Mapping of Cybersecurity Start-ups in Europe

2023
APRIL

Skopai
AI Power to Find Start-ups

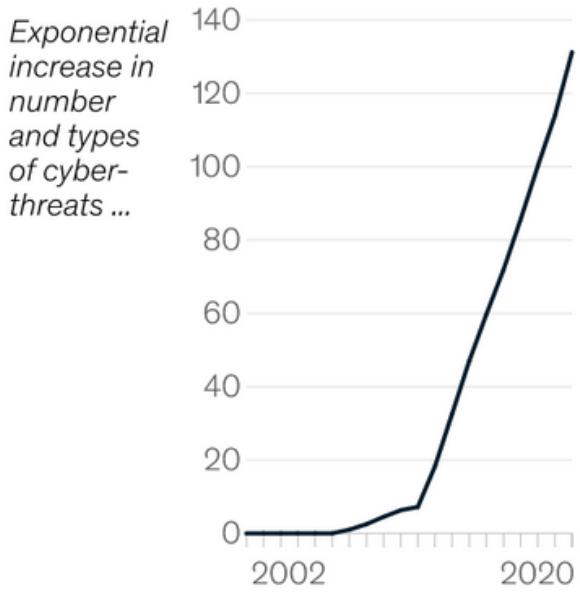
CYBERTHREATS ARE ON THE RISE

Cybersecurity threats are rapidly increasing in sophistication as attackers use new techniques and social engineering to extort money from organizations and users, disrupt business processes, and steal or destroy sensitive information.

According to a recent IBM report, **the average cost of a data breach in the United States is $9.44 million**. **Worldwide, the average price tag of an enterprise breach is $4.35 million.** As noted by McKinsey, the costs related to cybercrime **increase by 15%** every year. Over the last years, there has been an exponential increase in the number and types of cyberthreats. Furthermore, spending on cybersecurity has shifted from preventing cyberattacks to actively managing ongoing ones.

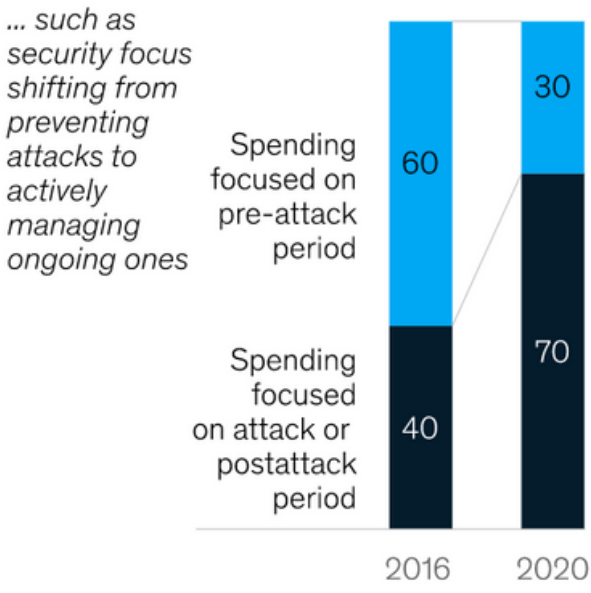
UNIQUE MALWARE STRAINS

Millions $



SPENDING ON CYBERSECURITY

% share



Source: McKinsey

Accelerated digitalization of businesses and more sophisticated IT systems to support digital processes, improve customer experience, and generate value create potential new vulnerabilities. The scope of the threat is growing and organizations are looking to reinforce their defensive capabilities to ensure the resilience.

CYBERSECURITY TECHNOLOGY AGAINST THREATS

Cybersecurity is protecting critical systems and sensitive information from digital attacks. Also known as information technology (IT) security, cybersecurity measures are designed to combat threats against networked systems and applications, whether they originate from inside or outside an organization.

Cybersecurity's importance is on the rise. Fundamentally, our society is more technologically reliant than ever, and there is no sign that this trend will slow. Data leaks that could result in identity theft are now publicly posted on social media accounts. In addition, sensitive information like social security numbers, credit card information, and bank account details are now stored in cloud storage services like Dropbox or Google Drive.

Cybersecurity is crucial for enterprises. They need cybersecurity to protect themselves from opportunistic hackers and thieves looking to steal data, sabotage systems, and extort funds. In the event of an attack, the damage can expand to include:

- Monetary losses
- Sullied business relationships
- A poor reputation among customers and across the industry

The fact is that computer systems are indispensable at every turn, whether for individuals, small businesses or large multinational corporations. Add to this the rise of cloud services, poor cloud service security, smartphones, and the Internet of Things (IoT). Numerous potential security vulnerabilities in today's Internet world did not exist decades ago.

