WAVESTONE

Cyber Benchmark

How is the market performing?

April 2023

Florian POUCHET
Director
florian.pouchet@wavestone.com
+44 7493 867 766

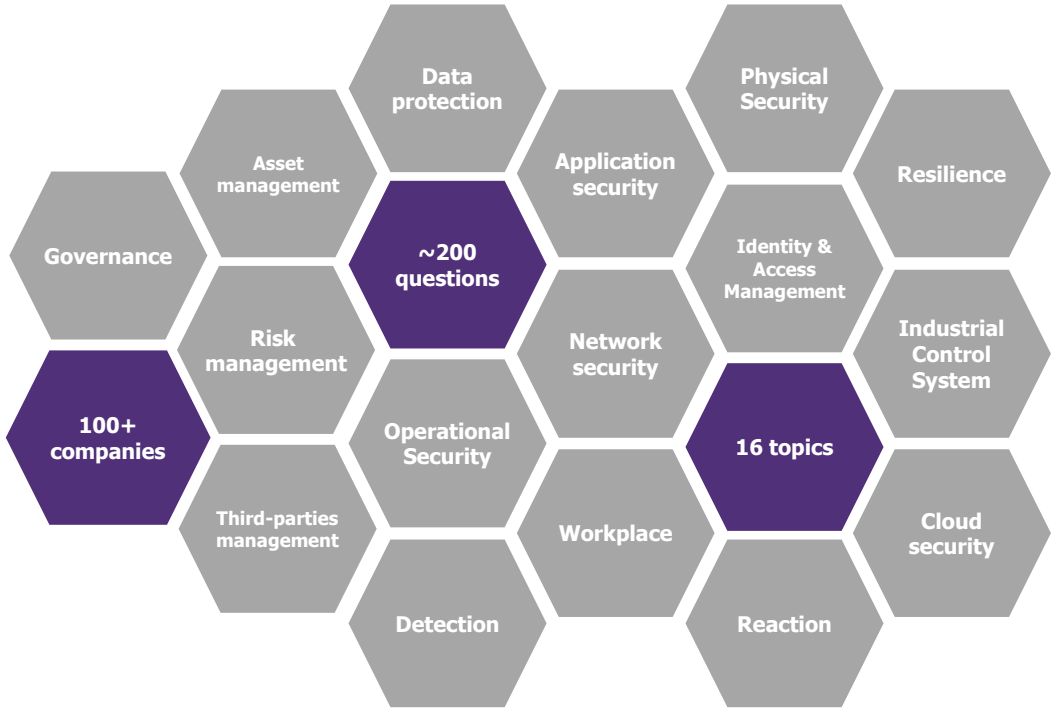
Maturity analysis based on Wavestone's benchmark

A new approach based on NIST CSF Framework & ISO 27001/2

A key innovation: the evaluation of the **maturity distribution** of each topic, covering **organizational** and **technology controls**

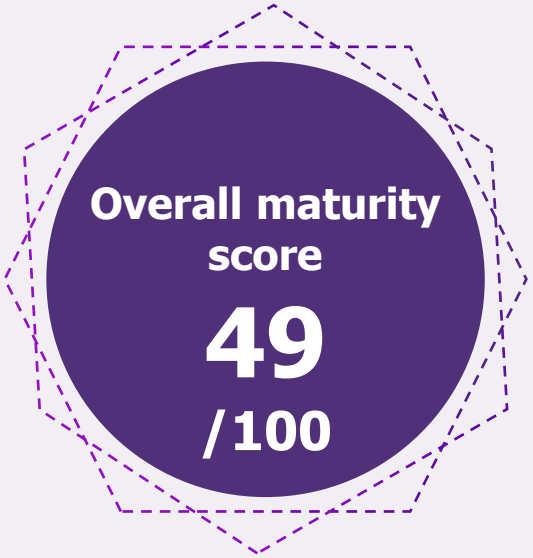
A **reliable approach**: data collected through in-person maturity assessments done over the last 4 years by Wavestone

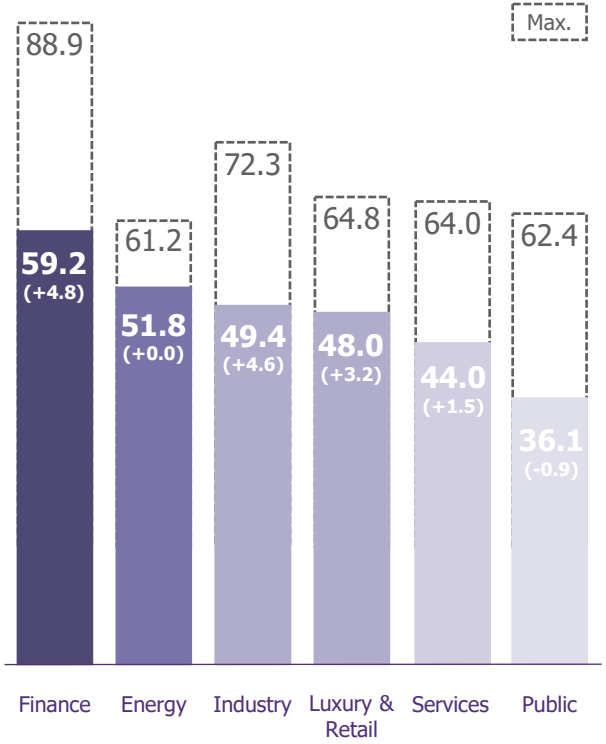
A dataset of 100+ companies among the **largest tier 1 companies**: industry, services, financial services, luxury, retail, energy and public… Representing nearly **5 millions user accounts!**

