

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

Quel niveau de maturité du marché ?

Avril 2023



Gérôme BILLOIS

Partner

gerome.billois@wavestone.com

(+33) 6 10 99 00 60

 @gbillois



Clément JOLLIET

Consultant Senior

clement.jolliet@wavestone.com

(+33) 6 46 14 80 12

Wavestone, indépendance et croissance



Pure player
indépendant

470 M€
en 2022



12 bureaux
dans 8 pays



+4 000
collaborateurs

Wavestone, un cabinet de conseil en management et leader en cybersécurité & résilience



Accompagnement 360°

au travers de grands programmes de transformation

Une expertise développée depuis plus de 20 ans

RH cyber • Efficacité • Résilience Opérationnelle • Gestion de crise • Zero-trust • Cloud • Convergence IT/OT • Identité 360° • Risque 3rd party • Purple team • Sécurité de l'AD

Benchmarks de maturité cyber & CERT-W

CyberLab & expertise tech/produit

Outils prêts à l'emploi (OpRes, Awareness...)



Indépendance et expertise

avec une approche internationale

+900 experts de la cybersécurité

travaillant ensemble et partageant des valeurs communes



Centré sur l'humain

L'écosystème

En s'engageant auprès d'ONG, de systèmes éducatifs et de publications

Votre écosystème

Du management à vos équipes cyber et vos clients, nous prenons tout en compte pour instaurer durablement un climat de confiance.

Nos collaborateurs

Avec des équipes formées et accompagnées tout au long de leur carrière

Une analyse de maturité en profondeur basée sur le benchmark Wavestone

Une nouvelle approche s'appuyant sur les référentiels internationaux
NIST CSF et ISO 27001/2



Une innovation clé : l'évaluation de la **distribution de la maturité** sur chaque sujet majeur, incluant les **contrôles organisationnels et technologiques**



Une **approche fiable** : données collectées par Wavestone à travers des évaluations de maturité directement chez nos clients sur les 4 dernières années

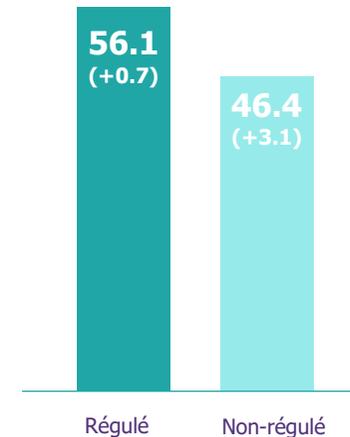
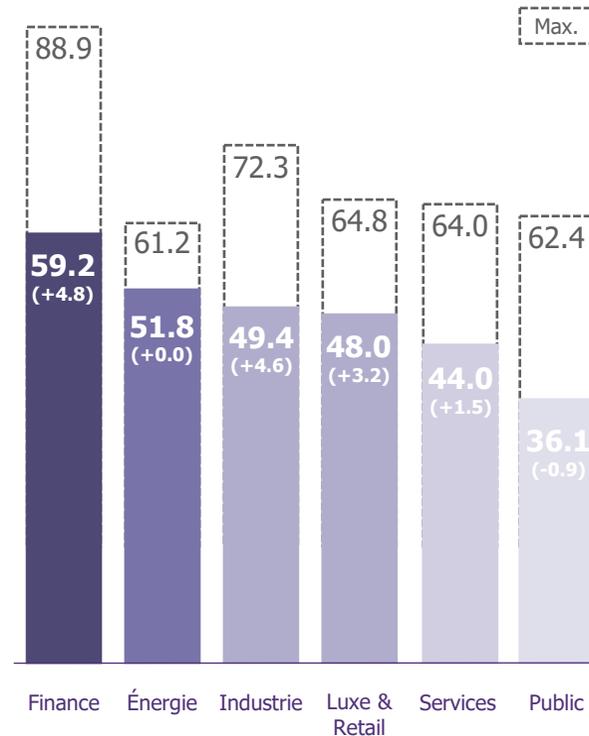


Une base de données de plus de 100 organisations parmi **les plus grandes** : industrie, services, finance, énergie, secteur public... Représentant **près de 5 millions de comptes utilisateurs** !



