



BAROMETER
OF EUROPEAN INVESTMENT
IN CYBERSECURITY

in partnership with

IN CYBER
FORUM

6TH EDITION – MARCH 2025

PREFACE

by Ms Clara CHAPPAZ



France is globally renowned as a cybersecurity expert and pioneer. Our country very quickly realised the strategic importance of cybersecurity in shoring up digital infrastructure and protecting sensitive data. However, the cyber threat is constantly evolving and we now face major challenges due to the spread of artificial intelligence applications and generative AI.

These new technologies are radically changing the cybersecurity landscape.

On the one hand, they enable cybercriminals to readjust their line of attack with unprecedented speed and precision. On the other, they give cybersecurity specialists innovative defensive resources of unprecedented efficiency. At the same time, new AI technologies need rigorous cybersecurity measures to keep them safe and compliant with regulations.

In the face of these developments, France remains at the forefront of international research and action. The success of the AI Action Summit, which in February 2025 brought together heads of state, leaders of international organisations and major AI players from every country, showed our ability to shape a constructive global debate and provide concrete solutions to technological challenges.

At a legal level, we are preparing to take a key step as Parliament discusses the “Resilience of critical infrastructure and reinforcement of cybersecurity” bill, which I had the honour of submitting on the Government’s behalf. This ambitious piece of legislation will allow us to scale up our ability to anticipate, prevent and respond to cyber threats. Our citizens, local authorities and businesses are increasingly faced with attacks from criminal organisations and foreign hackers specialised in interference. ANSSI’s reports show that cyber threats are growing all the time across every sector, with a particular rise in the number of ransomware attacks. The question is no longer whether an institution will be hit, but when. The resilience of our digital infrastructure has become a vital component in our sovereignty and the trust that our citizens place in digital services.

The Resilience bill reflects Europe’s determination to develop a firmer response. A system is only as strong as its weakest link, and by harmonising rules across all member states, the European Union is enabling us to strengthen the whole chain. The bill is set to enact three major directives: RCE (resilience of critical entities), NIS2 (network and information system security) and DORA (financial sector resilience). As a result of this framework, more than 15,000 public and private entities will be better protected against cyber risks in 18 sectors that are key to the nation’s economic and social wellbeing.

However, ambitious legislation won’t be enough without the right support. This is why the Government has made supporting businesses and authorities a priority. The price of security is far exceeded by the consequences of a successful attack, which generally costs a business 5%-10% of its revenue, regardless of its size or industry, and can often lead to bankruptcy. Anticipating, preparing for and knowing how to react are imperative if we are to protect our economy and jobs.

This bill is also a great opportunity to develop France’s cyber ecosystem. Implementation of the NIS 2 directive will boost a rapidly expanding market in which our start-ups are performing very well and exporting their skills widely.

The amount of money raised by cybersecurity start-ups soared in 2024. Support from investment funds specialised in cybersecurity is a big help in the development of innovative start-ups that can address the technological breakthroughs we are now seeing; AI today, quantum computing tomorrow. France is lucky to have globally recognised talent in each of these two industries. Such assets are essential if it is to remain a cybersecurity pioneer.

Ms Clara CHAPPAZ

*Minister Delegate for Artificial Intelligence
and Digital Technologies*

ABOUT TIKEHAU CAPITAL

Tikehau Capital is a global alternative asset management group with €49.6 billion of assets under management (as at 31 December 2024).

The group has developed a wide range of expertise in four asset classes (credit, real assets, private equity, capital markets strategies) along with strategies based on multi-asset solutions and special situations. Led by its co-founders, Tikehau Capital has a distinct business model, strong balance sheet, special access to potential deals around the world, and lengthy experience of supporting businesses and top managers. Deeply rooted in the real economy, Tikehau Capital provides innovative and bespoke alternative financing solutions to the companies that it supports, and looks to create long-term value for its investors while having a positive impact on society. With own funds of €3.2 billion at 31 December 2024, the Group invests its capital in each strategy alongside its investor clients. Controlled by managers working with leading institutional partners, Tikehau Capital is guided by strong entrepreneurial DNA and a mindset shared by its 747 employees (as at 31 December 2024) across its 17 offices in Europe, Asia and North America.

Tikehau Capital is listed on Euronext Paris, compartment A (ISIN: FR0013230612; Ticker: TKO.FP).

