

A nighttime cityscape with a network overlay of white lines and dots connecting various points across the scene, suggesting a digital or cyber theme.

WAVESTONE

Cyber Benchmark

How is the market performing?

March 2022



Gérôme BILLOIS

Partner

gerome.billois@wavestone.com

(+33) 6 10 99 00 60

 [@gbillois](https://twitter.com/gbillois)



Clément JOLLIET

Senior Consultant

clement.jolliet@wavestone.com

(+33) 6 46 14 80 12

Wavestone, a fast-growing company



Pure-play
consultancy

€418m



15 offices
in 9 countries



3,500+
employees

WAVESTONE

An independent leader in cybersecurity

UNLOCK INNOVATION WITH TRUST

A team of **700+** cybersecurity consultants & experts serving **1000+** clients

US | UK | FR | BE | CH | LU | HK

INNOVATIVE & MAKER

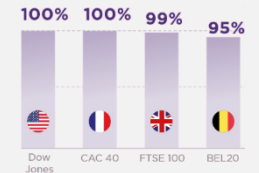
- / Cloud & Next-gen security
- / Digital Identity
- / Risk management & Compliance



CISO & Start-ups radars

CORE-BUSINESS PARTNER

- / Financial Services
- / Manufacturing & Industry 4.0
- / IoT & Smart Products



Sectorial benchmarks

TRUSTED & EXPERT

- / C-levels
- / Incident Response
- / Ethical hacking



CyberLab

Maturity analysis based on Wavestone's benchmark

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



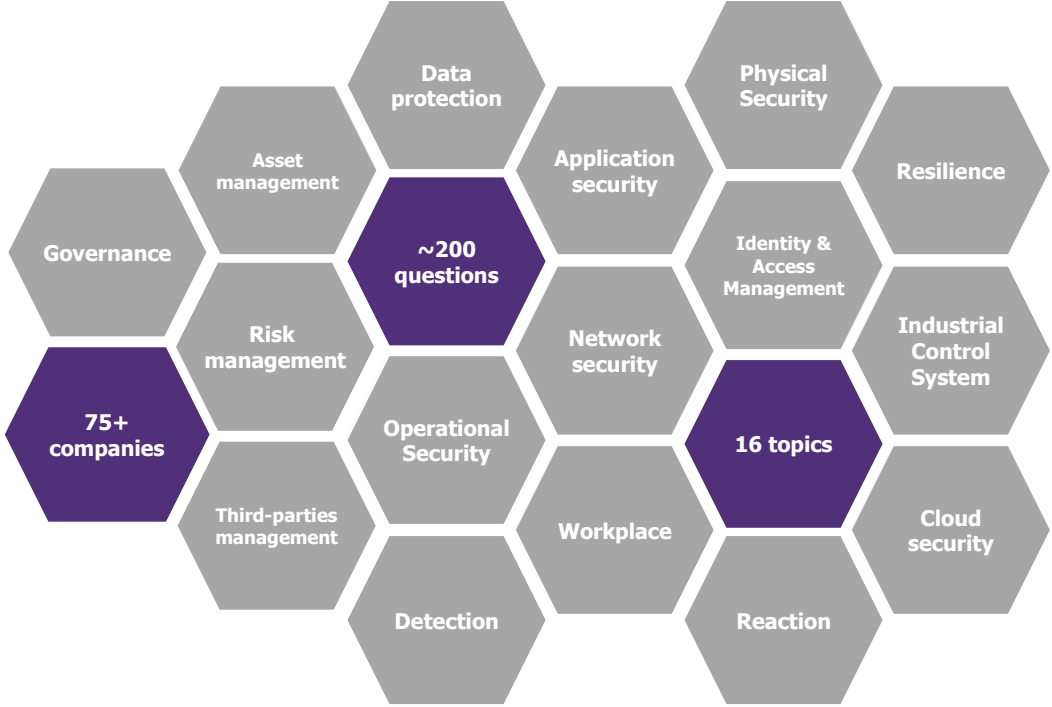
A key innovation: the evaluation of the **maturity distribution** of each topic, covering **organizational** and **technology controls**



A **reliable approach**: data collected through in-person maturity assessments done over the last 3 years by Wavestone



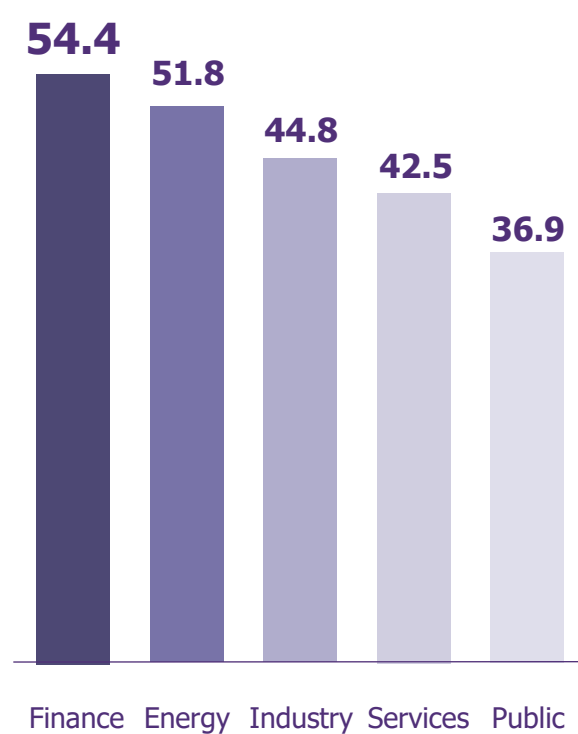
A dataset of 75+ companies among the **largest tier 1 companies**: industry, services, financial services, energy and public... Representing **more than 3,000,000 user accounts**



