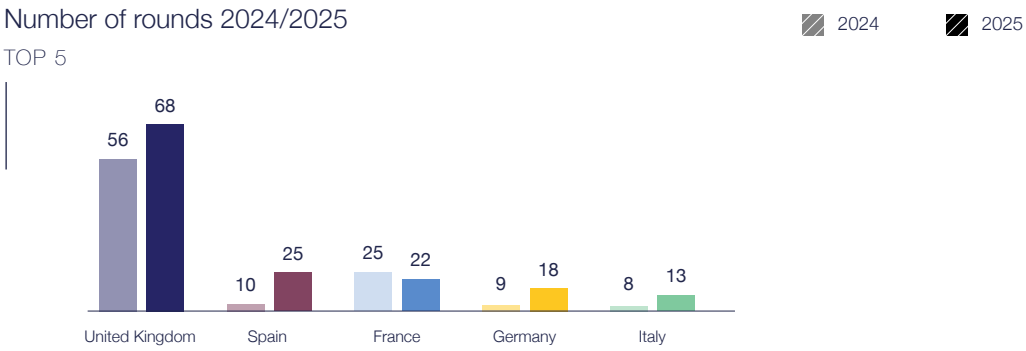


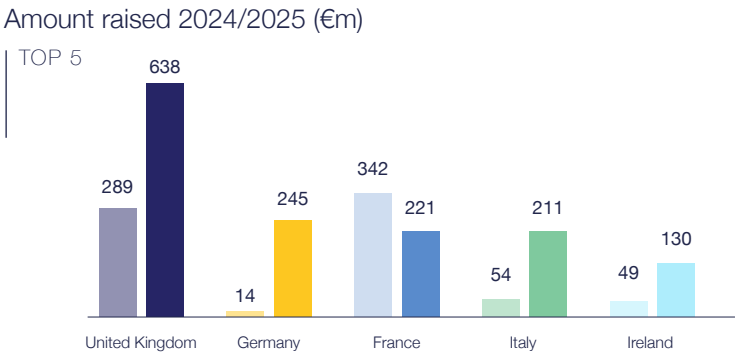


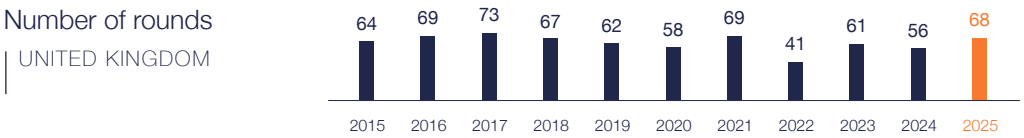
FOCUS 2025

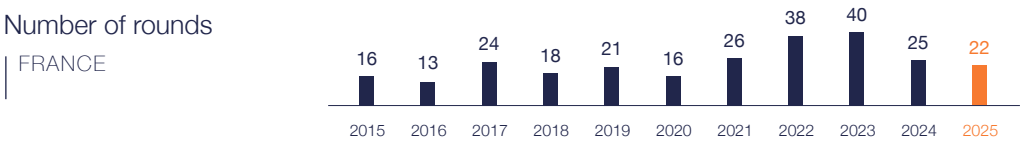
France is emerging as a major player in cybersecurity financing in Europe, ranking third in both amounts raised and number of deals.

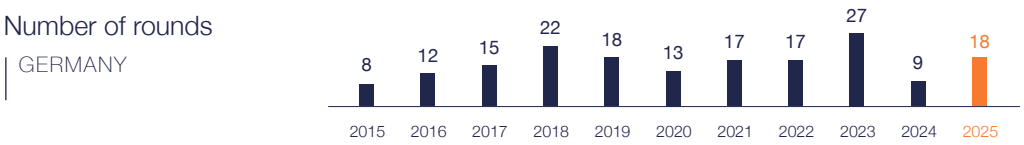
The United Kingdom continues to dominate the European market and has regained positive momentum after a 2024 decline, in both volume and value.











2025
THE 10 LARGEST GLOBAL CYBERSECURITY FUNDRAISINGS

In 2025, the ten largest rounds worldwide totalled €4.7 billion and mostly involved US companies. Half of the companies also appeared in the 2024 ranking (Cyera, Quantinuum, NinjaOne, Armis, Island), signalling the concentration of capital around a core group of leaders.