PANORAMIC VIEW OF 1,300+ CYBERSECURITY START-UPS IN EUROPE

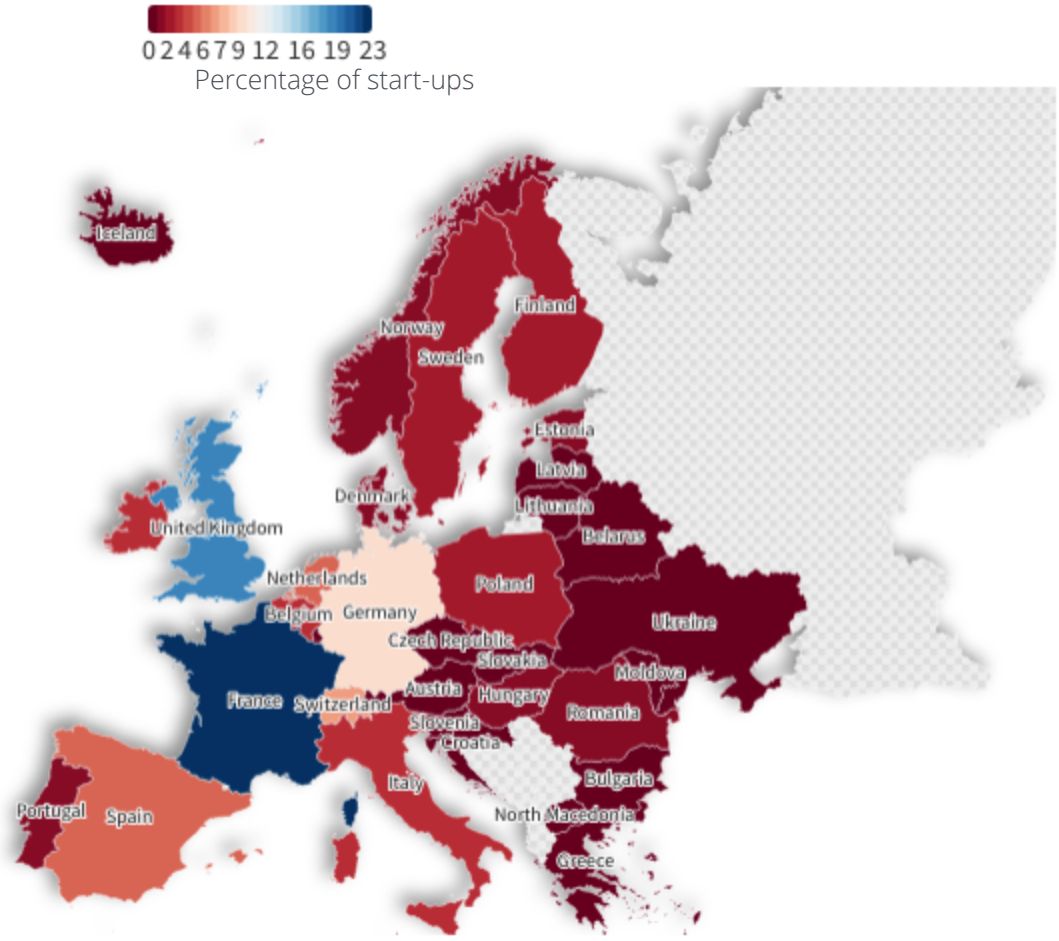
The mapping of European cybersecurity start-ups is based on the data on **more than 1,300 start-ups** listed on the Skopai platform in March 2023. These companies have their headquarters in Europe, were created after year 2010, develop cybersecurity solutions, and employ less than 500 employees. This report presents an overview of the current landscape of cybersecurity start-ups in Europe with a particular focus on French start-ups.

The analyzed start-ups are spread across **36 countries.** The most presented countries include **France (22.8%)** and the **United Kingdom (18.3%),** followed by **Germany (9.5%), Switzerland (6.5%), Spain (5.4%),** and the **Netherlands (5.3%),** among others.

All the information on the basis of this report, including **the profiles of more than 1,300 European cybersecurity start-ups**, can be accessed here:

- New user : link
- Skopai user: link

HEADQUARTERS OF CYBERSECURITY START-UPS



Note : Based on the data on 1,314 start-ups. The number of start-ups is defined according to the availability of public data.

