WAVESTONE

Cyber Benchmark

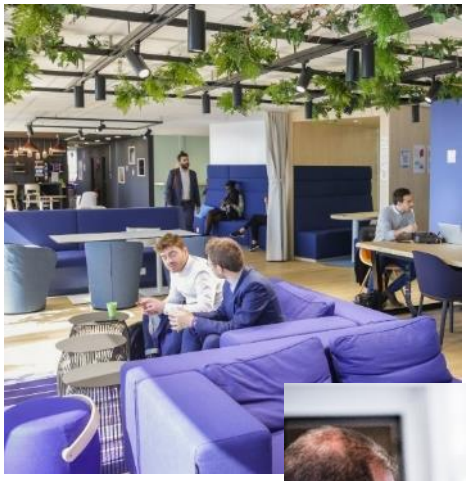
Quel niveau de maturité du marché ?

March 2022

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

418 M€

15 bureaux
dans 9 pays

+3 500
collaborateurs

WAVESTONE

Un leader indépendant en cybersécurité

LIBÉRER L'INNOVATION PAR LA CONFIANCE

Une équipe de plus de 700 consultants et experts au service de plus de 1000 clients

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

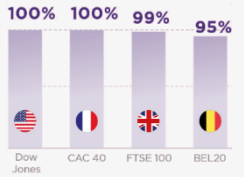
INNOVANT & DOER

- / Sécurité Cloud & Next-Gen
- / Identité Numérique
- / Gestion des risques et conformité

Radars RSSI & Start-ups

PARTENAIRE CŒUR DE MÉTIER

- / Secteur financier
- / Manufacturing & Industrie 4.0
- / IoT & Smart Products



Benchmark sectoriel

CONFIANCE & EXPERTISE

- / Direction générale
- / Réponse à incident
- / Hacking éthique

CyberLab

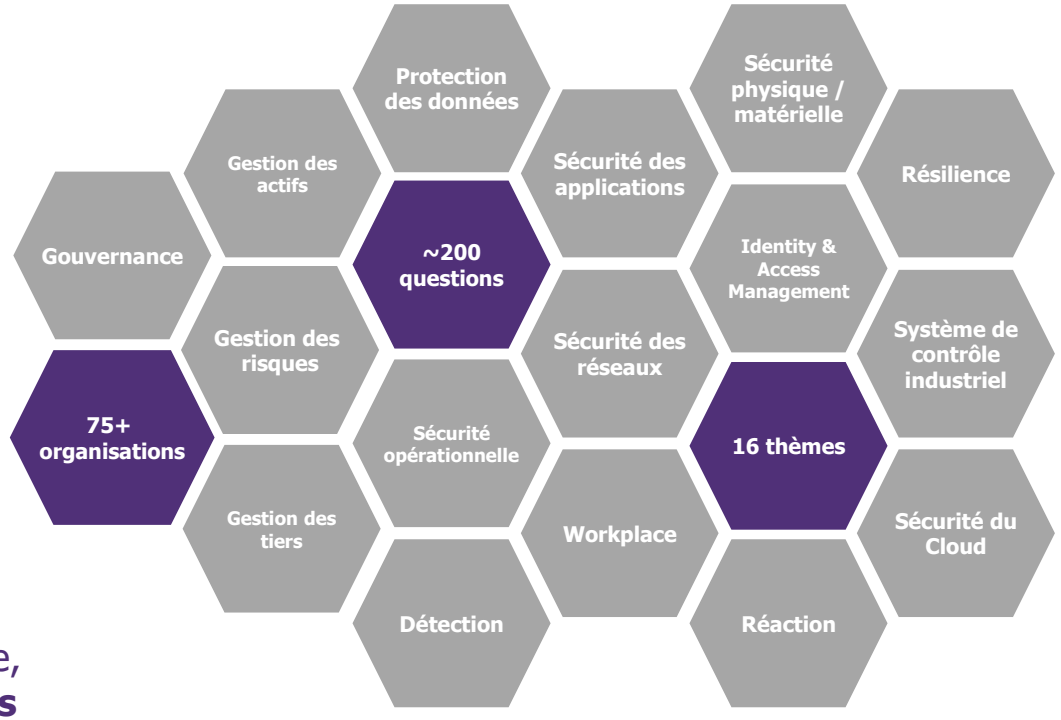
Une analyse de maturité en profondeur basée sur le benchmark Wavestone

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

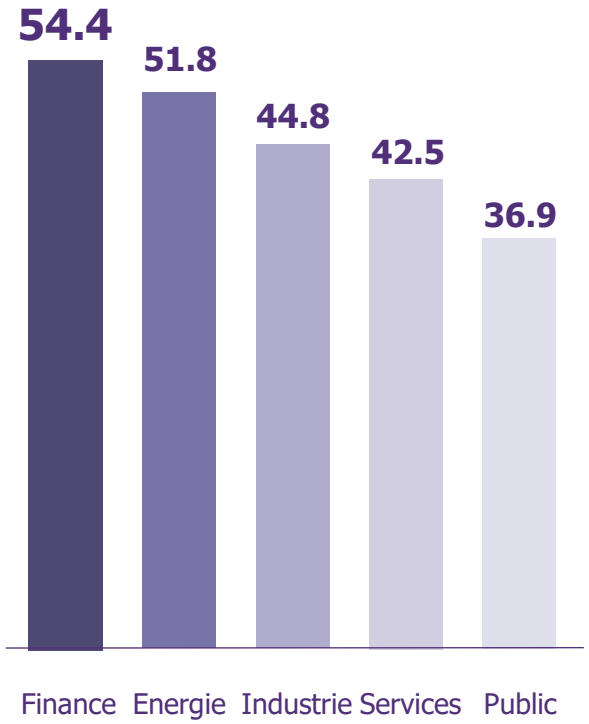
Une innovation clé : l'évaluation de la **distribution de la maturité** sur chaque sujet majeur, incluant les **contrôles organisationnels et technologiques**

