

Wavestone Cyber Benchmark

2026 Edition

What is the market maturity?

June 2026

WAVESTONE



Wavestone Cyber Benchmark: an in-depth analysis of the level of cybersecurity maturity

Based on NIST Cybersecurity framework, ISO 27001/2 and NIS 2, the **W-CyberBenchmark***, our **360° assessment approach**, goes further and provides:



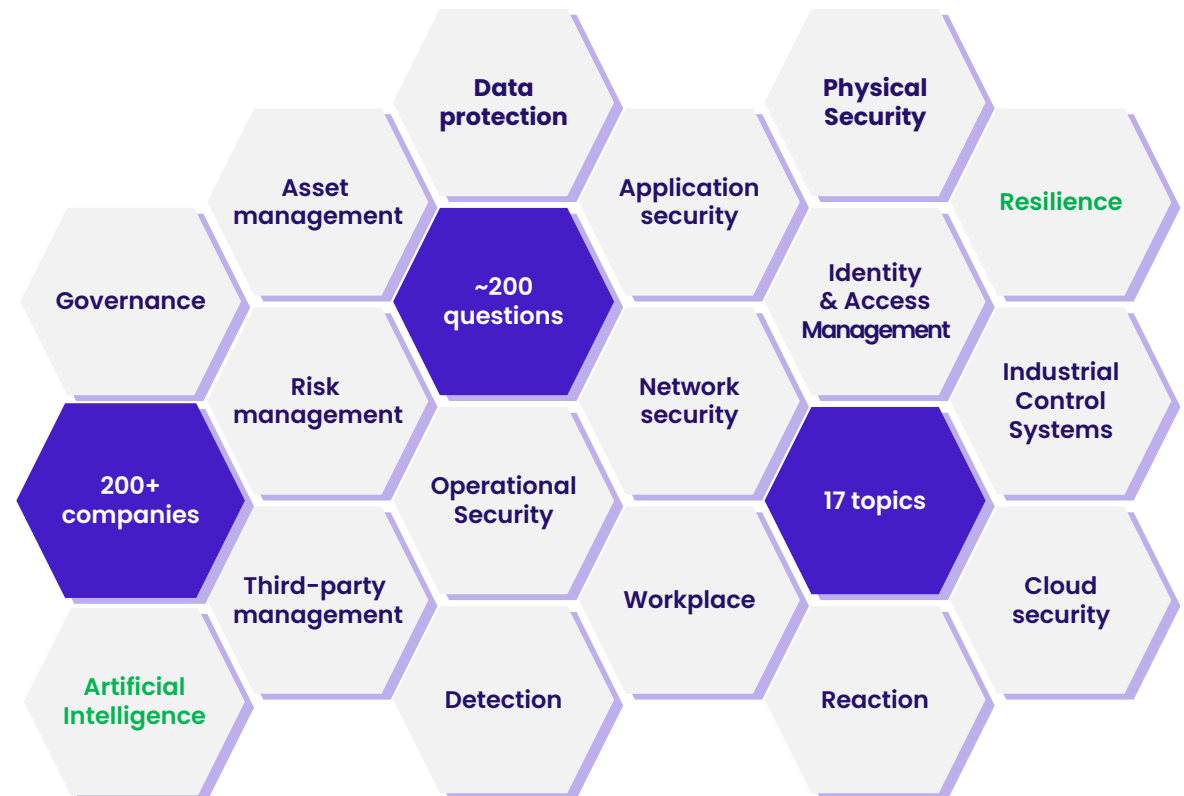
A comprehensive approach with an **organizational** and a **technology maturity assessment** including a **pioneer level** that capture innovation



An assessment built for **multi-entity complexity**, now expanded to include **AI security**



200+ Wavestone customers including **100+ companies** with a turnover above 1 billion and presenting more than 7 million employees