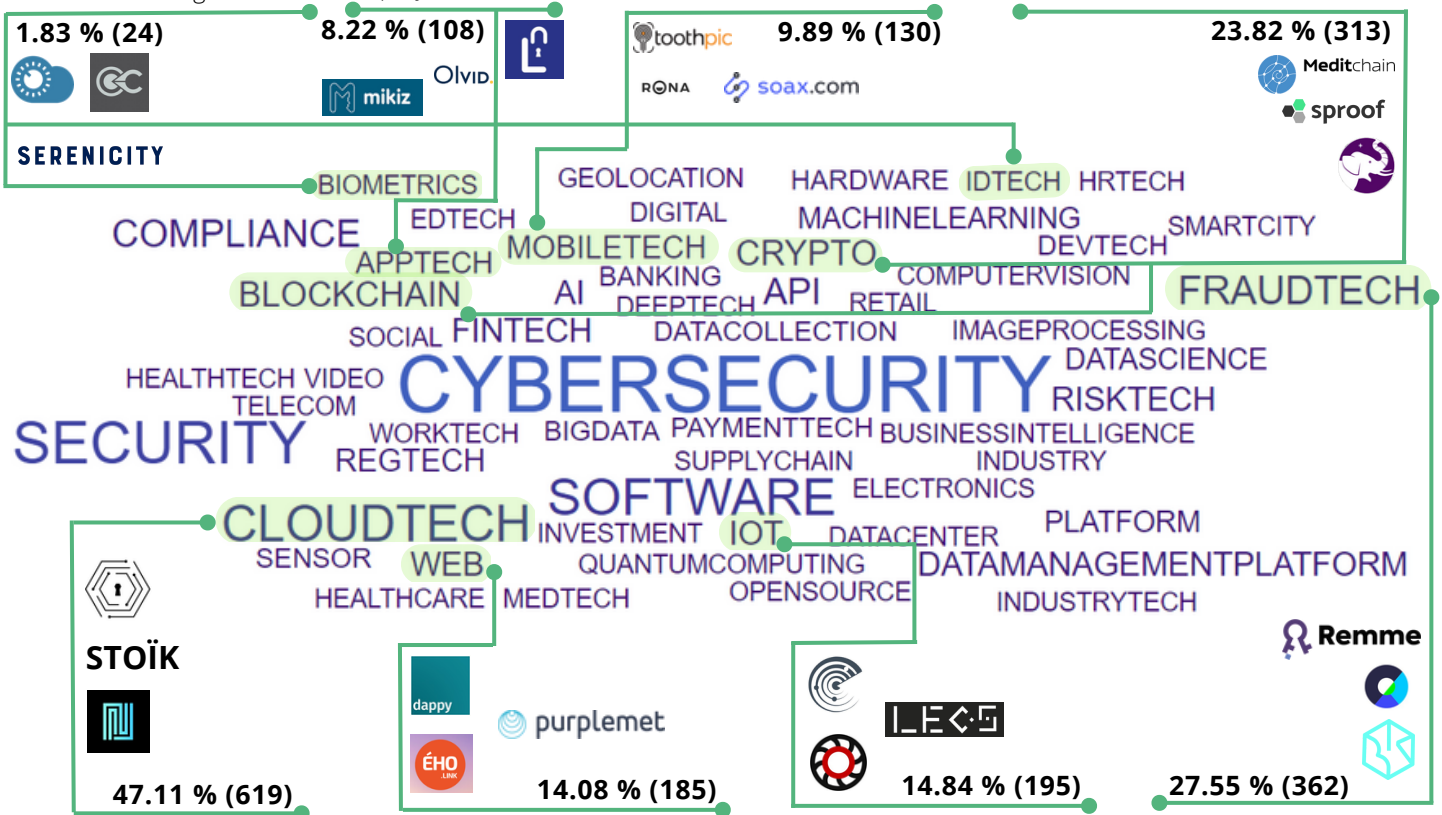
INNOVATION MAP OF CYBERSECURITY START-UPS

Identity and access management (IAM) is a cybersecurity discipline that manages user identities and access permissions on a computer network. The goal of any IAM initiative is to ensure that the right users and devices can access the right resources for the right reasons at the right time.

Application Security aims to protect software application code and data against cyberthreats. Application security should be applied during all phases of development, including design, development, and deployment.

Mobile Security or mobile device security is the protection of smartphones, tablets and laptops from threats associated with wireless computing.
The future of computers and communication lies with mobile devices. With ubiquitous wireless internet access, all varieties of mobile devices are becoming more vulnerable to attacks and data breaches.

- ***Blockchain*** is a secure database shared across a network of participants, where up-to-date information is available to all participants simultaneously.
- **Cryptography** is an important mechanism to secure information in computer systems. It is used in cybersecurity to design algorithms and other security measures that protect company data.



Cloud Security is a set of control-based security measures and technology protection designed to protect online stored resources from leakage, theft, and data loss. Security applications use software the same as SaaS (Software as a Service) model.

Website Security refers to the measures taken to secure a website from cyberattacks. That may include protecting a website from hackers, malware, scams or phishing, and errors. In this sense, website security is an ongoing process and an essential part of managing a website.

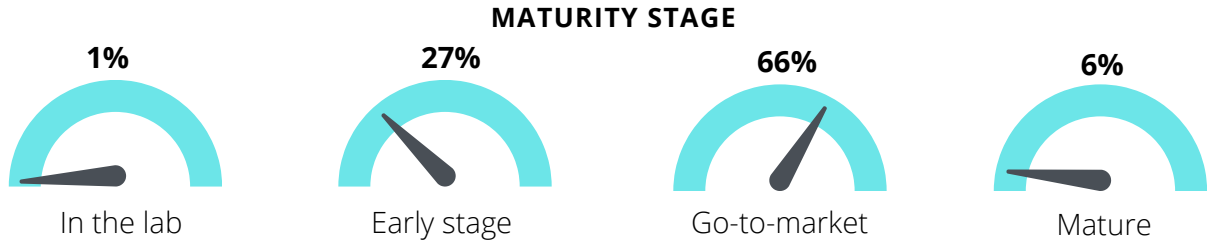
- ***IoT Security*** is the practice that keeps IoT systems safe.
- IoT Security tools protect from threats and breaches, identify and monitor risks and can help fix vulnerabilities.
- IoT Security ensures the IoT solution's availability, integrity, and confidentiality.

Anti-fraud is a service that identifies a fraudulent activity, including transaction fraud, online fraud, telephone fraud, card fraud and number theft. Online anti-fraud is an essential part of internet finance.