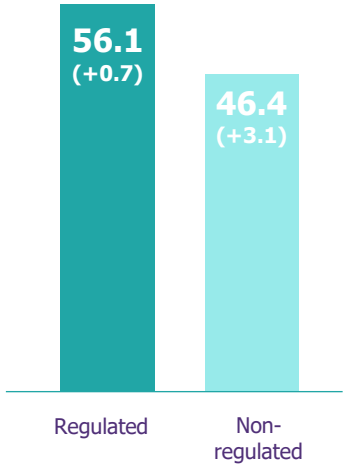


Wavestone Cyber-Benchmark

2023 global overview







Average is up 3 points
compared to last year

Wide differences between sectors

Regulation have a positive impact

Companies spend **an average of 5.6% of their overall IT budget on cybersecurity**

Average IT budget percentage
dedicated to cybersecurity*

Last quartile: **2.9%**

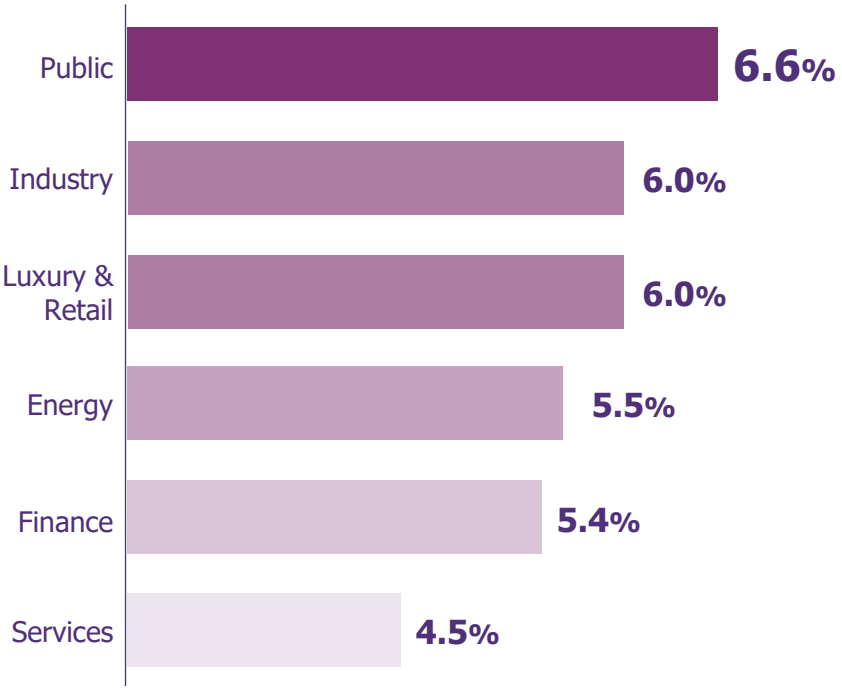
5.6%

First quartile: **7.1%**

Example of yearly budget
Based on Tier 1 companies' investment declaration

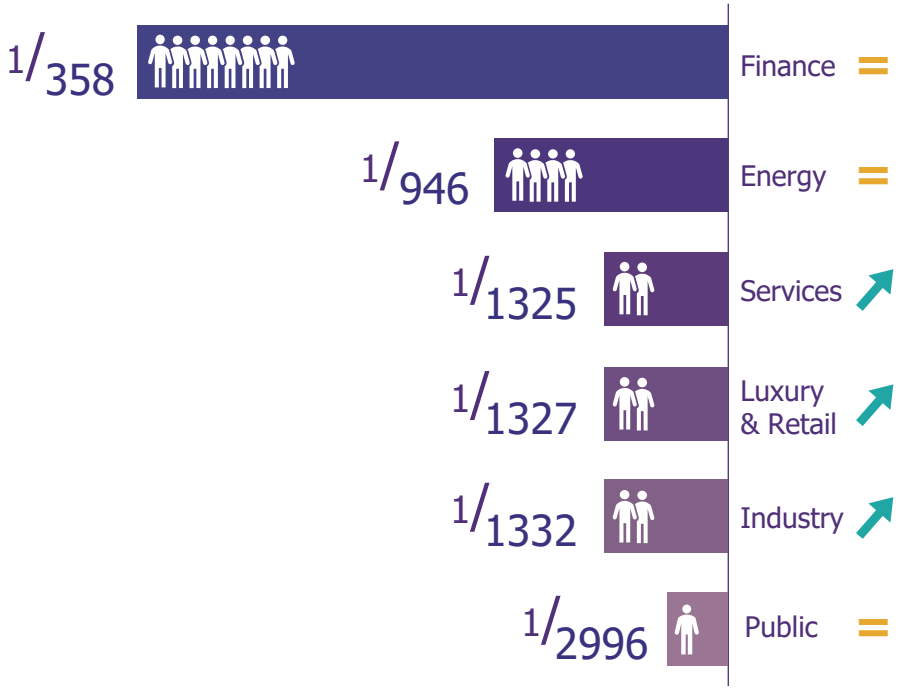
Financial services	Other sectors
200 – 900 M€	30 – 250 M€

