

A woman with blonde hair is shown in profile, looking at a large digital display. The display shows a complex network diagram with white lines and blue nodes. The background is dark with blurred city lights. The overall tone is professional and technological.

cyber**v**adis

Cybersécurité : Comment construire un programme de gestion des tiers efficace pour réduire les risques liés à la Supply-chain ?

●●● La solidité d'une chaîne n'excède pas celle de son maillon le plus faible



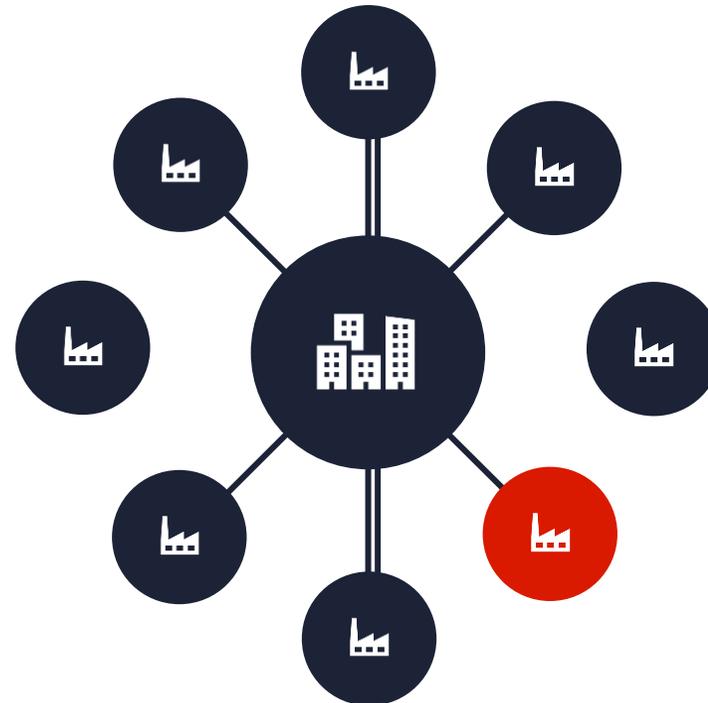
Pourcentage d'incidents de sécurité qui proviennent d'attaques indirectes (tierce partie)

Etude - Ponemon Institute - 2020



Pourcentage des entreprises qui se considèrent immatures dans leur gestion du risque lié aux tiers