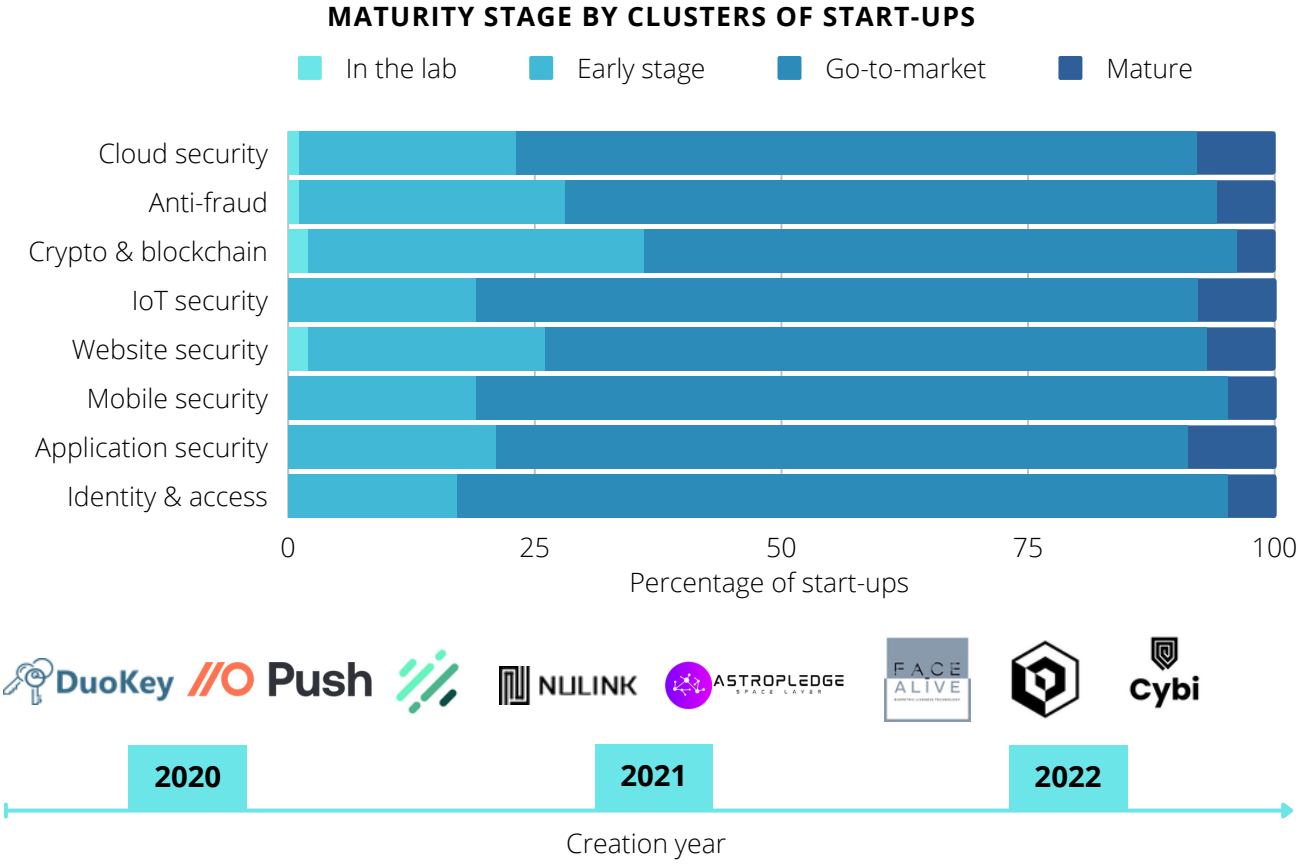
Note : Based on the data on 1,314 start-ups. The number of start-ups is defined according to the availability of public data.
A start-up can have several tags. The presented solutions and start-ups are non-exhaustive examples.

MATURITY STAGE

Most cybersecurity start-ups in the landscape are on the **go-to-market stage (65.9%)**: they have defined their markets and search for the first customers. More than a quarter of start-ups are on their **early stage (26.7%)**: they focus on product development and search for the initial funding. Observing the clusters of start-ups shows a similar pattern: in each cluster there are more go-to-market start-ups compared to other maturiy stages. Another observation is that start-ups using crypto and blockchain technologies are more present in the early stage of maturity compared to cybersecurity start-ups from other categories. Blockchain technology is one the most ground-breaking technologies in recent years. It offers a decentralized method of data storage and uses encryption to encode transaction information, which, as a result, enhances data security against breaches.



Note: Based on the data on 1,263 start-ups.

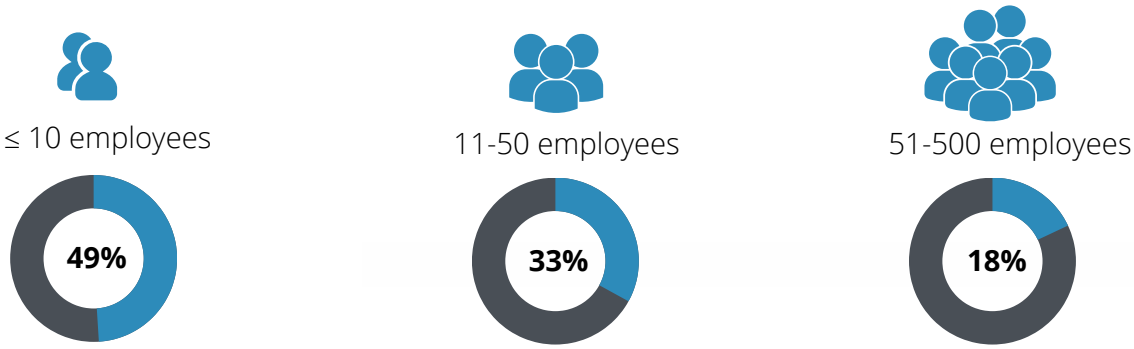


Note : One start-up can belong to several clusters. The presented start-ups are non-exhaustive examples. The number of start-ups is defined according to the availability of public data.

TEAM SIZE AND BUSINESS MODEL

In terms of team size, almost half of cybersecurity start-ups analyzed have **less than 10 employees (49.4%)** and one third of start-ups have **between 11 and 50 employees (32.7%).** Nearly 18% of companies are larger and employ between 51 and 500 employees.

TEAM SIZE



Note: Based on the data on 324 start-ups.

The dominant form of commercial transaction of European cybersecurity start-ups is **Business-to-Business (B2B, 93.2%)**. The data on business models show that the majority of start-ups operate in the sectors of **development and manufacturing (57.8%).** The share of start-ups with **SaaS** (software as a service) and **R+D+I Services** (Research, Development and Innovation/Industrialization) business models is equal (21% each).

BUSINESS MODEL

Note: Based on the data on 154 start-ups.

Seclab develops a hardware-based system enabling bi-directional communications between systems on the IT and OT networks and providing protection against network-layers attacks.

CyberSmart develops an all-in-one platform providing cybersecurity technology for small and medium businesses, and cyber insurance if things go wrong regardless.

QuBalt provides cryptographic algorithms and methods which protect against quantum and cryptanalysis attacks. Its solutions combine algorithms, software, hardware and intellectual property to meet specific security requirements.

