European
Champions Alliance

Cybersecurity Whitepaper

Threats and challenges of the European Cybersecurity Landscape in 2022

2022

TABLE OF CONTENTS

Introduction

Dominique Tessier

Dear reader,
Thank you for reading the last White Paper of the European Champions Alliance on Cybersecurity.

This white paper reflects some of the ideas set forward by the ECA Cybersecurity Focus Group during our campaign on European Cybersecurity industry, between September 2021 and February 2022. During that period, it became obvious that Cybercrime was not only about fund extortion but in some cases could be a piece of warfare. The new circumstances with the massive military attack of Ukraine by Russia have, alas, shown how this idea of cyber attacks being part of warfare is sadly true.
It also shows how much we need an European response, including a strong independent Cybersecurity industry, part of our strategic independence. This is no task for « the next year ». It is a compelling emergency.

This document's objective is to present the capabilities of the European Cybersecurity industry, in a time when Cyber crime has never been so active and, alas frequently, successful.
Cybercrime has now become a modern pandemia. In 2021 only, more than 5 000 billion € will have been lost due to it, and the cost is slated to amount to more than 8 000 billion € in 2025. Across the world, no organization, no company, can ignore this threat : hospitals as well as cities have been attacked, especially during the Covid crisis, and the same for many private players; large US suppliers, such as Solarwinds or Kaseya, have been compromised, leading to malicious attacks against thousands of companies …
On the other side, some brighter news : the response is ready. Altogether, European Cybersecurity companies provide a wide scope of functions to stop all of these attacks, they cover the full range of cyberthreats: from industrial control systems to ID and access management to automatized threat detection and response, and more. Their technical basis is sound and proven. Their capabilities to scale up large deployments and support are tested. Moreover, they comply to high level certification standards, as well as to an European regulation which protect the use of data and specifically of personal data.

Last but not the least, as the borders between cupidity-moved hackers and state-backed actors are often blurred, supporting European alternatives is also meant to ensure freedom of choice and strategic autonomy in the future.
This White paper's purpose is to present the different segments of the European Cybersecurity offering. As such it is based on statements and stories by those suppliers which are campaigning with the ECA to promote the industry. These documents exemplify the level of performance and the capabilities which we trust the European Cybersecurity industry has reached.
We hope that readers will find here useful information and be reassured, if necessary, in respect to the maturity of the European Cybersecurity offering.

Dominique Tessier
ECA Head of Cybersecurity Focus group

Aim of the Paper

Who we are?

The European Champions Alliance is a not-for-profit association created in February 2020 that builds an ecosystem of start-ups, scale-ups, SMEs, corporates, and industry experts committed to European Tech and values. The Alliance leverages its European network by sharing market knowledge and activating joint business opportunities between the members to support the growth of European Champions. We do this in several focus groups, for example, Cybersecurity, Smart Industry, Mobility, Innovation & Governance, and now also Space Tech. For more information please have a look at our website www.european-champions.org or see the Linkedin button at the end of the page.

Why did we create that Paper?

The whole Cybersecurity campaign, on which this paper is based, was initiated to generate more attention for European companies, point out common/serious problems, and generally create a high-quality document that gives an idea. The ECA has given 9 core messages and asked members of the Cybersecurity Campaign to write a short article on 1 to 2 core messages each. The result of these articles can be seen on the following pages of this paper.

At this point, we would like to thank all members who participated and contributed one or even more articles.

Table of contents: Articles

Topics of Choice (9 messages about European Cybersecurity)

01. Innovation

European cybersecurity Companies (ECCs) are innovative and mature. In an environment of fast-growing and industrialized cybercrime, ECCs will help develop businesses in a secure way.

02. Full range

Taken together, ECCs cover the full range of cyber threats:from industrial control systems to IT systems to ID and access management to threat detection and response, etc.

03. Proven robust

ECCs products are tested in real and critical conditions and have been proven robust.

04. Experience

ECCs have grown from experience. They are ready to scale and deliver enterprise-grade products and support large scale deployment and maintenance.

05. Customer proximity

ECCs are close to their customers, understand their requests and are ready to implement those quickly. They have developed customer success programs and work hand in hand with their customer base.

06. Certification & standards

ECCs live in an environment of high-level and demanding certifications, providing a technical and quality standards warranty. Ongoing evolution towards European-level certification criteria increases pan-European validity of such warranty.

07. Compliance

ECCs comply with EU regulations and transparency values. This is a must at a time where both national authorities and C-Level are more and more sensitive to regulatory issues.

08. Need for sovereignty

While we see that cybercrime borders are often blurred between cupidity-moved hackers and state-backed actors, sovereign cyber solutions are a necessity to protect against all malicious attacks. Supporting European alternatives is also meant to ensure freedom of choice in the future.

09. Integrated ecosystem

ECCs are working hard to create a cyber shield, they are open to operate as an integrated ecosystem to improve the value offered to European companies and to prevent the disruption of their operations

Advens

published on blog

Benjamin Leroux

Messages we wanted to illustrate:

2. Taken together, European Cybersecurity Companies cover the whole range of Cyberthreats: from industrial control systems to IT systems, from ID and access management to threat detection and response, from on-prem to cloud environment, from mobile devices to workstations.
3. European Cybersecurity Companies have matured and learned from numerous experiences. They are fit for scaling up, deliver enterprise-grade products as well as services, and support large-scale deployment and maintenance

Our story

Advens: helping our customers to face cyber-attacks

Advens is the first French cybersecurity pure player. For more than twenty years, our services have helped numerous organisations (private companies and public service agencies) to define, enhance and implement their cybersecurity policy. We serve 300+ customers in France and we began our European growth with Benelux.

Our services cover a large range of cybersecurity challenges. We wanted to share the way we helped many organisations to face ransomware attacks in 2020 and 2021. While under attack, an organisation has reached us to get some urgent assistance. Our CERT (Computer Emergency Response Team) has been involved to handle the crisis (EMOTET malware infection). Our experts directly went to the victim offices to understand the situation, get required information to perform the investigations and define the right reaction process. We managed the crisis hand in hand with the organisation (that quickly became a new Advens client). From media & communication guidelines to forensic operations, our CERT has been present 24/24 during the first days of the attack.

We quickly identified the need for a solution to gain visibility on the attacked perimeter. That's why our team deployed an EDR (Endpoint Detection & Response) provided by one of our editors' partners. Within 3 days, the whole list of assets (PC and servers) was protected by the EDR. It really helped to understand the attack and get the list of infected assets. But it has been more than useful for the reaction as EDR provides efficient features to block an attack and protect IT systems.