Une **approche fiable** : données collectées par Wavestone à travers des évaluations de maturité directement chez nos clients sur les 3 dernières années

Une base de données de plus de 75 organisations parmi **les plus grandes organisations** : industrie, services, finance, énergie, secteur public… Représentant **plus de 3 000 000 comptes utilisateurs !**



Wavestone Cyber-Benchmark : vue d'ensemble



La moyenne est à peine atteinte

Des différences importantes entre les secteurs

La réglementation a un impact positif

Les organisations consacrent **en moyenne 6,1% du budget IT à la cybersécurité**

Moyenne du budget IT
dédié à la sécurité

Troisième quartile
1%

6.1%

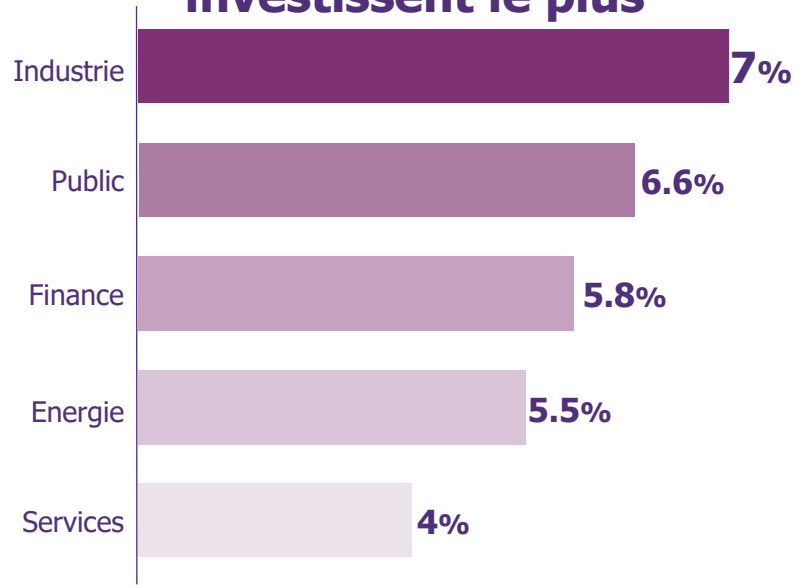
Premier quartile
13.0%

Programmes cyber majeurs
Total des investissements sur 3 ans

Finance
100 – 800 M€

Industrie
15 – 80 M€

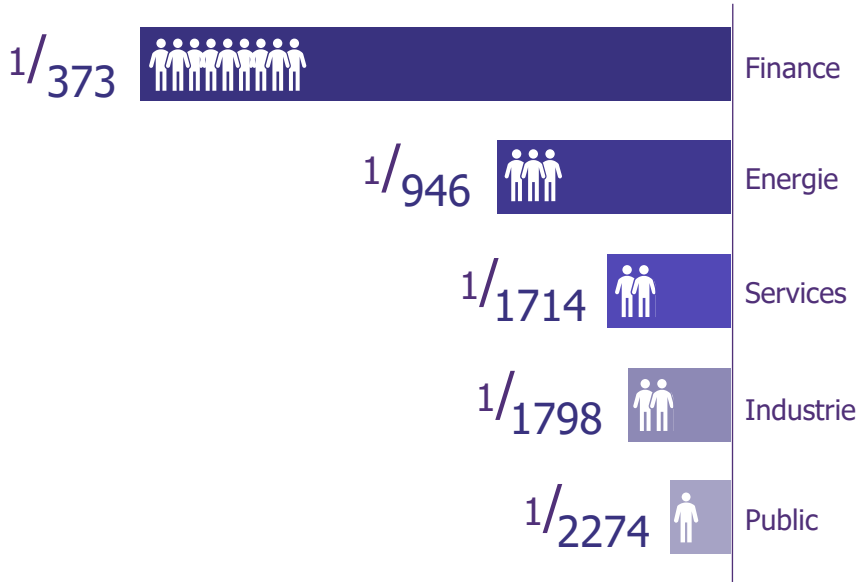
Actuellement, c'est principalement les secteurs les moins matures qui investissent le plus



Les services financiers sortent de la phase de remédiation et sont aujourd'hui en fonctionnement normal avec moins de programme cyber dédié. Les autres **secteurs concentrent encore leurs efforts** grâce à des programmes de transformation spécifiques.