Note: A start-up can have several business models. The number of start-ups is defined according to the availability of public data. The presented start-ups are non-exhaustive examples.

TECHNOLOGY AND PATENTS

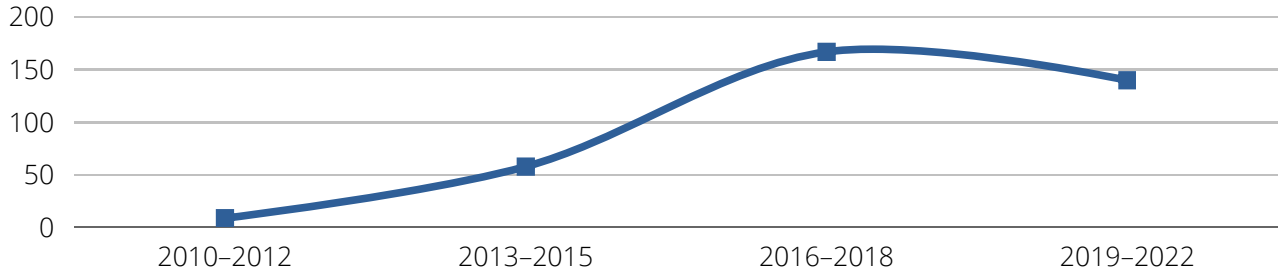
According to the data, **122 cybersecurity start-ups have filed patents**, which represent about 9% of the analyzed start-ups in the landscape. In total, **375 patent filings** have been registered by the start-ups, with an average of **3 patents per start-up**. The number of patents filed by the start-ups has generally a positive dymanics. The years between 2016 and 2018 have shown the most number of patent filings (167 patents). When considering the clusters of start-ups, most of the patented cybersecurity start-ups operate in the anti-fraud (145 patents), cloud security (117 patents), and crypto and blockchain (111 patents) domains.

122 (9%) start-ups with patent filings

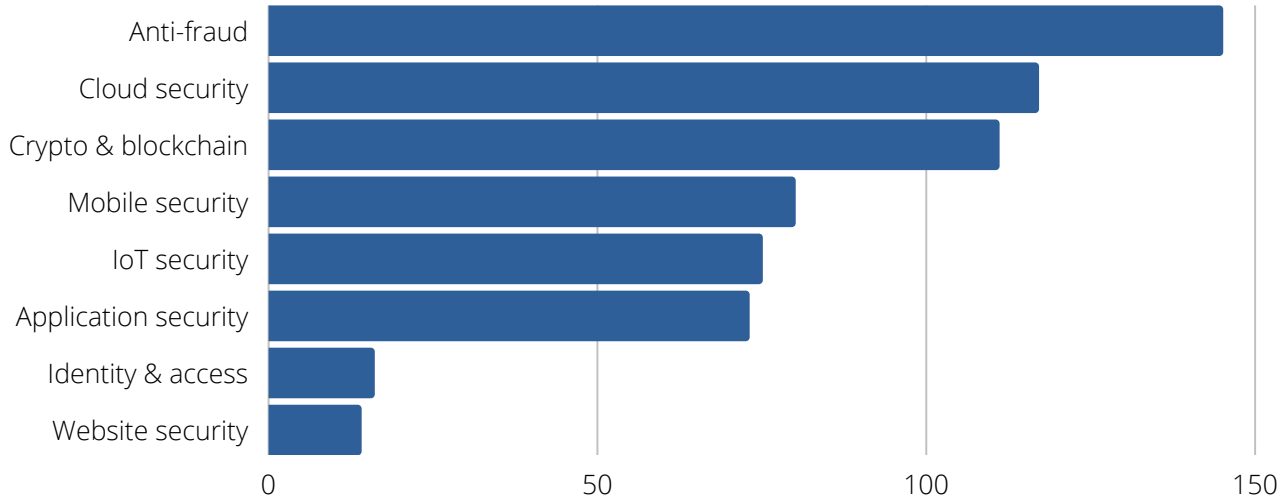
375 patent filings

3 average number of patents of start-ups

NUMBER OF PATENTS BY YEARS



NUMBER OF PATENTS BY CLUSTERS OF START-UPS

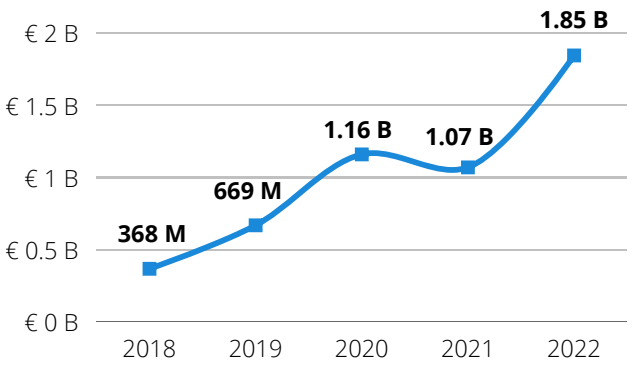


Note : One start-up can belong to several clusters.

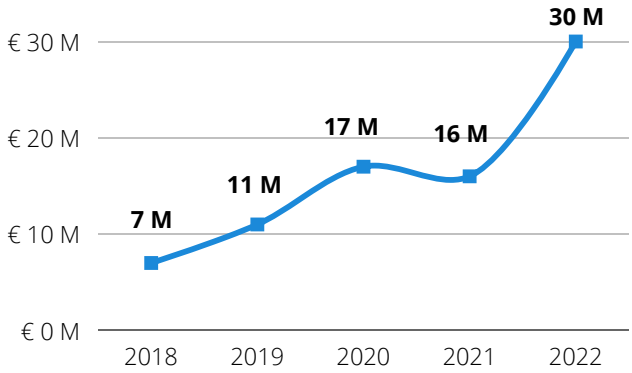
START-UP FUNDRAISING

According to the data, over the last five years (2018-2022), cybersecurity start-ups raised **more than 5 billion euros in funding**. There is generally a positive trend in total fundraising over time. In **2022**, start-ups in the landscape raised **1.85 billion euros** in funding which is more compared to the previous years. The average fundraising amount raised by cybersecurity start-ups has also been increasing over the last years and reached **30 million euros in 2022**. Start-ups operating in cloud security (€ 2.40 B), anti-fraud (€ 1.67 B), and crypto and blockchain (€ 1.28 B) domains raised more capital compared start-ups from other cybersecurity clusters, according to the data.