Wavestone Cyber-Benchmark

vue globale 2023



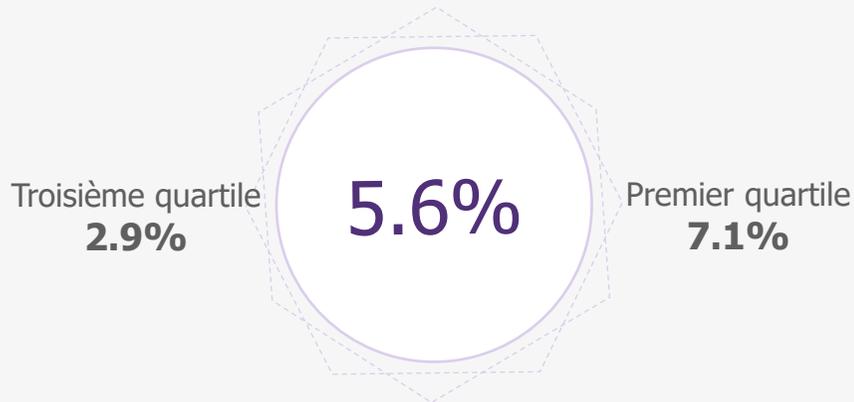
La moyenne est en hausse de 3 points par rapport à 2022

Des différences importantes entre les secteurs

La réglementation a un impact positif

Les organisations consacrent **en moyenne 5,6%** **du budget IT à la cybersécurité**