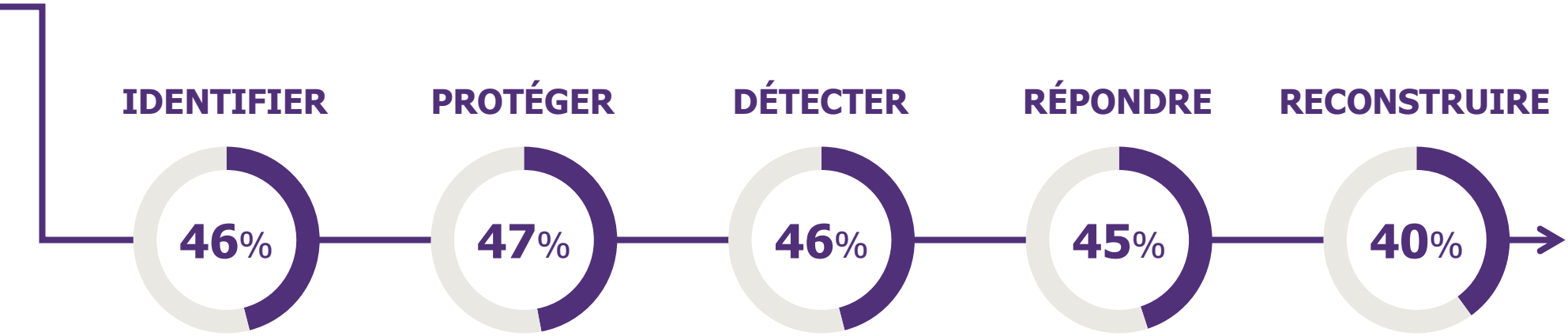
Il faut prendre en compte que le pourcentage du budget investi varie beaucoup en fonction des investissements passés et de l'équilibre financier entre les projets et la production

Les équipes cyber se développent rapidement : **de nombreuses ont doublé de taille récemment**



Dans le contexte actuel de **pénurie de compétence**, les ressources humaines devraient être une priorité en matière d'**attractivité** et de **rétention.** Les standards cyber internationaux ne prennent majoritairement pas en compte ces questions.

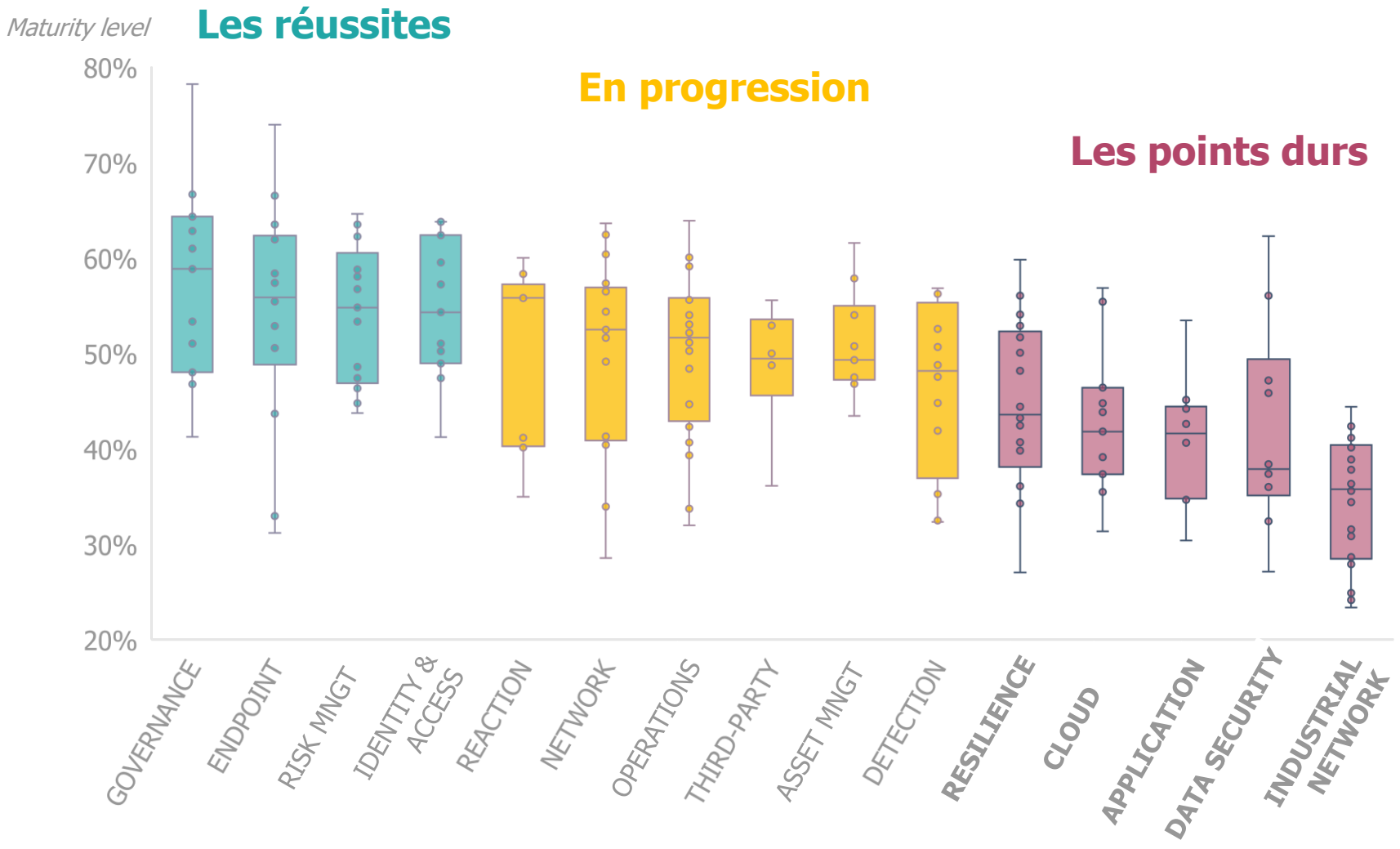
Quelle est la **MATURITÉ** *du marché sur les* **axes cyber ?**



Les piliers NIST sont aujourd'hui homogènes, témoignant de l'investissement important réalisés ces dernières années sur les thèmes « *détecter* » et « *répondre* ».