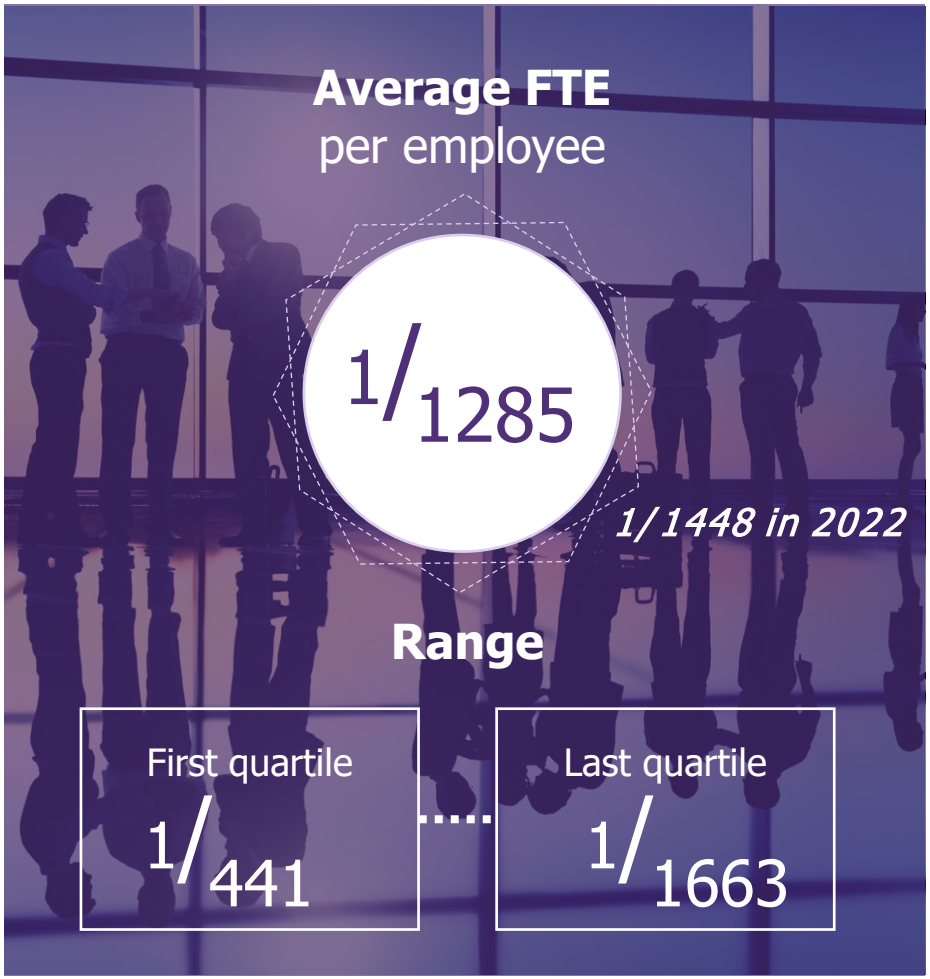
Today, less mature sectors are mainly the ones investing most



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

Cybersecurity teams are growing quickly, **many companies have doubled the size** of their team