Etude - Ponemon Institute - 2020



●●● Un manque de ressources pour faire face à des enjeux critiques

Fournisseurs / Partenaires / Filiales

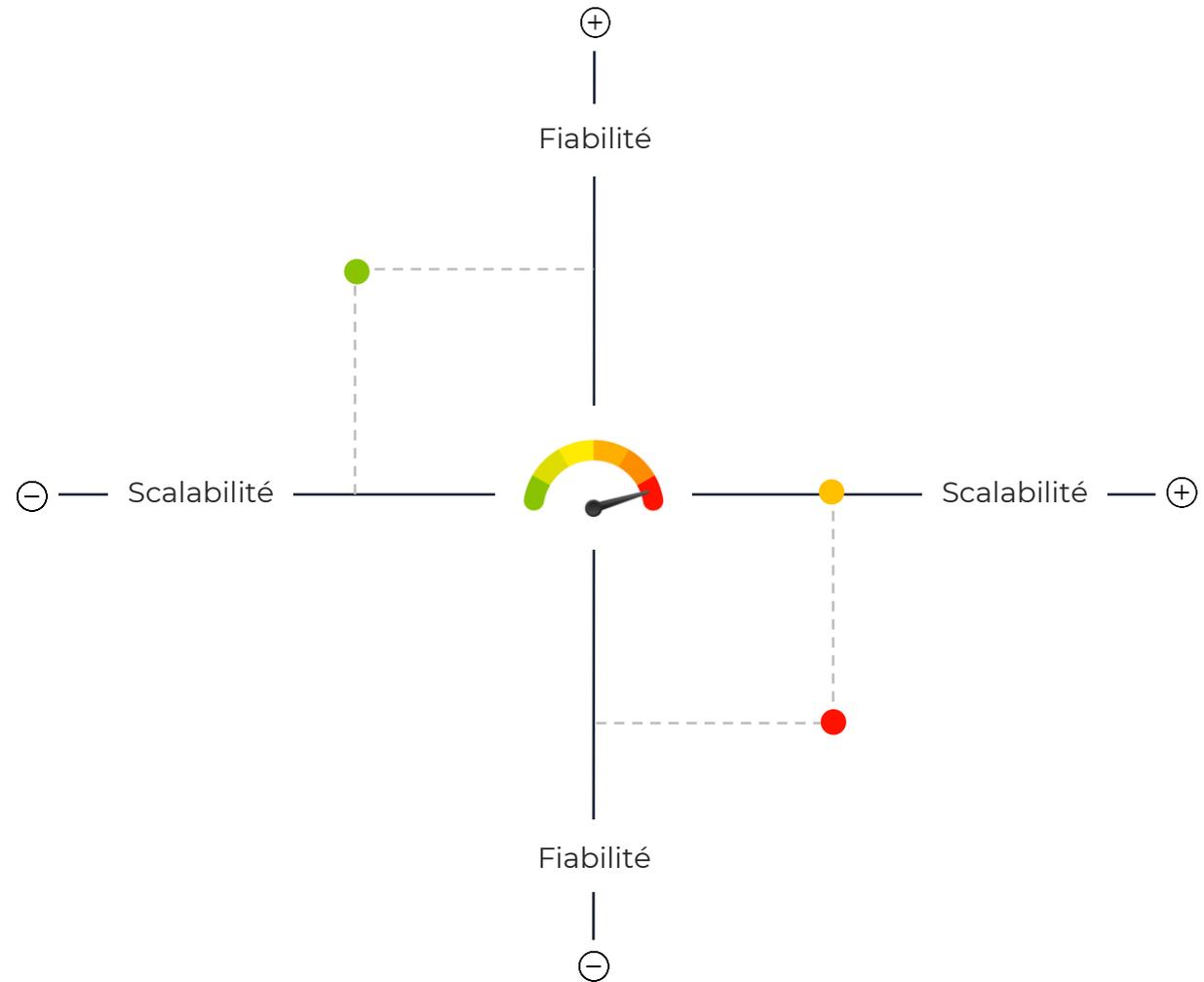
- IT / Non IT
- Criticité 1 / 2 / 3
- Existants | Nouveaux | RFP

Pratiques d'évaluation des tiers

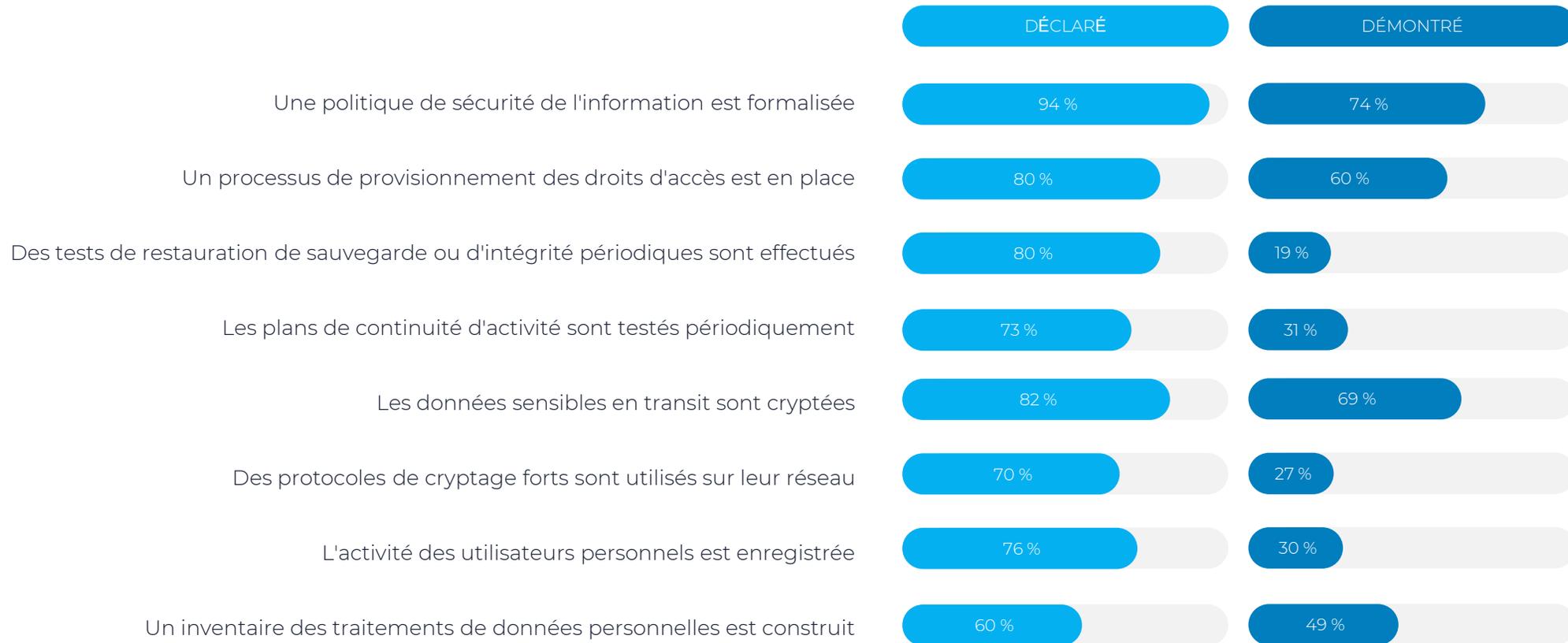
- ● Audit sur site
- ● Audit externe
- ● Questionnaire déclaratif

