



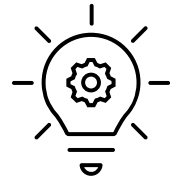
CYBALGORIS



Who we are

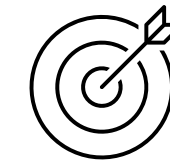


CYBALGORIS is a European SaaS cybersecurity company.



We believe security should ...

- have **the same priority as functionality**
- be implemented **from the start**, not patched on later.

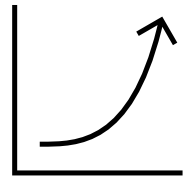


We develop **the first Secure by Design Assistant.**

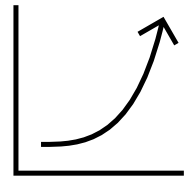
It helps teams embed security across **the entire lifecycle** of software production or integration, and of AI systems.



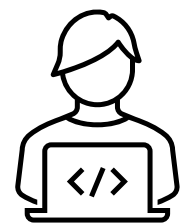
The problem we solve



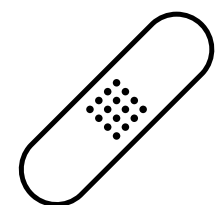
Cyberattacks are growing in numbers and sophistication.



Conformity obligations increase (CRA, NIS2, DORA, AI Act, CISA Secure by demand...).



Nevertheless, developers are under pressure to deliver quickly, focusing on functionality not on security.



Therefore, security is treated as a patch, an afterthought.



Systems are built first, secured later.

It is costly and poorly efficient.



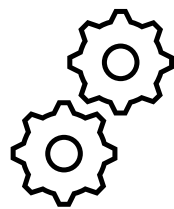
**Preventive security
is missing.**



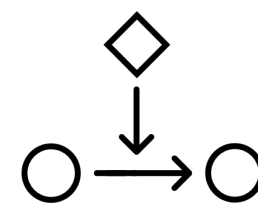
Our solution



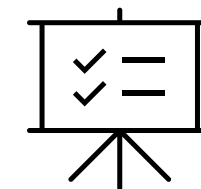
A fundamental shift in security:
from reactive to preventive



Security is an **industrial process**, not a checklist.
An AI solution that combines **agentic AI with NLP**.



Security is **integrated** into development from the requirement to production.



Security is **factual, visible and traceable**.



Who we support



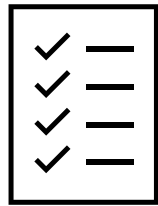
- ✓ **Developers** to embed security directly into how they think, code, and deliver.
- ✓ **Integrators** to integrate software in Information System without disrupting the security.
- ✓ **AI builders** to get traceable, explainable, and defensible security across every stage of their pipeline.



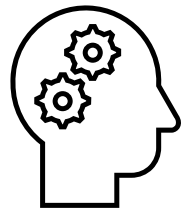
How CYBERNOE® works



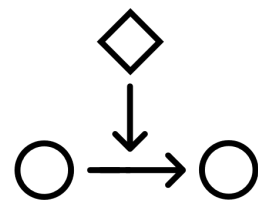
We **analyse** the **risks** of the project.



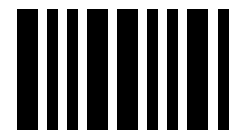
We provide security **rules** for every task or feature.



We **train** the developer along their needs.

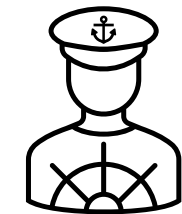
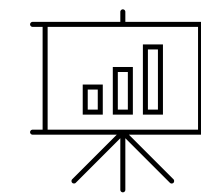


We **manage** the **flow** of security in the project.



We provide a detailed **traceability** of security.

In addition, our solution provides detailed **statistics** and **dashboards** tailored to **each department**, from HR and management to executive leadership.





When it starts

Before to write any line of code, risk must be understood, and choices for security must be done.



The developer receives development tasks.

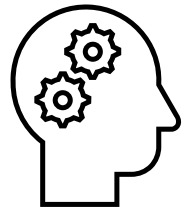


We provide security Rules for each specific task, to be applied right from the start.