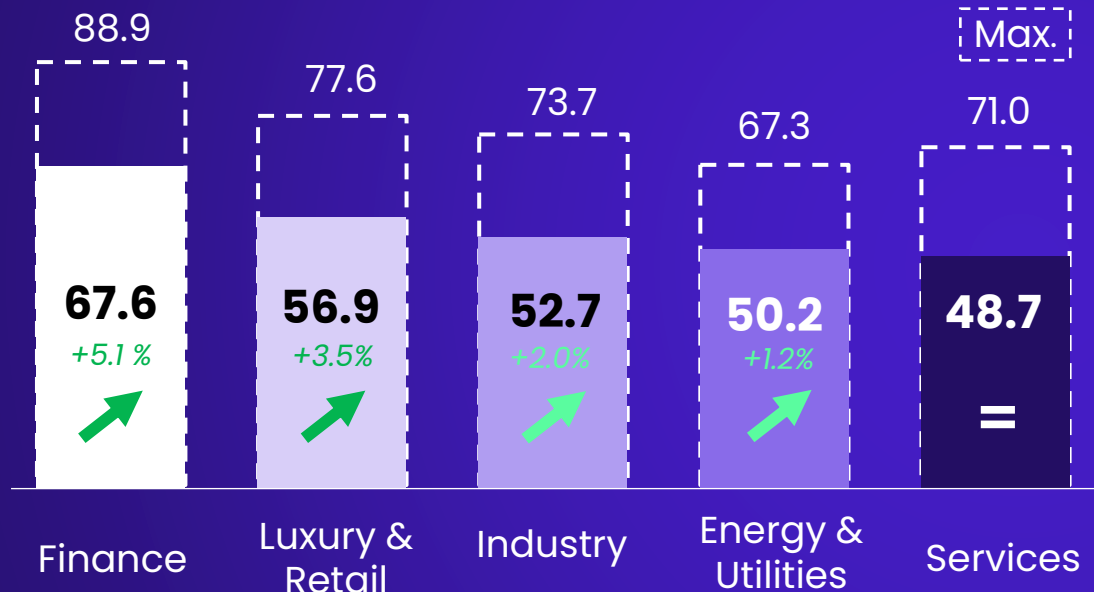
Large Organizations Cyber Maturity Keep Accelerating



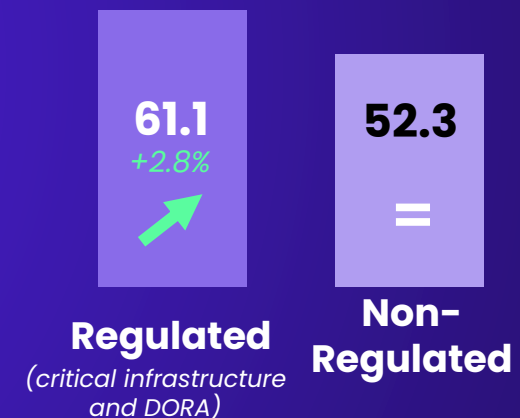
Large organizations showed a sustained rise in cyber maturity, and growth is now speeding up **(+1.3 pts vs. 2025)**

*Companies with a turnover over \$1B (100+ org.)

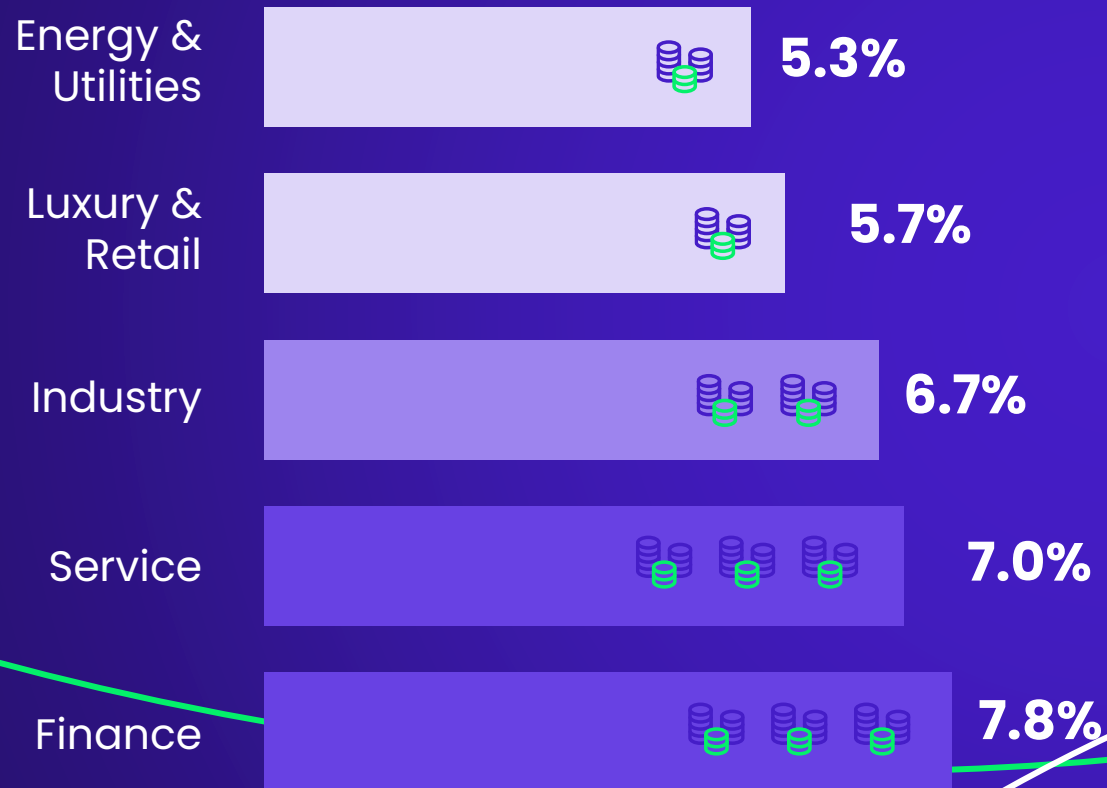
Financial sector is well ahead in overall maturity



Regulations have a major impact on maturity



Cybersecurity spending remains **mostly stable** in large organizations*



Average IT budget percentage dedicated to **cybersecurity***

6.7%

2025: 6.4%

Range

First quartile
3.1%

Last quartile
8.0%

**Taking into account that budget percentages can vary a lot depending on previous investments and current build VS run balance*

Despite the lack of resources, cyber teams are **still growing**...

