23e CONGRÈS DES ACTUAIRES

Stress tests cyber : threat intelligence et modélisation de la défaillance de cloud

Olivier LOPEZ
Maxime CARTAN
Daniel NKAMENI

Plan de la présentation

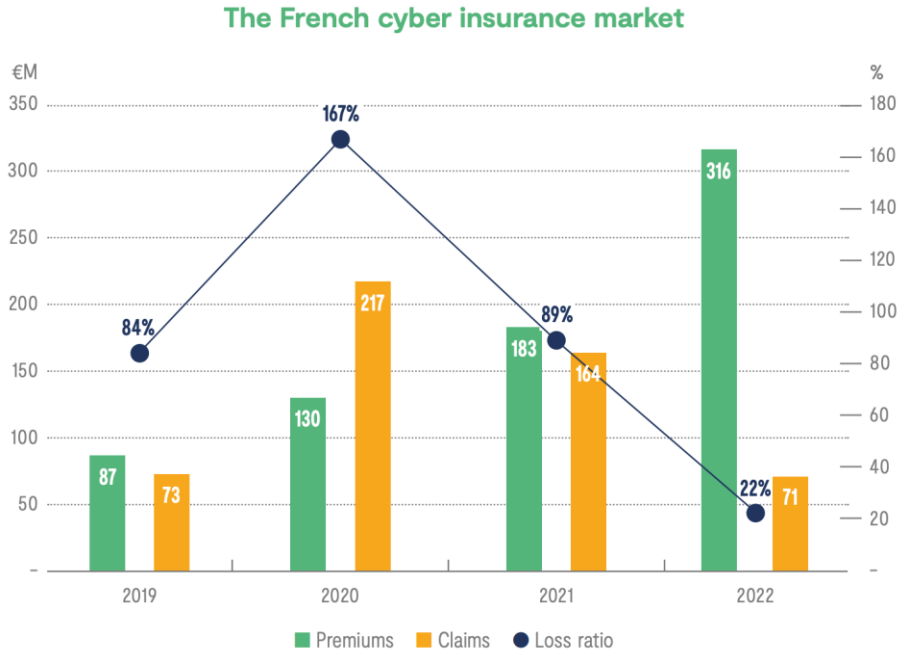
Etats des lieux de l'assurance cyber

Quelques statistiques

- L'«Association pour le Management des Risques et des Assurances de l'Entreprise » (AMRAE) a publié la troisième version de son enquête LUCY en 2023.

- Quelques chiffres clés en 2021:
  - Capacités d'assurance plus faibles
  - Franchises qui augmentent
  - Primes qui augmentent (+44,4% à comparer à une croissance de 27,5% du marché)
  - Couverture des grandes compagnies en baisse (-4,4%)

- Chiffres clés en 2022:
  - Loss ratio: 22%
  - Passe de 261% à 51% pour les entreprises « medium »
  - De 58% à 16% pour les plus grandes
  - **Passe de 36% à 100% pour les PME!**

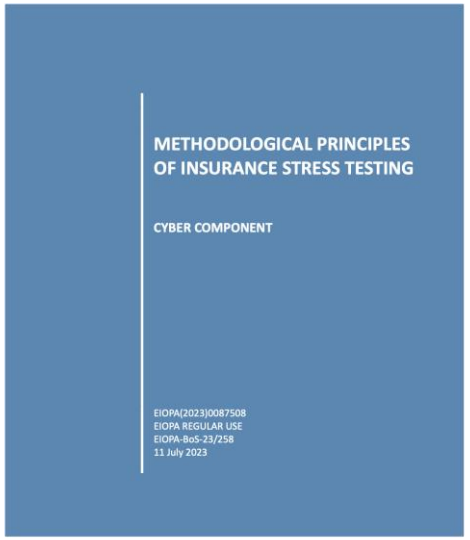


Etats des lieux de l'assurance cyber

Scénarios de stress

EIOPA liste quelques scenarios dont l'impact nécessite d'être évalué

- **Data center / infrastructure damage**
- Ransomware
- Ddos
- Data breach
- Power outage



eiopa
European Insurance and Occupational Pensions Authority

TABLE 3: RE/INSURERS' RANKING OF EXTREME CYBER SCENARIOS

Extreme cyber scenarios	Average ranking of scenario
Denial of service/interruption of operations	
Worm-like malware epidemic	1
Widespread ransomware attack	2
Mass data breach	
Exfiltration of sensitive information (PII, encrypted passwords, etc.) at key organisation/institution which has widespread effects on customers/suppliers	4
Disruption to critical infrastructure	
An extortion of supervisory control and data acquisition (SCADA) networks of industrial control systems	4
A cyberattack on a crucial participant in an industry/sector (e.g. hospital, food manufacturer/distributor, etc.)	5
A cyberattack on a key utility provider (power, water etc.)	2
A compromise of state/municipal services	5
Cross-sector IT failure	2