Considering the effectiveness of the solution, and the need to strengthen their detect & react capabilities, the attacked organization quickly decided to keep its EDR. They asked Advens to manage the solution through Advens Security-as-a-Service approach based on our SOC. We provide a global and comprehensive service to protect an organization and to help handle security events and incidents. EDR-as-a-Service, a service line of our Advens Security-as-a-Service offering, is an efficient and agile way to protect your endpoints, and to lay the cornerstone of a modern SOC and a powerful Cyber-defence.

Stormshield

both articles published on blog

Pierre-Yves Hentzen

European Cybersecurity Companies live in a context of high level and demanding certifications. That provides a warranty on technical issues but also on quality standards shaping the action of our companies. The ongoing evolution towards European-grade certification criteria will make such a warranty valid across Europe.

In order to ensure their critical mission, cybersecurity solutions are positioned at strategic points in a network or an information system; these solutions often have elevated rights and are placed as close as possible to the most sensitive resources, often without any gatekeeper. Thus, any weakness or vulnerability in these solutions is a major risk since it provides a direct point of access to protected resources. Protection systems must offer assurances of robustness and quality and, therefore, be considered to be trustworthy. For this, it is necessary to rely on technologies that are part of a continuous certification and qualification process.

With its first official certification obtained in 2004, Stormshield is fully engaged in this dynamic. Our trusted technologies are qualified and certified at the highest European level for VPN and Firewall products, with certificates and labels issued by French, Dutch, Spanish, NATO and EU institutions. Some of the related assessments go far beyond an external test of the product's security, integrating code audits and a review of design, development and vulnerability patch management processes. The proven robustness of our products enables us to support organisations and companies with extreme criticality regarding cybersecurity issues. Based on our strong experience in this field, we have been invited by the European Union Agency for Cybersecurity, ENISA, to work on the definition of the European product certification scheme, within the framework of the European Cybersecurity Act. This initiative is aimed to elevate the level of trust in technology, in a harmonized manner, within Europe.

While we see that Cybercrime borders are often blurred between cupidity-moved hackers and state-backed actors, sovereign Cyber solutions are a necessity to protect against all malicious attacks. Supporting European alternatives is also meant to ensure freedom of choice for the future.

In cyberspace, relations between the superpowers are strained. It is now impossible to talk about digital and telecommunications without thinking about politics and geopolitics. Between an ultra-controlled American model advocating extraterritoriality (e.g. Cloud Act) and closed or locked Chinese and Russian models (e.g. China's Great Firewall), Europe is looking for a third way, based on values of transparency, openness and protection of individual freedoms (e.g. GDPR).

In recent years, we have seen the various State-sponsored digital attack and defence strategies of the major international powers taking shape under the guise of cybersecurity. Cyber warfare is under way, as Florence Parly, French Minister of the Armed Forces, stated in January 2019. Controlling one's means of protection is becoming a strategic priority. This doesn't only affect state organizations; companies are also targeted. Even small businesses are affected, because they are often part of an ecosystem and can serve as an entry point for rebounds on the information system of a major client or one of their partners.
This shows that the origin of technologies, especially those that handle or protect sensitive data or those that secure vital and critical infrastructures, is paramount. Companies and organizations must therefore take this strategic factor into account in their reasoning before entrusting the security keys of their information system to a supplier. Relying on trusted European technologies allows EU companies and organisations to retain control over their protection and to make sure that efficient alternatives will remain.
Stormshield is a leading European cybersecurity company and the 1st French cybersecurity vendor* providing trusted products to protect IT and OT networks, endpoints and data. Stormshield is a subsidiary of the greatest European Industrial success, Airbus and is serving more than 17 000 customers worldwide. Our R&D is 100% located in France. The mission of our 400 passionate employees is to ensure cyber-serenity for organizations and companies operating critical and operational infrastructures, so that theses businesses can focus, with full peace of mind, on their core activities.

More from Stormshield

both articles published on blog

Will European digital sovereignty come soon?

For several years now, the issue of European digital sovereignty is back in the technological spotlights. And while Europe has a number of assets to move in this direction, what is (still) missing to finally witness the emergence of European digital sovereignty?

Digital sovereignty: Europe's assets

Espionage, backdoors, supra-national laws...: the climate of the last few years shows that we have every interest in assessing our confidence in the cybersecurity products we use. Today more than ever, each country must be able to ensure the security of its digital assets, to protect its economic and strategic interests. This current situation should encourage us to think about the solutions to be put in place at European level.

And it's clear that we already have solid assets for a strong digital Europe. On the one hand, the certifications and qualifications of the national agencies of leading countries such as France, Germany and Spain are recognised on the international scene and are a guarantee of quality, trust and security. On the other hand, a common regulatory framework has been structured with the NIS (Network and Information Security) Directive, the General Data Protection Regulation (GDPR) and the recent Cybersecurity Act. An obvious help to shape the notion of digital trust at European level in the wake of the European Network and Information Security Agency (ENISA).

When will European champions emerge?

But these first steps towards European cooperation remains still tentative. And among the major challenges awaiting Europe on the road to digital sovereignty, the ability to bring about the emergence of genuine European cybersecurity champions is one of the greatest. Digital sovereignty is also a financial and commercial issue, to give European players the means to compete with their international counterparts on the basis of a commercial and marketing strike force. To achieve this, the protection of European unicorns and the creation of a true common European digital market are essential steps.

Beyond equal or even superior performance, the challenge is to gain the trust of cybersecurity solutions users. Europe's digital sovereignty can only really be achieved at the price of this trust. In the end, this is the most precious intangible asset in these times of widespread suspicion.

Stormshield Linkedin Flagship ideas

Among the major challenges awaiting Europe on the road to digital sovereignty, the ability to bring about the emergence of genuine European cybersecurity champions is one of the greatest.

Or

Digital sovereignty is also a financial and commercial issue, to give European players the means to compete with their international counterparts on the basis of a commercial and marketing strike force.

Or

The challenge is to gain the trust of cybersecurity solutions users. Europe's digital sovereignty can only really be achieved at the price of this trust. In the end, this is the most precious intangible asset in these times of widespread suspicion.

YES WE HACK

published on blog

Rayna Stamboliyska

ECA Messages

1. European Cybersecurity Companies are innovative and mature. In the context of a fast-growing and industrialized cybercrime, European Cybersecurity Companies will help you develop your business in a secure way. You will not face operation disruption, loss of data, or loss of competitive advantage. You will deliver your projects without waking up at night.