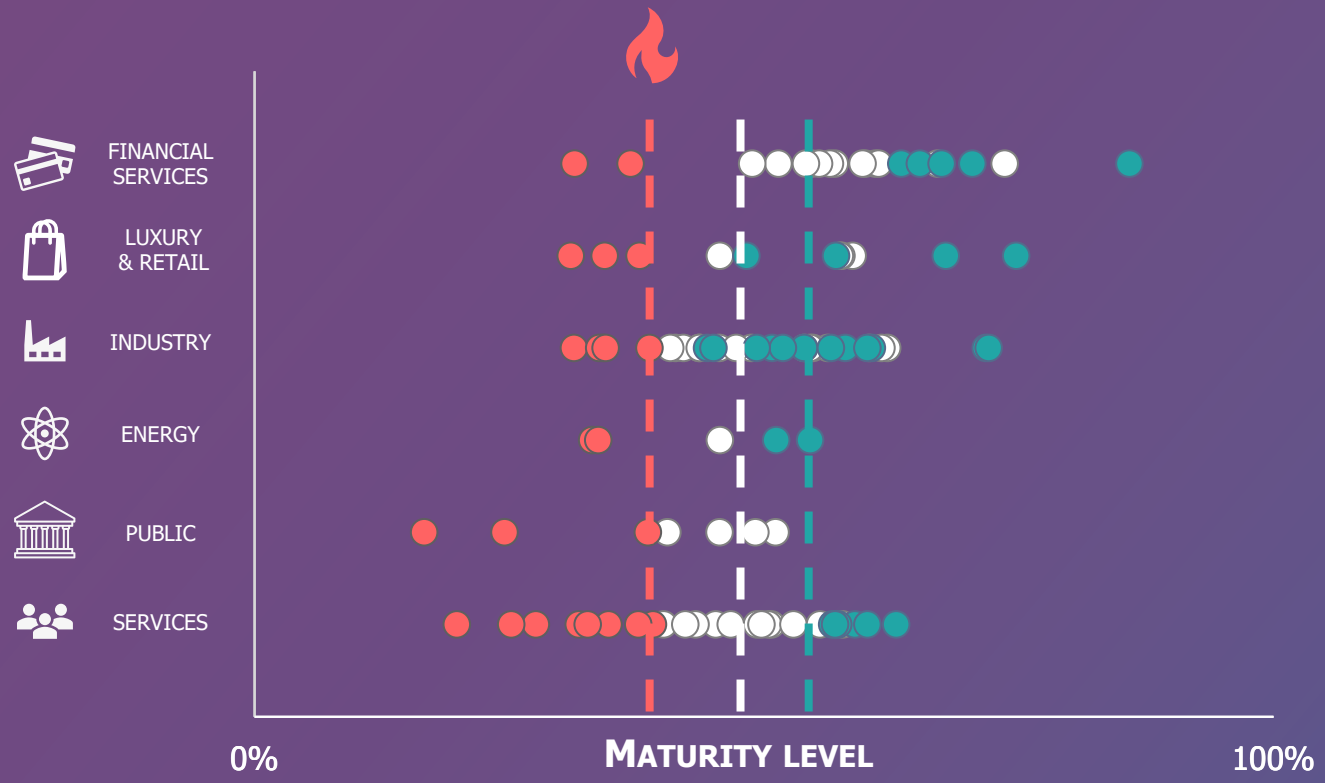





How does the
MARKET stands
against the latest
cyberattacks?
49.8%
(+3.6%)
of overall resilience against
RANSOMWARE

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

Specific investments against **ransomware** have paid off, less companies are easy targets.



ALL WAVESTONE CLIENT'S AVERAGE: 49.8%

TIER 1 COMPANIES' AVERAGE: 59.8%

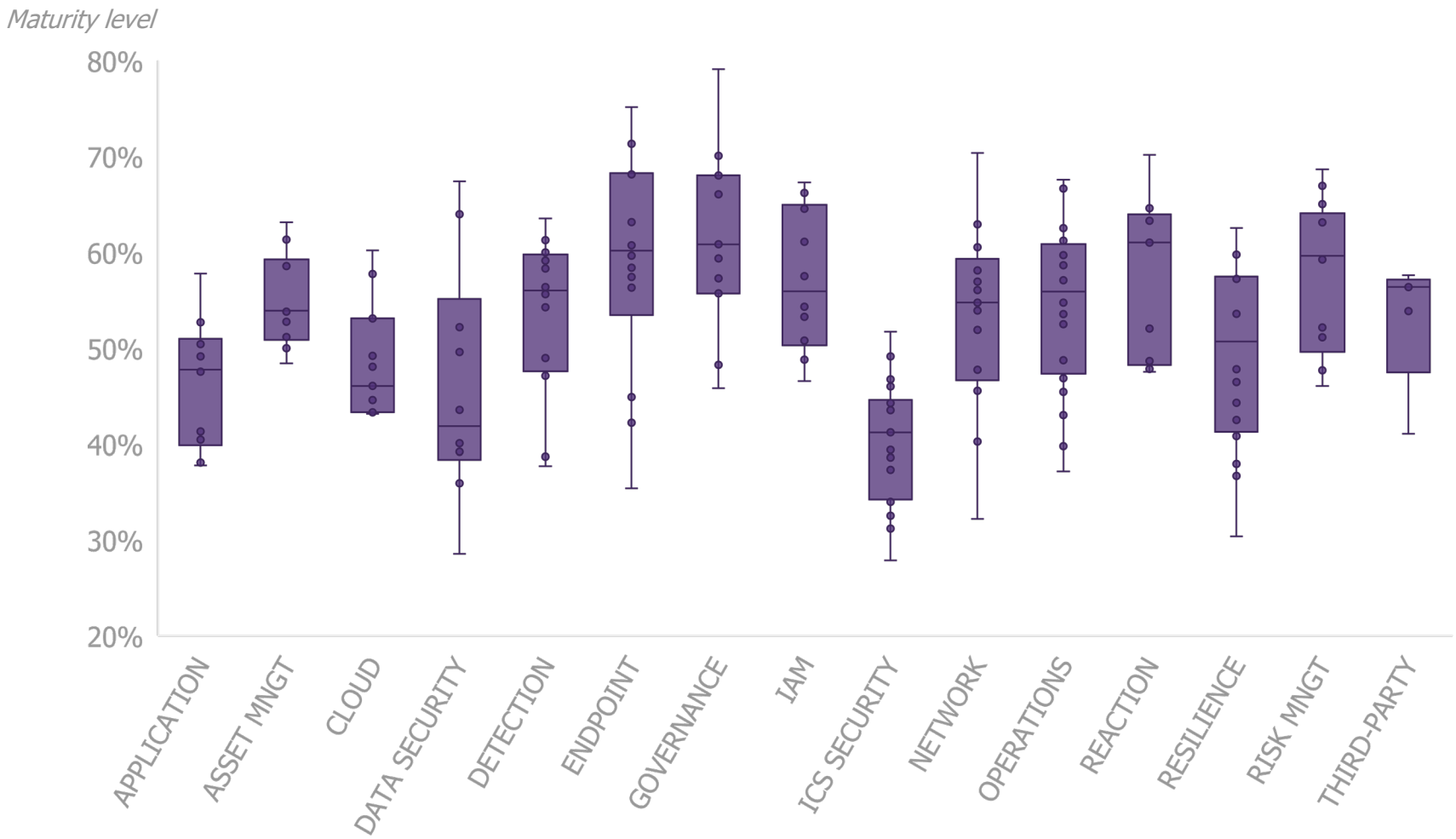
23% COMPANIES CONSIDERED IN A CRITICAL SITUATION (30% IN 2022)

*Based on the latest cyberattack the CERT-Wavestone managed, we selected **29 anti-ransomware controls** and evaluated maturity on these topics*

How is the **MARKET** *doing on* **cyber topics?**

NIST pillars are nowadays mostly **homogeneous** with a coherent investment on **all topics**.
The **Recover** topic is still slightly lacking behind due to its complexity and the number of systems concerned.