Quel est le réel niveau de risque ?

- Continuité d'activité
- Fuite de données personnelles
- Fuite de données sensibles



●●● Il n'y a pas de sécurité sans preuves de sécurité



## ●●● Approche 360 – Conformité et Gestion de risques

### Fournisseurs / Partenaires / Filiales

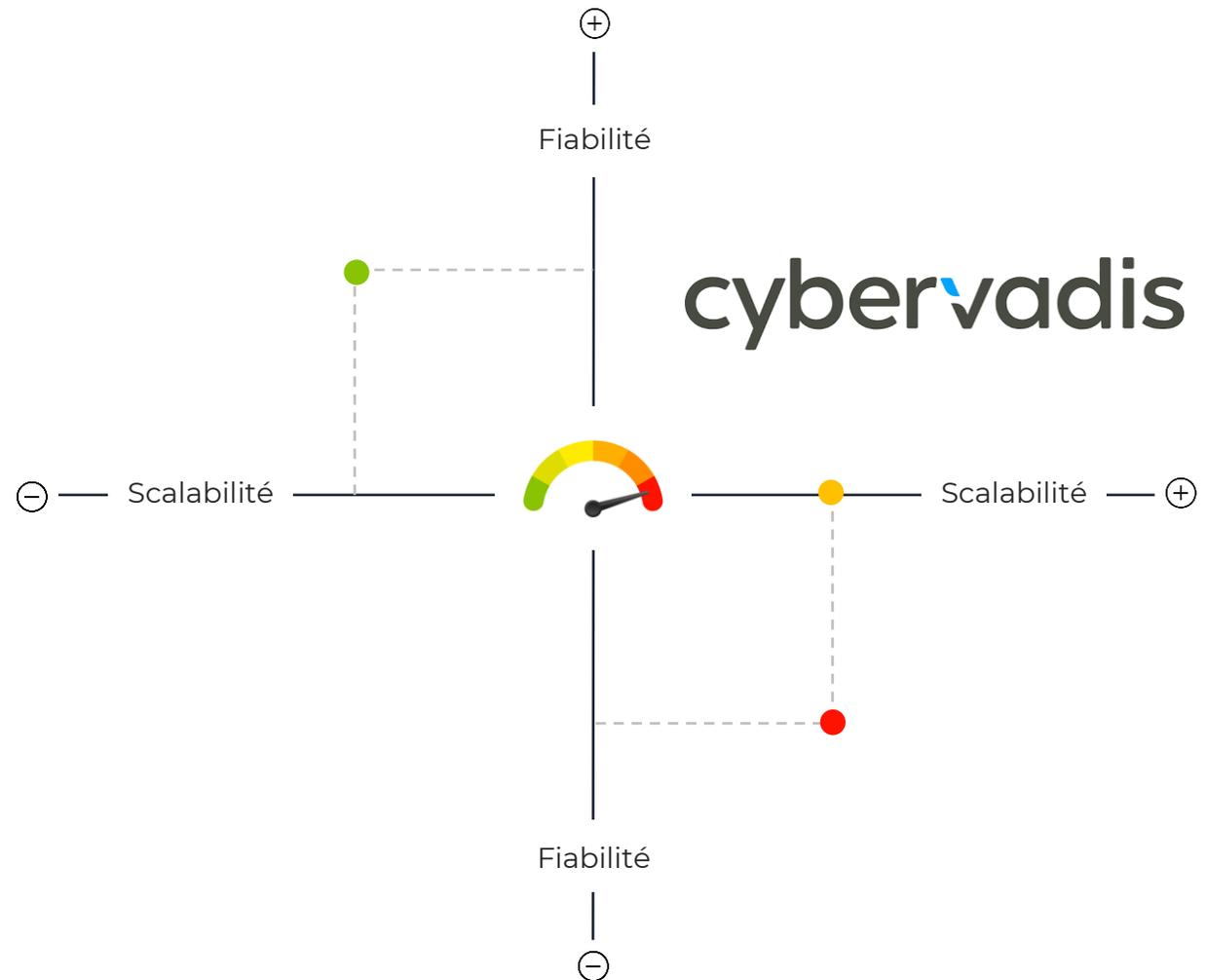
- IT / Non IT
- Criticité 1 / 2 / 3
- Existants | Nouveaux | RFP