5. European Cybersecurity Companies are close to their customers. They understand their specific expectations, they are ready to listen and to incorporate Customers' requests as quickly as possible. They have developed a Customer Success Program and work hand in hand with their customer base on their roadmap.

7. European Cybersecurity Companies comply with the EU regulations and transparency values. That means no unnecessary data capture, no Cloud Act, no backdoors, compliance with GDPR. It is a must at a time where both national Authorities and C-Level are more and more sensitive to regulatory issues.

--- YesWeHack response ---

Summary_

Critical sectors and organisations are the targets of growing cyber threats. A 'cyber Cold War' with China and Russia on the one hand and the United States and Europe on the other is a trend of concern. Europe has the means to protect its institutions and companies: foster innovation in cybersecurity that predominantly benefits the Digital Single Market and strengthen investment capabilities to enable a robust cybersecurity ecosystem. YesWeHack is a striking example that bold innovation in cybersecurity is a winning bet in the European context.

Body_

The security of digital innovations is a primary concern for organisations and individuals alike. The number of connected digital services grows. And with it, the issue of vulnerability management is becoming increasingly urgent. Digital security risk undermines consumer trust and causes tremendous economic

and social costs; it is estimated to have a yearly global cost ranging between EUR 85 billion and 5 000 billion and is increasingly threatening individuals' safety.
Accordingly, the EU encourages the Member States to harmonise global cybersecurity policy through these regulatory commitments because the benefits are manifold. Thanks to common cybersecurity requirements inscribed in law, the European Union will create a unified market for its companies and enhance the level of expertise of the products. Moreover, organisations will no longer be restricted to their national market; instead, they will extend their offer to the entire European digital single market more efficiently.

New ways of testing the safety and quality of digital services emerge and establish themselves, bringing with them new possibilities to shape security and a fresh entrepreneurial dynamic. Bug Bounty, also known as crowdsourced security, is one such unique way. Bug Bounty leverages the collective knowledge and skillsets of the crowd to hunt for technical vulnerabilities and business logic errors alike. Ethical hackers thus make significant contributions to increasing digital security. Furthermore, Bug Bounty is an agile and easy-to-scale security testing model that fits organisations of all sizes and budget breadth.

Our clients understand that. For example, we have been instrumental in raising the security posture of a European world-renowned luxury brand with worldwide operations . Two months from the launch of this client's Bug Bounty programme, around 30 vulnerabilities have been identified, 60 percent of which have been corrected. This first glimpse of the Bug Bounty model enabled our customer to realise the extent of the flaws in their infrastructure. Now that our client has a clear understanding of how a Bug Bounty programme works, they are expanding its scope, increasing the rewards, and inviting new researchers. This first phase is essential to understand how researchers work and think and how best to implement effective vulnerability management across the relevant business lines.

Continuous monitoring of the information systems as occurring through Bug Bounty is an emerging standard. Identifying vulnerabilities at any moment of the product lifecycle is an essential step towards cyber risk reduction. Moreover, introducing a Coordinated Vulnerability Disclosure (CVD) programme is critical in limiting the cyber risk that has proven its worth worldwide.
YesWeHack has won the trust of hundreds of global companies as it focuses on creating stellar customer experiences and providing outstanding program results. From understanding the security requirements and designing customised programs to adapting the program to changing business requirements, our Customer Success Team sets YesWeHack apart. The platform's research & development and infrastructure are based in Europe, thus setting high-quality standards and providing unique data sovereignty guarantees.
Founded in 2015, YesWeHack is a Global Bug Bounty & VDP Platform. YesWeHack offers companies an innovative approach to cybersecurity with Bug Bounty, connecting more than

25,000 ethical hackers across 170 countries with organisations to secure their exposed scopes and reporting vulnerabilities in their websites, mobile apps, infrastructure and connected devices.

Nect

published on blog

Benny Bennet Jürgens

Message we wanted to illustrate:

European Cybersecurity Companies have matured and learned from numerous experiences. They are fit for scaling up, deliver enterprise-grade products as well as services, and support large-scale deployment and maintenance

Use Case:

2020 meant Nect's entry into e-government. The digitization of public administration had to be implemented unexpectedly at short notice in many areas due to the Corona pandemic. The Federal Employment Agency, for example, also had to act quickly and nevertheless in a customer-oriented manner. The challenge? The collapse in sales at many companies caused by the Corona pandemic had and still has serious consequences: Layoffs, short-time work and unemployment. As a result, the Federal Employment Agency had to deal with an above-average number of new registrations. At the same time, in-person office visits should be reduced as much as possible to curb Covid-19. Therefore, a digital solution for identifying applicants was needed. Not only did it have to be quick to implement and meet the high security requirements, it also had to be as intuitive to use as possible and flexibly scalable. Therefore, the decision was made in favor of Nect's Selfie-Ident. At that time, Nect was able to perform up to 3,500 successful identifications per hour by using their Robo-Ident technology. In the meantime, Nect has been able to increase this number to up to 5,000 per hour. Further adaptation is possible at any time. The Hamburg online magazine Hamburg News mentioned in their article that Nect has proven to be a supporter with its technology, during the crisis.
https://hamburgnews.hamburg/en/innovation-science/ai-comes-rescue-corona-era

Message we wanted to illustrate:

European Cybersecurity Companies are innovative and mature. In the context of a fast growing and industrialized cybercrime, European Cybersecurity Companies will help you develop your business in a secure way. You will not face operation disruption, loss of data, or loss of competitive advantage. You will deliver your projects without waking up at night.

Use Case:

Substitute insurers, Company health insurance funds and guild health insurance funds rely on Nect to register their policyholders in the service app or in the customer portal. Since 2021, German health insurers have also been offering members the electronic patient record (ePA). To protect patient data, secure identity verification is required before accessing the ePA. For this purpose as well, more and more health insurers already rely on the Nect app. In addition, Nect offers an extension of the process to include an additional document to be validated, such as the electronic health card (eGK), in order to check, for example, whether the eGK sent by mail has been properly received by the insured person. Nect is in use by a growing number of German health insurance companies and is constantly developing the technology according to customer needs.

Message we wanted to illustrate:

ECCs live in an environment of high-level and demanding certifications, providing a technical and quality standards warranty. Ongoing evolution towards European-level certification criteria increases pan-European validity of such warranty.

Use Case:

An increasingly fast-paced dynamic dominates both regulated and unregulated industries and companies within the digital ecosystem. In a time of change and dwindling transparency, it is a must for every business, customer and consumer to be assured that their data is protected and will not fall victim to misuse.