Le sujet de la reconstruction est le moins mature.

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

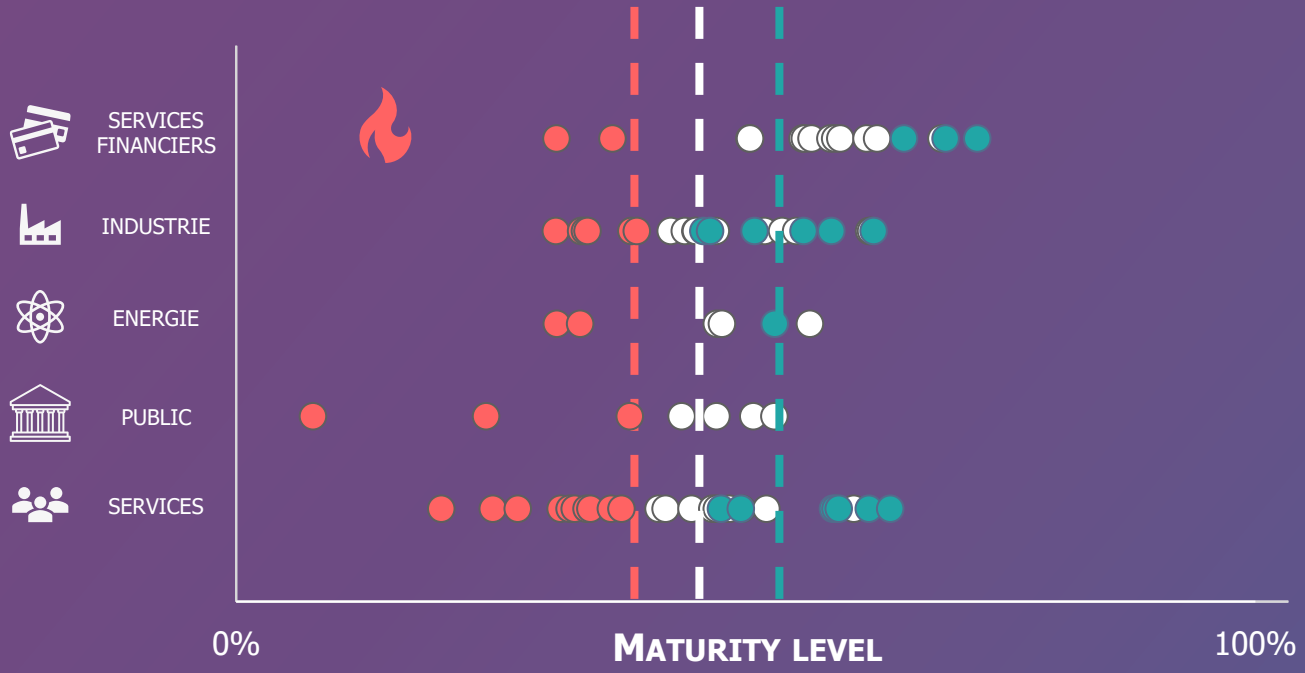


La vue du niveau de maturité pour chaque "boîte à moustache": Maximum / 1st quartile / Médiane / 3rd quartile / Minimum.
1 point = 1 point de contrôle dans notre évaluation de maturité


Comment le
MARCHÉ est-il protégé
face aux dernières
cyberattaques ?
46.2%
de résilience globale contre les
RANSOMWARE

FACE AUX RANSOMWARES :
30% DES ORGANISATIONS SONT EN SITUATION CRITIQUE

À partir des dernières attaques cyber gérées par le CERT-Wavestone, nous avons sélectionné **31 mesures anti-ransomware** et évalué la maturité de nos clients sur chacune d'elles

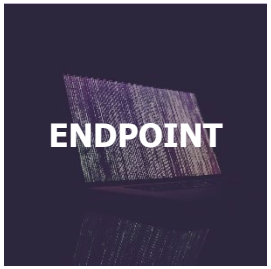


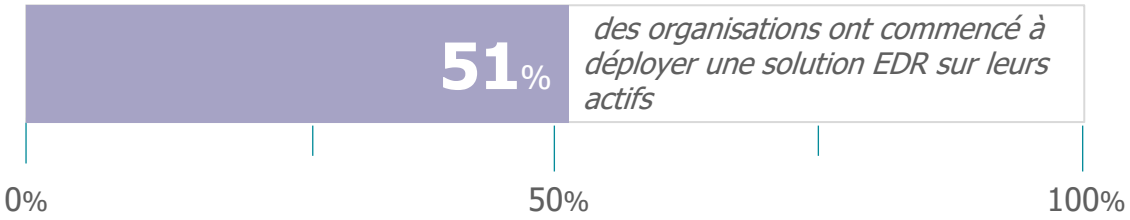
NIVEAU MOYEN DES CLIENTS WAVESTONE: 46.2%