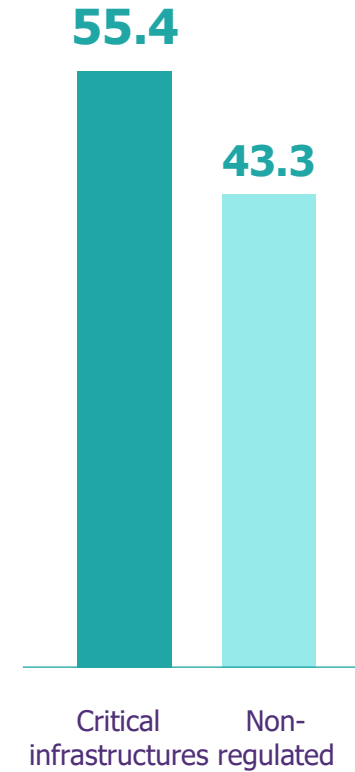
Wavestone Cyber-Benchmark: global overview



Average is barely reached



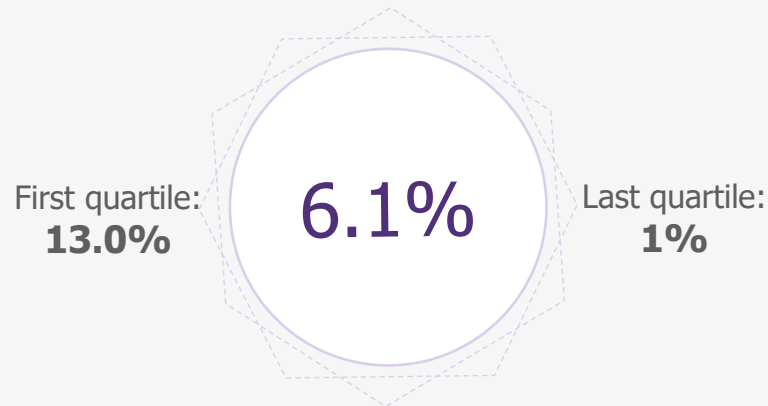
Wide differences between sectors



Regulation have a positive impact

Companies spend an average of 6.1% of their overall IT budget on cybersecurity

Average IT budget percentage
dedicated to cybersecurity

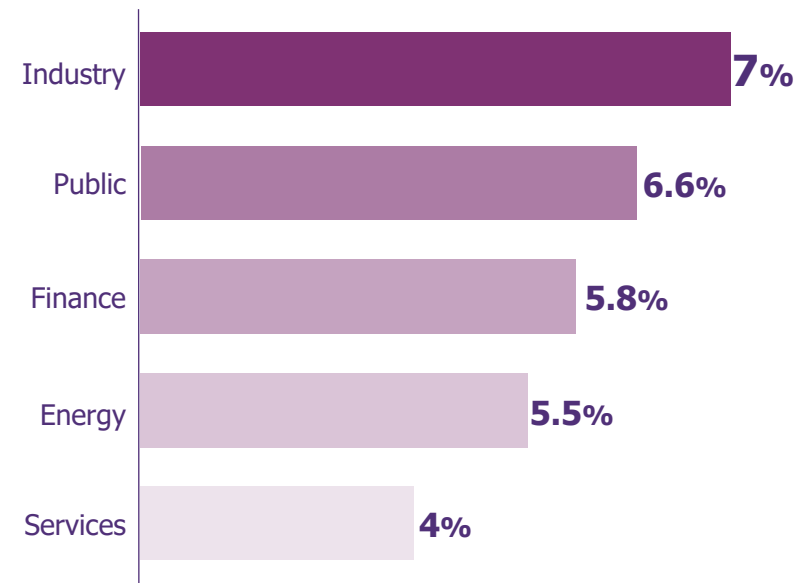


Major cybersecurity programs
Total 3-years investments

Financial services
100 – 800 M€

Industries
15 – 80 M€

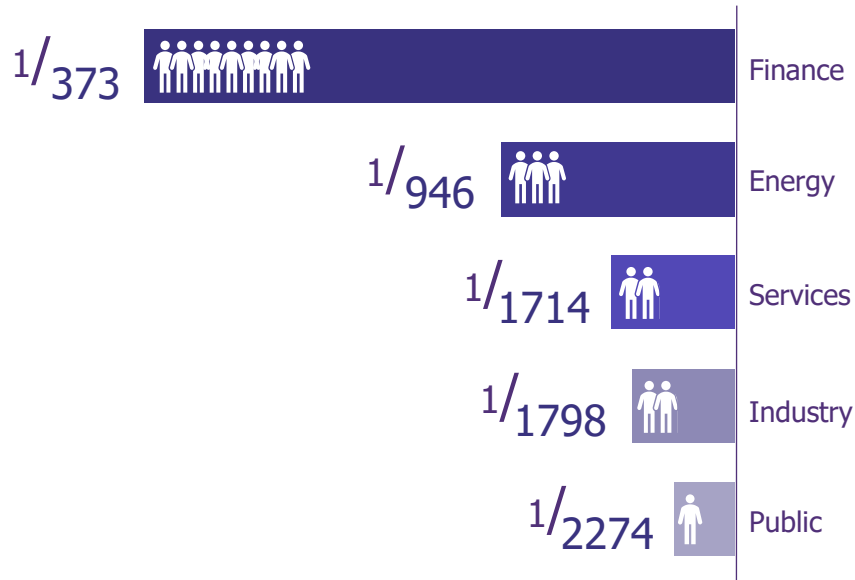
Today, less mature sectors are mainly the ones investing most*