### Pratiques d'évaluation des tiers

- Audit sur site
- Audit externe
- Questionnaire déclaratif

### Quel est le réel niveau de risque ?

- Continuité d'activité
- Fuite de données personnelles
- Fuite de données sensibles



- Une solution fiable pour évaluer et suivre le niveau de maturité des tiers

Évaluation du système de management de la sécurité de l'information des entreprises

Bilan de maturité / de performance

Évaluations basées sur la revue de preuves systématiques

Méthodologie s'appuyant sur les principaux référentiels de sécurité : NIST, ISO 27001, RGPD ...

Niveau de performance global & spécifique

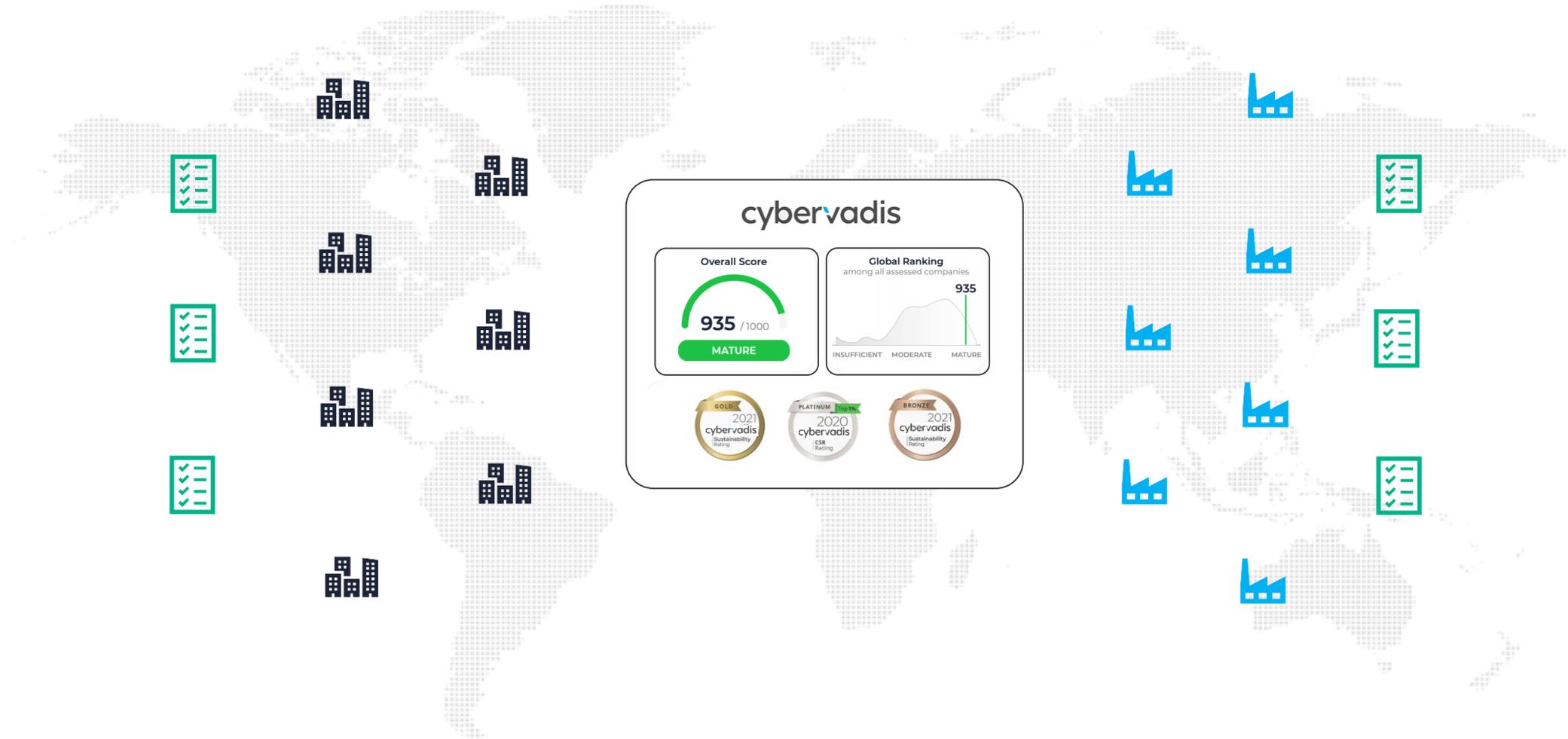
Niveau de risque qui dépend du contexte partagé avec le tier