Task security rules				Re-generate security rules		
The security rules generated for this task:						
4 Priority Security Rules						
Sélectionné				Trained	Applied	Criticité
	DP04. Prevent users from downloading server -side source code by implementing strict security measures. Ensure that server configurations and access controls restrict access, permitting only authorized personnel to view or modify the source code. You need to protect the integrity and confidentiality of your application's backend logic.					5
	FM02. Ensure authentication is mandatory before permitting any file uploads to enhance security measures effectively.					5
	FM03. Restrict file uploads to essential business -related file types to mitigate security risks associated with unauthorized or potentially harmful file uploads.					4
	FM04. Verify the uploaded files by inspecting their file headers to confirm they match the expected type, as relying solely on file extensions for validation is inadequate.				<input type="checkbox"/>	3
	FM05. Store files in locations separate from the web application context, either on a content server or within the database, to enhance security and prevent potential vulnerabilities.					



To get the skills which you really need




Training along the needs.
Including explanation, best
practices and code
examples.


 CYBERNOE


Dashboard Projects Trainings Conformities Audit

[< Back](#)

Sections

 Lesson

 Quiz

 Code example

Lesson

Before granting access to the admin section or hidden directories of the application, re-authenticate users. This ensures that access to sensitive areas is securely controlled and only authorized users, confirmed via a secondary authentication check, can enter.

Explanation

Implementing a requirement for users to undergo re-authentication before accessing sensitive areas of an application, such as the admin section or hidden directories, adds an additional layer of security. This process involves prompting users to confirm their credentials a second time, even if they are already logged in, particularly before accessing high-stakes functions or data. This step ensures that the person attempting to access these areas is indeed the authenticated user and not someone who has gained access to a user session that was left unattended.

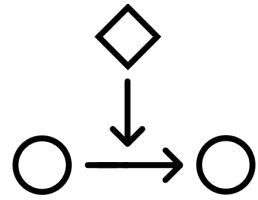
The primary security concern this addresses is the unauthorized access to sensitive parts of the application, which could lead to data breaches, unauthorized modifications, or exposure of confidential information. Re-authentication mitigates risks associated with session hijacking, where an attacker takes control of a legitimately established session. It also protects against scenarios where a user might leave their workstation unattended, and another individual attempts to access sensitive areas without consent.

Use cases

This rule is crucial in environments where sensitive transactions or data manipulations occur, such as financial systems, content management systems, cloud-based administration interfaces, and internal corporate applications. It is applicable across various programming environments and frameworks including, but not limited to, Java EE for enterprise applications, Microsoft's ASP.NET for web applications, and PHP-based administrative interfaces.



Managing the security...



We **manage the security** according to the process decided within the company (decision review, code review by the lead...).

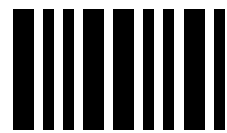
This can be integrated in the usual project management flow of each company.

The screenshot displays the CYBERNOE dashboard with the 'Projects' tab selected. The interface is organized into several columns and sections:

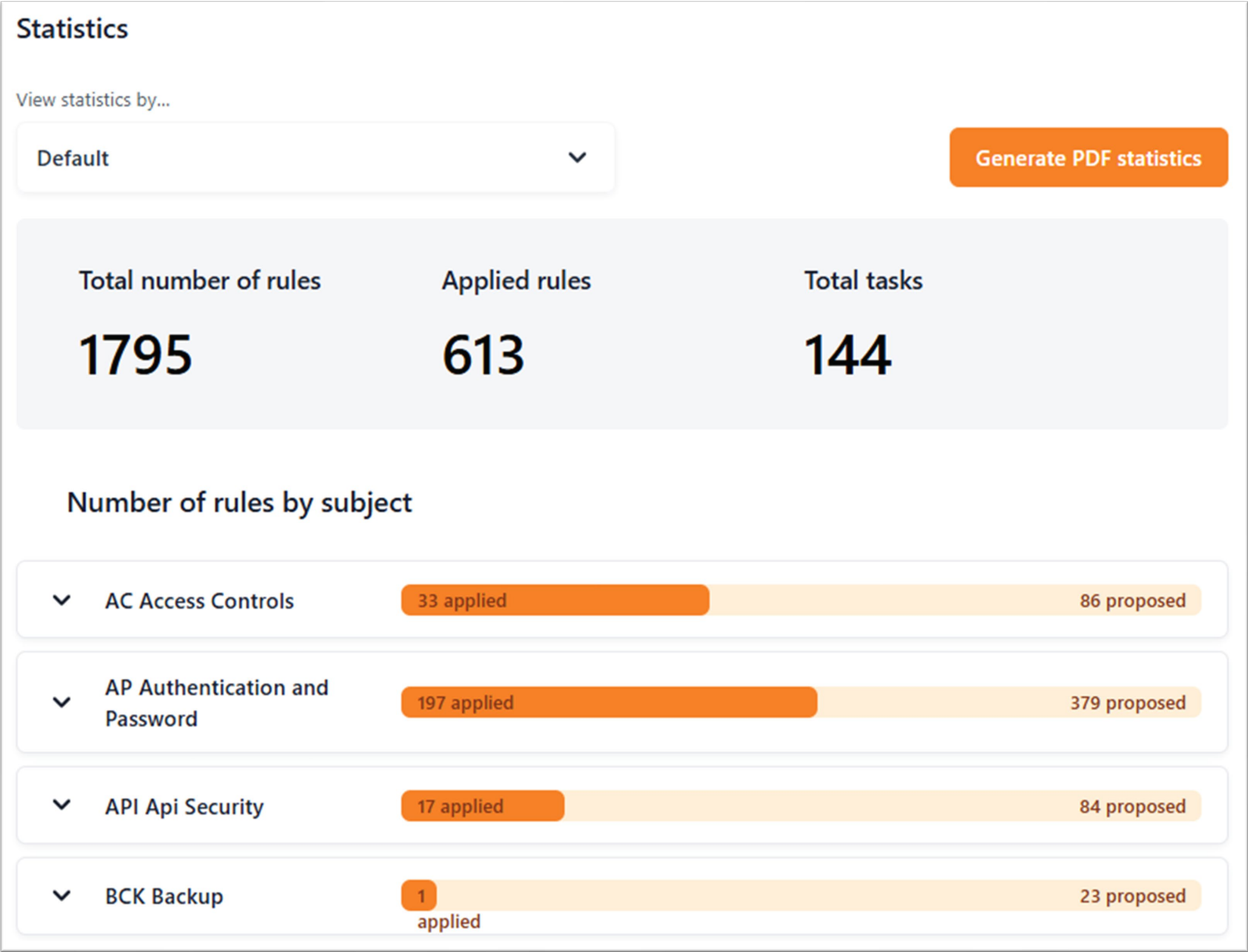
- Left Sidebar:** Labeled 'Logiciel Data1', it contains a list of sprints with their durations and names: Sprint 21 (10.09 - 23.10), Sprint ESN développeur isolé (24.10 - 24.11), Sprint RGPD (07.01 - 12.02), Sprint 24 (17.02 - 22.03), Sprint 25 (23.03 - 02.04), Sprint 26 (03.04 - 23.04), and Sprint 27 (01.05 - 31.05).
- Main Content Area:**
 - Logiciel Data1:** A section header for the main content.
 - Rules choice:** A column containing tasks like 'Importing data from HR reports', 'New files upload for managers', 'Protect connexion logs', 'Send data to SIRH', and 'Create an admin access for BU managers'. Each task has a 'Criticité' (Criticality) indicator and a 'BL' (Blocked) status icon.
 - Team validation:** A column containing tasks like 'Updating data by the user', 'A new dashboard for CEO and COMEX', and 'create an upload log'. These also have 'Criticité' and 'BL' indicators. A '+ Create task' button is at the bottom.
 - To be applied:** A column containing tasks like 'Oblige to regularly change password', 'Create an authentication statistics dashboard', 'Enforce strong passwords', and 'Recuperate data from CRM'. These have 'Criticité' and 'BL' indicators. A 'pdf upload' task is at the bottom.



Until getting a clear view of it

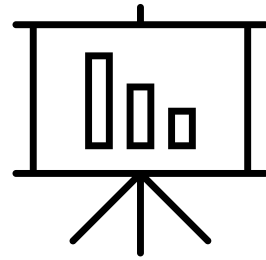


The company gets the **traceability** of the security implemented in the application.





Securing company approach



We have **a wide approach of security** based on audits, specific trainings about development organization and process, security debt of a software, global security of the company...