Moyenne du budget IT dédié à la sécurité*

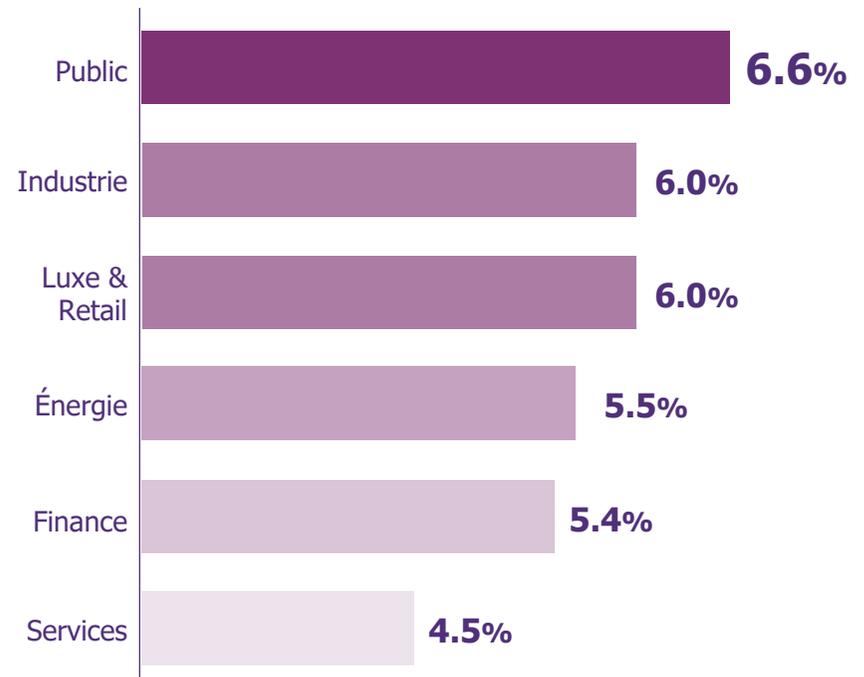


Programmes cyber majeurs Total des investissements sur 3 ans

Finance
200 – 900 M€

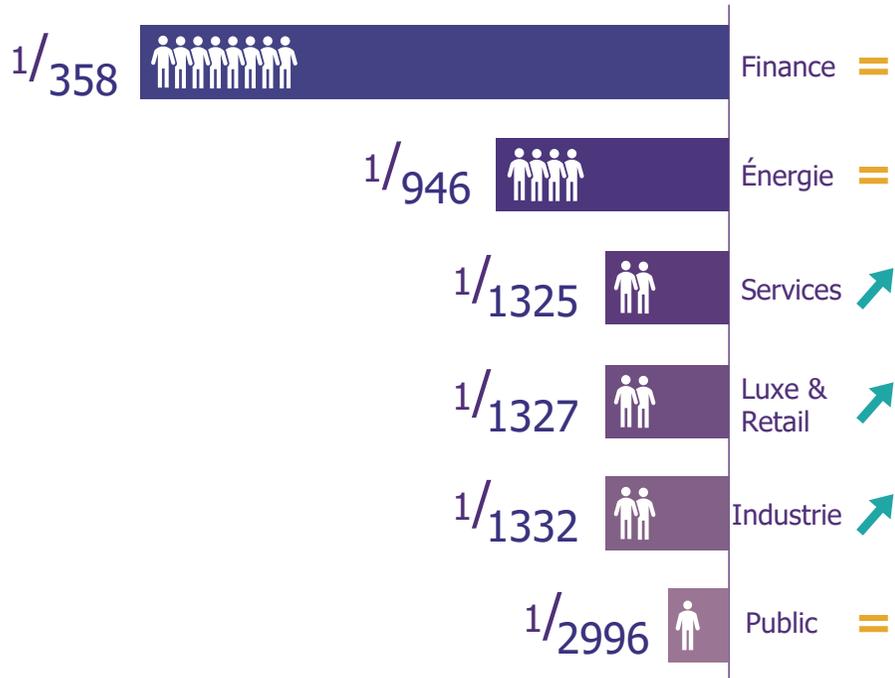
Industrie
15 – 100 M€

**Actuellement, c'est principalement
les secteurs les moins matures qui
investissent le plus.**



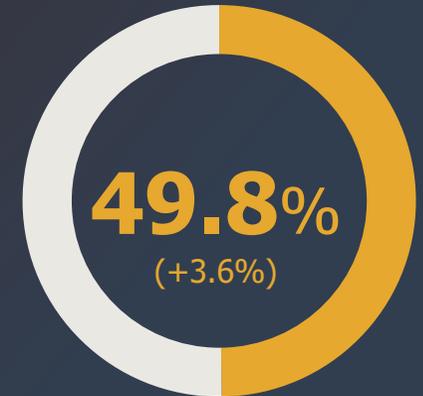
**Il faut prendre en compte que le pourcentage du budget investi varie beaucoup en fonction des investissements passés et de l'équilibre financier entre les projets et la production*

Malgré des **pénuries de ressources**, un développement des équipes cyber porté par des **initiatives RH**