Average **FTE** dedicated to cybersecurity per employee in large organizations

1/979

Range

2025: 1/1016

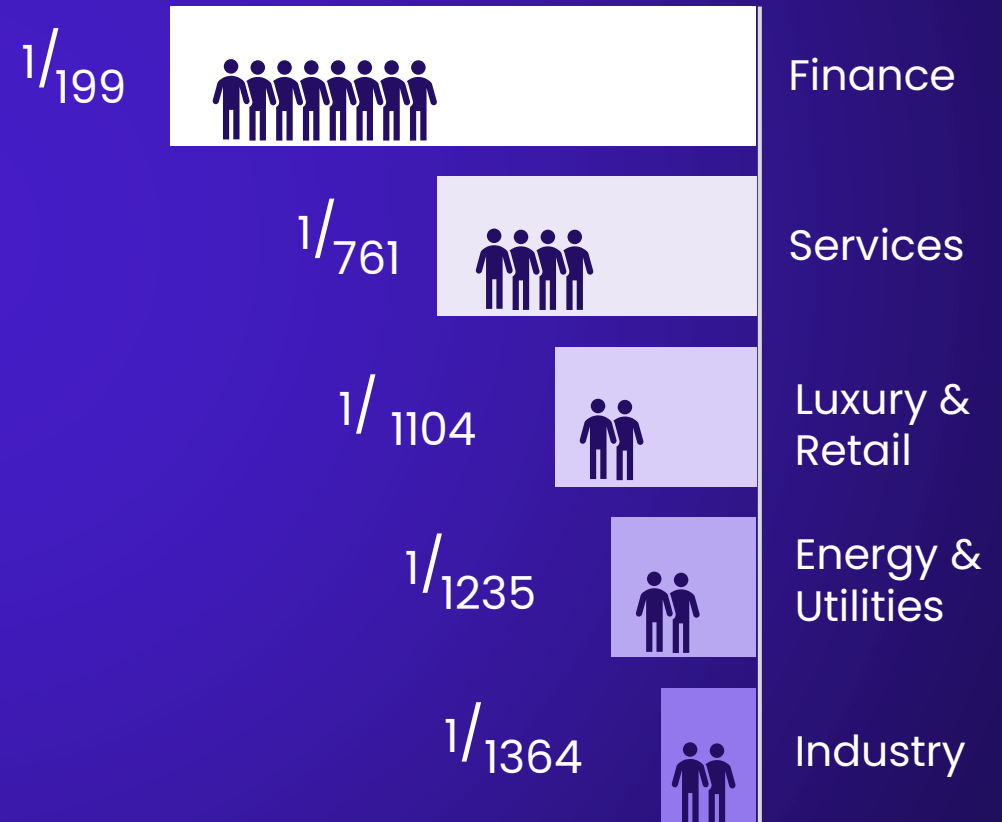
Best in class (top 10)