TK TIKEHAU
CAPITAL



Tikehau Capital's portfolio notably includes the following positions
in cybersecurity and trusted technology companies:

TRUSTSOFT

EGERIE
INTEGRATED CYBERSECURITY MANAGEMENT

Quarkslab

iscrambler

VMRAY

EclecticIQ

TEHTRIS

GLIMPS

PROVENRUN

yogosha

buildd

CHAPSVISION
DATA MAKE SENSE

trustpair

HORNETSECURITY

FTAPI

Ekimetrics.

codrive

claranet

www.tikehaucapital.com

METHODOLOGY

In the preparation of this barometer, which covers the last 10 years from 2014 to 2024, Tikehau Capital used, cross-referenced and analysed various sources of information, including:



The concept of “private equity” includes pre-seed, seed, and Series A through to H operations, i.e. business angel, venture capital and growth fund raisings (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

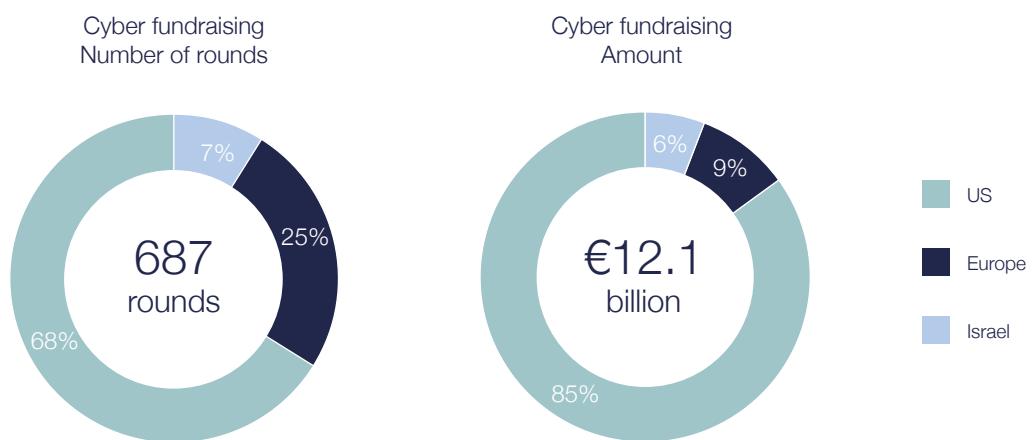
You may reproduce or quote the analyses and forecasts shown in this barometer provided you mention the source of this information by including the following text:

“Source: Tikehau Capital – Tikehau Capital Barometer of European Investment in Cybersecurity – 6th edition 2025”.

US, ISRAEL AND EUROPE

2024 SUMMARY

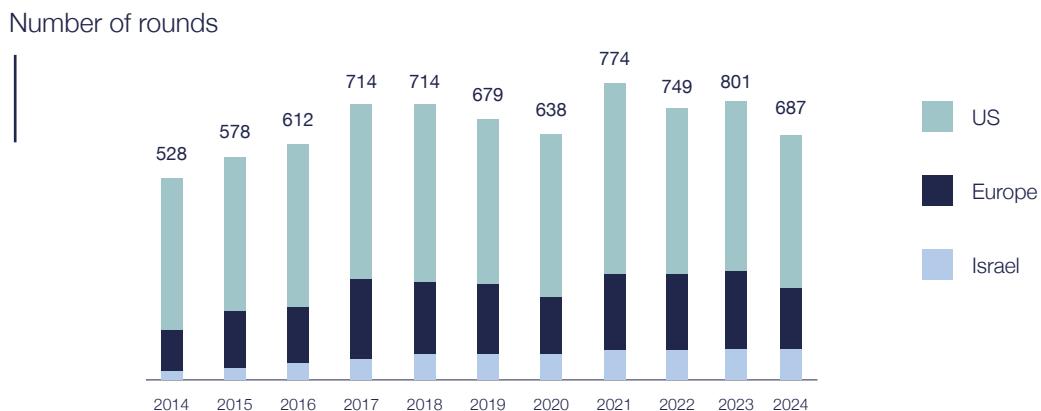
Start-ups specialised in cybersecurity raised a total of €12.1 billion in 2024, spread across 687 deals. As in previous years, the US dominated in terms of both volume and total amount raised. Compared with 2023, Europe contributed a similar number of rounds but saw a reduction in its contribution in terms of the amount raised. For geopolitical reasons, Israel accounted for a much lower share – mainly to the benefit of the US – and represented just 6% of the total amount raised (vs 13% in 2023).



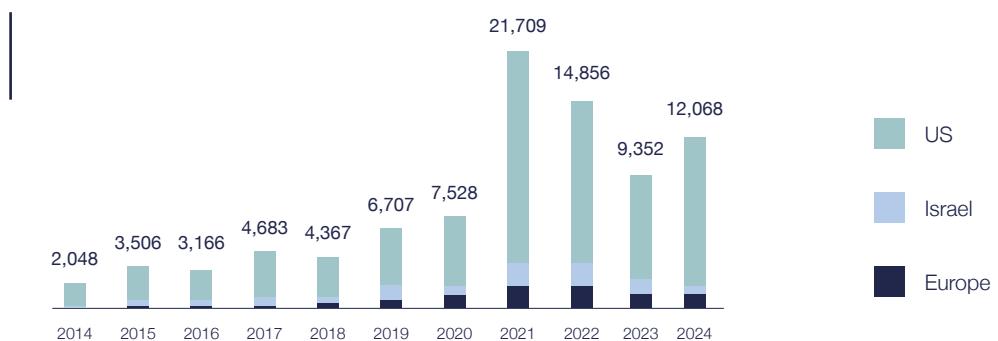
TRENDS 2014–2024

The total amount raised for cybersecurity in the US, Israel and Europe was 29% higher than in 2023, reflecting a real global bounce.