Software production : basic audit

GDPR Debt of the software

Security debt of a software

< Back

Chapters

Access to the Hosting and Backup Service

Developer: Personal s

Software production: security policy

Developer : Secure by

Global security of the

The service is accessible only through individual accounts

Individual account: the login ID allows identification of its owner (usually an email or name). A non-individual account (like compta@... or admin@...) does not identify a specific user. Such accounts are less secure (lack of accountability, difficult traceability) and are often shared, which increases risk.

☐ yes

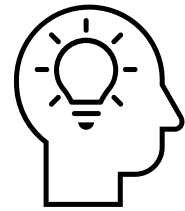
☐ no

☒ partially ✓

Security debt of a software

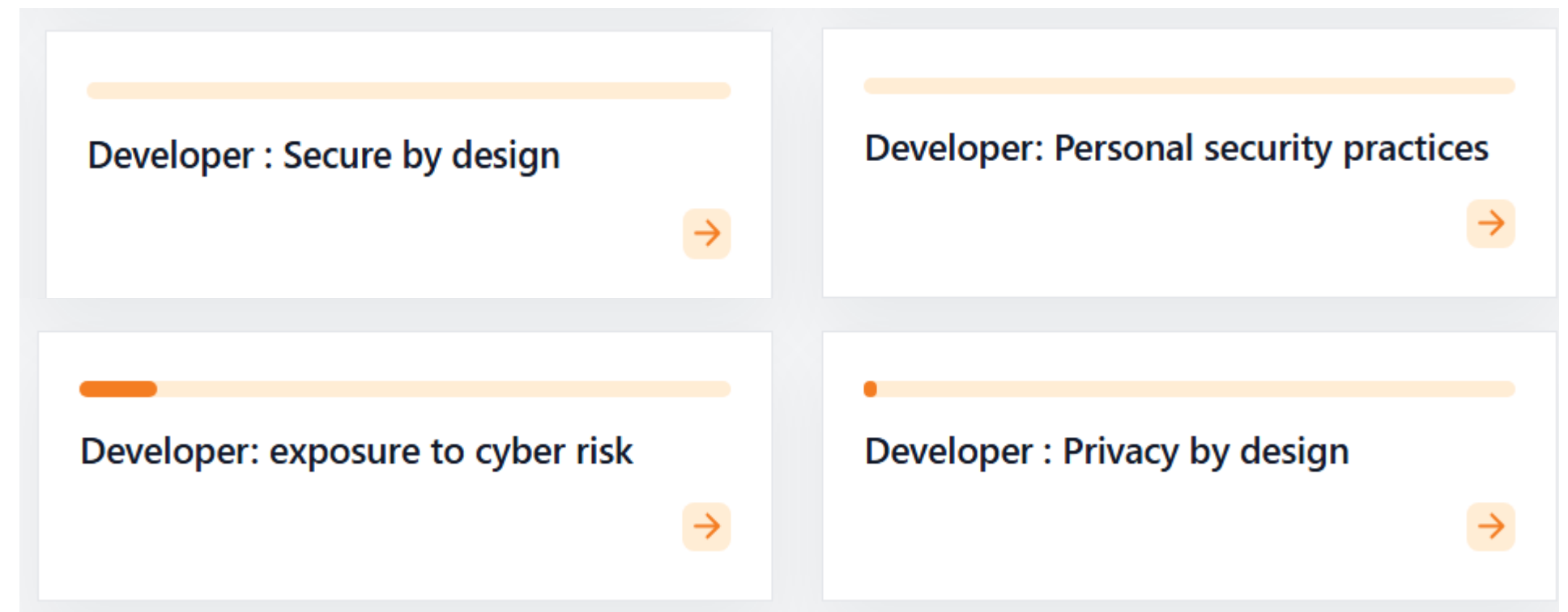


Helping developers in the change



We offer **training** to help developers understand the threats that target software and how those threats relate to the way they build and deploy code.

We also provide **evaluation systems** that assess their current practices and guide them in strengthening their skills in Secure by Design, Privacy by Design and personal cybersecurity hygiene.



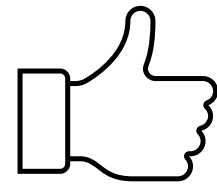
Evaluation system



Value for the community



For companies, we reduce the **cost** to secure software, increase **security** and **resiliency**. We improve the **commercial** relationship due to trust and conformity.