How is the **MARKET** *doing on* **cyber topics?**



Box plot view of maturity score for every topic: Maximum / 1st quartile / Median / 3rd quartile / Minimum. One dot is one control.

How is the **MARKET** *doing on* **cyber topics?**

Box plot view of maturity score for every topic: Maximum / 1st quartile / Median / 3rd quartile / Minimum. One dot is one control.

Cyber reaction and detection has been in the top priorities in terms of investment

Incidents are better and faster handled…

48% (+16pts) of companies have put in place a **Red Button** to isolate a part of the network. Red button's coverage is **58%** on average

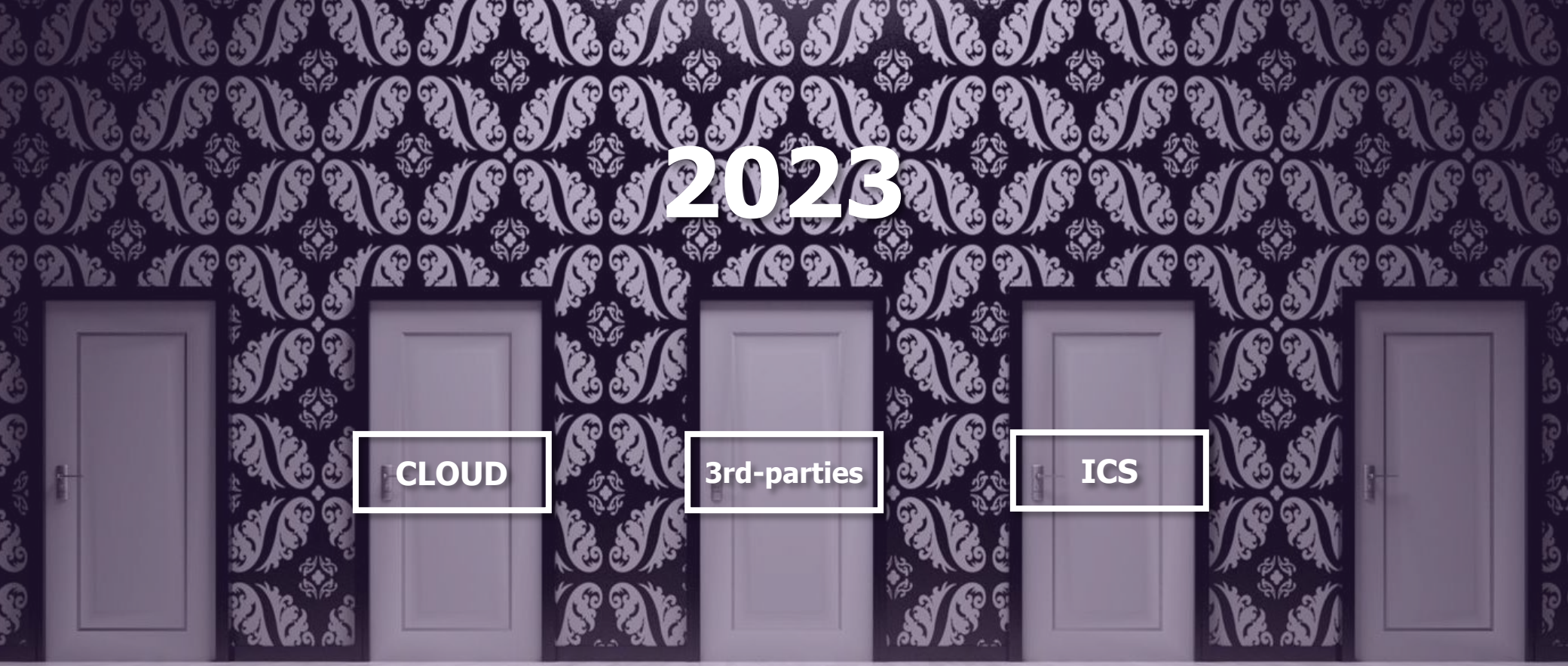
43% (+20pts) of companies have formalized all **emergency shutdown procedures** and communicate all types of incidents to their teams

58% (+15pts) of companies have detection probe connected to the SIEM, and **22%** (+3pts) have started deploying **behavioral analysis** probes

29% (+11pts) of companies have improved **IOC handling** and **operational use**

…with tools allowing a better detection

… resulting in **a better handling of attacks** and **less operational impact**



Some entry points are being
increasingly exploited by
cybercriminals

Cloud is a key topic concentrating important investments now reaching **44.5% (+8.4pts) of maturity**