JUNE 25 - DEC. 25

CYERA

Data Protection

RAISE: $940m

DEC. 25

Saviynt

IA IAM

RAISE: $700m

AUG. 25

QUANTINUUM

Computers and quantum software solutions

RAISE: $600m

FEB. 25

ninjaOne

IT security and Management

RAISE: $500m

NOV. 25

ARMIS

Cyberthreat exposure management & Security

RAISE: $435m

JUNE 25

CATO NETWORKS

Single-Vendor SASE Platform

RAISE: $359m

APRIL 25

chainguard

Secure-by-default open source software

RAISE: $356m

DEC. 25

harness

AI for Everything After Code

RAISE: $240m

DEC. 25

EON

Turn cloud backups into live, Strategic assets

RAISE: $300m

MARCH 25

Island

Entreprise Browser

RAISE: $250

Rest of the World Europe

2025
THE NEW GLOBAL CYBERSECURITY UNICORNS

The number of new cybersecurity companies reaching unicorn status worldwide (valued at over $1 billion) was divided by seven between 2022 and 2023. In 2025, the number halved again relative to 2024, with only four new companies. This trend reflects heightened investor discipline and more exacting valuation criteria.

FEB. 25

tines

Intelligent workflow platform

FEB. 25

DREAM

Cyber offensive to protect critical infrastructure

APRIL 25

tailscale

Connectivity platform for devs, IT, and Security teams