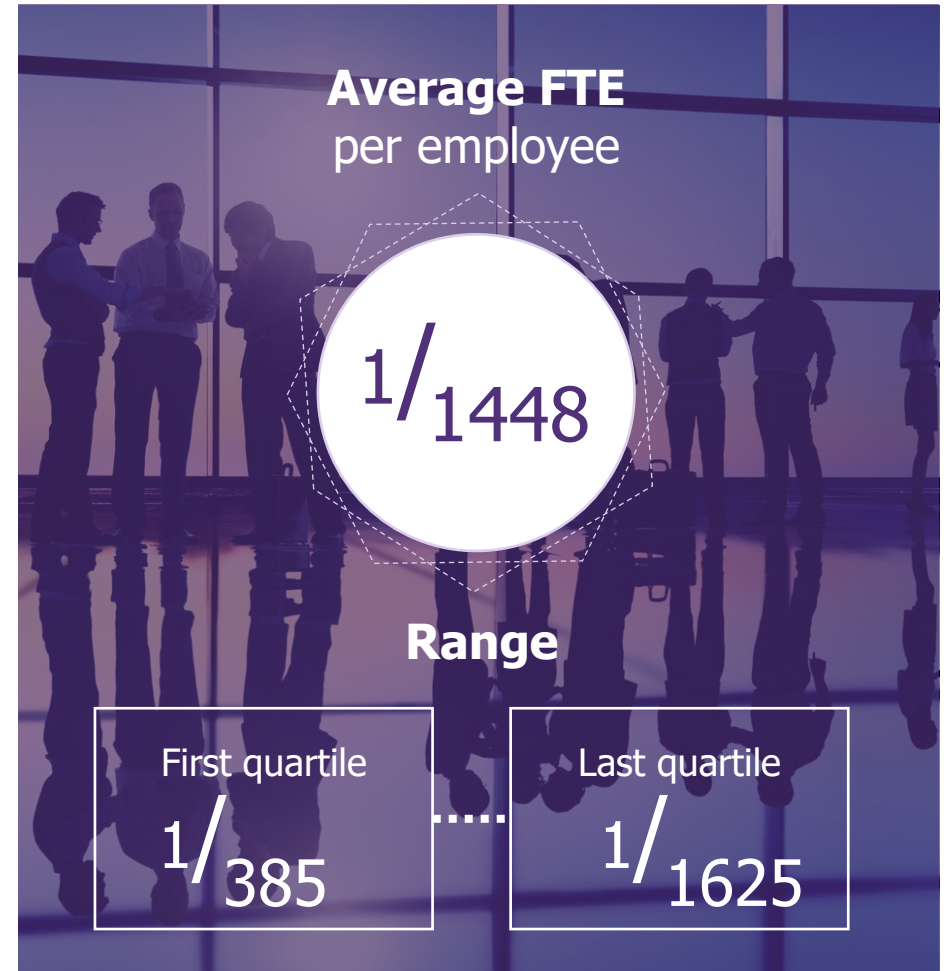
Financial services have gone through their remediation phase and are now in RUN mode with lesser program.
Other sectors are still concentrating their efforts through dedicated transformation program.

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

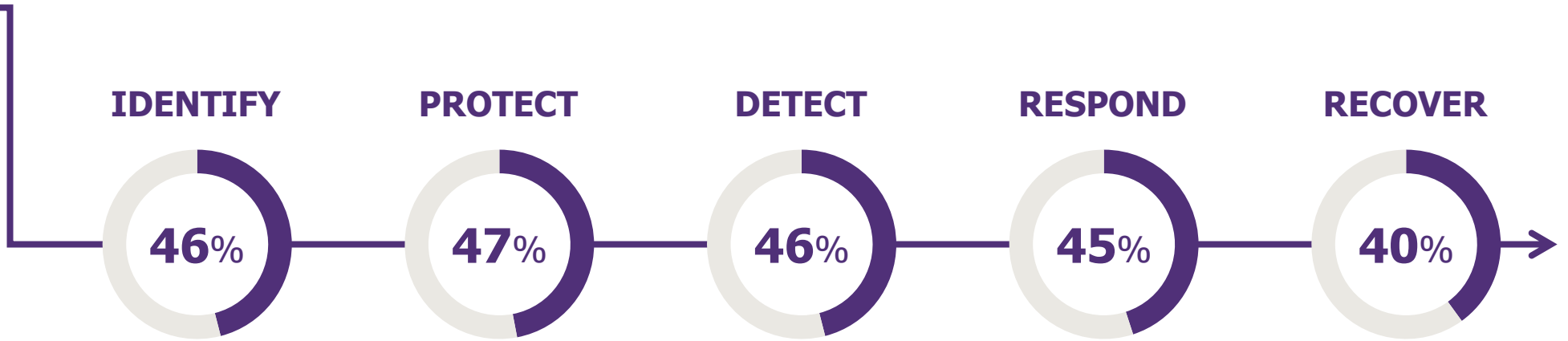
Cybersecurity teams are growing quickly, **many companies have doubled the size of their team**



In the current tense job market, **HR management** should be a **priority** on both **attractivity** and **retention**. International standards on cybersecurity are mostly missing these key actions.



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



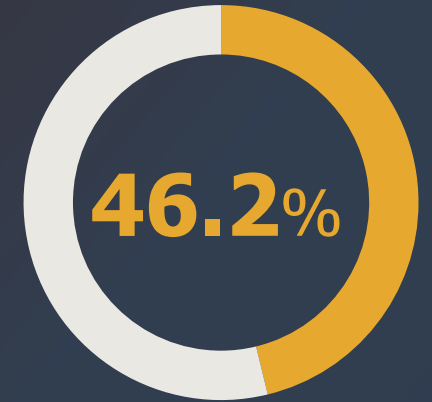
NIST pillars are nowadays **homogeneous** depicting the strong investment on **Detect & Respond** topics. The **Recover** topic is still lacking behind.

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 point from our maturity assessment.