1/83

Last quartile

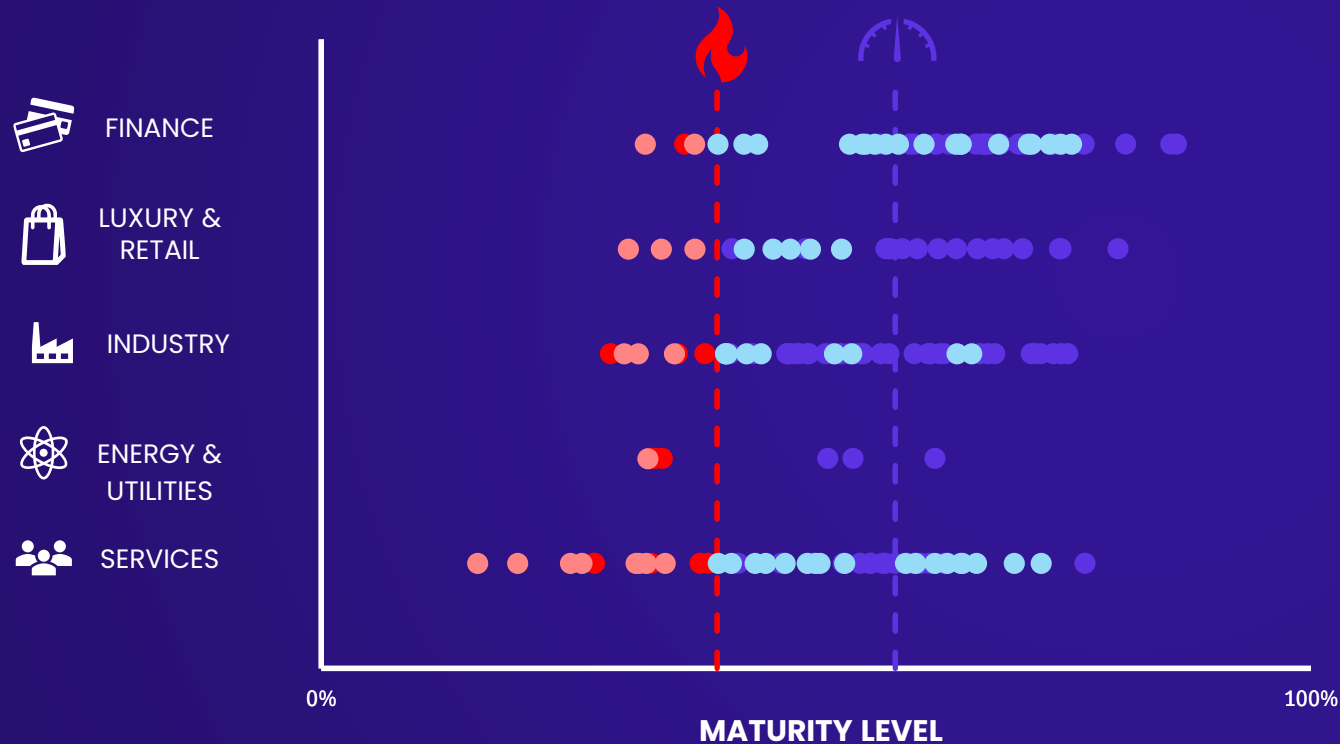
1/1188

... but disparities between sectors remain strong



How does the market stand against the latest **cyberattacks**?

Based on the latest **cyberattacks managed by CERT-Wavestone**, we have selected 29 anti-ransomware measures and assessed our customers' maturity on (attack entry point protection, crisis management, backups, red button...)



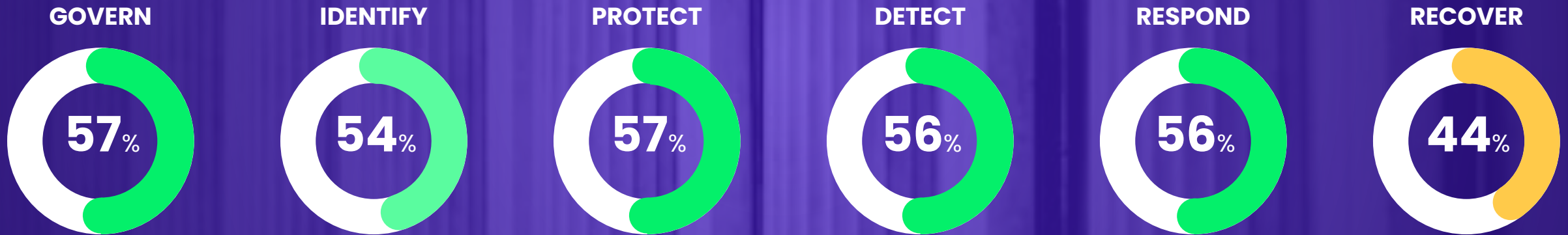
58% (+2%)
ANTI-RANSOMWARE MATURITY
OF **LARGE ORGANIZATIONS***
AND ONLY A FEW IN CRITICAL
SITUATION

25% (-11%)
OF **MEDIUM ORGANIZATIONS**
CONSIDERED TO BE IN A
CRITICAL SITUATION

Above the critical threshold	Below the critical threshold	Reference points
● Large organizations	● Large organizations	— Average maturity of large organizations
● Medium organizations	● Medium organizations	— Critical threshold

*Companies with a turnover over \$1B (100+ org.)