JUNE 25

ZAMA

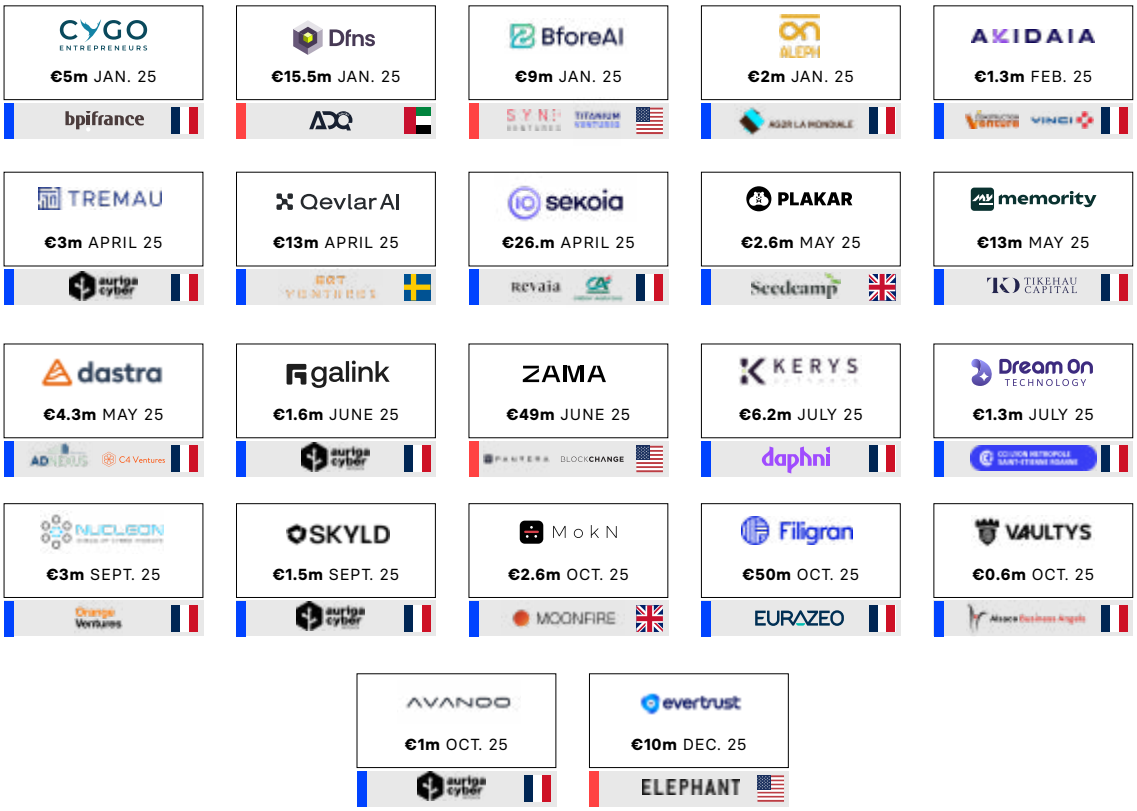
Open Source Cryptography

Rest of the World Europe

2024 & 2025
CYBERSECURITY FUNDRAISING IN FRANCE

22 ROUNDS OF FRENCH CYBERSECURITY FUNDRAISING ANNOUNCED IN 2025

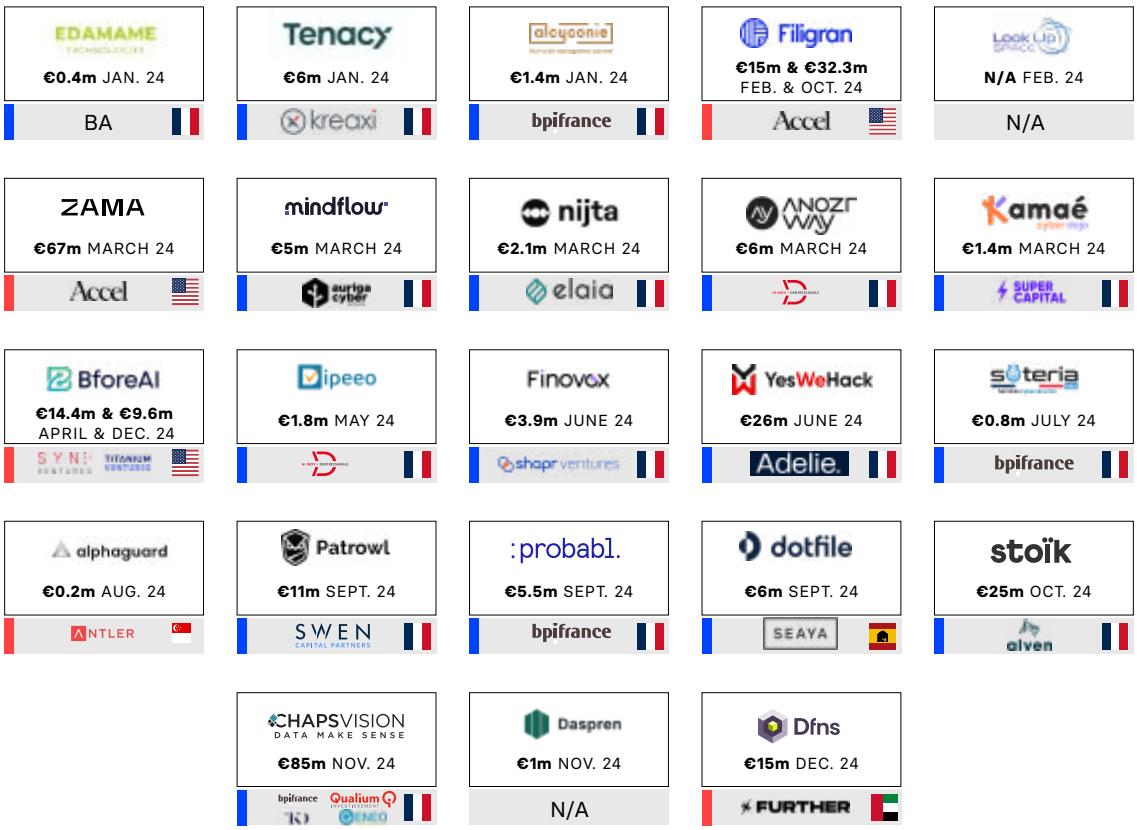
The French ecosystem remains dynamic. In 2025, 22 fundraisings were announced for a total of €221.6 million, implying an average ticket of around €10.1 million. Activity was driven by a handful of significant rounds and a sustained fabric of mid-market transactions. In 2024, 25 fundraisings were recorded, confirming the market's resilience despite ongoing normalisation.



Rest of the World Europe

2024
CYBERSECURITY FUNDRAISING IN FRANCE

25 ROUNDS OF FRENCH CYBERSECURITY FUNDRAISING ANNOUNCED IN 2024



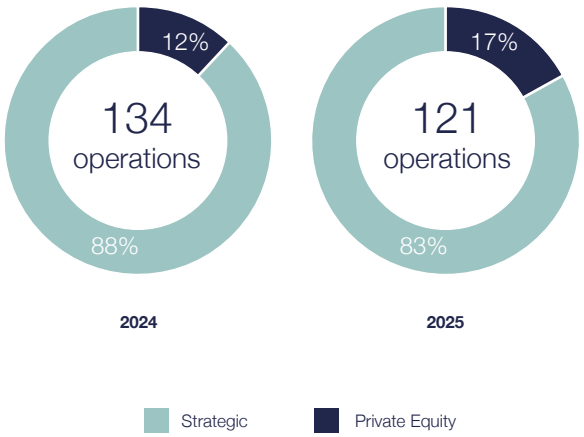
Rest of the World Europe

ACQUISITIONS AND CONSOLIDATION IN 2025
FOCUS ON EUROPE AND FRANCE

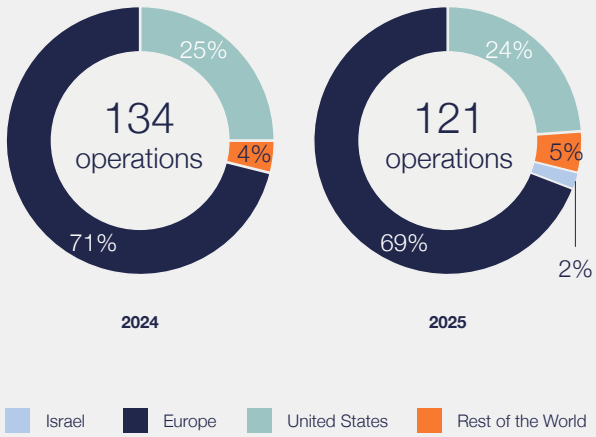
In Europe, 121 cybersecurity companies were acquired in 2025, a decrease of roughly 9% versus 2024. Most transactions (83%) were consolidation moves, and 69% of acquisitions were carried out by European players — evidence of gradual consolidation within the continent.