For developers, we provide skills and proofs of it, increasing their long-term **employability**.



For investors, we open a **new market** : secure-by-design as a service, a future standard in a world facing rising cyber threats and regulatory pressure.



Budget holders and strategic entry points



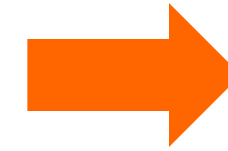
CYBERNOE® targets strategic budgets in **application security, secure development, and digital transformation**. We reach decision-makers committed to reducing security debt and embedding security earlier, before incidents happen.

We access funding lines dedicated to:

- Secure software development
- Regulatory compliance (CRA, NIS2, DORA, ISO 27001...)
- Innovation and AI system integration
- Developers training

These budgets are owned by:

- **CTOs**, leading secure digital transformation
- **CISOs**, focused on measurable security and compliance
- **Product Security Leads** and **Engineering Managers**, accountable for secure-by-design delivery.



CYBERNOE® supports both **technical implementation** and **compliance traceability**, making it a relevant solution across **security, engineering, and governance** domains.



CRA makes Secure by Design a legal obligation

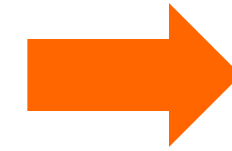


The **Cyber Resilience Act (CRA)** establishes **Secure by Design** as a legal requirement for software products in the European Union.

Starting in 2027, all digital products placed on the EU market must prove that security is integrated across the development, release, and maintenance lifecycle.

This includes:

- Security can no longer be reactive or optional,
- Compliance must be proven with evidence and traceability,
- Secure development becomes a condition for **CE marking***.



CYBERNOE® is aligned with this shift.

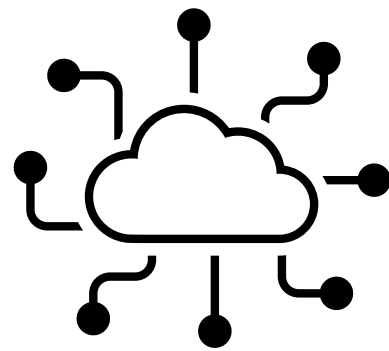
It helps engineering teams implement Secure by Design in daily development and generate the traceable proof required by CRA audits.

**CE marking, the mandatory EU label required to sell digital products in Europe, certifies that a product complies with EU regulations, including the cybersecurity requirements introduced by the CRA.*

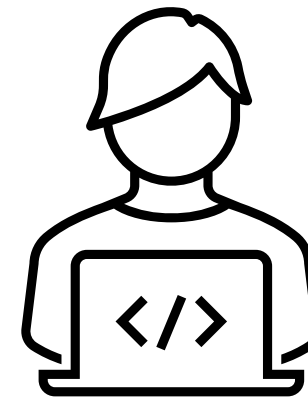


Barriers to entry

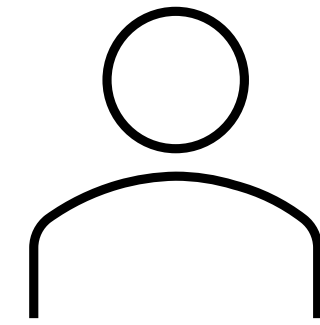
In addition to investment and time, overcoming barriers requires a wide range of skills.



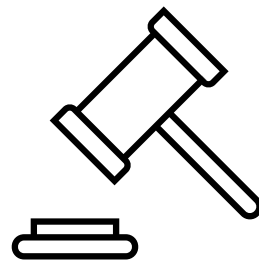
Complex platform
with decision-making AI



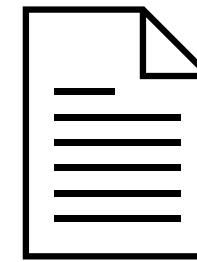
Change management approach
tailored to developers



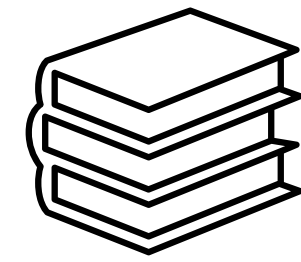
Privacy by design
included apart of security