To ensure this, technical standards that shape the rapidly growing digital cybersecurity ecosystem apply. The hotly debated topic of a pan-European ID wallet shows the challenges facing society, companies and government and how important it is to define and implement secure technology. The balancing act that must be mastered here is between conforming to the security standard and maintaining good usability and customer experience. Simple, appealing and intuitive usability must be combined with high security standards.

The highest asset of any cybersecurity company is the trust of the customer. To gain this trust, it is important that companies can demonstrate the certifications it needs to fully meet security standards. Certifications that prove the security of a technology. For this purpose, demanding criteria are established that offer consumers the guarantee that their data is protected. With the appropriate certification, a company achieves a new standard and can operate throughout Europe. This gives companies the opportunity to expand markets and conquer new industries, both at B2B and B2C level.

Trust is also a top priority for Nect. Complete in-house development and independence from a third-party provider as well as three ISO-certified data centers in Germany ensure data protection. The patented Robo-Ident technology is a certified eIDAS trust module that allows us at Nect to offer secure and qualified online identification not only within Germany, but also in the European market. The challenging time of the pandemic has shown how fast and easy an implementation and handling has to work for the consumer. Nect's Selfie-Ident offers simple, secure and fully automated identification in regulated industries such as insurance and health insurance, but also in other industries such as the automotive sector, the sharing economy or in the context of age verification. Thanks to our proprietary infrastructure and certified quality, we can build the trust our customers need to feel secure in an ever-growing cyber landscape

Cyberwatch

published on blog

Maxime Alay-Eddine

Cyberwatch

Healthcare institutions are being targeted by cyberattacks on a daily basis. Those attacks happen to be increasingly violent, which explains the growing concern regarding this industry. Thus, they are now being asked by authorities to comply with challenging cybersecurity policies, without actually taking into consideration their business constraints.

The obsolescence of healthcare information systems is probably one of the main constraints of this sector. In fact, a large part of manufacturers supply brand new appliances that are still based on old technologies. Matthieu Garin, Partner at Wavestone, explains that 25% of healthcare institutions in the US and the UK are still using the Windows XP operating system [1]. This operating system is no longer supported by Microsoft and does not receive any new security update, resulting in very high risk of successful cyberattack. .

The second main constraint of Healthcare institutions is their budget. The Club des Experts de la Sécurité de l'Information et du Numérique (CESIN, or Information and Digital Security Experts Club) mentioned in one of its meetings dedicated to health institutions that only 6% of their budget is used for cybersecurity, versus 16% for other industries. Small budget allocated to critical missions results in lower level of maintenance and of security, with less human resources and adequate software.

However, France launched in 2021 a new funding for cybersecurity called France Relance with 136 million euros targeted to help public organizations securing their IT. This program is additional to HOP'EN, another program launched in 2019 with 420 million euros dedicated to modernization of healthcare equipment. These initiatives have allowed multiple organizations to run their first cybersecurity audit or to buy and implement several cybersecurity tools, improving their IT maturity.

Cyberwatch hopes to see new developments for these fundings, at a European scale, to address the cybersecurity issues of European Union health institutions as a whole.

Cyberwatch is involved in the security of the healthcare industry, through its cooperation with the CSF, the CLUSIF, Hexatrust, and APSSIS.

Cyberwatch provides solutions that help to find, prioritize, and fix vulnerabilities and compliance issues. These solutions are available at the UGAP, CAIH, and UniHA stores for healthcare IT professionals, and fit the requirements for the France Relance program.

Tehtris

both articels published on blog

Laurent Oudot

The benefits of European solutions vs non-European and insights from TEHTRIS on placing innovation and research well above promotion

"Just like we were among the first members of the E C A, taking part in the Cybersecurity campaign, promoting European solutions for companies and administrations was a no-brainer for us.
There is an ecosystem of European cybersecurity companies, capable of ensuring a 360° and 24/7 protection of companies. Performance and innovation are at par with, or even superior to, non European solutions with additional benefits
- creating local jobs and Champions in Europe
- ethical coding and European hosting of data
- no backdoor (as per the ENISA requirements)
- compliance to GDPR
- local teams serving clients
...
Research and innovation have been at the heart of TEHTRIS' strategy since the beginning in 2010: performance has always been and will always be first and above promotion. Our teams are dedicated to our mission: the protection of IT and OT, cloud and networks against all cyberattacks.
As a result, we are happy to share that our clients advocate for us, stating that right after set-up the TEHTRIS XDR Platform spotted attacks that their former non-European solution hadn't detected.

More from Tehtris

both articels published on blog

The threat landscape is constantly changing. For worse and for better. In the face of this constant evolution, the needs expressed by companies are changing. There is also a more insidious and harmful risk of espionage in the long term, with a very negative impact on the innovation and competitiveness of our companies and administrations.
A risk-based approach must be adapted to all industries and their needs. Defenders have understood this and are finding solutions to protect all companies. The XDR technology is one of these solutions.

Let's look at this innovative technology and how it works, its advantages and how it can help in the fight against cyberattacks!

What is XDR technology?
TEHTRIS was the pioneer in Europe. After more than 8 years of deployments, we are now able to offer an XDR platform recognized in more than 100 countries
.
But what do we mean by the XDR solution?
The XDR infrastructure is the way to extend EDR capabilities. While the Endpoint Detection and Response focuses on endpoints and acts on detection and blocking, the eXtended Detection and Response platform monitors a layer of security beyond the endpoint, including the network, cloud, FW, etc., via other building blocks that TEHTRIS offers, such as NTA, MTD, etc. It's a more comprehensive approach.
It is essential to have tools that provide a holistic view of activity on networks, systems, cloud, but also to simultaneously protect workstations, servers, ... Current cybersecurity solutions must also allow the detection of increasingly advanced threats and suspicious behavior, capitalizing on artificial intelligence and its algorithms, international databases, and like the TEHTRIS XDR Platform effectively neutralize attacks in real-time, without human intervention.

Cryptshare

Dominik Lehr

Message we want to ilustrate:

ECCs comply with EU regulations and transparency values. This is a must at a time where both national authorities and C-Level are more and more sensitive to regulatory issues.

Summary:

Compliance with EU data regulations include of course respect of GDPR. CRYPTSHARE, a company member of the ECA, has developed an easy-to-use, secure technology for distribution of emails and transfer of files, which makes it easier for organizations to comply with GDPR.

Among others, GDPR compliance means:

· Data Loss Prevention (DLP): with Cryptshare's technology, transferred files are protected in case the wrong recipient is selected. Only the correct recipient knows the agreed upon password and can decrypt the message or the file.