Comment le

MARCHÉ est-il protégé *face aux* dernières **cyberattaques ?**

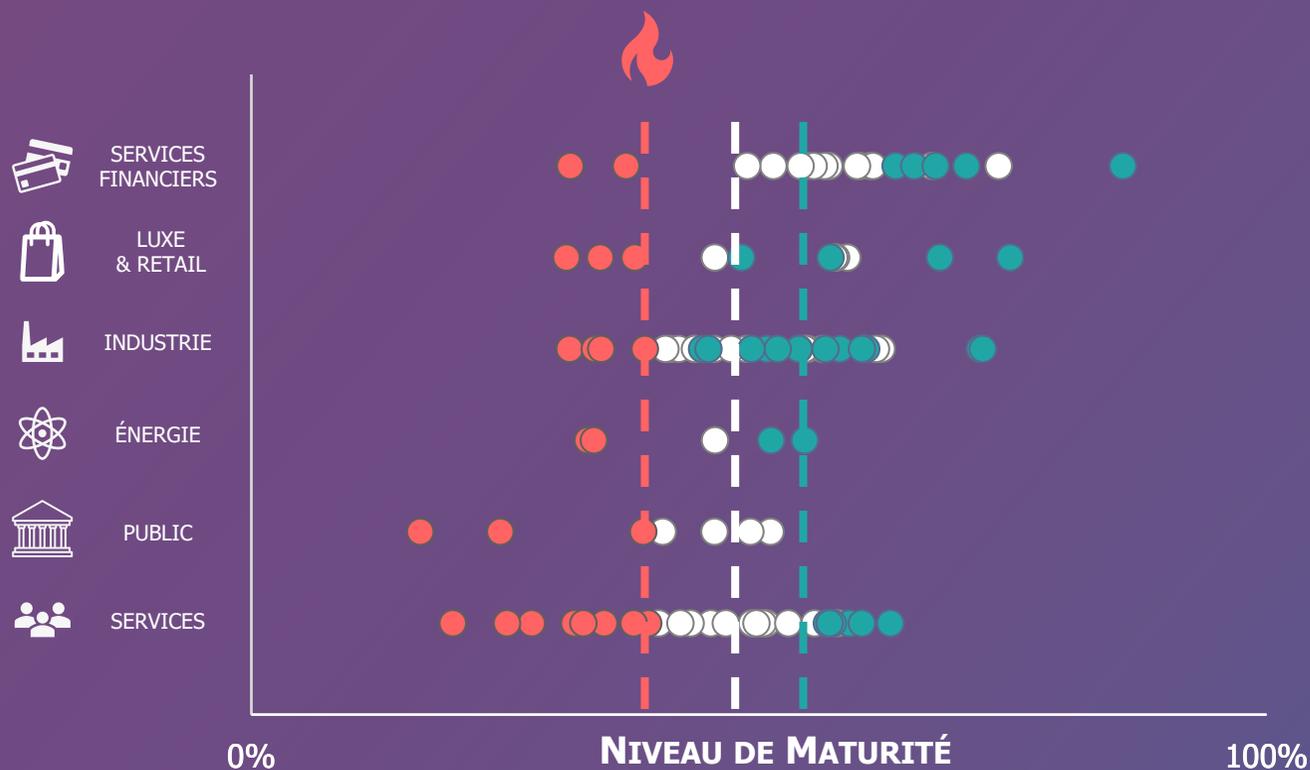


de résilience globale contre les

RANSOMWARE

Comment le **marché** est-il protégé face aux **dernières cyberattaques** ?

Des investissements spécifiques contre les **ransomwares** ont porté leurs fruits, moins d'organisations sont des proies faciles.



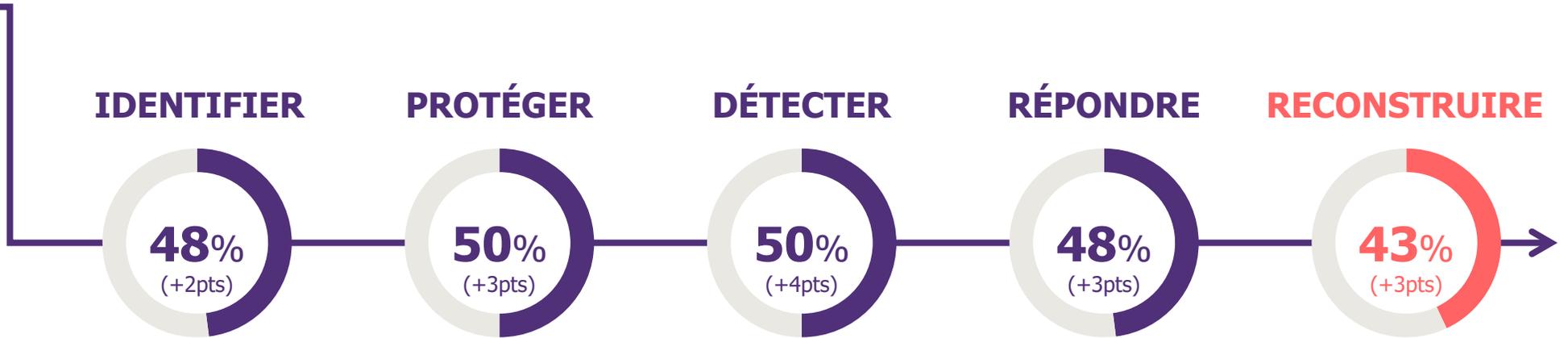
NIVEAU MOYEN DES CLIENTS
WAVESTONE : **49.8%**

MOYENNE DES GRANDES
ENTREPRISES (TYPE CAC40)
59.8%

23% DES ORGANISATIONS
CONSIDÉRÉES EN SITUATION
CRITIQUE (30% EN 2022)