How does the
MARKET stands
against the latest
cyberattacks?



of overall resilience against
RANSOMWARE

RANSOMWARE RESILIENCE

30% OF LARGE ORGANIZATIONS ARE STILL LACKING KEY CONTROLS

Based on the latest cyberattack the CERT-Wavestone managed, we selected **31 anti-ransomware controls** and evaluated maturity on these topics

Organisations:



FINANCIAL SERVICES



INDUSTRY



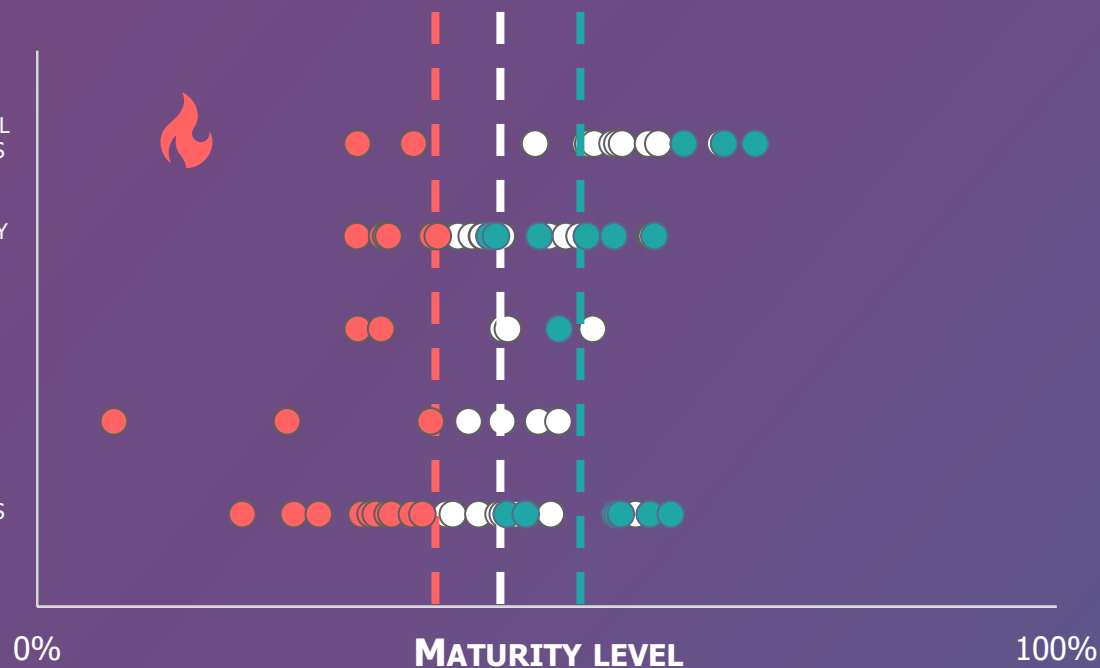
ENERGY



PUBLIC



SERVICES

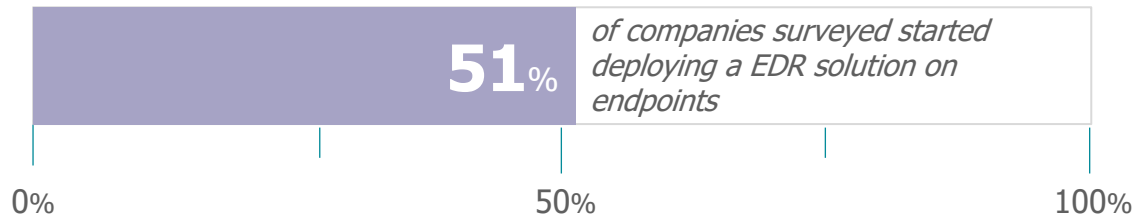


ALL WAVESTONE CLIENT
AVERAGE: **46.2%**

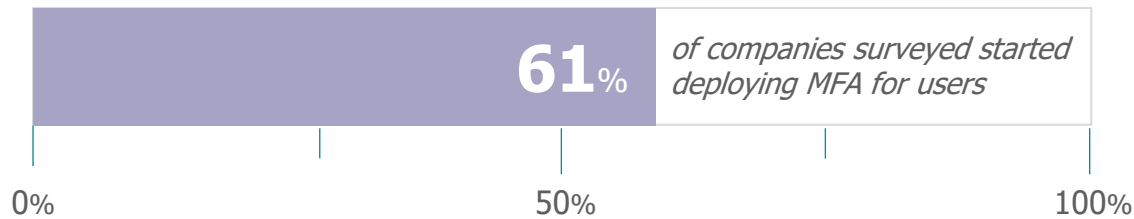
TIER 1 COMPANIES
AVERAGE: **54.5%**

30% COMPANIES
CONSIDERED IN A CRITICAL
SITUATION

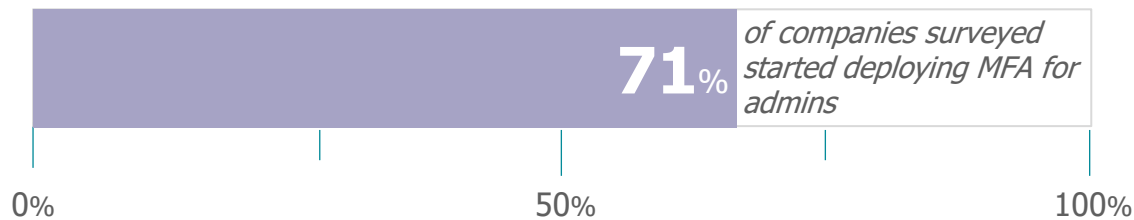
EDR & MFA, most large organizations succeeded, there is no reason to wait anymore!