Compliance and
juridical expertise



Rule framework



Training content

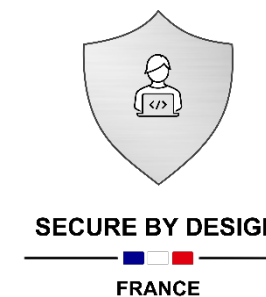


Go-to-market strategy



Acquisition Channels

- Community engagement (conferences, workshops)
- Software publishers to reach their integrators
- Software integrators to reach the publishers they integrate
- Partnership with schools and universities
- Distributors or co-marketing with other suppliers of our targets
- Position as a trust enabler for compliance (CRA, NIS2, DORA, ISO 27001, AI Act)
- B to C for developers





Achievements

150 developers are using our tool

Our customers :

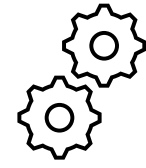


According to ECSO, Cybalgoris is one of the 4 most promising cybersecurity startups in Europe.





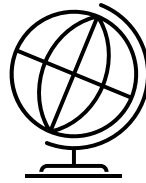
CYBALGORIS is built to scale



- ✓ Technology
SaaS, cloud-native, API-driven.



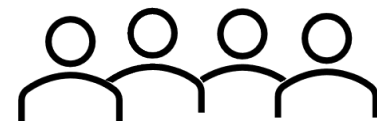
- ✓ Conformity
we master cybersecurity compliances.



- ✓ Natively international
French & English language



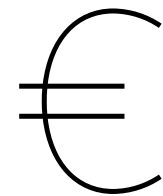
The team



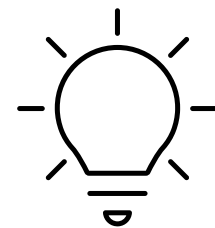
A complementary team collaborating with great efficiency



Deep expertise and experience in cybersecurity, software and AI.



High entrepreneurial experience



Strong ability to innovate



The team

Co-founders



Teodor Suteu
MS2 Digital
CTO



Alexandra Sfrijan
Executive ACE MIT
Product development

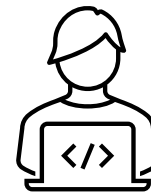


Laurent Bernier
Engineer & MBA HEC
Marketing and commercial



Roland Carbonnel
IT companies management
CEO, Marketing and commercial

The developers



6 senior
developpers

Cybersecurity certifications

Governance, Architecture & Audit

CISSP
CISSP-ISSAP
CISA
ITIL v3 Foundation

Infrastructure & Network Security

CCNA
Cisco ISCW
Cisco BCMSN
CompTIA Security+
CompTIA Network+
RSA Certified System Engineer

Software Security

CSSLP
CyberArk Certified PIM Suite Professional

Cryptographic Hardware & Key Management

Thales nCipher Certified System Engineer
Safenet Luna SA Certified Engineer
Safenet ProtectServer Certified Engineer
Safenet-Aladdin eToken Certified Engineer

Identity & Access Management

Oracle Identity Solutions Workshop
Safenet – Technical Training (Luna HSM, DataSecure, PSE, SEE)

AI

PhD in Human-Computer Interaction
Assistant Professor in IT – National
University of Science and Technology
Politehnica Bucharest



Our vision



Secure by Design defines how resilient software must be built. And resilient software is essential to **national security**.

We aim to bring this methodology into the hands of developers, **to improve** how software is designed, written, and maintained.

When security is part of the development mindset, it becomes **a natural part** of how systems grow and scale.

Secure by Design needs to become **a common practice** across the industry, embedded from the start of every project, in every team.

We will make this shift real, through technology, through engineering practices, and through a **shared commitment** to change.

We are ready to lead, to listen, and to grow, so that **preventive security** becomes **a standard** of excellence in software development.



Contact us ...



Email contacts

alexandra.sfrijan@cybalgoris.com
laurent.bernier@cybalgoris.com



Phone numbers

RO +40 740 062 235
FR +33 671 212 775



www.cybalgoris.com



Company info

SIREN: 922 089 628

EU VAT: FR04922089628

Incorporation Date: 09 December 2022

NAF / APE: 5829C – Software publishing

Legal Form: SAS – Société par Actions Simplifiée



Address

12 rue de la Part-Dieu
69003 Lyon, France