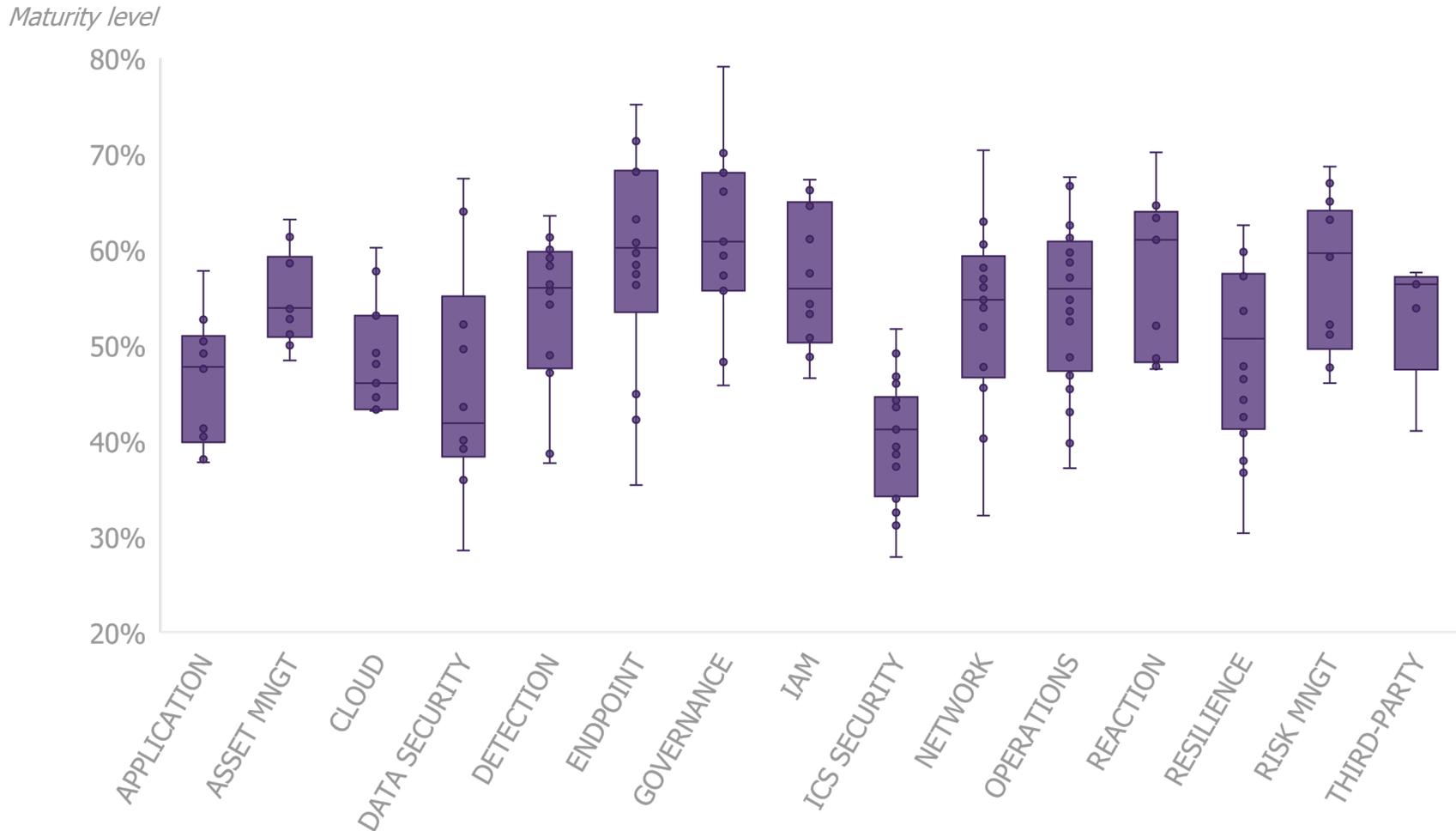
À partir des dernières attaques cyber gérées par le CERT-Wavestone, nous avons sélectionné 29 mesures anti-ransomware et évalué la maturité de nos clients sur chacune d'elles

Quelle est la **MATURITÉ** du marché sur les **axes cyber** ?