TOTAL FUNDRAISING, 2018-2022

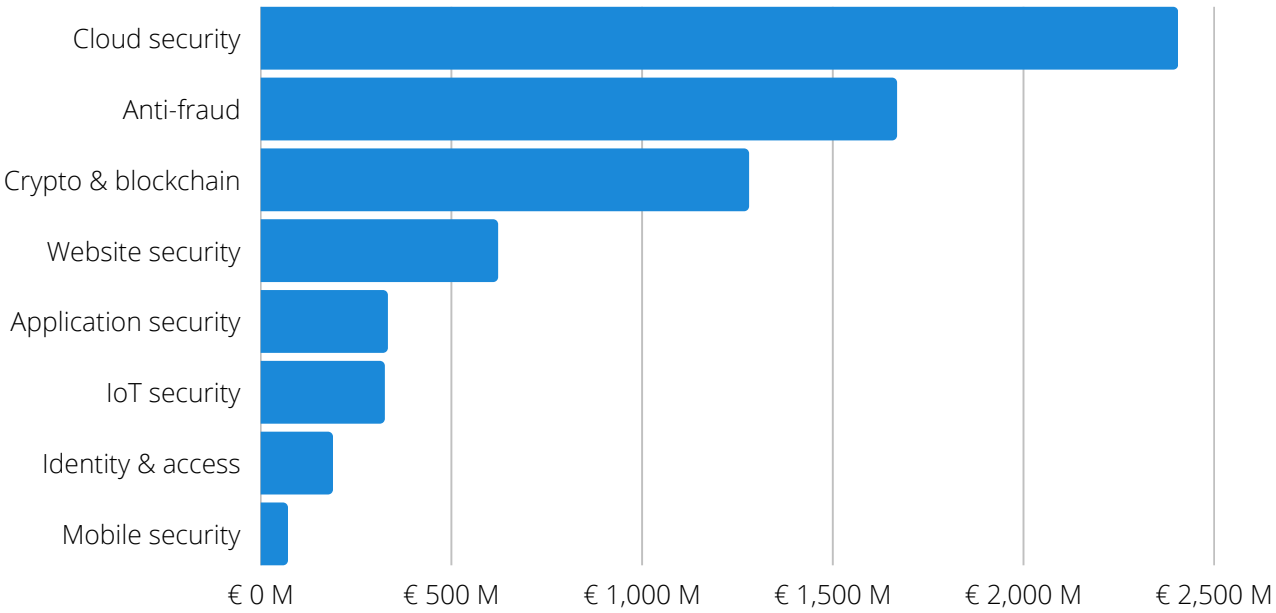


AVERAGE FUNDRAISING, 2018-2022



Note: Based on the data on 311 funding rounds of 210 start-ups.

TOTAL FUNDRAISING BY CLUSTER OF START-UPS, 2018-2022



Note : One start-up can belong to several clusters.
The number of start-ups is defined according to the availability of public data.

INVESTMENTS IN 2022

> 80 M €

In February 2022, **InterCloud** raised €100M in a Series D funding round. The new capital will drive international expansion plans through acquisitions and bolster its services offer. This round was led by Aleph Capital, with participation from existing investors Ventech and Open CNP

In April 2022, **SEON Fraud Fighters** raised $94M in a series B round to expand globally, led by private equity investment firm IVP. The round also included existing investors Creandum and PortfoLion and angel investing from founders and senior executives from several tech companies, including Coinbase, Wise and Slack

40-80 M €

In June 2022, **Upvest** raised $42M in a Series B funding round to provide the core banking infrastructure for finance companies behind-the-scenes. Bessemer Venture Partners led the round, along with Earlybird, ABN AMRO Ventures, Notion Capital, Partech, 10x Group, Speedinvest, and N26 cofounder Maximilian Tayenthal

In October 2022, **Immersive Labs** raised $66M in funding. Ten Eleven Ventures led the round with participation from Goldman Sachs Asset Management, Summit Partners, Insight Partners, Menlo Ventures, and Citi Ventures. The company intends to use the funds to continue its growth and investment in its Cyber Workforce Resilience platform

15-40 M €

In October 2022, **IriusRisk** raised $29M in Series B funding. The round was led by Paladin Capital Group, with participation from SwanLaab Venture Factory, BrightPixel Capital, 360 Capital and Inveready. The company intends to use the funds to expand globally further, focusing on the US and Asia Pacific markets

In June 2022, **CybSafe** closed a $28m Series B funding round. The round was led by Evolution Equity Partners, with participation from Emerald Development Managers and existing investors IQ Capital and Hannover Digital Investments (HDI) GmbH. The company intends to use the funds to accelerate its product development and expand into new geographies

5-15 M €

In June 2022, **Code Intelligence** raised $12M in Series A funding. Tola Capital led the round with participation from LBBW, Occident, Verve Ventures, HTGF and Thomas Dohmke, CEO of Github. The company intends to use the funds to invest in product development