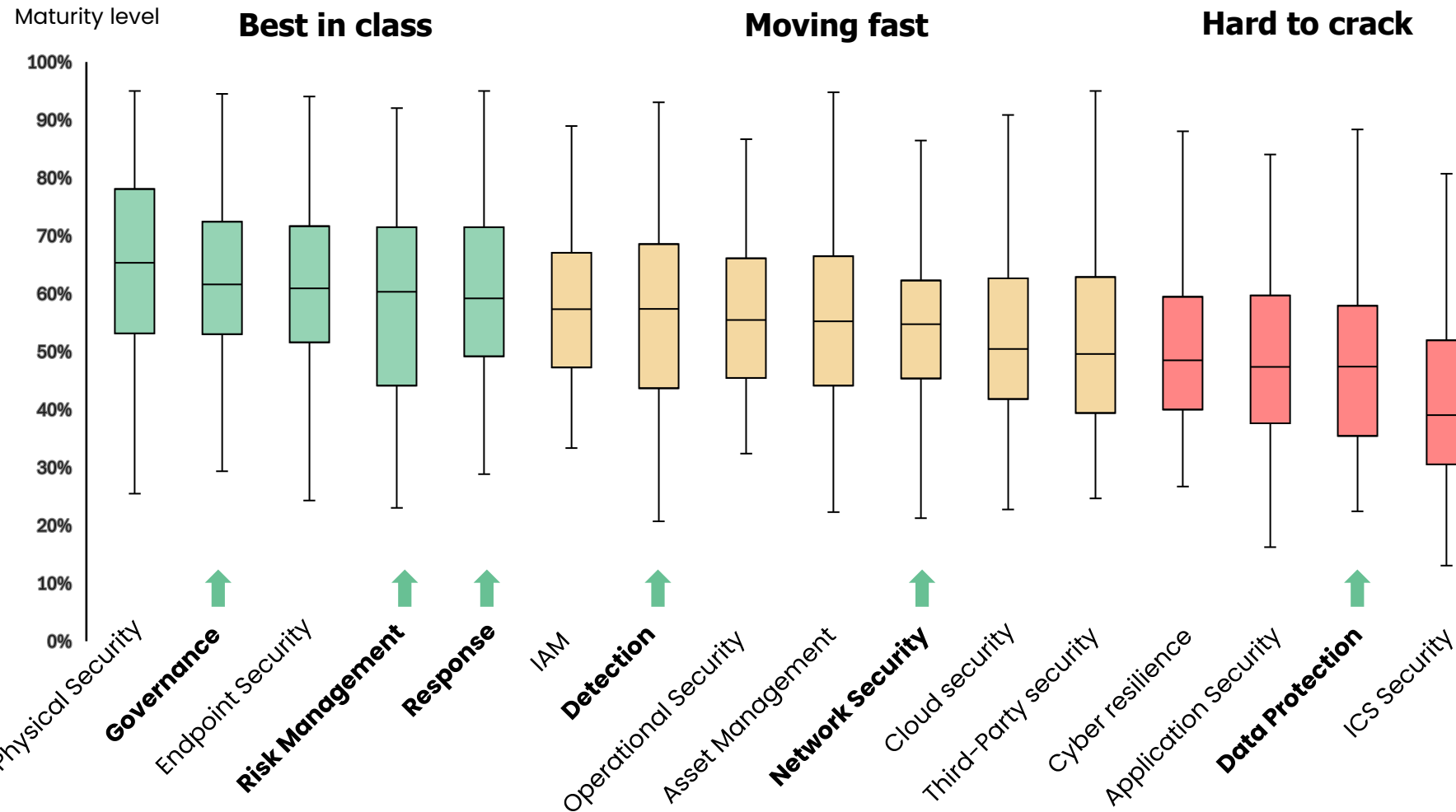
What is the market **MATURITY** in adopting the new **NIST Cybersecurity** Framework?



The **high consistency** across the **NIST CSF 2.0 pillars** highlights the **significant cybersecurity investments** made in recent years. The only exception is the "**Recover**" pillar, which lags behind in **crisis management** and **resilience capabilities** though the **financial sector stands out** with a higher maturity level (58%)

High-level snapshot of cybersecurity performance

Large enterprises' cyber maturity overview



Legend

↑ Topics that have gained maturity since 2024

Box plot view of maturity score for every topic: Minimum / 1st quartile / Median / 3rd quartile / Maximum

Governance

Governance has improved (+2%), driven by regulatory pressure and stronger executive involvement, with clearer roles and better integration of cybersecurity into business strategy.

Risk management

Risk management is progressing (+2%) with more structured approaches, improved risk prioritization, stronger treatment plans, and increasing use of proactive measures like bug bounty and agile integration.

Detection

Detection capabilities are advancing significantly (+5%) thanks to SOC maturity and the adoption of SIEM, EDR/XDR, and AI, improving visibility despite ongoing operational challenges.

Incident response

Incident response has improved (+2%), supported by better team availability, external support, and more structured documentation, enabling faster and more coordinated reactions.

Resilience

Cyber resilience has improved (+3%), with organizations strengthening their preparedness through expanded cyber insurance coverage, more frequent crisis exercises, and increased testing of backup restoration, helping ensure better continuity in the face of major incidents.

What TO EXPECT in the years to come?