· Right to be forgotten: using this technology, the client can configure how long a file will be stored on the server. This way, "data graveyards" are avoided.

· Right of access and right to rectification: meta data, for instance an email's subject line, often contains personal information which needs to be protected in exchanges with data subjects. Cryptshare's technology allows for the encryption of metadata.

Cryptshare is a great example of how European cybersecurity technology can be used to ensure a key regulation is adhered to.

Cryptshare Whitepaper Summary for our own Whitepaper:

Our friends from Cryptshare discuss the important topic of secure email encryption in the here-referred whitepaper. They raise the question, in how far S/MIME and PGP are suitable models for secure communication in modern companies.
This exemplifies how insightful and thorough European Cybersecurity solutions can be.

Email is still the most commonly used communication medium in businesses. Hence, focus of the discussion are the most commonly used email encryption methods, S/MIME and PGP. Cryptshare finds that to date, neither of these two methods have been able to support enterprises regarding the encryption of their business communication on a holistic approach.
On the one hand, S/MIME is limited in its scope. Everything that is transferred in encrypted form can only be read by fellow S/MIME users. Contacts who do not use S/MIME are left out, meaning that encrypted emails can no longer be exchanged between anyone or at any time.
PGP on the other hand, requires quite a lot of expertise so for the greater majority it is a time and cost intensive (hiring an expert, training employees for its utilization) solution.
Moreover, both encryption methods are prone to user errors and can be bypassed by third parties. Efail, a type of attack, can use the active part of emails like externally loaded images or styles to decrypt the content of emails encrypted with S/MIME or PGP.
Therefore, secure communication cannot yet take place spontaneously and easily – and is in most cases reduced to those who also use S/MIME and PGP. In addition, the dependence on email infrastructure and the way email clients work not only restricts the scope of services, but can also directly affect security, -cue Efail.
However, business communication regularly contains sensitive data, and email still needs to be secured and data in transfer protected from unauthorized access.
Cryptshare suggests that business communication solutions should be more user friendly while keeping email as the preferred medium for communication in businesses.

Tranquil.IT

published on blog

Denis Cardon

Having participated in the 1st edition of the Autonomy and Digital Sovereignty days organized by the General Directorate for Enterprises at Bercy in the heart of Paris this Monday, September 27, I learnt an excellent lesson from the round table led by Loreline Descormiers-Thollot of Hexatrust and the Directorate.

The objective of the event was to remind large French companies and administrations that there is a perfectly serious and perfectly sovereign offer in the field of cybersecurity. What's nice is that the ECA aims to amplify that exact same message at a European level.

Indeed, the cyber procurement of large corporations is often the result of ingrained habits and lack of knowledge of the offer. The French offer is often drowned out by the very effective marketing of the giants, especially American, and to a lesser extent Israeli.

Having presented the interest and the objective of the event, let's go back to what I learned. I don't want to be judged too harshly, because some obvious things remain hidden for a long time until someone shows them to you. Yes, I know: "When the sage points at the moon, the fool looks at the finger."

The ISSP (Information Systems Security Policy) is a long list of points of vigilance to which CISOs (Chief Information Security Officers) and their teams attach action plans.

No solution, no matter how elegant, is able to cover the entire list and CISOs will immediately find suspicious the individuals who will come to and tell them that THEIR solution solves ALL problems. A solution is only able to cover a part of the problems and the humility approach and the understanding of the complete issues gets a much better listening from the CIOs.

Let's take for example a software and configuration deployment, system update deployment and compliance auditing tool such as WAPT from Tranquil IT. WAPT is an operational management tool that provides the same functions as Microsoft SCCM / Intune and WSUS for example. Having a separate ITSM tool, i.e. a tool to help dematerialize approval processes in the enterprise, or having a separate software license tracking tool,
is not shocking, these mechanisms tick other boxes, all of them very useful.

So in conclusion, no solution can do everything. However, it is interesting to note that Hexatrust and ECA members have narrow scoped
solutions that go very deep. It is now a matter of putting them together
judiciously to check off more in the list of the needs of the CISOs.

CyberVadis

published on blog

Ekaterina Grekhova

Introduction of their Whitepaper:

The increased volume and complexity of cyber attacks linked to the COVID-19 pandemic crisis has created new cybersecurity challenges that organisations must address. This, coupled with the widespread remote working and the need for digitalisation, begs the question: Are organisations and their supply chain partners prepared for today's cybersecurity challenges?"
This report analyses the cybersecurity measures declared by organisations against the evidence-based assessments that CyberVadis conducts. The report focuses on five key areas of cybersecurity to uncover potential reporting gaps that could lead to increased third-party risk through uncertified assessments. For this study, CyberVadis analysed the self-assessment results of 1,289 organisations of different sizes and industries across 67 countries. CyberVadis analysts then independently assessed all cybersecurity controls declared by the rated companies based on evidence provided. Data privacy & GDPR Access management Cloud security Incident detection and response (IDR) Business Continuity and Crisis management.

Summary of their report:

5 key challenges to overcome: Data privacy & GDPR, Access management, Cloud security, Incident detection & response and Business continuity & Crisis management.

Data Privacy & GDPR:

A state-of-the-art personal data protection program is now becoming mandatory, as the number of cyber attacks targeting personal data are on the rise: 80% of breaches involved customer PII (Personaly identifiable infromation). In 2020 there was a 40% increase in GDPR fines.Organisations must therefore put in place a strong data protection program to ensure compliance with various data privacy laws and regulations.

Access management:
The COVID-19 crisis forced many organisations to consider a remote workforce: 62% of rated organisations said they allow remote access to their systems. At the same time, the number of insider threats is rising: 60% of companies had more than 30 insider-related incidents per year. This highlights the importance of establishing more effective remote access strategies. It becomes crucial to adopt advanced authentication practices to deal with these growing insider risks.

Cloud security:
As a result of the pandemic, organisations are actively switching to cloud solutions to store their data. 81 % of organisations declared using cloud models. According to NIST, in addition to on-premise traditional methods, cloud computing offers on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service.
However, this introduces specific risks that need to be considered. 19% of malicious breaches were caused by misconfigured clouds.

Incident detection % response:
Today, organisations must build a strong incident detection and response process to identify and contain a cyber attack at the earliest possible stage.
This is crucial because, in 2020: 52% of breaches were caused by malicious attacks, which represents a 10% increase compared to 2014. When developing incident response plans, organisations should incorporate a lessons learned process that helps them identify the root cause of incidents. This lowers the probability of having similar problems in the future.