Plan de remédiation collaboratif

Intégration dans les processus d'achat - Aide à la décision Business



●●● Devenir un standard de notation européen de la cybersécurité



●●● Des questionnaires adaptés au profil de l'entreprise



●●● Résultats – La liste des contrôles de sécurité classés par Forces & Améliorations

Compliance

440 Basic

Strengths (0)

Improvement actions (3)

|                   |   |           |
|-------------------|---|-----------|
| ▲ High priority   | Insufficient evidence or only statement provided - Identify the impacts of potential legal or regulatory non-compliance affecting your organization's data privacy                      | Completed |
| ▲ High priority   | Insufficient evidence or only statement provided - Define roles and responsibilities to ensure compliance with laws and regulations affecting your organizations' Information Security. | Completed |
| ▲ Medium priority | Insufficient evidence or only statement provided - Identify the impacts of applicable laws and regulations affecting your organization's data privacy                                   | To do     |

Data privacy

529 Basic

Strengths (4)

Improvement actions (21)

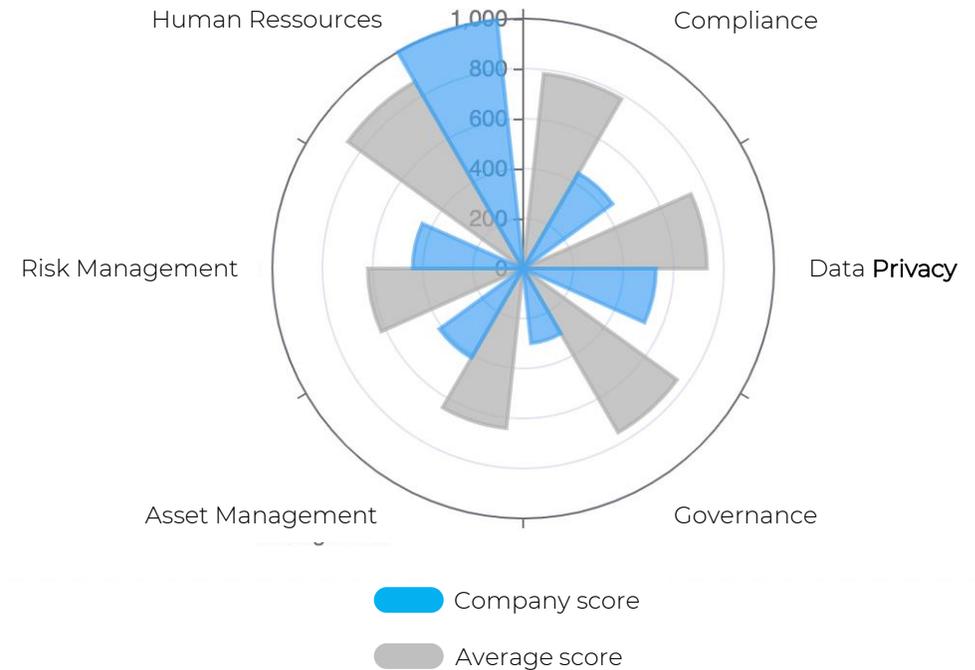
|                 |  |
|-----------------|--|
| ⓘ High impact   | A responsible for personal data (PII) protection is appointed  |
| ⓘ High impact   | A process to notify individuals, data controller and/or regulators in the case of a personal data breach event is formalized |
| ⓘ Medium impact | A privacy by default procedure is formalized   |
| ⓘ Medium impact | Best practices on data privacy principles are formalized   |