Cloud monitoring & detection

62% (+4pts)
of companies send Cloud logs to their **SOC** (and 11% (+7pts) have specific use cases)

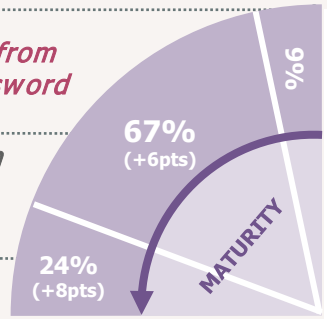
38% (-4pts)
of companies rely only on **alerts** from their Cloud provider

Cloud administration

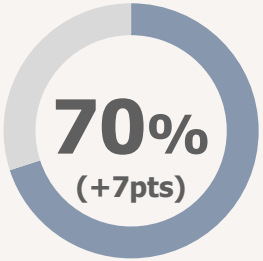
Cloud console always accessible from anywhere, using a login and password

*Access uses **multi-factor authentication** (MFA) for privileged accounts*

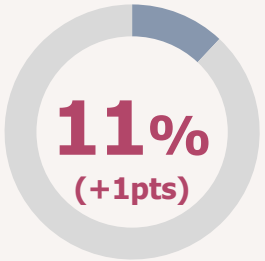
*Access is performed via a **bastion***



Cloud compliance



of organizations have tools to **check Cloud compliance**

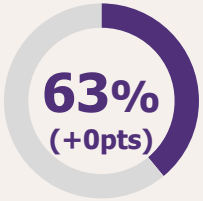


of organizations automatically **remediate** Cloud compliance **issues**

Third-party security remains a thorny issue* due to the increasing interconnection with partners & suppliers

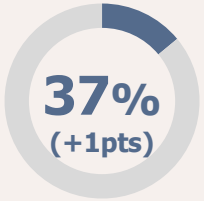
*with 46.9% (+2pts) of maturity

Contract management



of companies **includes security clauses in contracts** when contracting

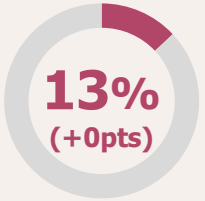
3rd-party audits



of companies **audit regularly** their critical IT suppliers

even if more than 61% of companies have correctly inventoried their suppliers

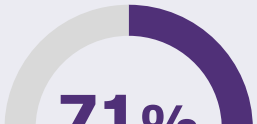
Resilience testing



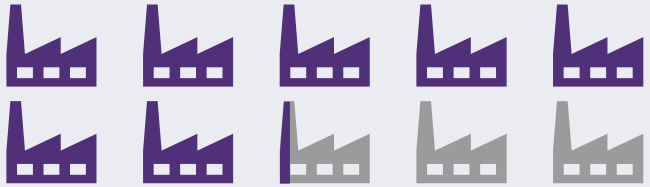
of companies **test** their **response** and **recovery plan** with their partners/suppliers on **all critical perimeters**

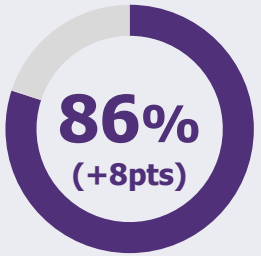
OT / Industrial systems security has an overall **maturity of 37.6% (+3.4pts)**

Good news: security basics are being achieved…



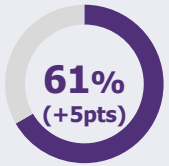
of companies have started deploying a **cybersecurity organization** on their industrial scope





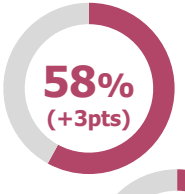
of companies are using **firewalls** to separate corporate networks from ICS networks

and

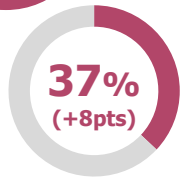


of companies have setup **Demilitarized Zone** (DMZ) to enable advanced filtering

…but still important lacks on **key security good practices**:



of companies use **dedicated tools to remotely administrate** ICS

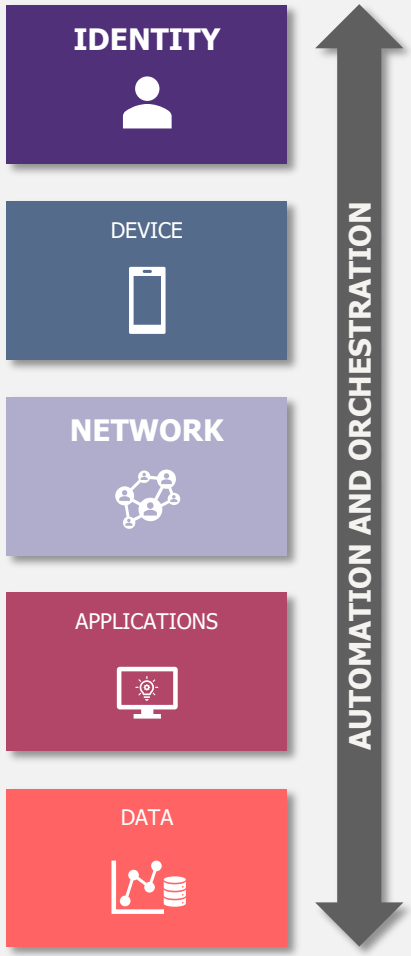


of companies inject OT security logs into a **proper monitoring tool (SIEM)**


How do we move forward regarding the
2 PRIORITIES for many CISO**?**
ZERO-TRUST
RESILIENCE