Current maturity:



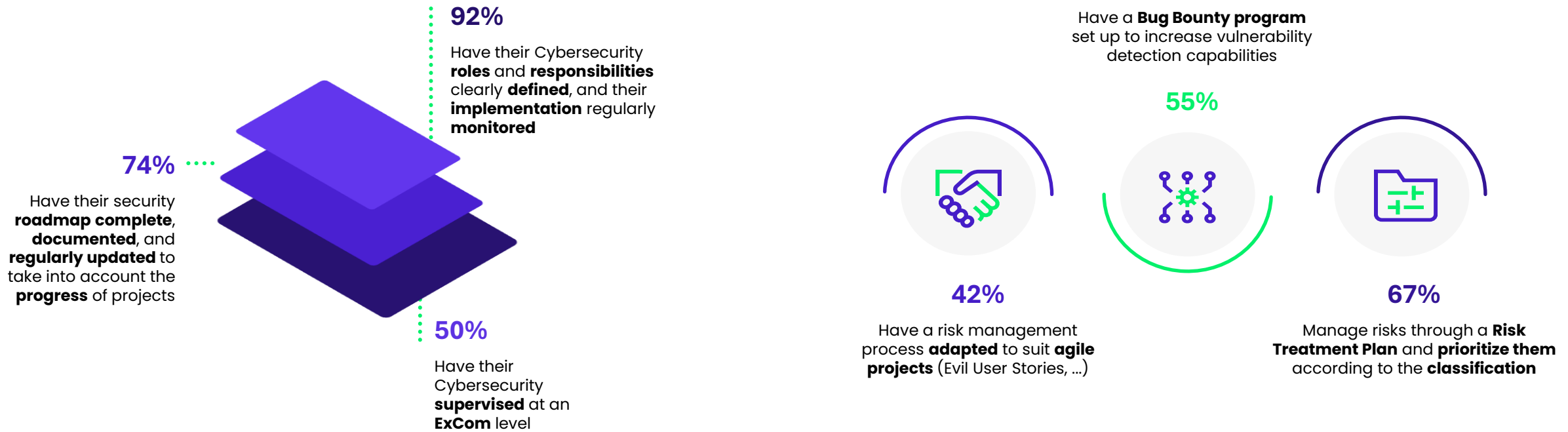
5 key topics from 2026

Governance & Risk Management: Strongly Established, Constantly Advancing

62%

58%

These figures highlight the **continued strengthening** of **governance** and **risk management**, with maturity levels reaching 62% for governance (+2% since 2024)* and 62% for risk management (+2%)* reflecting **sustained investment** and **steady progress** despite their high level of maturity.



New activities to be integrated regarding to AI



AI Risk Management

Design and maintain the **AI risk management framework**, lead and coordinate **AI risk assessments**



AI Compliance Office

Lead **AI compliance** (AI Act, NIST AIRMF) and define the **AI system classification** (high risk, etc.)



AI Governance

Define and maintain **AI policies, standards, controls**, and facilitate **AI decision-making processes**



AI Third-Party Risk Manager

Evaluate **AI suppliers** and manage **SAAS/API risks** (LLM, etc.)

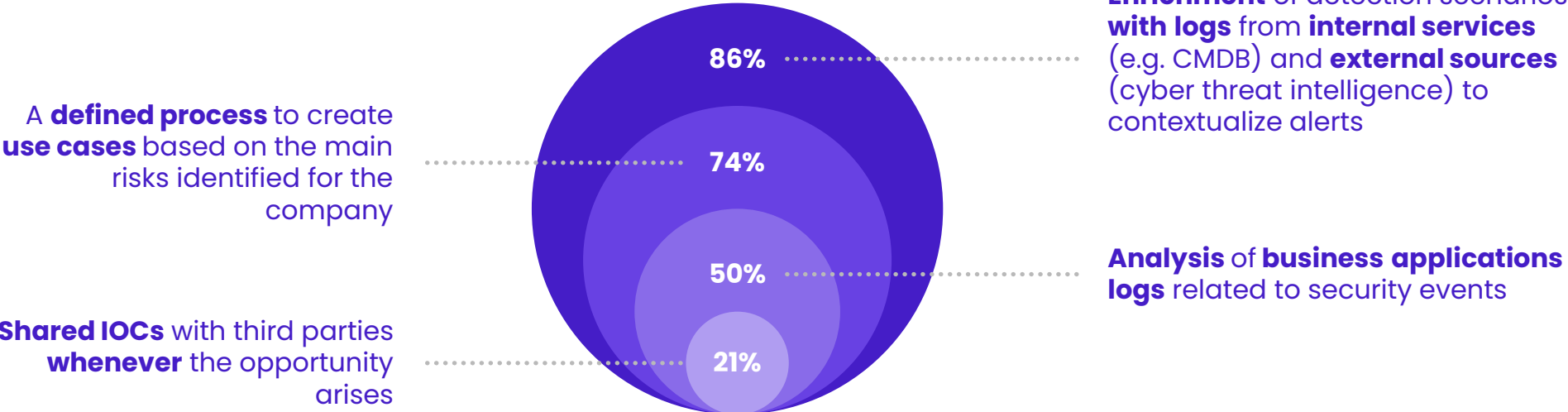
*Companies with a turnover over \$1B (100+ org.)