EUROPE

Type of buyer



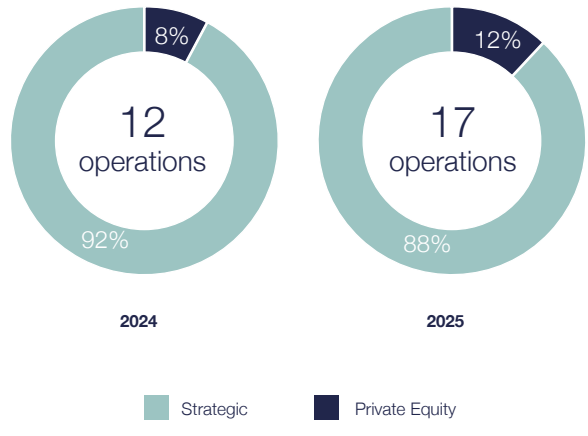
Nationality of buyers



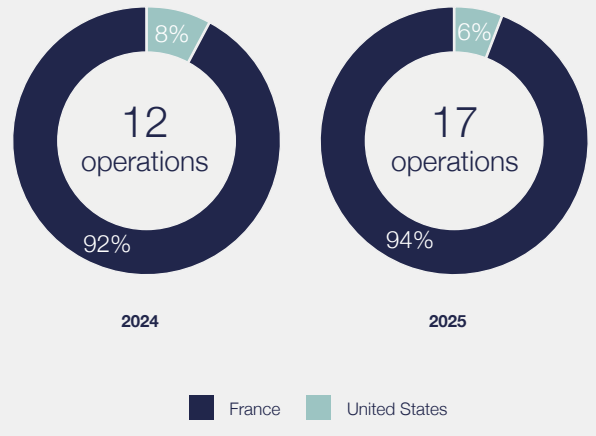
In France, 17 acquisitions were recorded (+40% versus 2024), 88% of which were led by strategic acquirers; 94% of transactions were undertaken by French companies, indicating a largely domestic dynamic.

FRANCE

Type of buyer



Nationality of buyers



CONCLUSION

After a low point in 2024, 2025 marked a clear rebound in cybersecurity financing, with €15.6 billion raised and 866 transactions.

In France, activity remains elevated with 22 fundraisings and an average ticket of around €10.1 million, while the United Kingdom regains its vigour. The increase in average tickets in Europe and Israel suggests a return of investor confidence, a normalisation of valuations, and a greater need for capital to scale. M&A activity, up in France and predominantly local, attests to a strategy of building regional champions.

For 2026, several factors should support the trajectory: the strengthening of regulatory requirements (NIS2/DORA) and sovereignty issues (trusted cloud), mounting pressure to protect industrial value chains, and the emergence of disruptive technologies (e.g., quantum), which will create new vectors of both risk and investment. In this context, we anticipate continued selective allocation focused on:

- → platforms in an expansion phase, capable of industrialising distribution and multi-geography support.
- → cloud-native, AI, data-driven solutions that can be integrated into hybrid environments.
- → value-creating consolidations combining portfolio extension, sector coverage, and commercial reach.

For investors, the combination of a growing addressable market, a structuring regulatory environment, and a pipeline of more mature assets offers an attractive risk/return profile. The 2026 cycle should confirm cybersecurity's place as a lasting pillar of European innovation.

ABOUT INCYBER FORUM

Organized since 2013 by Forward Global, the INCYBER Forum has become the leading event in Europe for security and digital trust.

The INCYBER Forum is a hybrid event, associating a trade show (700 exhibit partners, 20,000sqm), a high-level forum (550 speakers) and an international summit (40 official international delegations). It brings together for 3 days the entire European ecosystem: major private end-customers (CIOs, CISOs, CTOs, Data Protection Officers, Security Directors), business leaders, political decision-makers, senior civil and military authorities, diplomatic representatives, academic researchers and ethical hackers.

PRESS CONTACTS

TIKEHAU CAPITAL

Valérie SUEUR

press@tikehaucapital.com

Tel.: +33 (0)1 53 59 03 64

IN CYBER FORUM

Charles CITROËN

charles.citroen@forwardglobal.com

Tel.: +33 (0)1 40 17 91 28

7E EDITION – MARCH 2026

TIKEHAU CAPITAL

in partnership with

IN CYBER FORUM