Business continuity & self-assessment:
During the last year, organisations worldwide have come to realise the importance of anticipating unplanned events and implementing the measures to manage a critical situation.
95% of business leaders reported that their crisis management capabilities needed improvement. A critical element of any successful crisis management plan is to ensure the dedicated team is well trained and prepared to react promptly if a major event occurs. The crisis management team should lead the activation of Business Continuity Plans (BCP) to contribute to business resilience.

Starboard Advisory

published on blog

Marie de Freminville

Financial & Cyber performance:

Why not assess the cyber performance of companies in the same way as their financial and non-financial performance (governance and CSR - corporate social responsibility)? Why not certify the cyber performance of companies in the same way as their financial performance via auditors, whose intervention is mandatory for companies of a certain size? Despite some progress, the vast majority of shareholders, and therefore the Board of Directors and management, are primarily interested in the company's financial performance. However, the digital age is introducing upheavals in the company and in its ecosystem. Indeed, the "all-digital" concerns all stakeholders, administration, public services and national and international infrastructures, defense and intelligence services. We have reached a stage of non-return, which offers important opportunities, but which is also a source of fragility and major risks, particularly because cyber threat actors are becoming more professional and have significant resources to defraud, spy and sabotage. The risks for companies are systemic: shareholders are financially exposed and directors, in charge of defining their strategy and ensuring their sustainability, are legally exposed if they do not inform themselves about the quality of data security and information system protection and if they do not ensure that an organization, procedures and tools for a high level of cybersecurity are in place. There is no such thing as zero risk, but the negligence of a board of directors would be associated to it if no action were taken in the field of cybersecurity of the company and if the attacks had significant consequences for its proper functioning, profitability and reputation. Financial performance should therefore no longer be the only priority. Financial performance and cyber performance should now be the two priorities of corporate governance bodies. Should we therefore reinvent the governance body designated by the national actions, namely its competences, its functioning, its agenda and its partners? The digital world is borderless, immaterial, the threats are invisible. Digital and related new technologies are transforming the way companies operate and business models.

The main cyber-risks are risks of malfunctioning of the industrial or commercial process, financial risks but also risks of loss of considerable confidential information (strategic information, personal information) and affect different sectors: hospitals, autonomous cars, banks, telecom operators, energy, etc., with potential human consequences. According to a study conducted in the United States by the National Archives and Records Administration in 2018, 93% of companies that lost their data for ten or more days declared bankruptcy in the year of the disaster and half (50%) filed for bankruptcy immediately after the attack. The question is not "when will we be attacked?", but "what can we do to protect the company as much as possible, what can we do in the event of an attack, what can we do to restore systems as quickly as possible?" Cyber-risk is an integral part of companies and also of personal organizations (everyone is concerned individually and as a member of an organization). It is not just a technical risk. Man is the weakest (and strongest) link in the entire safety chain. Companies are judged on their financial performance: their accounts, their results, their balance sheet, their cash position, their share price, their growth and earnings potential, their non-financial performance (their governance and their social and environmental performance), but... What about their cyber performance? Data governance, data security: integrity, confidentiality and accessibility, protection of the personal data they collect, use and archive, protection of computer systems that allow the exchange, storage and modification of these data. A company may be financially successful, but a failure of its IT system or digital security can seriously affect its ability to sell or produce, to pay its suppliers, to exchange with its subcontractors and thus degrade its financial results, its reputation, the confidence of shareholders and stakeholders. Cyber-risks are not the prerogative of a handful of specialists in the company but affect overall governance. In addition to the regulatory obligations regarding data security, it is a matter of protecting the company against the risk of loss of value, linked for example to the dissemination of confidential information. "All connected, all committed, all responsible" is the slogan communicated by Guillaume Poupard, ANSSI's Director General at FIC 20191 , from top to bottom and from bottom to top of private or public organizations: the Board of Directors, the Executive Committee and all the teams. There are cyberdeaths among the victims.

Cyber-silence is a barrier to awareness. There are too many executives and directors burying one's head in the sand. The missions of Starboard Advisory are mainly to: - Raise the awareness of executive and non-executive directors about the necessity of a digital strategy, responsibilities and liabilities of the directors, - Advise them on how to implement cyber risk management and cyber security programs in their companies - Support them in the building of a cyber culture in their companies, through training programs (users, IT teams, developers, managers and directors), and security policies - Help them defining the appropriate cyber governance (organization, competences, processes and policies, internal audit, external audits) - Advise them defining their digital strategy and allocating the right level of resources. Marie de Fréminville is a non-executive director and founding partner of Starboard Advisory. She is also a member of the IFA (French Institute of non-executive Directors), HEC Governance and Swiss Association of Women Directors. In addition, de Fréminville is an expert in governance, financial performance, risk mapping and data protection. Author of "Cybersecurity and decision makers" awarded by the International Cybersecurity Forum, in 2020.

Atempo
published on blog

Luc d'Urso

Data Management: The heart of European sovereignty

What is the most precious resource of our times? Which is also almost limitless? Data, obviously! At the heart of so much essential activity, its exploitation is the source of all progress: social, economic, ecological… Today, data is a genuine growth lever for public and private entities alike.
Faced with the challenge of a global data explosion, with volumes expected to multiply by 45 in the next ten years, data management will become even more strategic.
Let's take a closer look at the drivers behind US and Chinese dominance, why European digital sovereignty should be a cornerstone policy and lastly how organizations -increasingly dependent on their data creation and management systems- should prioritize protecting their digital assets.

Putting an end to US and Chinese data dominance

US and Chinese digital leaders -including GAFAM and BATX- have dominated data-driven industries for over a decade. As a result of highly successful B2C approaches, the major players are now carving out significant B2B revenues. Amazon is an excellent example of a B2C (online bookseller) growing into a leading B2B cloud platform with AWS. Facebook (Meta) has grown inorganically through a huge buy-up strategy: the company has acquired more than 20 entities since its creation. Their common ground is cornering the data market because the value extracted from data will be the major wealth driver this century.

Why is this such an issue for Europe? Put very simply: handing over data to distant, highly competitive, and not always scrupulous providers does not make sound business sense particularly for sensitive and strategic industries. Storing an entire country's social security details on a data center on a different continent with different rules is ill advised at best. Europe is home to thousands of small yet essential SMBs as well as world-leading industrial players in the defense, telecoms, automotive, health and food sectors. The only way for these sectors to not only survive but thrive is to allow them to keep full control over their data.

What is at risk?

Risks to data can be classified in different categories: chronic disasters caused by human activities, such as ransomware which today are the greatest threat faced by businesses. According to Sophos, 51% of companies worldwide have been victim to ransomware, a growing trend since the beginning of the pandemic. Data loss has damaging impact on businesses. In 2021, Statista estimates the cost of one data breach exceeds 4 million euros for both Germany and the UK!