MOYENNE DES GRANDES ENTREPRISES (TYPE CAC40) 54.5%

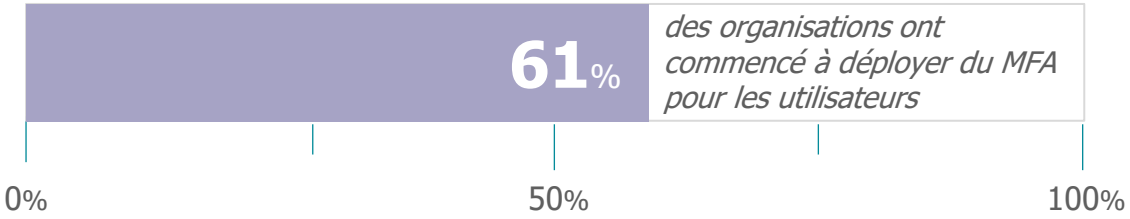
30% DES ORGANISATIONS CONSIDÉRÉES EN SITUATION CRITIQUE

EDR & MFA, une majorité d'organisations a réussi, il n'y a plus de raison d'attendre !

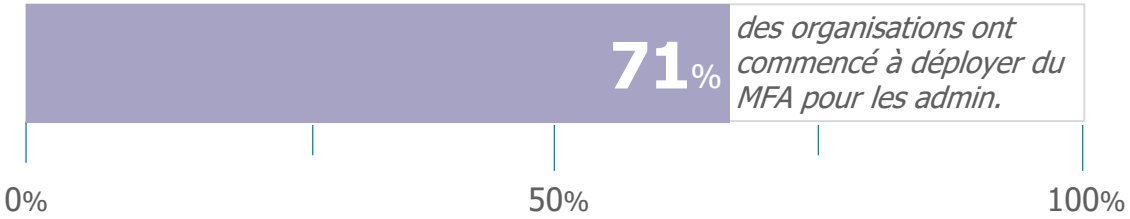




La couverture des outils *Endpoint Detection & Response* est de **67%** en moyenne



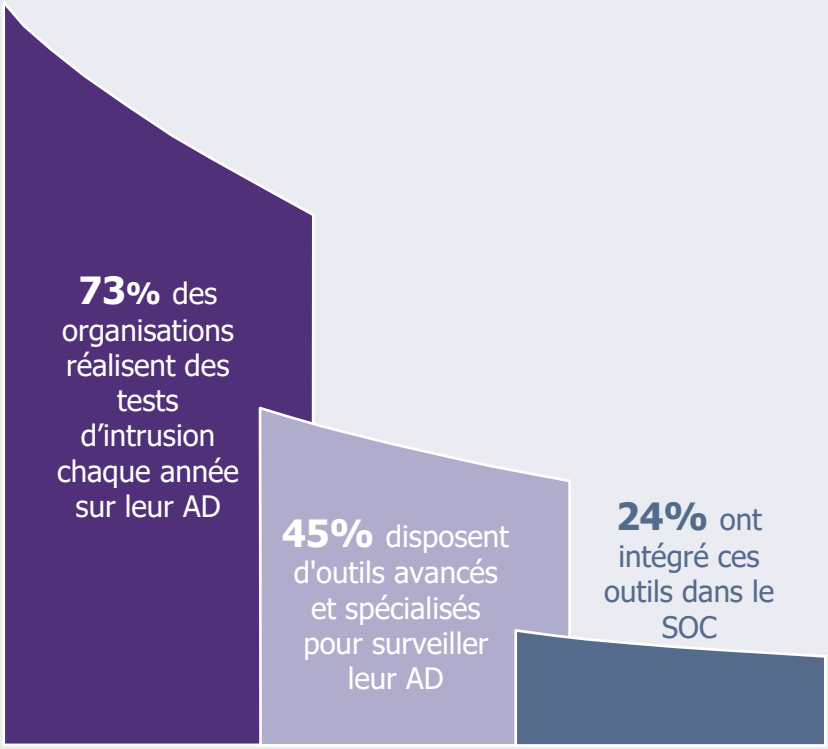
La couverture de *l'authentification multi-facteurs* pour les utilisateurs est de **63%** en moyenne