Over ten years, the total number of rounds has increased by 30% while the amount raised is 5.9 times higher – largely due to efforts in the US between 2023 and 2024.

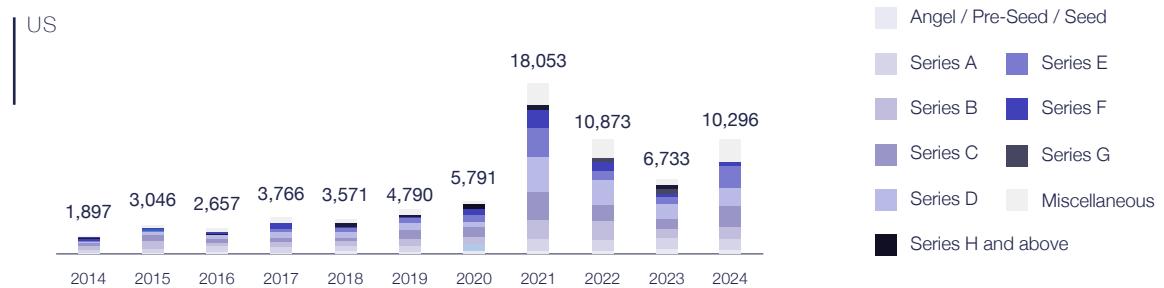


Amount raised (€m)



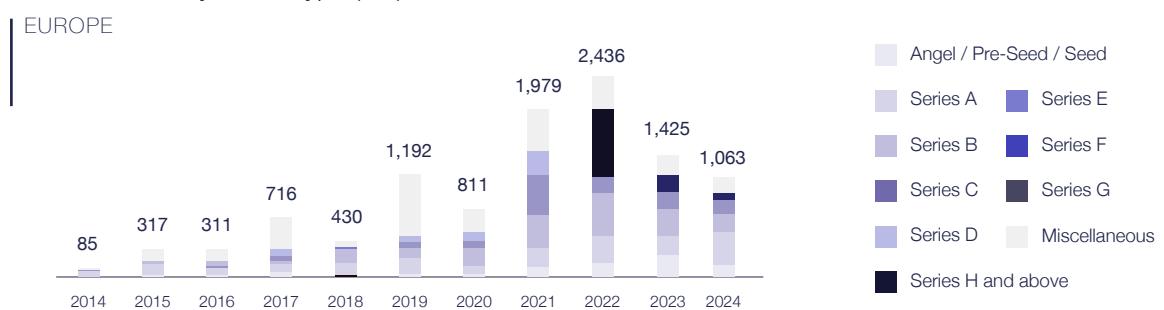
In 2024, the amount raised by US cybersecurity companies mostly came from Series C, D and E fundraising rounds (51% of the total amount raised). Growth in the total amount raised (+53% vs. 2023) is mainly attributed to a number of huge rounds (the twelve biggest cybersecurity fundraising rounds in 2024 were all US).

Amount raised by Series type (€m)

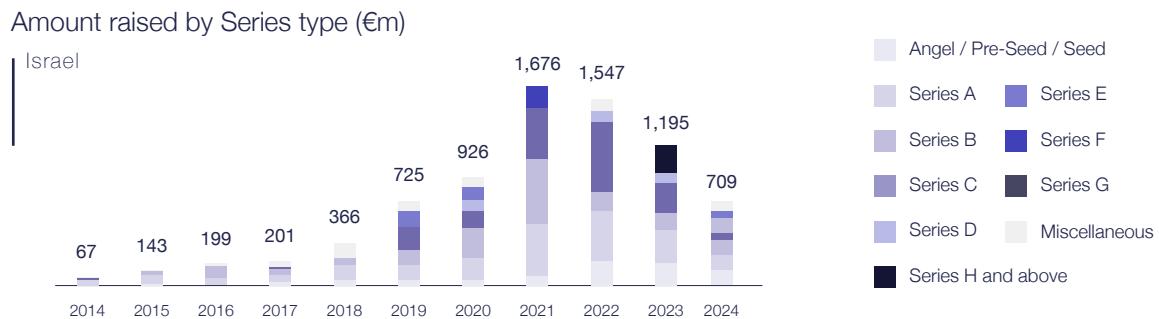


In 2024, European cybersecurity companies mainly financed their business through fundraising rounds having a maturity of a Series C or less, which accounted for 62% of the total amount raised. As in 2022, a large amount of money was raised through Series F rounds in 2024 (8%).