Endpoint Detection & Response tool deployment is on average **67%**



Multi-factor authentication for users' coverage is on average **63%**



Multi-factor authentication for admins' coverage is on average **76%**

Securing **Active Directory** is ongoing but it's still a challenge to change practices and architecture

Dedicated tools have been deployed but **consolidated surveillance is still lacking**



73% of companies yearly pentest their Active Directory

45% have advanced and dedicated tools to monitor their AD

24% integrated these tools in their SOC



Active Directory administration security stays a complex activity

30% have also a dedicated infrastructure for Tier-0

40% have dedicated workstations for high risk (Tier-0) admin tasks

63% of companies have dedicated and restricted accounts for high risk (Tier-0) admin tasks

Cyber resilience has been and still is a difficult topic today, especially on **operational testing**

Huge investments on crisis management...



82% of companies have a least partially defined, shared and applied a **cyber crisis management process**



53% of companies have a full set of **tools dedicated to crisis management:** videoconference tool, shared follow-up file, crisis handbook and directory... and for **25%** of them, these tools are **resilient against a cyber-crisis!**



47% of companies are regularly organizing **cyber crisis simulation**

10% of companies have tested their Disaster Recovery Plan with key suppliers



17% of companies have tested their Disaster Recovery Plan on the whole value chain



with major investments on-going in the financial sector

...hiding real difficulties on operational resilience testing

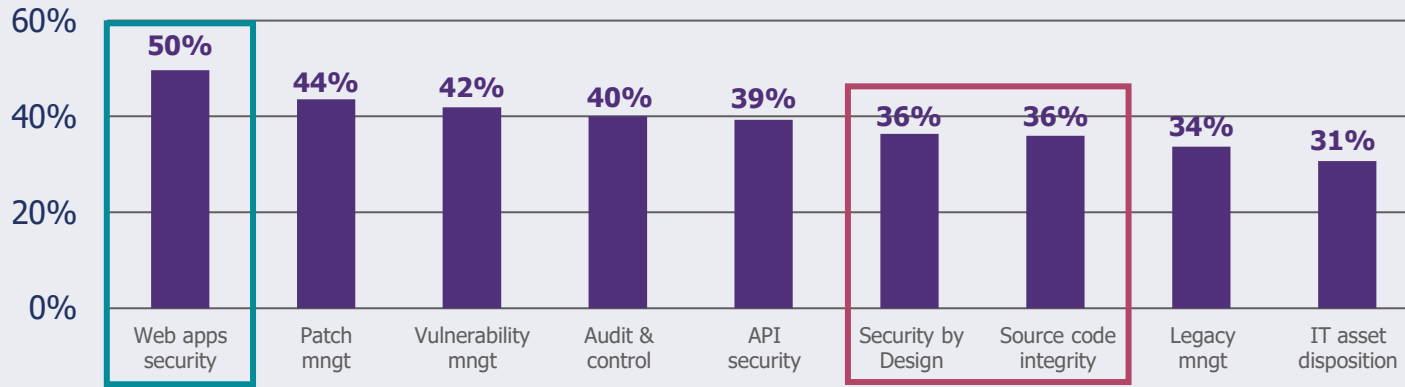
DISCOVER
the



next
CHALLENGES

Data & Application security: many challenges due to the volume of items (38.8% and 38.3% maturity)

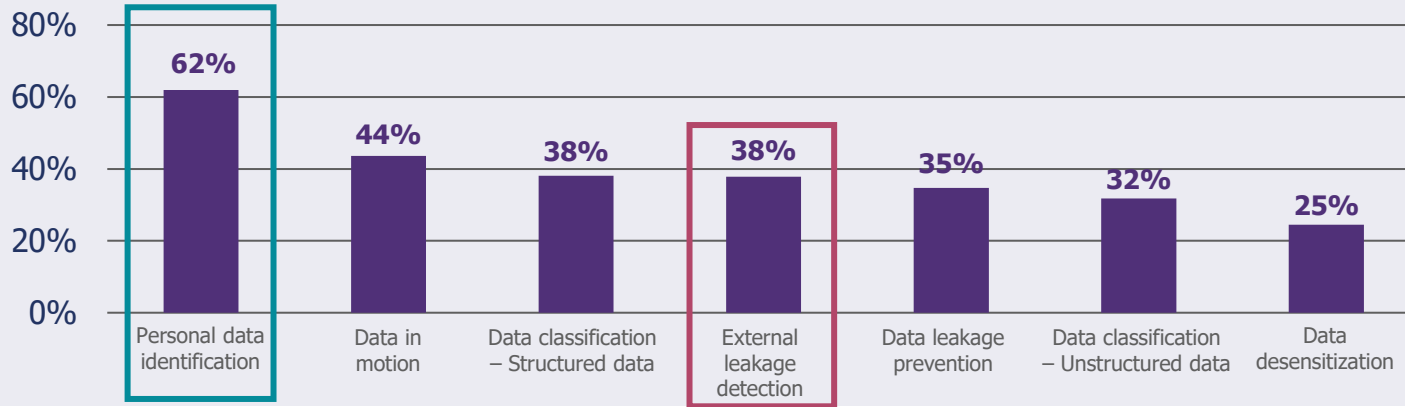
Application security



72% of companies have implemented a **Web Application Firewall (WAF)**

Difficulties are observed on **software lifecycle related topics**, which have high stakes for future attack: **supply chain, CI/CD, SBOM...**

Data security



Because of existing regulation, this topic has now a quite high level of maturity

57% of companies have not invested in an external data leakage detection **tool even if easy to implement**

Cloud is a key topic concentrating important investments but reaching **only 36.1% of maturity**

Cloud monitoring & detection

53%

of companies send Cloud logs to their **SOC** (and 4% have specific use cases)

47%

of companies rely only on **alerts** from their Cloud provider

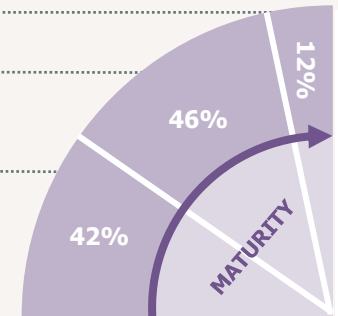
Cloud administration

Access is performed via a bastion

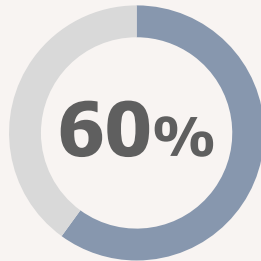
Access uses multi-factor authentication (MFA) for privileged accounts