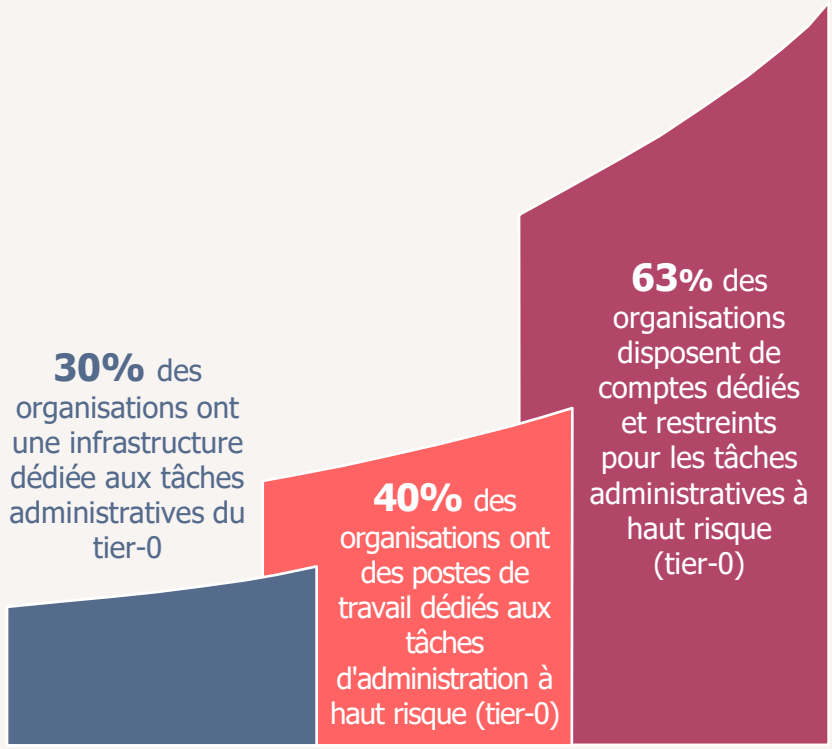
La couverture du *l'authentification multi-facteurs* pour les administrateurs est de **76%** en moyenne

La sécurisation de **l'Active Directory** est en cours, mais changer les pratiques et l'architecture reste un défi majeur

Des outils dédiés ont été déployés mais **la surveillance intégrée fait toujours défaut**.



La sécurité de l'**administration de l'Active Directory** reste une activité complexe



La résilience reste encore un sujet clé difficile à traiter, en particulier en ce qui concerne les **tests opérationnels**

Des investissements importants dans la gestion de crise…

- **82%** des organisations ont au moins partiellement défini, partagé et appliqué un **processus de gestion de cybercrise**
- **53%** des organisations ont un ensemble complet d'**outils dédiés à la gestion de crise**: outils de vidéoconférence, dossier de suivi partagé, manuel et répertoire de crise … et pour **25%** d'entre eux, ces **outils résistent aux cybercrises !**
- **47%** des organisations organisent régulièrement des exercices de **simulation de cybercrises**

10% des organisations ont testé leur plan de réponse à un incident avec leurs fournisseurs clés

17% des organisations ont testé leur plan de résilience sur l'ensemble de la chaîne de valeur (métier / informatique)

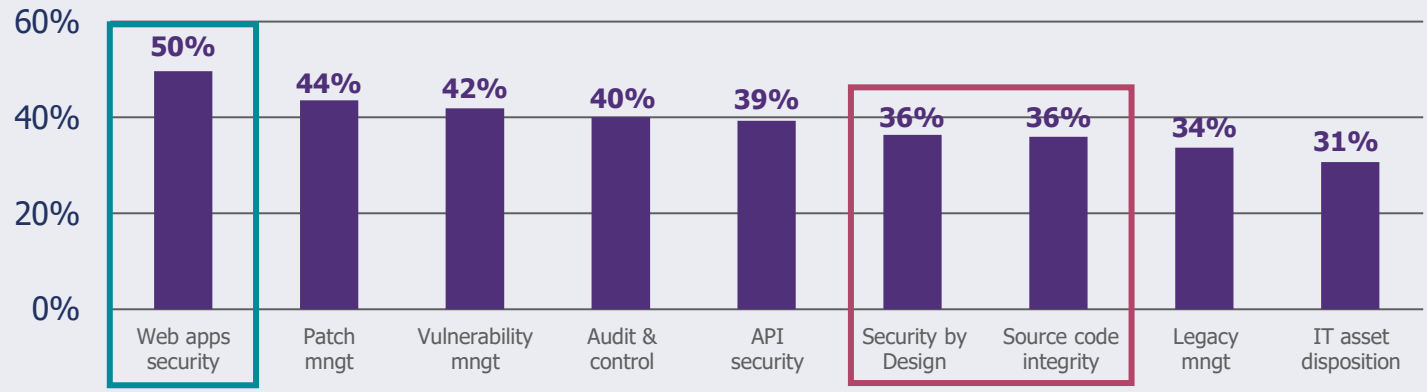
avec des investissements majeurs en cours dans le secteur financier

…cachant des difficultés réelles concernant les tests de résilience opérationnelle


DECOUVREZ
vos
prochains
CHALLENGES

Sécurité des applications et des données : plusieurs défis liés au volume des actifs concernés (38.8% & 38.3% de maturité)