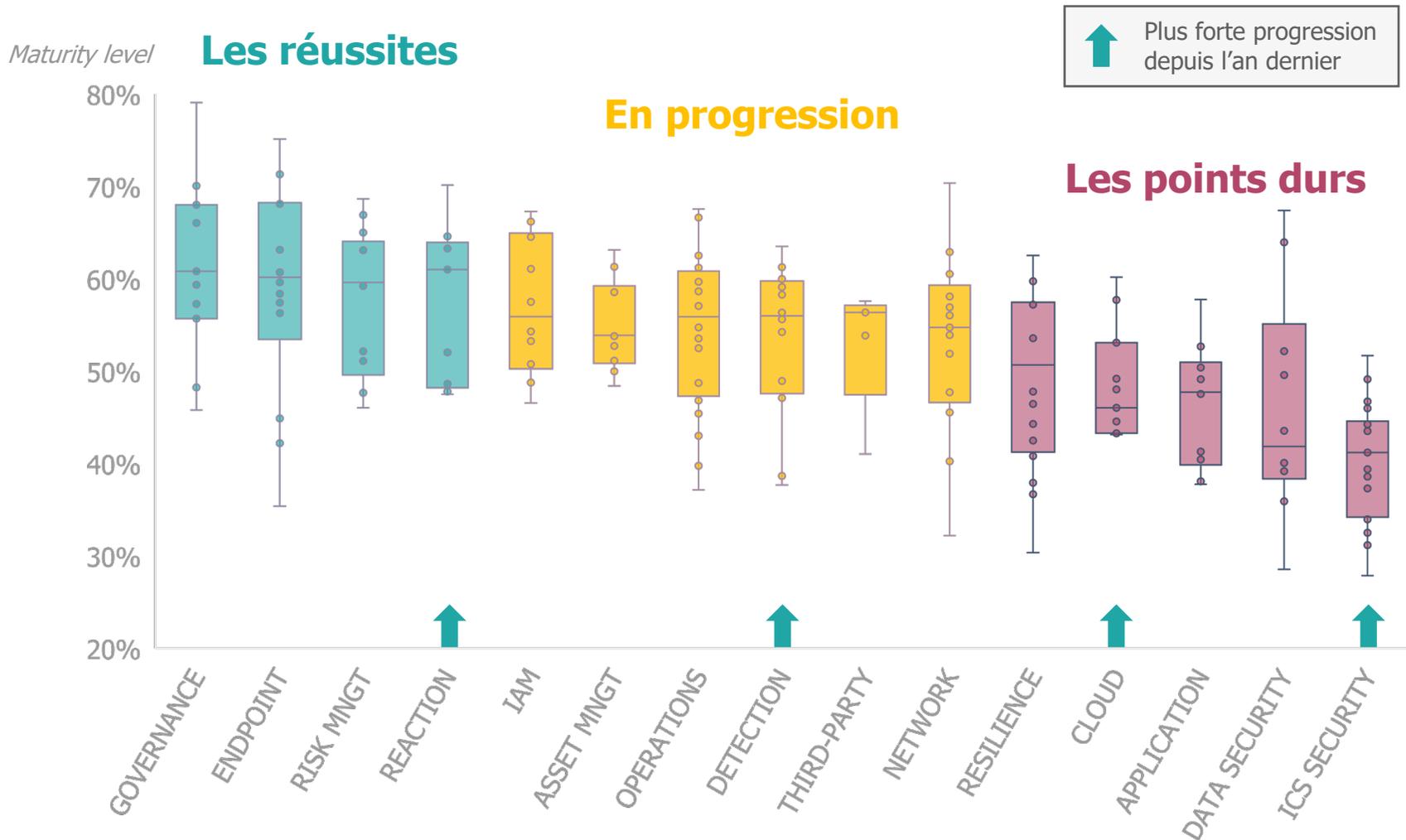
Les **pilliers NIST** sont aujourd'hui principalement **homogènes**, témoignant des investissements importants réalisés ces dernières années sur **l'ensemble des thèmes**. Le sujet **Reconstruire** est encore légèrement en retard à cause de sa complexité et du nombre de systèmes concernés.

Quelle est la **MATURITÉ** du marché sur les **axes cyber** ?



La vue du niveau de maturité pour chaque "boîte à moustache": Maximum / 1st quartile / Médiane / 3rd quartile / Minimum.
1 point = 1 point de contrôle

Quelle est la **MATURITÉ** du marché sur les **axes cyber** ?



La vue du niveau de maturité pour chaque "boîte à moustache": Maximum / 1st quartile / Médiane / 3rd quartile / Minimum.
1 point = 1 point de contrôle

La réaction et la détection figurent parmi les priorités d'investissement

Les incidents sont mieux gérés et plus vite...



48% (+16pts) des organisations ont mis en place un **Red Button** pour isoler une partie du réseau. La couverture du Red Button est en moyenne de **58%**.



43% (+20pts) des organisations ont formalisé toutes les **procédures d'arrêt d'urgence** et communiquent **tous les types d'incidents** à leurs équipes

58% (+15pts) des organisations ont des sondes de détection **connectées au SIEM**, et **22%** (+3pts) ont commencé à déployer des sondes **d'analyse comportementale**



29% (+11pts) des organisations ont amélioré le traitement et l'utilisation opérationnelle des **IOC**



... avec des outils améliorant la détection

... permettant de mieux **gérer les attaques** et de **réduire l'impact opérationnel**



2023

CLOUD

TIERS

ICS

Certains points d'entrée sont
de plus en plus exploités par
les cybercriminels

Le **Cloud** est un sujet clé concentrant des investissements importants et qui atteint maintenant **44.5%** (+8.4pts) **de maturité**

Surveillance et détection du Cloud

62% (+4pts)

des organisations envoient les journaux du Cloud à leur SOC (11% (+1pt) ont des règles de détection spécifiques)