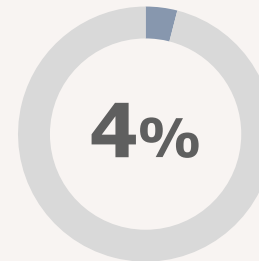
Cloud console always accessible from anywhere, using a login and password



Cloud compliance



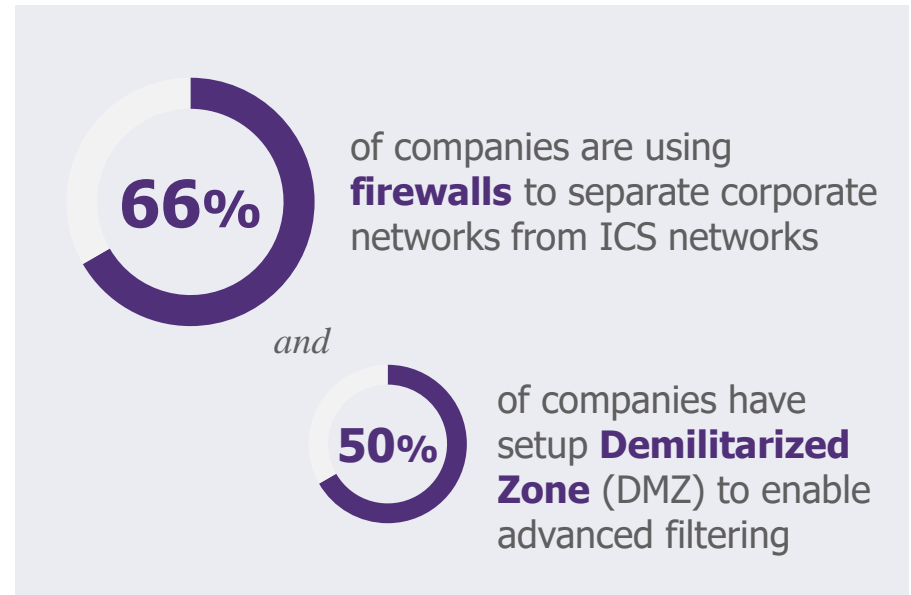
of organizations have tools to **check Cloud compliance**



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

OT / Industrial systems security has an overall maturity of 34.1%

A few encouraging points...



...but a key topic identified for all new projects : security of third parties



A short glimpse on **current market trends...**
 ... many other **data to dive in and insights to get!**



Additional 2022 key topics



HR MANAGEMENT



**C-LEVEL
RELATIONSHIP**



THIRD-PARTY



ZERO TRUST



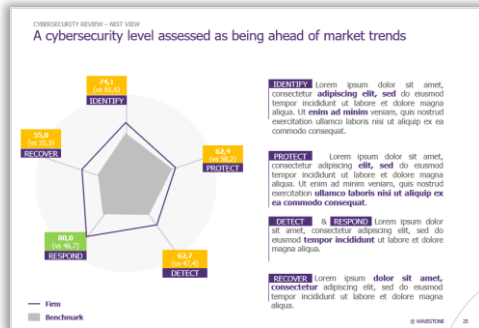
AUTOMATION



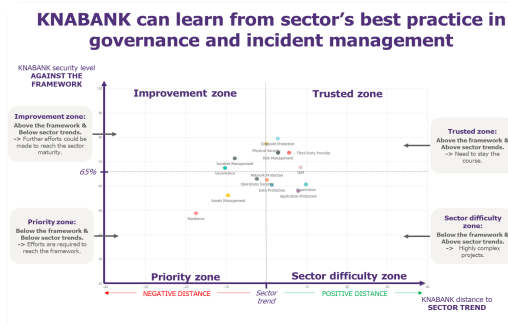
**PRODUCT
SECURITY**

How do you fare? Get your own evaluation

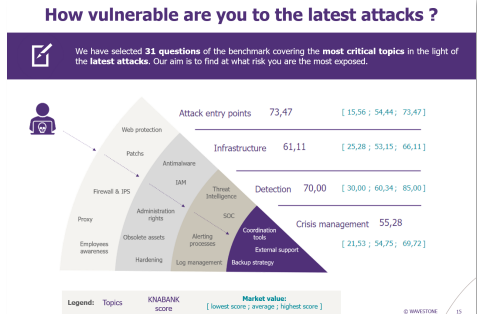
Many different analysis



International standards: NIST and ISO 2700X

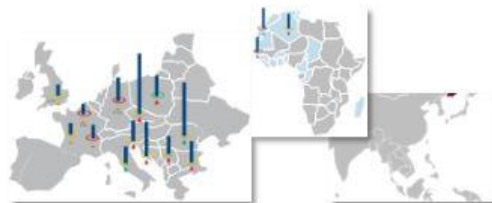


Topic maturity against peers

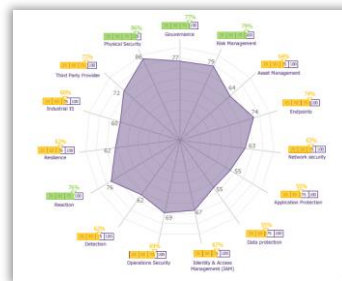


Robustness against latest attacks

Additional views to go further



Entities view



Program management and yearly progress



Integration with Citalid's platform for a quantitative risk approach aligned with your threat landscape