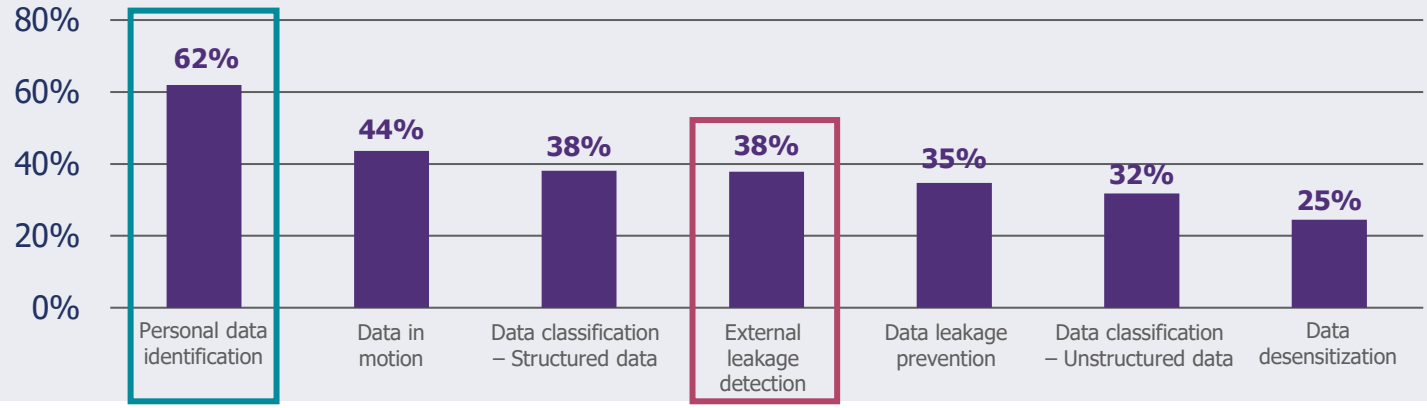
Sécurité des applications



72% des organisations ont implémenté un ***Web Application Firewall*** (WAF)

Des difficultés sont observées sur les sujets du cycle de vie des applications: agile, DevSecOps, CI/CD, SBOM…

Sécurité des données



En raison des réglementations, le sujet présente un bon niveau de maturité

57% des organisations n'ont pas investi dans un outil externe de détection de fuite de données, pourtant facile à mettre en œuvre

Le **Cloud** est un sujet clé concentrant des investissements importants mais qui atteint seulement **36.1%** de maturité

Surveillance et détection du Cloud

53%

des organisations envoient les journaux du Cloud à leur SOC (4% ont des règles de détection spécifiques)

47%

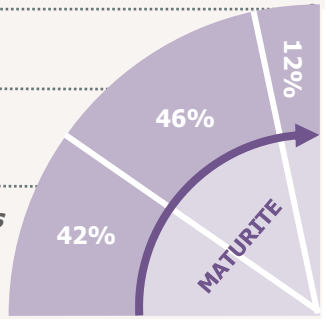
des organisations comptent uniquement sur les alertes de leur fournisseur Cloud

Administration du Cloud

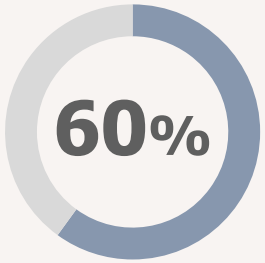
L'accès se fait par un bastion

Authentification multi-facteur (MFA) pour les comptes d'administration.

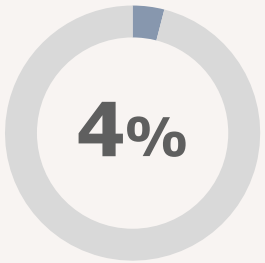
Console Cloud accessible depuis n'importe où, à l'aide d'un login et d'un mot de passe.



Conformité du Cloud



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

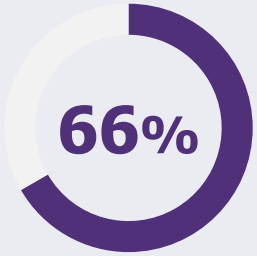


des organisations **corrigent** automatiquement les **problèmes** de conformité du Cloud

La sécurité des systèmes industriels a une **maturité** globale de **34.1%**

Quelques points encourageants

des organisations ont commencé à déployer une **organisation dédiée à la cybersécurité** sur leur périmètre industriel



des organisations utilisent des **pare-feux** pour séparer les réseaux d'entreprise des réseaux industriels