Amount raised by Series type (€m)

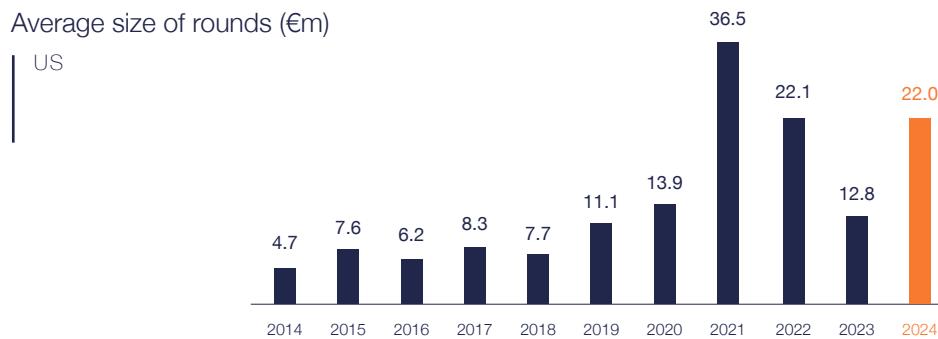


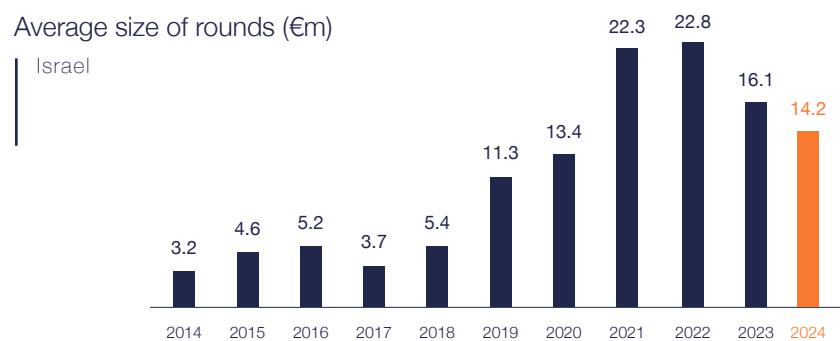
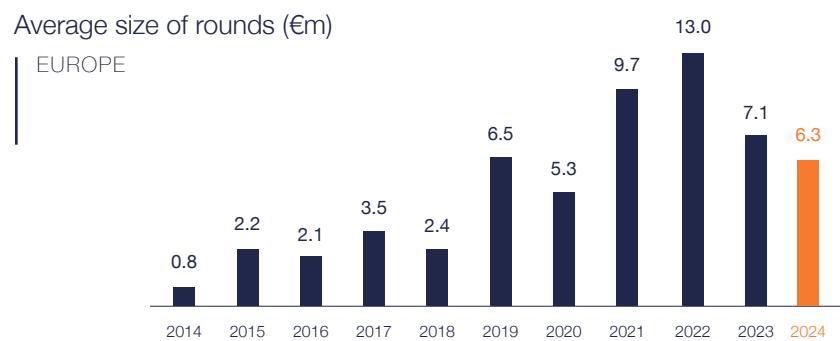
In 2024, the amount raised by Israeli cybersecurity companies fell sharply (–40% vs. 2023). This was largely due to the geopolitical situation and the consequences of the Hamas terrorist attack against Israel on 7 October 2023. Notably, there were no rounds above Series E (€60 million by Aqua Security in January 2024).



2014 – 2024 AVERAGE FUNDRAISING SIZE

2024 brought stagnation in the average amount of money raised in Europe and Israel. In the US there was an increase of nearly +70% vs. 2023 with significant average amounts above the pre-Covid trend, mainly owing to a number of massive rounds such as those by Wiz (\$1 billion), Cyera (\$600 million) and Kiteworks (\$456 million).