Detection: stronger controls, faster response

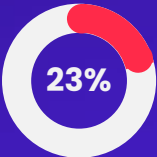


Detection continues to make progress in **2026**, reaching a maturity of **57%** among large organizations (**+5%** compared to **2024**)*

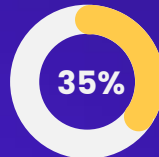
Percentage of large organizations that have implemented each specific practice:



Main challenges to be overcome with the arrivals of AI solutions?



Creation of custom detection scenarios for advanced threats (e.g. rogue administrators, lack of client segregation)



Integration of behavioral analysis capabilities into detection probes

*Companies with a turnover over \$1B (100+ org.)

Response: An Ever-Evolving Incident Challenge



Maturity of **response** capabilities by **large organizations** rose significantly (+2% compared to **2024**)*

Percentage of large organizations that have implemented each specific practice:

A Solid Foundation



Definition, communication, and enforcement of a security **incident management process**

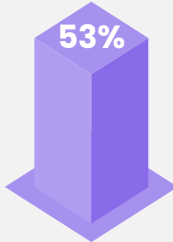


Establishment of **clear 24/7 emergency SLAs** and **confidentiality requirements** with cyber response contractors

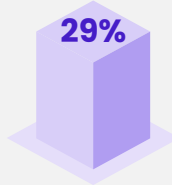


A **24/7 assistance team** can be mobilized with **limited means** (expertise, size...)

Ongoing Challenges



Documentation of **distinct cyber response plans** tailored to **different incident** and **attack types**



Deployment of a **SOAR** solution to **automatically isolate resources** upon alert detection



Main challenges to be overcome

AI-enabled threats

Increased and more **sophisticated phishing** and **deepfakes**, as well as the first **malware leveraging AI** in its deployment, are emerging

AI transformation

First successful deployments have **automated the response on spam and phishing**, improving alert qualification,

AI response team

Dedicated **AI-focused response teams remain limited**

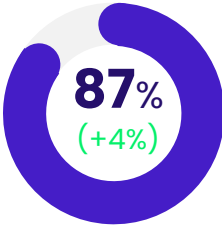
*Companies with a turnover over \$1B (100+ org.)

Cyber Resilience: a strategic ambition still hard to achieve

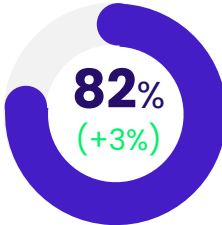


Cyber resilience remains a **complex topic** (+3% compared to 2024, notably in **Finance +5%)***, as **few organizations** are truly prepared to maintain their business in the event of a **major attack**

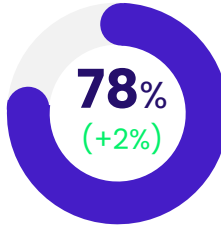
Percentage of large organizations that have implemented each specific practice:



are covered by a **cyber insurance policy**

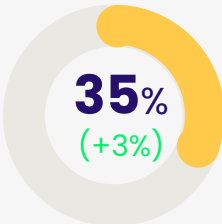


conduct crisis management exercises at least every two years

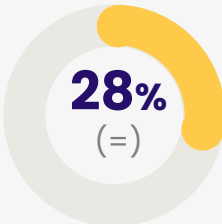


regularly conduct **restoration tests** in accordance with their backup policy

Despite the progress, certain areas still need strengthening



deploy **degraded mode processes** tailored to users and critical functions



assess **dependencies across each business chain** at a global level



In 2026, resilience teams are currently **reviewing their risk evaluation and response** due to **political evolutions** (technology bans, data flow limitation, local regulations, ...)

*Companies with a turnover over \$1B (100+ org.)

Securing a critical asset: artificial intelligence

38%

We are reaching a first level of maturity in AI security, based on insights from +20 large organizations

AI governance and risk identification is already a thing ...

...but the journey has just started for complete maturity

76%

Have an **AI security policy**

62%

Give clear **go/no go decision** at AI project risk review

57%

Identified a team to assess **AI projects compliance**

48%

40% of clients **adapted their Third-Party assessment methodology** for AI vendors