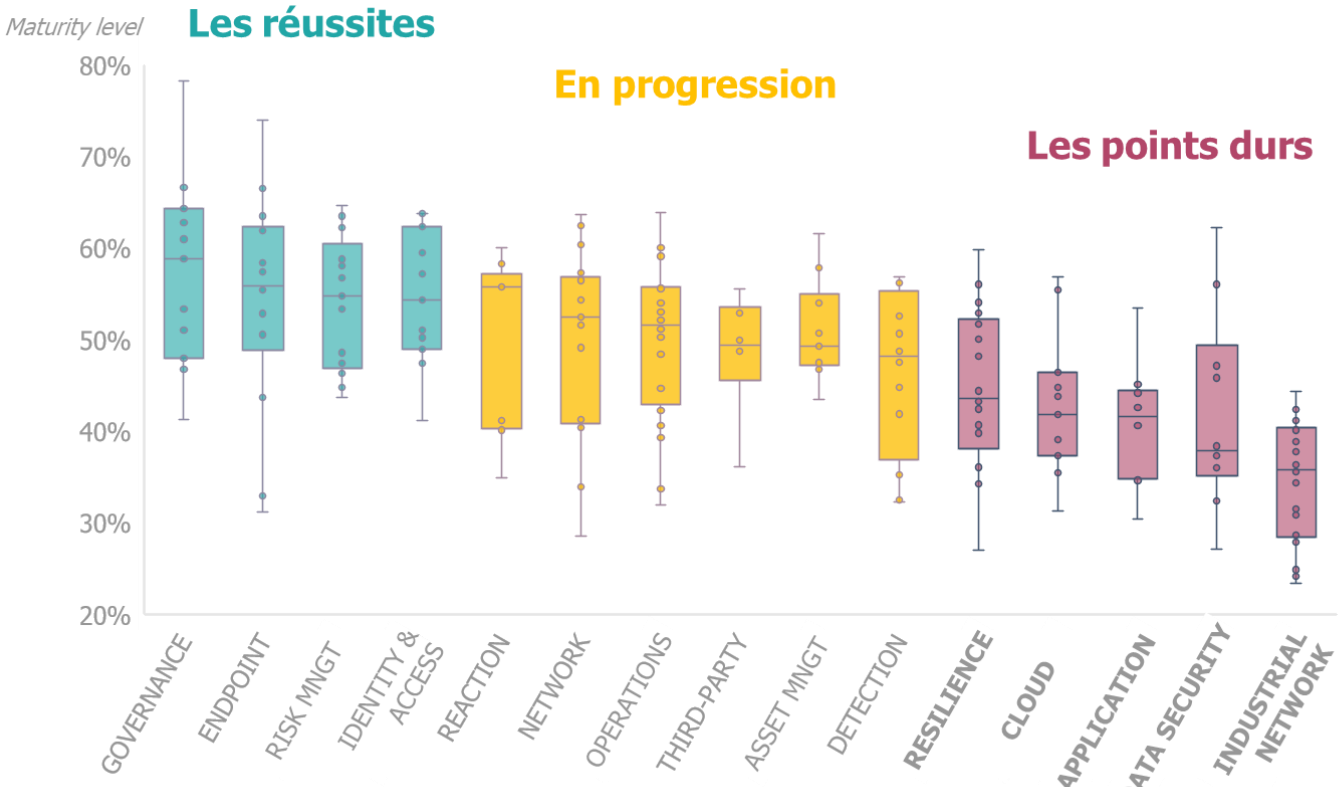
et

des organisations ont mis en place une **Zone Démilitarisée** (DMZ)

… et un thème clé à risque pour le futur : la **sécurité des tiers**

des organisations ne contrôlent pas leurs **exigences en matière de sécurité avec des tiers**

Un rapide aperçu des **tendances actuelles du marché…** *de nombreuses autres* **données à explorer !**



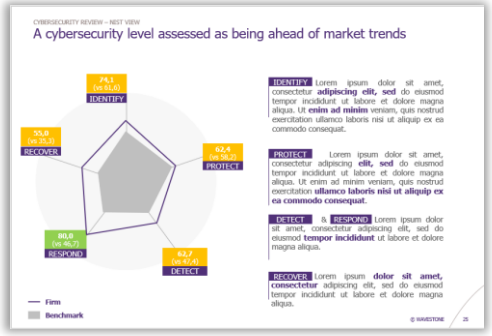
Les sujets clés pour 2022

- **GESTION RH**
- **RELATION AVEC LE COMITÉ EXÉCUTIF**
- **GESTION DES TIERS**
- **ZERO TRUST**
- **AUTOMATISATION**
- **SÉCURITÉ DES PRODUITS**

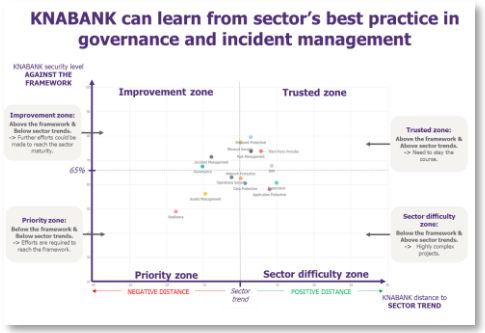
Quelle est votre posture ?

Réalisez votre propre évaluation

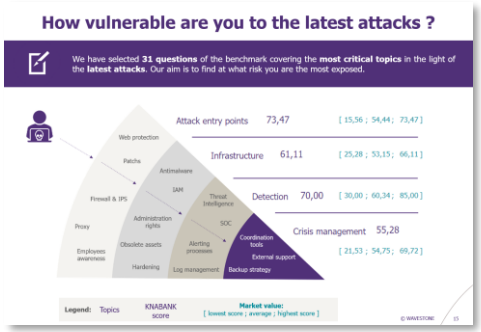
Plusieurs analyses différentes



Standards internationaux: NIST and ISO 2700X

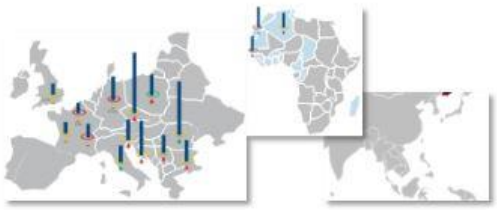


Maturité sur les sujets clés

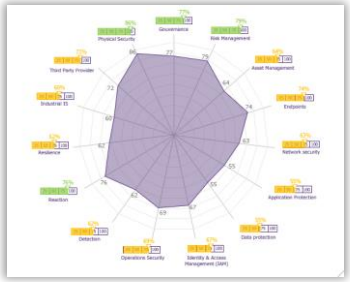


Résilience aux attaques les plus récentes

Pour aller plus loin



Vue par entité



Vue par niveau de risque cible
Gestion de programme et progression annuelle

Intégration à la plateforme Citalid pour une approche quantitative des risques alignée à votre évaluation de la menace

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_