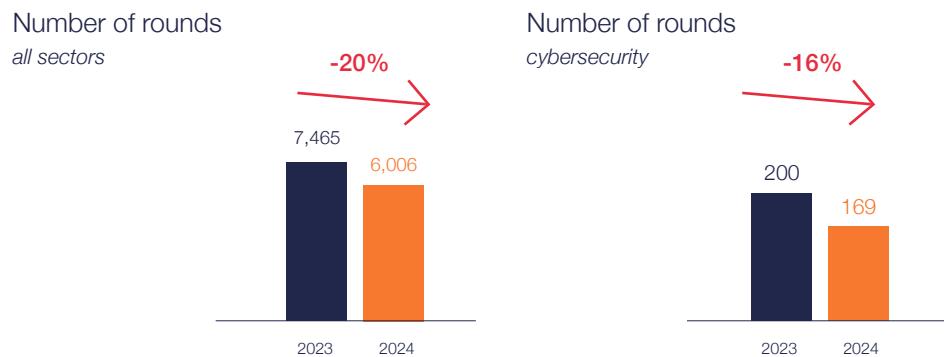


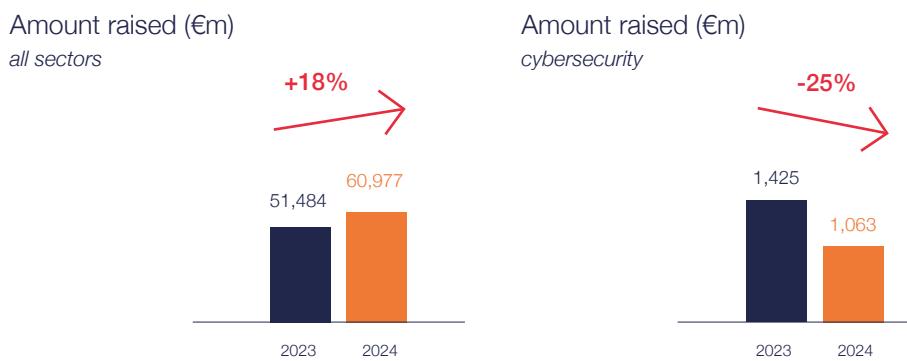


EUROPE

TRENDS 2024 VS. 2023

The drop in the number of rounds in Europe – all sectors combined – amounted to 20% in 2024. The decrease was just 16% in terms of the number of deals in European cybersecurity, with 169 rounds in 2024 vs. 200 in 2023. In line with this drop in the number of deals, the total amount of funds raised for cybersecurity in 2024 was down nearly 25% on the level of 2023. The total amount for all sectors combined in Europe was up 18%, on the other hand, boosted in particular by significant fundraising for AI and defence.





2014 – 2024 TRENDS

Europe has seen remarkable growth in cybersecurity over the past decade. The number of rounds has increased 1.6 times, while the amount raised has multiplied by 12.5 times.

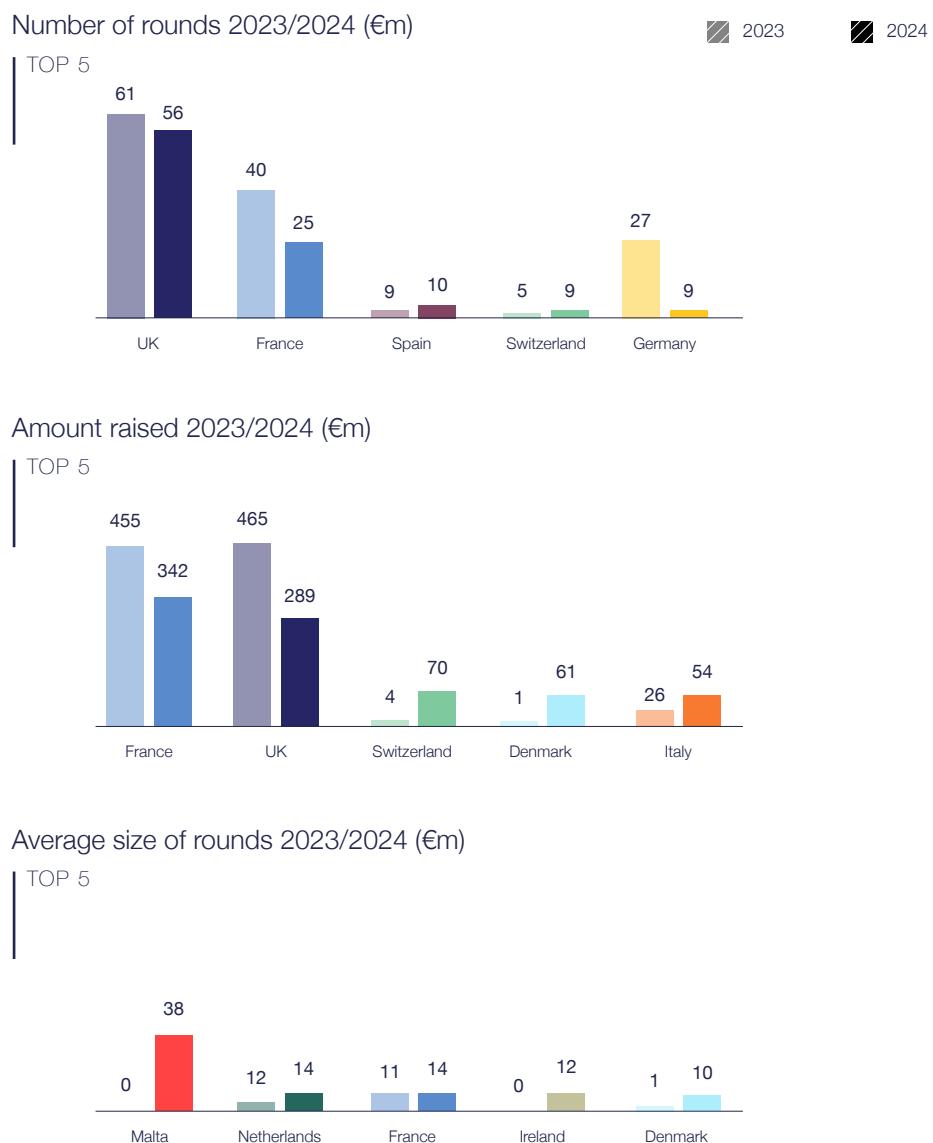
As mentioned previously, the amounts raised in 2024 were 25% lower than in 2023 – mainly due to the 16% fall in the number of deals over the same period.