38% (-4pts)

des organisations comptent uniquement sur les alertes de leur fournisseur Cloud

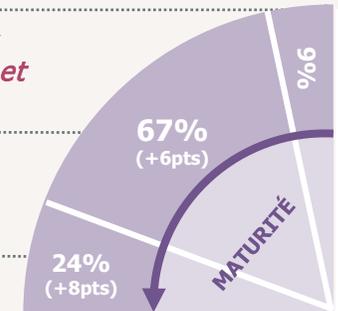
Administration Cloud



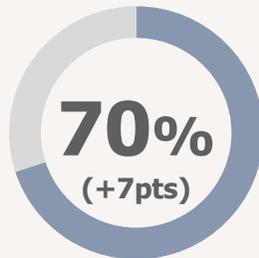
Console Cloud accessible depuis n'importe où, à l'aide d'un login et d'un mot de passe.

Authentification multifacteur (MFA) pour les comptes d'administration.

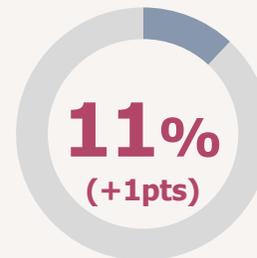
*L'accès se fait par un **bastion**.*



Conformité du Cloud



des organisations **vérifient** la **conformité du Cloud** à l'aide d'outils



des organisations **corrigent** automatiquement les **problèmes** de conformité du Cloud

La sécurité des tiers reste un problème épineux* en raison de l'interconnexion croissante avec les partenaires et les fournisseurs

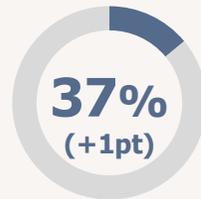
*avec **46.9%** (seulement +2pts) de maturité

Gestion des Contrats



des entreprises **incluent des clauses de sécurité dans les contrats** lors de la signature

Audit des tiers



des entreprises **auditent régulièrement** leurs fournisseurs informatiques critiques.
même si 61% des entreprises inventorient correctement leurs fournisseurs

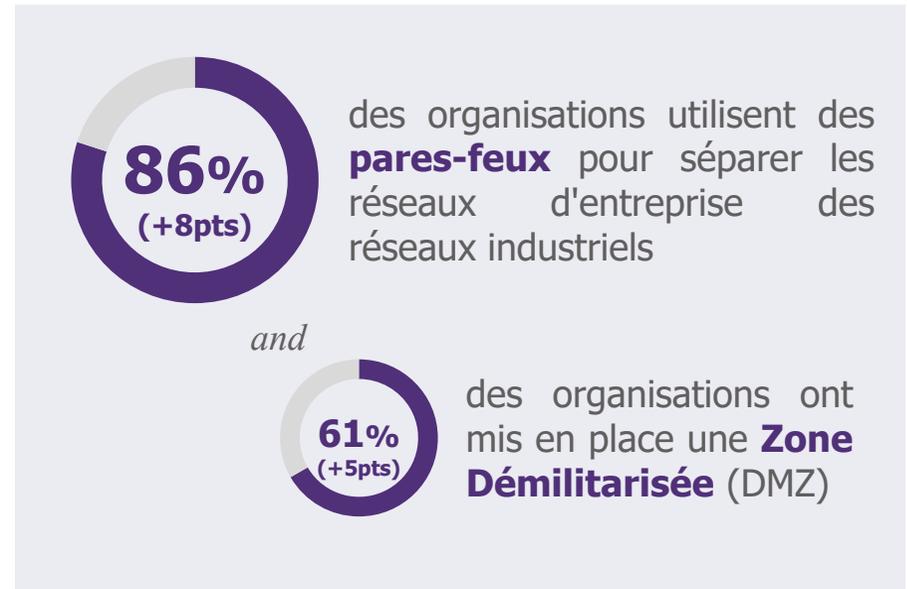
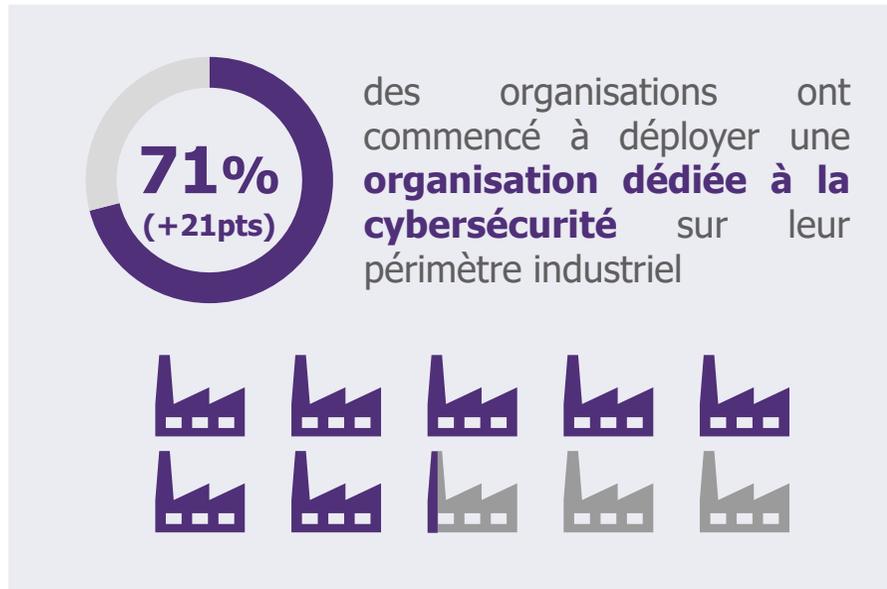
Continuité des activités