●●● Résultats – Scorecards : Niveau de performance globale & spécifique

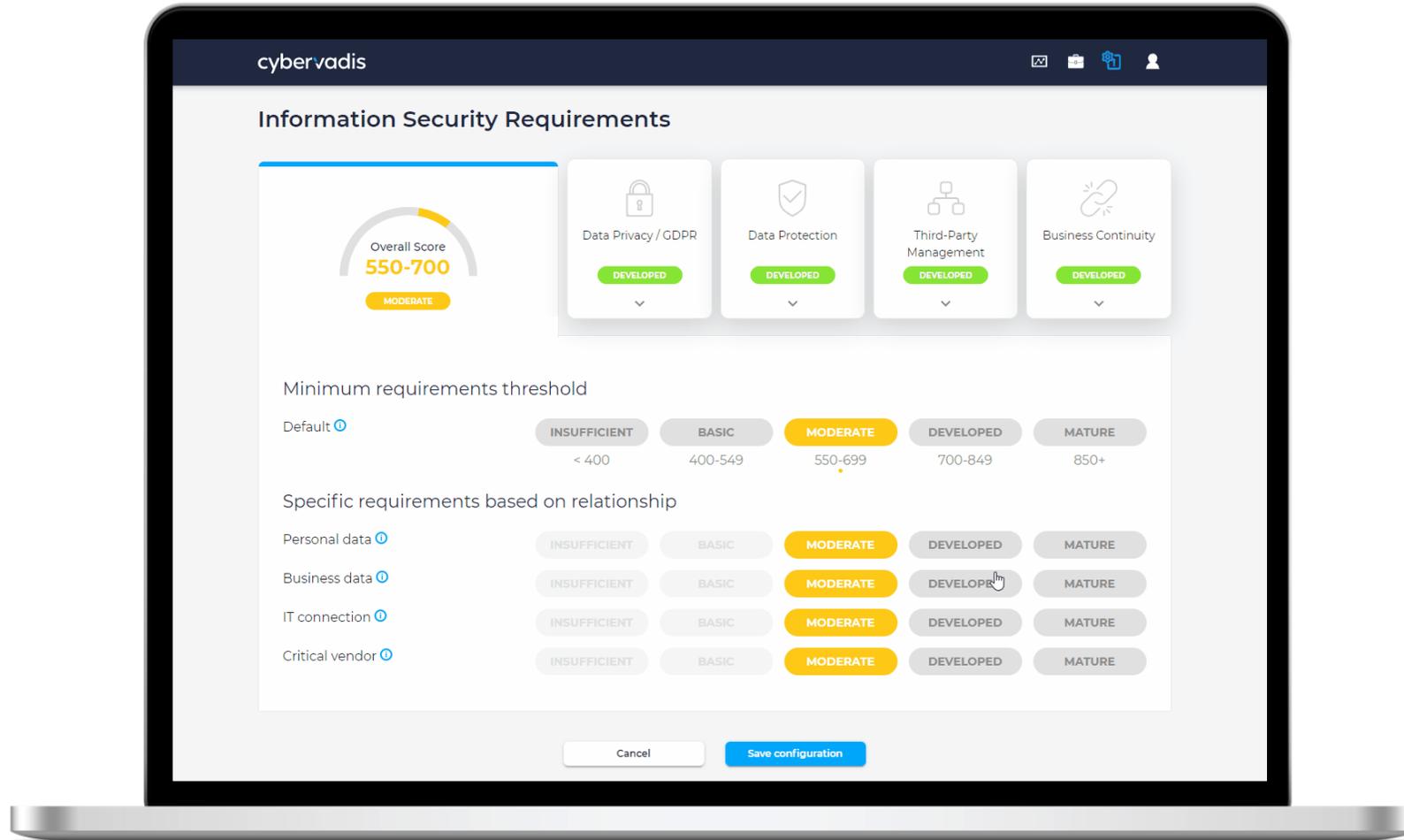
**NIST**

|          |            |              |
|----------|------------|--------------|
| Identify | 936 / 1000 | Mature       |
| Protect  | 850 / 1000 | Moderate     |
| Detect   | 520 / 1000 | Basic        |
| React    | 350 / 1000 | Insufficient |

|                  |            |
|------------------|------------|
| Compliance       | 900 / 1000 |
| Compliance       | 900 / 1000 |
| Data Privacy     | 860 / 1000 |
| Governance       | 800 / 1000 |
| Asset Managt.    | 550 / 1000 |