FOCUS 2024

Despite the trends seen on the European cybersecurity market in 2024, France proved itself to be a big hitter in the continent's financing of the industry. It ranked first by amount raised, second by number of deals and third by average size of rounds, which at €14 million was higher than in 2023.

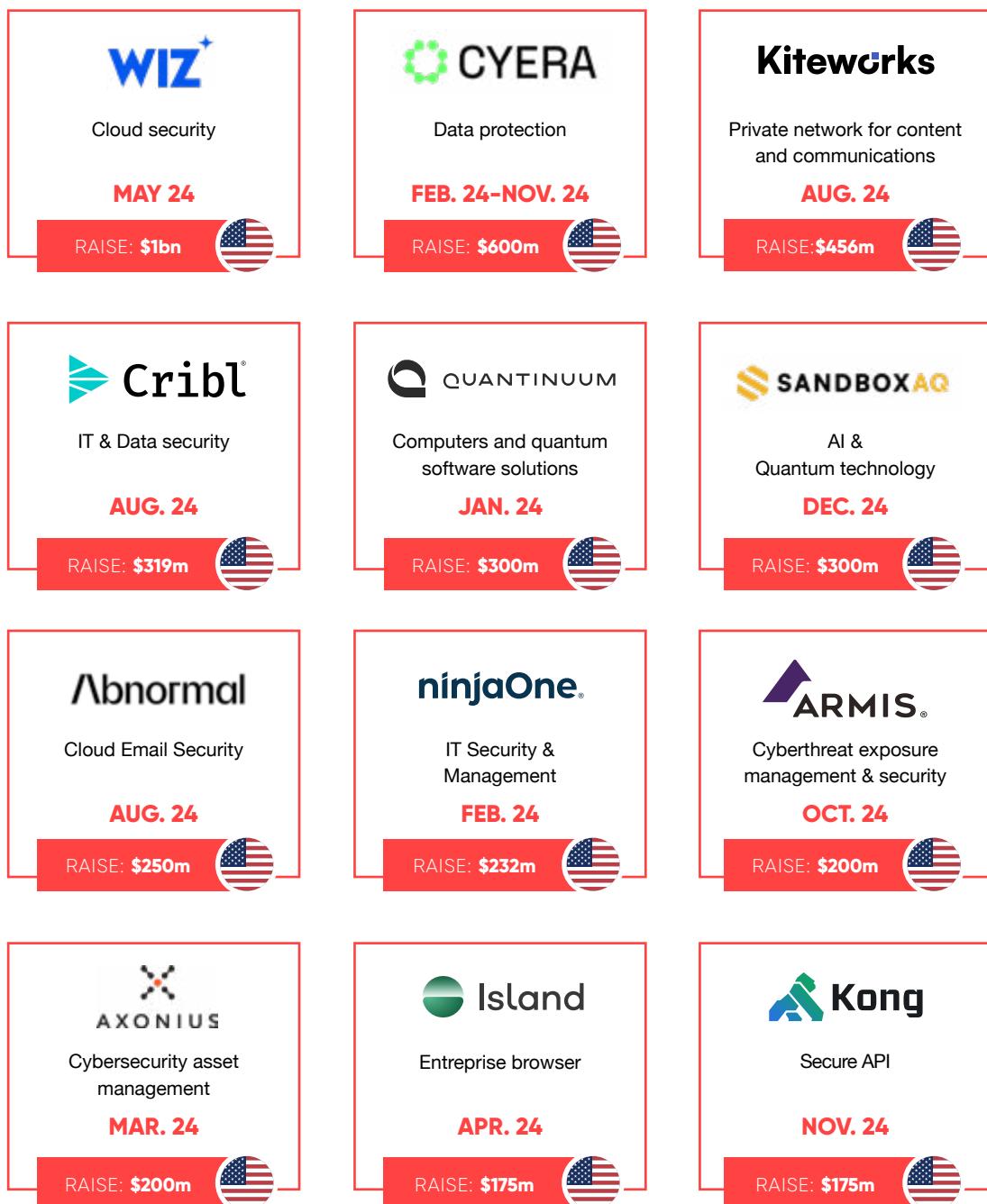
This performance contrasts with that of the UK, which for the second consecutive year recorded a sharp drop in the total amount raised (-37% vs. 2023) and number of transactions, even if it did retain its lead.



2024

THE LARGEST GLOBAL CYBERSECURITY FUNDRAISINGS

The world's 12 biggest rounds of cybersecurity fundraising in 2024 were all completed by US companies and added up to €4 billion, almost twice the level of 2023.