Serious physical incidents such as server crashes or network outages can cause severe data loss. Environmental disasters are also on the rise with climate change including natural disasters such as fires, floods, tornadoes etc.
All these risks need mitigating of course. But this requires strong political leadership.

Towards European Autonomy

The loss of economic autonomy will impact political power. In other words, data and economic frailty will only further weaken Europe's role at the global power table and open the door to a variety of potential flash points (military, cyber, industrial, social…). Europe should be proud of its model which reinjects tax revenues into a fair and respectful social and cultural framework. The GDPR policy is clearly at the heart of a European digital mindset.

Many European partners have risen to this challenge which is central to the upcoming French presidential election and the current French Presidency of the Council of the European Union. One stated aim is to help European champions prosper or in the words of Thierry Breton, European Commissioner for the internal market: "Europe has to regain its technological sovereignty". The French Presidency of the Council of the EU will clearly place data protection into the spotlight of political debates. It is not about protectionism, but Europe must safeguard its data against foreign competition to enhance its autonomy and build a prosperous future.
Sovereignty is essential because in any digital economy, data is considered the raw material of prosperity. Assisted by technologies such as AI and soon quantum computing, European sovereignty will condition our regional autonomy, employability, attractiveness, and our ability to meet tomorrow's challenges.

Data Protection, Data Management

To protect their digital assets, on-premises or in the cloud, the implementation of a data protection and management infrastructure is key. Each company should be able to recover its data in the event of an unplanned incident and avoid irreversible data loss with dramatic impact on activities. Atempo is a leading European data protection and management provider. In 2019, a major French hospital was hit by a cyberattack. Atempo enabled the institution to recover its backed up data and return to full operational capacity in under 48 hours.

Conclusion

To counter American and Chinese dominance with their monopoly on exploiting the value of data, Europe must regain control of its digital destiny and rely on its industrial sector to build trustworthy cloud platforms and infrastructures. Labels can now be granted to European cloud providers who commit to respect the highest standards in terms of data protection and data privacy.
Today, organizations need to be transparent in their data protection strategy, and resilient to risks. In terms of sovereignty, only data control will allow Europe to assert itself internationally, showing that there is a digital “third way” that genuinely respects fundamental freedoms.

Rohde & Schwarz Cybersecurity

published on blog

Stephane de Saitn Albin

Hard lessons you can learn from the Log4j catastrophe:

Is there a way to prevent, detect and protect yourself when the next Log4j hits?

Well, it is possible and we will show you how to do it in this article. Being proactive is definitely one way to stop Log4j and its variants. But there are more and we will get to it.

Log4j has been lurking in the news headlines since its discovery in December 2021. It seems to be more ominous than any other case of late due to its immense usage in Java solutions. Any Java web application using Log4j is vulnerable and can be hacked. This presents a giant opportunity for exploitation to hackers everywhere as they can now perform a remote code execution (RCE) attack on any target computer.

In fact, there have been massive attempts to exploit the Log4j vulnerability in the wild. By easily exploiting the java naming and directory interface (JNDI) lookups feature exposed by Log4j in log messages, hackers can hack into your application, run any code they want, steal your sensitive data and take full control of your system. So you can imagine why companies, governments and individuals all around the globe are under such huge pressure. It is due to the extensive impact and seriousness of this vulnerability.

A real incident that tends to impart some significant lessons to us all. Let's have a look in depth.

A wakeup call for less mature organizations

One of the main things we have learnt from Log4j is that you need to be always prepared to deal with zero day attacks. Keep monitoring your environment, logging and reporting any issues to check if you are being attacked. You need to have a proper process outlined for vulnerability assessment in the company. Such processes will tell you what the existing risks are, their criticality, which are the vulnerable components and products, if they are exploitable etc. You need alert logs and access logs that will help you look back and grasp any tentative exploitation. You can equip your teams with security orchestration, automation and response (SOAR) technologies that extract information related to threats from logs.

Security information and event management (SIEM) tools can also be helpful to identify exploitation activities in real-time.

Scaling your response to zero-day attacks

Big organizations like google cloud platform (GCP) were prepared and so able to manage the risk well. They ensured that their customers upgraded to the newest available version of Log4j quickly. Any vulnerable images were prevented from being deployed in production. You also need to have the best crisis response actions in place, scale up patching of the affected systems, to reduce any further exposure. Zero-day attacks are inevitable in everyday life. They are potent and costly attack tools. When the worst happens, you should be able to invoke the best practices diligently. Only prepared companies will succeed in times of such disasters.

One of the main things we have learnt from Log4j is that you need to be always prepared to deal with zero day attacks. Keep monitoring your environment, logging and reporting any issues to check if you are being attacked. You need to have a proper process outlined for vulnerability assessment in the company.

Third-party components can lead to insecure code

Disasters happen more likely due to third party dependencies. For example, even if your company is not using Log4j directly, you might be dependent on another third-party library that uses it. In fact, most of the Java applications using Log4j use it indirectly. You need to keep all third-party products updated to their latest versions. We saw that the vulnerability has not affected the latest Log4j versions. Ask your software vendors if they are covering themselves from this flaw.

Many organizations focus on static application security testing (SAST) tools as a part of their DevSecOps implementation, but we see that early adopters are engaging more with software composition analysis (SCA) tools these days. Even less mature customers are realizing the need for SCA tools to report instances of CVEs like Log4j and know which applications are running such vulnerabilities.

Being cautious when choosing your open source libraries

Log4j is one of the open source logging libraries that helps Java developers keep track of their applications' past behavior. Code in millions of internet facing devices worldwide use Log4j. However, open source code is out there for everyone to see and very few people actually maintain it. You need to pay heed to the community size.

This incident does not necessarily tell that all open source software components that companies have embedded in their tools are hazardous. However, more security researchers should watch these open-source projects for any changes and search for possible vulnerabilities in their code sources, like the Log4j vulnerability. Do not hesitate to participate in an open source project (reporting bugs, proposing improvements, providing bug fixes, etc…)

Introducing a proactive approach to prevent zero-day attacks

Vulnerabilities like the Log4j prompt you to develop a zero trust mindset, build cloud automation and rethink your entire application security posture. To contain such vulnerabilities effectively, you need an intelligent web application & API protection (WAAP) solution. However, do not rush into buying any such solution. Take the time to assess your options in the market.