In April 2022, **Beamy** secured €8.31M in a Series A round of funding. The Aglaé Ventures, ISAI, and Evolem funds led the current round. Beamy's solution can detect and control the explosion of SaaS applications used in a decentralised way

< 5 M €

In November 2022, **HOLM SECURITY** raised €4M in funding led by Subvenio Invest. The company intends to use the funds to enhance its platform, which is already enabling cyber-defence strategy for customers, covering both technical and human assets

In June 2022, **COSMIAN** raised €4.2m in funding. Backers included 115K, Elaia Partners, Guillaume Amblard, and the family-holding company Fiblac. The company intends to use the funds to accelerate the distribution of its first products and continue to innovate its solutions

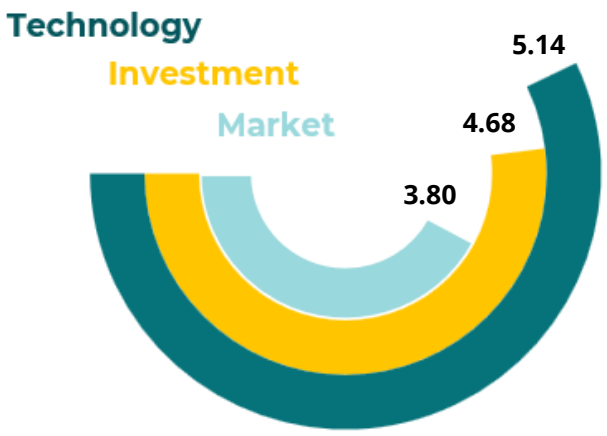
Note : The presented start-ups are non-exhaustive examples.

READINESS LEVELS OF CYBERSECURITY START-UPS

The readiness levels assess the maturity of technology, investment, and market of start-ups. The estimation is based on the methodology developed at NASA that enables consistent and uniform discussions of maturity across different types of technology. Each start-up is evaluated against the parameters for each dimension of technology, investment, and market on a 9-point scale (1-lowest, 9-highest).

On average, the analyzed cybersecurity start-ups are estimated to have **higher level of technology readiness (5.14)**, followed by **investment (4.68)** and **market (3.80) readiness levels**.

POSITION IN THE 3 DIMENSIONS: TECHNOLOGY, INVESTMENT AND MARKET



Technology Readiness Level

TRL 1: Basic principles observed and reported.
TRL 2: Potential application or solution validated.
TRL 3: Proof-of-concept demonstrated, analytically and/or experimentally or mock-up.
TRL 4: Component and/or breadboard and/or prototype laboratory validated or first tests.
TRL 5: Component and/or breadboard and/or prototype validated in simulated or real space environment or first market (pilot).
TRL 6: System or solution or service adequacy validated in simulated environment or in limited area.
TRL 7: System or solution service adequacy validated.
TRL 8: Focus on quality and cost.
TRL 9: Post market surveillance.

Investment Readiness Level

IRL 1: Team in place.
IRL 2: Potential application or solution validated.
IRL 3: Attractive solution, solid IP.
IRL 4: Regulatory, certainty regarding difficulty.
IRL 5: Business model validated, first market pilot.
IRL 6: Recurrent revenue.
IRL 7: Profitable growth.
IRL 8: Focus on capacity, quality and cost.
IRL 9: Post market surveillance.

Market Readiness Level

MRL 1: Need validated.
MRL 2: Potential application or solution validated.
MRL 3: Key competencies, regulatory or trials or tests for market access.
MRL 4: Pilot, first revenue.
MRL 5: Distribution or commercial partnerships, first recurrent revenue.
MRL 6: Recurrent revenue.
MRL 7: Profitable growth.
MRL 8: Focus on production ramp up.
MRL 9: Post market surveillance.

Note: Based on data on 1 175, 907, and 875 start-ups for technology, investment, and market readiness levels, respectively. The number of start-ups is defined according to the availability of public data.

INTERNATIONAL CYBERSECURITY FORUM - FIC 2023

Forum International de la Cybersécurité

Organized since 2013, the **International Cybersecurity Forum (FIC)** is Europe's leading event on digital security and trust issues, which brings together the main actors in cybersecurity ecosystem. The aim is twofold:

- to advance the construction of a digital future in line with European values
- to face the operational challenges of cybersecurity

In April 2023, 15th edition of FIC takes place in Lille, France, around the theme "In Cloud we trust?".

The **FIC Start-up Prize** aims to encourage innovation and entrepreneurship in the cybersecurity sector. Each year, the jury distinguishes the most innovative start-ups in the field. The 2023 FIC Start-up Prize selected **12 start-ups** out of 81 applications. Out of these finalists, 5 start-ups became the prize winners.

ANOZR WAY Start-up Prize

ANOZR WAY develops a platform to discover executives and employees vulnerabilities before attackers. Its solutions guide security team and users to mitigate human-related risks.

ASTRAN Jury's Favorite Prize

Astran develops Distributed data Vault designed for securing data with encryption keys, data encryption and data immutability.

bfore.ai

Bfore.Ai develops a software designed for predicting attacks before they occur.

computablefacts

ComputableFacts develops solutions to protect infrastructure and data from attackers.

Cybi

Cybi develops a platform to automatically reproduce all the attack paths identified within an information system to deduce an analysis of risks and propose treatment plans.

CYSEC

CYSEC develops technologies designed for confidential computing by protecting data in use by running critical applications in a trusted execution environment, mitigating the major business cyber risks.

Defants develops collaborative and automated solutions to accelerate DFIR and Threat Hunting missions through a semantic investigation-based approach.

defants

Dust Mobile develops end-to-end secured mobile communications solutions designed for protecting businesses and their most valuable assets from cyber threats.

dust MOBILE Jury Prize

Filigran develops cybersecurity and crisis response solutions designed for helping governments, large enterprises and service providers to manage and mitigate risks.