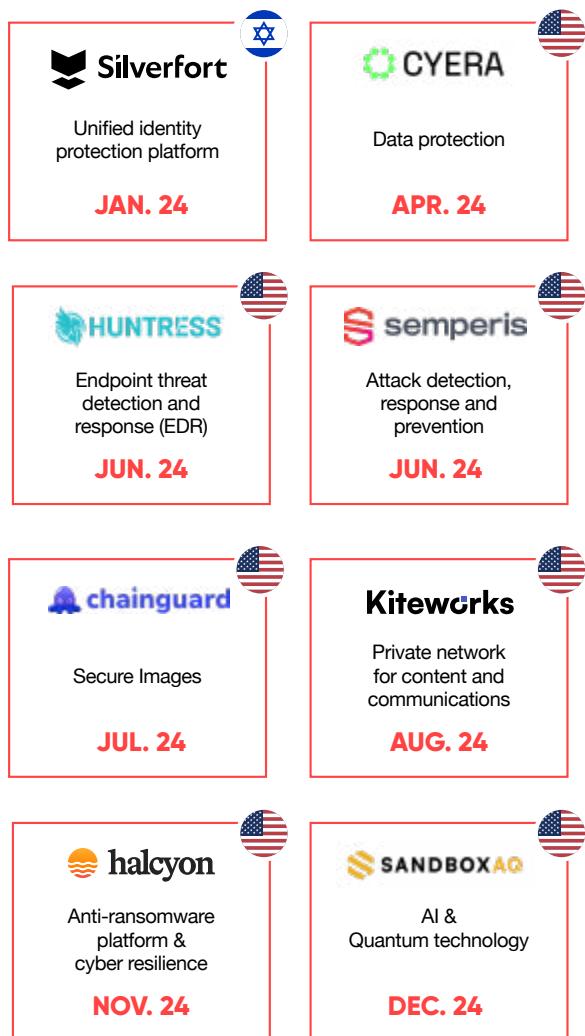


 Rest of the world  Europe

2024

THE NEW GLOBAL CYBERSECURITY UNICORNS

The number of new cybersecurity companies achieving unicorn status globally (with a valuation of over \$1 billion) dropped 7-fold between 2022 and 2023. 2024 saw a doubling of the number of new unicorns versus 2023, with 8 new companies.



2024

CYBERSECURITY FUNDRAISING IN FRANCE

25 ROUNDS OF FRENCH CYBERSECURITY FUNDRAISING ANNOUNCED IN 2024

EDAMAME TECHNOLOGIES €0.4m JAN. 2024 BA	Tenacy €6m JAN. 2024 kreaxi	alegoonie €1.4m FEB. 2024 bpifrance	Filigran €15m & €32.3m FEB. 2024 & OCT. 2024 Accel	LookUp N/A FEB. 2024 N/A
ZAMA €67m MARCH 2024 Accel	mindflow €5m MARCH 2024 suriga cyber	nijta €2.1m MARCH 2024 elaia	ANOZR WAY €6m MARCH 2024 D	Kamaé €1.4m MARCH 2024 SUPER CAPITAL
BforeAI €14.4m & €9.6m APRIL 2024 & DEC. 2024 SYNTHETIC TITANUM	ipeeo €1.8m MAY 2024 D	Finovox €3.9m JUNE 2024 shopr ventures	YesWeHack €26m JUNE 2024 Adelie.	soteria €0.8m JULY 2024 bpifrance
alphaguard €0.2m AUG. 2024 ANTLER	Patrwl €11m SEPT. 2024 SWEN CAPITAL PARTNERS	:probabl. €5.5m SEPT. 2024 bpifrance	dotfile €6m SEPT. 2024 SEAYA	stoïk €25m OCT. 2024 alven
CHAPSVISION DATA MAKE SENSE €85m NOV. 2024 bpifrance Qualium GENEO	Daspren €1m NOV. 2024 N/A	Dfns €15m DEC. 2024 FURTHER		