Zero Trust, a major strategy starting to be deployed

Zero-Trust foundations from CISA



IDENTITY

28% *of companies started deploying **multi-factor authentication** taking into account the **sensitivity of resources** and the **connection context**.*

0% 50% 100%

Multi-factor authentication with **conditional access** covers **73%** on average

NETWORK

24% *of companies started deploying automated **Micro segmentation** based on exposition, sensitivity, environment, etc.*

14% *of companies started deploying **Zero Trust Network Access** based on identity on their Cloud environment.*

0% 50% 100%

Micro Segmentation's coverage is **32%** on average

Zero Trust Network Access tools covers 46% on average

AUTOMATION AND ORCHESTRATION

13% *of companies started deploying a **Security Orchestration Automation Response** to **isolate resources** when an alert is raised.*

0% 50% 100%

SOAR coverage is **48%** on average

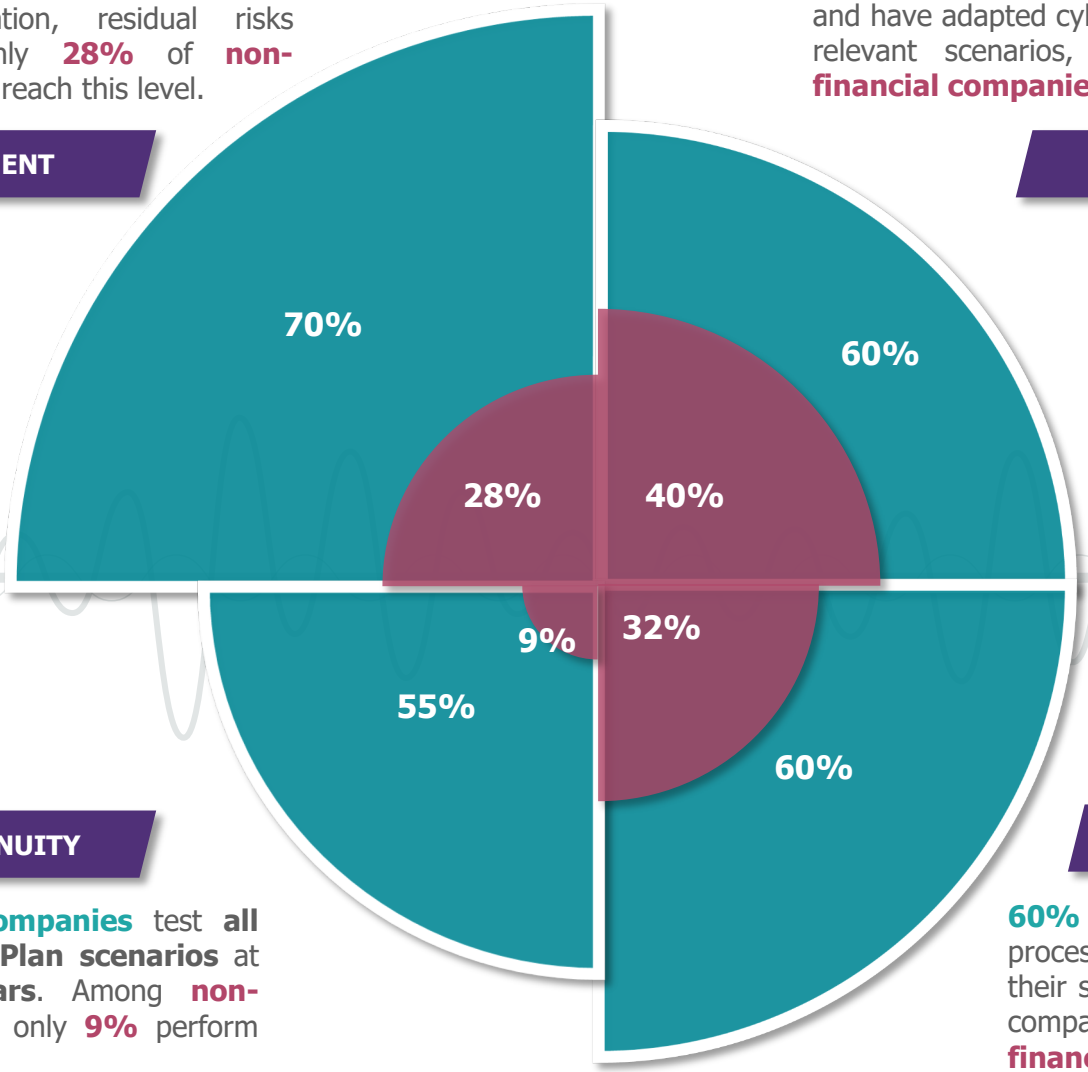
Cyber Resilience, a two-speed market

70% of **financial companies** have **industrialised** risk treatment practices (ownership, prioritization, residual risks reviews…), while only **28%** of **non-financial companies** reach this level.

RISK MANAGEMENT

60% of **financial companies** recently improved their **security incident management process** and have adapted cyber response plans for the main relevant scenarios, while only **40%** of **non-financial companies** do.