How do you fare? Get your own evaluation

Many

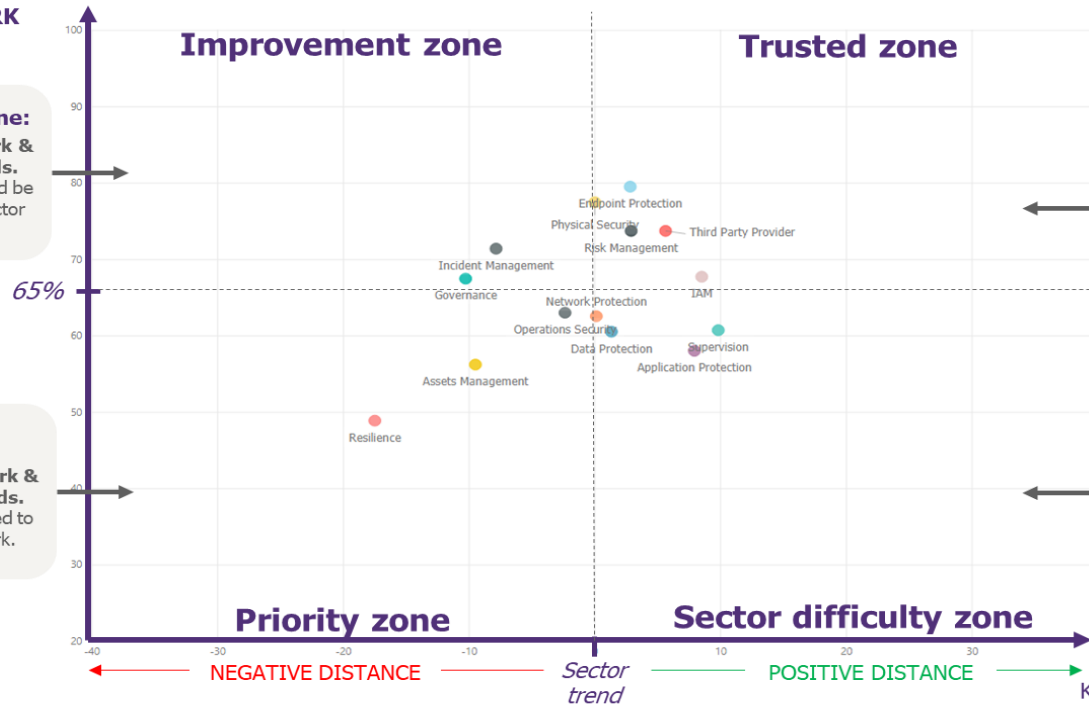
KNABANK can learn from sector's best practice in governance and incident management



KNABANK security level
AGAINST THE FRAMEWORK

Improvement zone:
Above the framework & Below sector trends.
-> Further efforts could be made to reach the sector maturity.

Inte
NI



Trusted zone:
Above the framework & Above sector trends.
-> Need to stay the course.

Sector difficulty zone:
Below the framework & Above sector trends.
-> Highly complex projects.

Priority zone:
Below the framework & Below sector trends.
-> Efforts are required to reach the framework.

Addit



cks ?

as in the light of

73,471
66,111
85,001
8
69,721

© HANSON 15

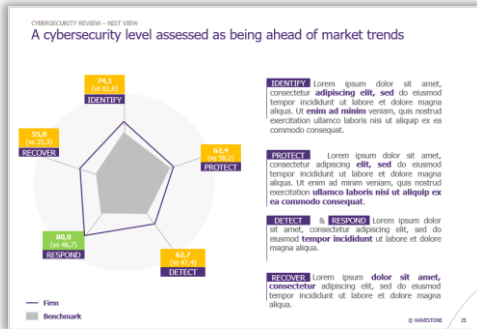
lid's

Program management
and yearly progress

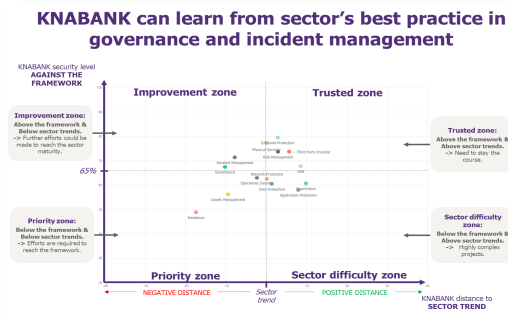
platform for a quantitative
risk approach aligned with
your threat landscape