des organisations testent leur **plan d'intervention** et de **reprise** avec leurs partenaires/fournisseurs sur tous les **périmètres critiques**

La sécurité des systèmes industriels a une **maturité** globale de **37.6%** (+3.4pts)

Bonne nouvelle : les bases de sécurité se concrétisent...



...mais encore d'importantes lacunes sur des **pratiques essentielles en matière de sécurité** :



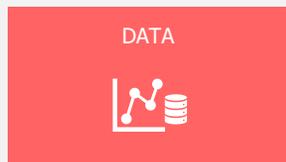
Comment faire avancer les
2 PRIORITÉS de nombreux RSSI ?

ZERO-TRUST

RÉSILIENCE

Zero Trust, une stratégie majeure en déploiement

Fondations
Zero-Trust
du CISA



La **couverture des MFA** avec **accès conditionnel** est de **73%** en moyenne



La **couverture de la Micro-segmentation** est de **32%** en moyenne

La **couverture des outils Zero Trust Network Access** est de **46%** en moyenne



La **couverture des SOAR** est de **48%** en moyenne

Cyber Résilience, un marché à deux vitesses

70% des **entreprises financières** ont **industrialisé** les pratiques de traitement des risques (appropriation, hiérarchisation, revue des risques résiduels...), contre seulement **28%** des **entreprises non financières**.

GESTION DES RISQUES

60% des **entreprises financières** ont récemment amélioré leur processus de **gestion des incidents** de sécurité et disposent de différents plans de cyber-réponse en fonction des scénarios, contre **40%** des **entreprises non financières**.

GESTION DE CRISE

70%

60%

28%

40%

9%

32%

55%

60%

CONTINUITÉ DES ACTIVITÉS

55% des **entreprises financières** testent **tous les scénarios** du **Plan de continuité des activités** au moins tous **les deux ans**. Parmi les **entreprises non financières**, seules **9%** effectuent ces tests.

TIERS

60% des **entreprises financières** **auditent régulièrement** leurs fournisseurs, en fonction de leur criticité, contre seulement **32%** pour les **entreprises des autres secteurs**.

Un nouveau **CYCLE STRATÉGIQUE** pour 2026

ZERO-TRUST

Une politique de plus en plus axée sur le Zero Trust, qui se traduit par des projets tels que le ZTNA, le SASE et la micro-segmentation.

GESTION DES TALENTS CYBERS

Plusieurs programmes visant à stimuler la gestion des ressources et à accroître l'attractivité pour lutter contre la pénurie de talents.

EFFICACITÉ OPÉRATIONNELLE

Un examen des modèles de coûts et des budgets de cybersécurité pour un nombre croissant d'entreprises.

LA CYBER EN POSITIONNEMENT DIFFÉRENCIATION

Deux approches principales pour démontrer la valeur des investissements dans la cybersécurité : l'une axée sur la résilience, l'autre sur la confiance du client.

Dans un contexte réglementaire grandissant (NIS2, DORA, CRA), les investissements futurs se concentreront principalement sur les investissements technologiques et l'efficacité opérationnelle

Quelle est votre posture ? Réalisez votre propre évaluation !

WAVESTONE



Gérôme BILLOIS
Partner

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



Clément JOLLIET
Consultant Senior

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



riskinsight-wavestone.com
@Risk_Insight

wavestone.com
@wavestone_