At Rohde & Schwarz Cybersecurity, we have seen no evidence of exploitation among our 600+ customers. Here is why:

- Generic signatures prevent zero-day events

We already had all the rules in place to block Log4j, which means we covered our clients already on every web-facing application. In fact, 88% of most zero-day attacks are blocked by our web application and API protection (WAAP) solutions, without having to customize the ruleset.

- Custom rules are the best defense!

While you should focus on generic signature-based protection, you need to react quickly if something is not included in it. For events like this, we are able to respond immediately to the issue with our WAAP Gateway and SaaS WAAP, generating the right custom rules, to ensure that no exploitation occurs. It is well known that writing custom rules can be difficult, giving rise to a high false-positive rate. However, this has been one of our reputable characteristics in the market.

Check out the advisory Rohde & Schwarz Cybersecurity has issued for their customers for more insights:
https://documentation.appsec.rohde-schwarz.com/display/SECURITYEN/CVE-2021-44228+-+Apache+Log4j2+JNDI+RCE

Invest in next-generation application security tools from a trusted vendor with the right custom rules that also prevent false positives. And you can enjoy your peace of mind.

Vade
published on blog

Georges Lotigier

Artificial Intelligence Opens a World of Opportunity in Europe:

Artificial Intelligence Opens a World of Opportunity in Europe
No longer a mere plot device in futuristic novels and films, Artificial Intelligence (AI) has reached the mainstream. Cybersecurity vendors have fully embraced AI, and French technology companies are seizing the opportunity.

The Growth of AI in Cybersecurity
AI has the ability to supplement human intelligence in ways that no other technology can. As a result, the AI in cybersecurity market has grown exponentially in recent years. The market is expected to reach 46.3 billion USD by 2027, a compound annual growth rate of 23.6% compared to 2020.
From the increase in network devices, to the rise of remote work, to the growth in third-party ecosystems, cyberthreats are the top concern facing businesses today. Since the beginning of the COVID-19 pandemic, both phishing and ransomware attacks have skyrocketed.
According to the National Cybersecurity Agency of France (ANSSI), ransomware attacks increased 255% in 2020 alone. Vade observed an even greater increase in phishing attacks. In 2021, Vade detected more than 1.2 billion unique phishing emails, a 340% increase from 2020. The situation has become so dire that President Macron earmarked €1 billion to combat cyberattacks in France, establishing a government program to increase cybersecurity in public and private sectors.

The Technology Behind the Buzzwords
Machine Learning is perhaps the most well-known subset of AI, but how exactly does it work in real-world applications? In the context of phishing, which is one of the most prevalent threats to businesses as well as the number one delivery method for malware, Machine Learning algorithms have the ability to compute email features and recognize patterns of malicious behavior to recognize threats. Compared to traditional methods of detection, which rely on the outdated practices, AI is superior in this respect and has been a game-changer in detecting email-borne cyberattacks.

Computer Vision, a subset of Deep Learning, analyzes images rather than text. Computer Vision algorithms see images as humans see them, but with far better clarity, and can recognize subtle changes to images that humans cannot. In one example, a hacker may paste an image of an email (rather than text) in the body of an email so that the email filter cannot read it. A Computer Vision algorithm can extract the text from the image, analyze the text (in multiple languages), and identify the attack.

Another area where AI has excelled is with incident response. Traditionally, incident response required significant cybersecurity resources, both human and technological. With AI, incident response can be autonomous. The alternative to AI, which involves significant time and IT resources, is not viable in today's threat landscape in which cybercriminals follow closely behind any technology designed to stop them.

AI in France: A Growing Community

While US companies typically make the most noise in the global media with respect to AI, French companies are making significant contributions to the field. AI is embedded into Vade's product line and at the forefront of our efforts in research and development. With 19 AI patents, including a recent US patent for our phishing awareness training technology, Vade is just one of many French vendors pioneering new uses for AI.

French startups focusing on AI has swelled in recent years. Shift, a Paris-based startup, has secured more than $320 million in funding for its AI platform to detect insurance fraud. Sophia Genetics, which secured $250 million in funding, offers an AI-based health analytics platform that helps healthcare professionals make better medical decisions.

While Shift and Sophia Genetics are just two examples of French companies using AI-based technology, French cybersecurity companies are also on the rise. The barrier to entry, however, is high. AI models are trained with data, and so they require considerable amounts of data to be effective. Not only this, but the data must be quality data.

Vade has achieved what it has in the email security space because we protect more than 1 billion mailboxes worldwide, second only to Google. This differentiates us from our competition and helps us maintain a highly intelligent AI engine that continually learns from billions of daily inputs. French companies looking to scale the AI barrier will need a strategy for the automated collection of quality data and a team of data scientists to maintain it.

Postface

As this White Paper comes to publication, the international situation is, alas, there to remind all of us that Cybercrime and warfare are now often close cousins.
Therefore it is hardly useful to stress the urgent necessity of a strong European Cybersecurity industry, to leverage Europe's strategic autonomy.
The articles which are displayed in this Whitepaper have all been written in the course of the pan-European campaign launched by the ECA to promote this same idea. No need to say they reflect the creativity and the robustness of our Cybersecurity industry.
So far, in functional or technical terms, this industry competes on an even basis with the best-in-class suppliers, most of them being American or Israelian. On the other hand, many decision-makers still ignore this fact and resort to US products « because we have always done it ». Our objective is to convince them they should give their chance to European Cybersecurity products. Products that comply with EU regulations and do not steal data from their customers. Products which are a part of the European resilience and autonomy which we all want to reinforce.

Dominique Tessier
ECA Head of Cybersecurity Focus group

About the European Champions Alliance

WHO WE ARE:

The European Champions Alliance is a not-for-profit association building an ecosystem of start-ups, scale-ups, SMEs, corporates, and industry experts committed to European Tech and values.

OUR VISION:

Unleash the hidden power of European Tech by creating a vibrant and open Alliance that fosters cooperation and supports the growth of European Champions.

OUR MISSION

Harnessing the power of a pan-European network, activating synergies between key stakeholders, and providing strategic and operational support to European Scale-Ups and SMEs to help them become European champions.

OUR GOAL:

The Alliance leverages its European network by sharing market knowledge and activating joint business opportunities between the members to support the growth of European Champions.

IMPRINT

THE EUROPEAN CHAMPIONS ALLIANCE

Publisher:

European Champions Alliance

Location:

European Champions Alliance
44 rue des Ecoles
75005 Paris, France

Contact:

welcome@european-champions.com

Recommended citation:

European Champions Alliance (Ed.), Title, France / Germany, 2022 Paris, March 2022

European Champions Alliance / Cybersecurity Focus Group