10%

Established measures to defend against **malicious prompts** and other threats

GOVERN	IDENTIFY	PROTECT	DETECT	RESPOND
48%	48%	43%	35%	8%

Maturity

100%

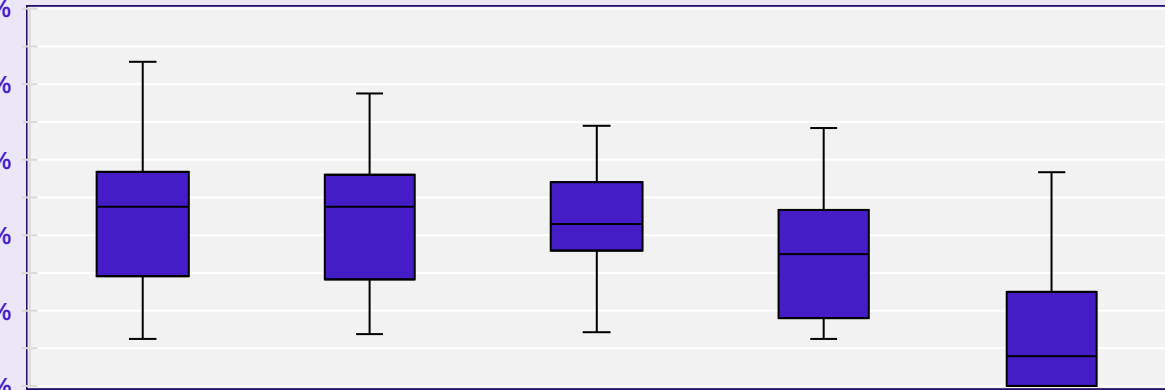
80%

60%

40%

20%

0%



There is no **'Recover'** pillar, as there is no **dedicated recovery specialization for AI.**

NIS 2: How compliant is the market with French security requirements (ReCyF)?

Large organizations*
60
/100

Organizations **not** currently **subject to cybersecurity regulations** achieve only **60%*** NIS2 maturity **highlighting** the **substantial efforts** still required to **reach full alignment**

First Observation

NIS2 compliance remains **heterogeneous**, with **French** pure players and **international actors** **progressing at different paces** due to the **uneven transposition of the directive across European jurisdictions**

Second Observation

The level of NIS2 requirements remains **uneven** across countries, from **highly stringent** to **more flexible approaches**, forcing large organizations to **align** at the **closest level** across **all subsidiaries**



Wavestone's added value

An AI-based tool comparing NIS2 regulations across countries, bringing clarity to a fragmented landscape

Hard-to-crack topics



Enhance Third-Party Risk Management



Ensure Resilience



Strengthen Asset management



Meet Administration requirements

Cross-country difficulties



Regulatory difficulties

Uneven regulatory involvement across countries creates inconsistencies in **oversight** and **expectations**



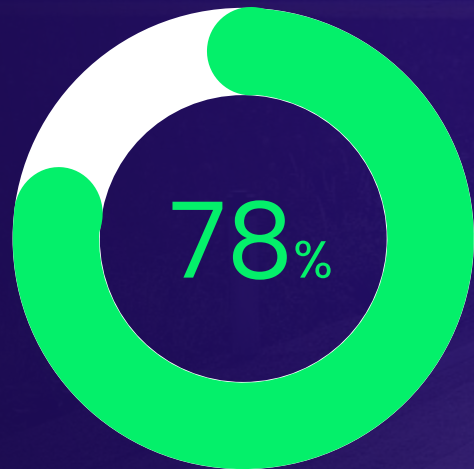
Scoping difficulties

Diverging audit scoping approaches (local vs global systems) across countries lead to **unclear regulatory submissions**

* Based on a sample of 15 large organizations across various sectors, assessed against local NIS 2 frameworks; evaluations covered either the full organization or specific scopes

The need to address **Emerging** and **innovative** topics

Many companies are **starting to reach a high level** of maturity against the international standards

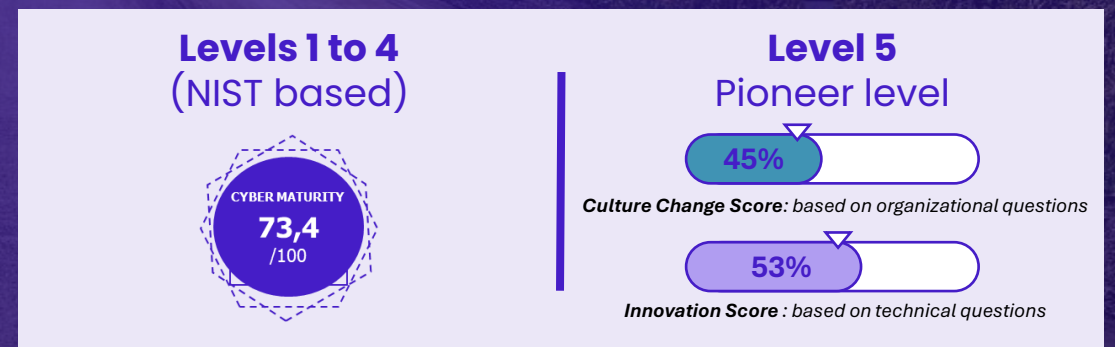


Average maturity score of TOP 10 companies in our cyber benchmark

A need to cover the new and innovative topics

- Quantum Cryptographic
- AI security
- Just-in-time / Just enough
- API based
- Quantification
- Security Data Hub
- Culture change
- Digital twin
- AI for cyber
- Platformization

Introduction of a new maturity level for pioneers



Wavestone Cyber Benchmark

2026 Edition



Gérôme BILLOIS, Partner
gerome.billois@wavestone.com



Julien MOREAU, Manager
julien.moreau@wavestone.com



Roya ALIYEVA, Consultant
roya.aliyeva@wavestone.com