How do you fare? Get your own evaluation

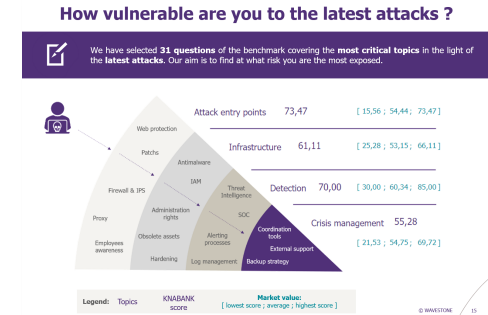
Many different analysis



International standards: NIST and ISO 2700X

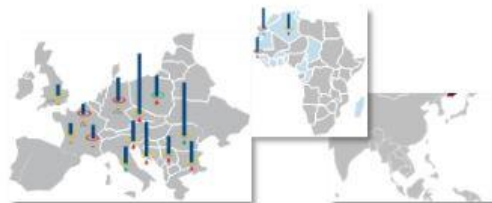


Topic maturity against peers

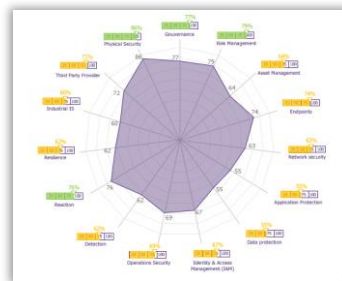


Robustness against latest attacks

Additional views to go further



Entities view



Target risk level view Program management and yearly progress



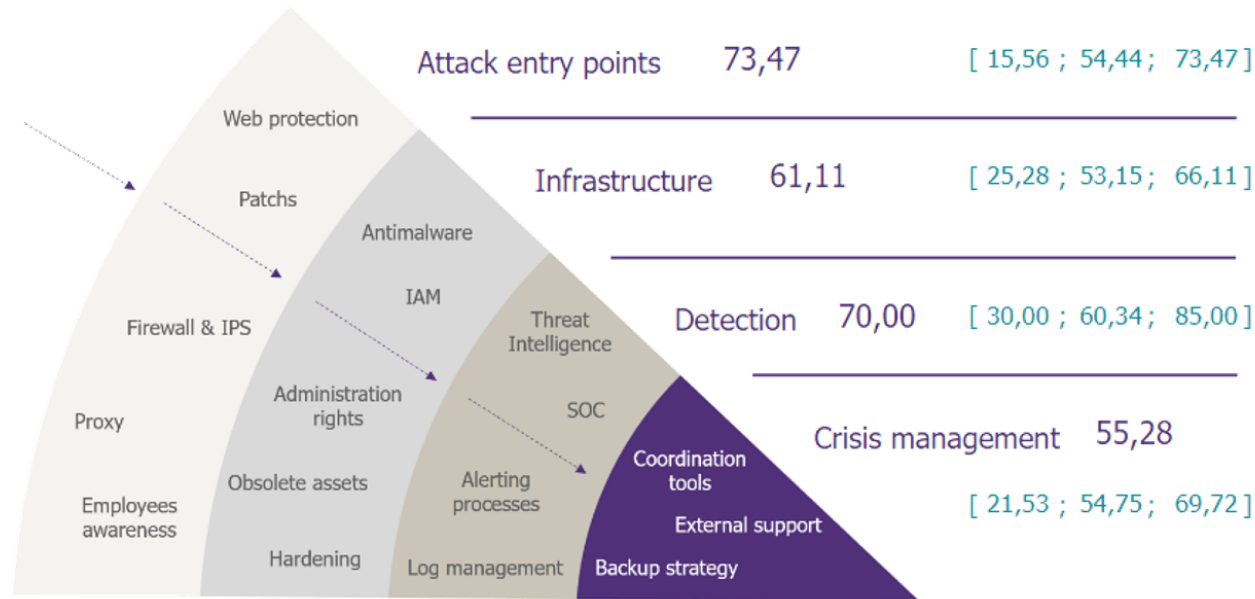
Integration with Citalid's platform for a quantitative risk approach aligned with your threat landscape

How do you fare? Get your own evaluation

How vulnerable are you to the latest attacks ?



We have selected **31 questions** of the benchmark covering the **most critical topics** in the light of the **latest attacks**. Our aim is to find at what risk you are the most exposed.



Many d



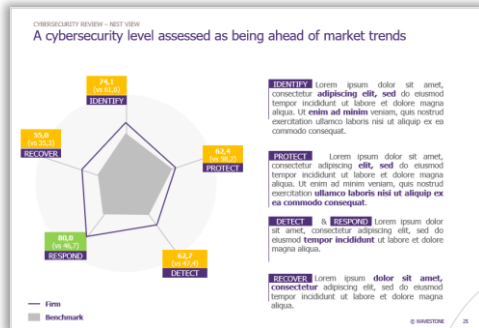
Intern
NIS

Additio

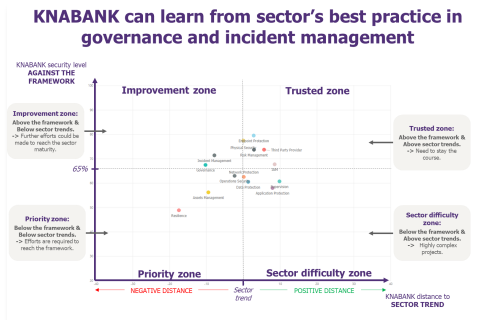


How do you fare? Get your own evaluation

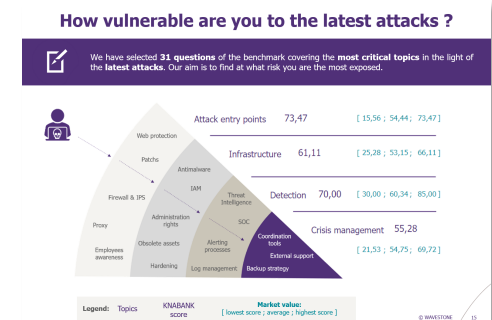
Many different analysis



International standards: NIST and ISO 2700X

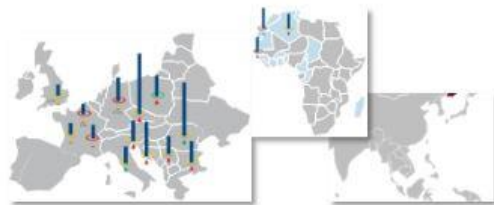


Topic maturity against peers

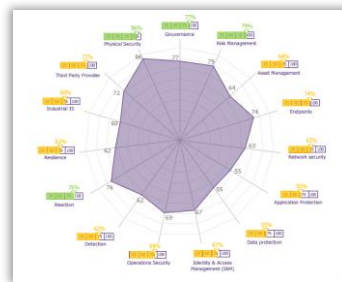


Robustness against latest attacks

Additional views to go further



Entities view



Target risk level view Program management and yearly progress



Integration with Citalid's platform for a quantitative risk approach aligned with your threat landscape

WAVESTONE



Gérôme BILLOIS
Partner

M +33 (0)6 10 99 00 60
gerome.billois@wavestone.com



Clément JOLLIET
Senior Consultant

M +33 (0)6 46 14 80 12
clement.jolliet@wavestone.com



riskinsight-wavestone.com
@Risk_Insight



securityinsider-wavestone.com
@SecuInsider

wavestone.com
@wavestone_