FILIGRAN Jury's Favorite Prize

Malizen develops all-in-one platform using data visualization and machine learning algorithms to accelerate cybersecurity operations.

Malizen

ONEKEY develops a platform for automated security and compliance analysis for industrial, manufacturing and IoT devices.

ONEKEY Cybersecurity for Industry Prize

Sarus develops an analytics and machine learning software to help data practitioners leverage the most sensitive data assets for innovation.

Sarus

METHODOLOGY

The study is based on the data on **1,314 cybersecurity start-ups in Europe**, presented on the Skopai platform and extracted in March 2023. The data on start-ups are collected from sources publicly available on the internet, using data science and AI algorithms.

CRITERIA

Europe

Solutions for **cybersecurity,** excluding consulting start-ups

Created **after 2010**

Employ **less than 500 employees**

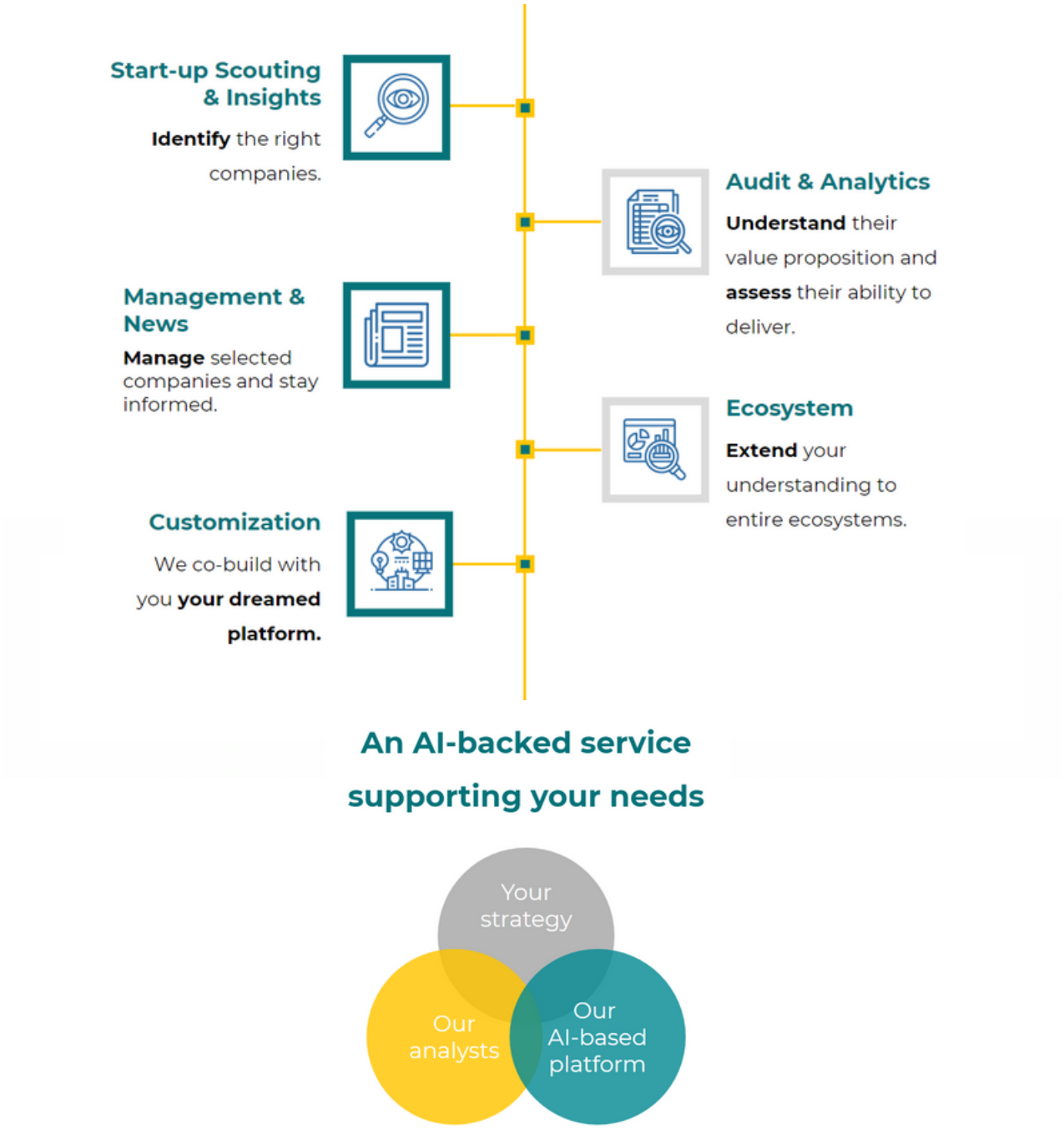
List of European cybersecurity start-ups

All the information on the basis of this report, including the profiles of more than 1,300 cybersecurity start-ups in Europe, can be accessed here:

- New user: link
- Skopai user: link

BIG DATA AND AI TO CAPTURE THE NUMBER AND DYNAMICS OF START-UPS

Skopai intelligence and innovation platform offers a full set of comprehensive and qualified real-time information on start-ups worldwide. Using the validated methodology and machine learning algorithms, the Skopai platform helps discover, monitor and evaluate technology companies and innovation ecosystems across all sectors by providing accurate and reliable information in real-time.



SKOPAI



CONTACTS

Tatiana Beliaeva
Senior Entrepreneurship Researcher
Skopai
tatiana.beliaeva@skopai.com

Zhen Huang
Innovation Analyst Intern
Skopai
zhen.huang@skopai.com

www.skopai.com

Skopai
AI Power to Find Start-ups