2023

CYBERSECURITY FUNDRAISING IN FRANCE

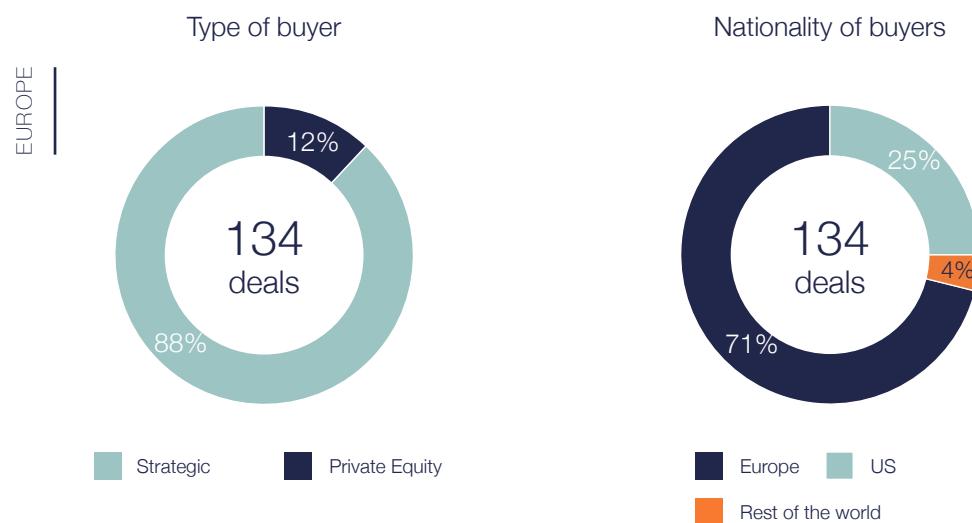
40 ROUNDS OF FRENCH CYBERSECURITY FUNDRAISING ANNOUNCED IN 2023



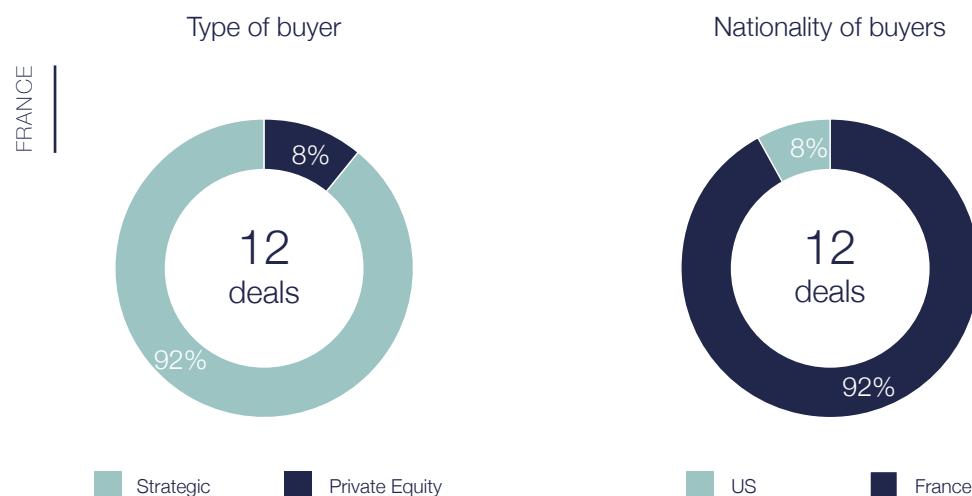
ACQUISITIONS AND CONSOLIDATION IN 2024

FOCUS ON EUROPE AND FRANCE

In 2024, 134 European cybersecurity companies were acquired by another company or by a private equity fund, i.e. a 19% increase on 2023. A large majority of 88% of these acquisitions were executed as part of consolidation strategies. Over two thirds (71%) were carried out by European actors.



France recorded 12 acquisitions in the field of cybersecurity in 2024, 92% of which were completed by strategic buyers. The number of acquisitions was up 33% on 2023. The majority of acquisitions were made by French companies (92%). 2024 was particularly notable for the reorganisation of I-TRACING's share ownership, based on a reported valuation of more than €500 million.



CONCLUSION

After 2023 brought a decline in cybersecurity investment due to adverse economic conditions, 2024 stood out thanks to the renewed dominance of the US. Although the total number of rounds dropped by 14%, the amount invested grew by 30% across all regions studied, reflecting a focus on more mature companies.

The US confirmed its leadership with a number of massive rounds and a strong tendency towards higher series (C, D and E), whereas Israel suffered a steep fall in its investments due to geopolitical tensions. In France, a drop in the number of rounds to 25 from 40 in 2023 correlated with the significant decrease in the total amount raised in 2024: down 25% on the previous year. France nevertheless showed resilience in 2024, retaining its unique position in the European cybersecurity ecosystem.

The European cybersecurity market has remained a key investment opportunity over the past decade with a 1.6x increase in the number of fundraising rounds and 12.5x rise in amounts invested. These trends show a changing industry – one that is still attractive, despite complex global economic conditions – and confirm the market's shift towards financing companies that are in the advanced stages of growth.

134 European cybersecurity companies were bought out in 2024, 71% of them by European investors; this shows a 19% increase on 2023. 12 acquisitions went ahead in France, with 92% of these completed by French companies. This illustrates the industry's consolidation at a national level.

ABOUT INCYBER FORUM



Organized since 2013 by CEIS, 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



Valérie SUEUR
vsueur@tikehaucapital.com

Tel.: +33 (0)1 40 06 39 30

image sept

Juliette MOURARET
jmouraret@image7.fr

Tel.: +33 (0)1 53 70 74 70



Charles CITROËN
charles.citroen@forum-incyber.com
Tel.: +33 (0)1 40 17 91 28



en partenariat avec

IN CYBER
FORUM