CRISIS MANAGEMENT



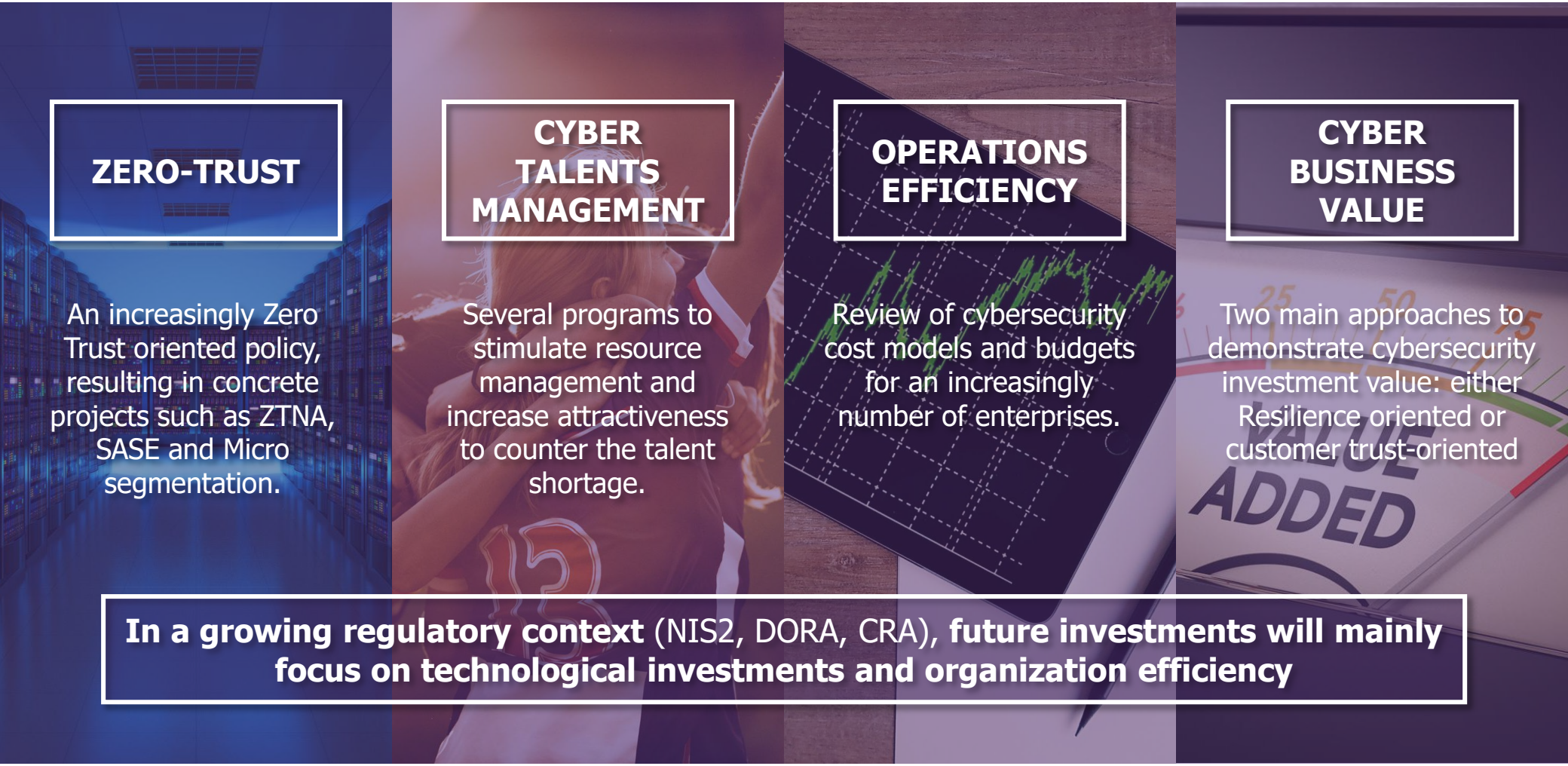
BUSINESS CONTINUITY

55% of **financial companies** test **all Business Continuity Plan scenarios** at least every **two years**. Among **non-financial companies**, only **9%** perform these tests.

THIRD PARTIES

60% of **financial companies** have a process in place to **regularly audit** their suppliers, based on their criticality, compared to only **32%** of **non-financial companies**.

A new **STRATEGIC CYCLE** *for 2026*



ZERO-TRUST

An increasingly Zero Trust oriented policy, resulting in concrete projects such as ZTNA, SASE and Micro segmentation.

CYBER TALENTS MANAGEMENT

Several programs to stimulate resource management and increase attractiveness to counter the talent shortage.

OPERATIONS EFFICIENCY

Review of cybersecurity cost models and budgets for an increasingly number of enterprises.

CYBER BUSINESS VALUE

Two main approaches to demonstrate cybersecurity investment value: either Resilience oriented or customer trust-oriented

In a growing regulatory context (NIS2, DORA, CRA), **future investments will mainly focus on technological investments and organization efficiency**

How do you fare? Get your own evaluation!

WAVESTONE

Florian POUCHET
Director

M +44 7493 867 766
florian.pouchet@wavestone.com

riskinsight-wavestone.com
@Risk_Insight

securityinsider-wavestone.com
@SecuInsider

wavestone.com
@wavestone_