| Risk Assesment   | 699 / 1000 |
| Human Ressources | 400 / 1000 |



- Résultats – Niveau de Risque qui dépend du contexte partagé avec l'entreprise évaluée

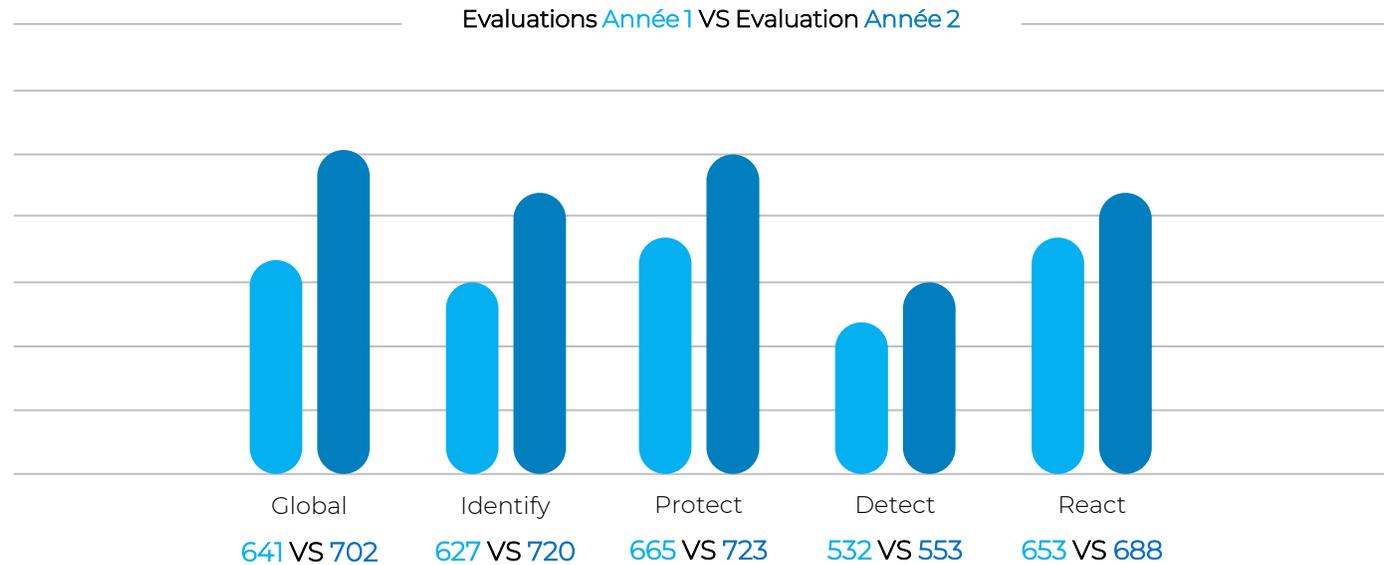


●●● Résultats – Plan de remédiation collaboratif entre donneurs d'ordre et répondants



●●● Résultats – Plan de remédiation

Cas Client : Etude d'impact réalisée sur 1000 entreprises évaluées (1 >299 ETP)



●●● Ils nous font confiance



**Merci pour votre écoute !**



**Julie Gaudin**  
Enterprise Account  
Executive



**Sarah Belhaddad**  
Sales Development  
Representative

**Retrouvez nous  
Sur LinkedIn !**