Refers to median ranking score assigned by survey respondents (1 being the highest-ranked scenario). Based on the results from a poll of 11 GA member cyber re/insurers

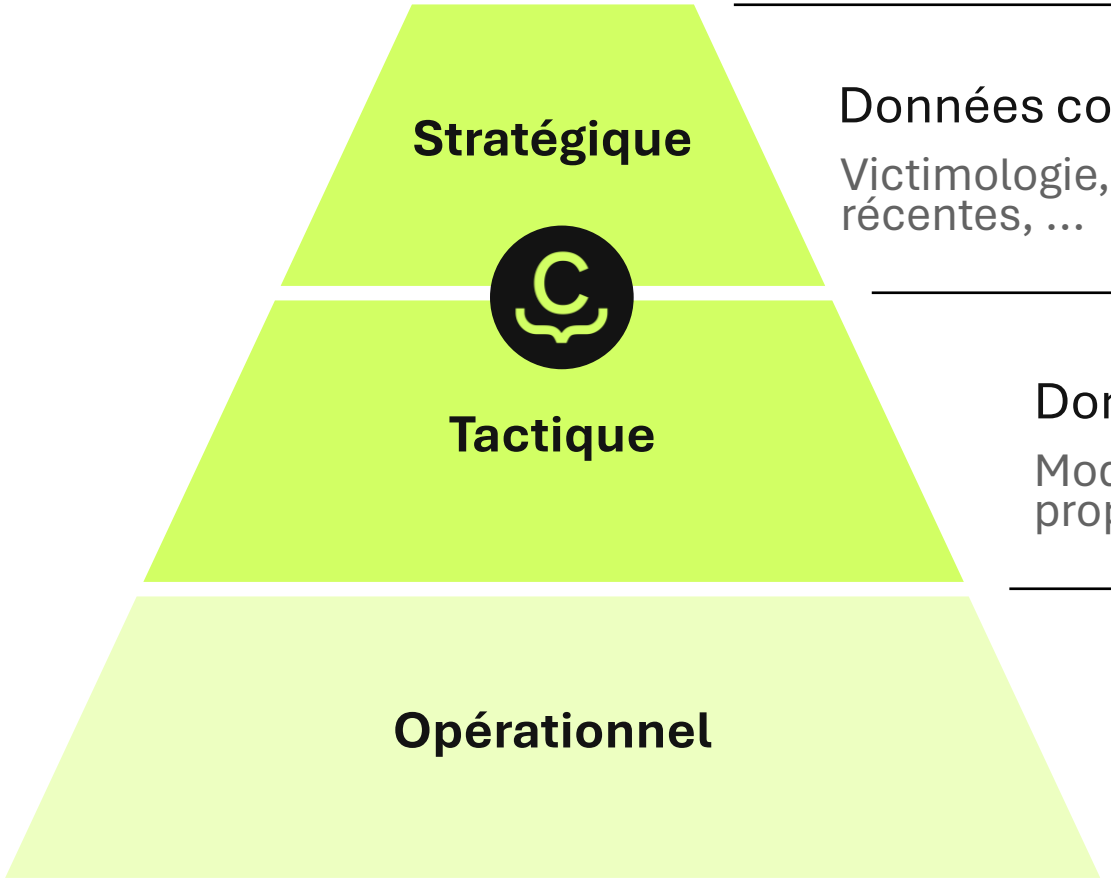
Source: The Geneva Association

Rapport de la Geneva association sur les risques cyber: identification de scénarios clés systémiques.

Plan de la présentation

- Etats des lieux de l'assurance cyber
- **La « Threat Intelligence »**
  - Contexte de l'étude
  - Focus sur la modélisation
  - Diversification et optimisation du portefeuille
  - Résultats empiriques
- Conclusion

La « Threat Intelligence »



Données contextualisées pour *décideurs business*

Victimologie, attribution, ressources opérationnelles, activités récentes, …

Données structurées pour *décideurs cyber*

Modes opératoires d'attaque, outils, rythmes de propagation, …

Données techniques pour *analystes*

Signatures techniques, infrastructure offensive, …

Expertise technique

Durée de vie

La « Threat Intelligence »

Pourquoi le renseignement cyber ?

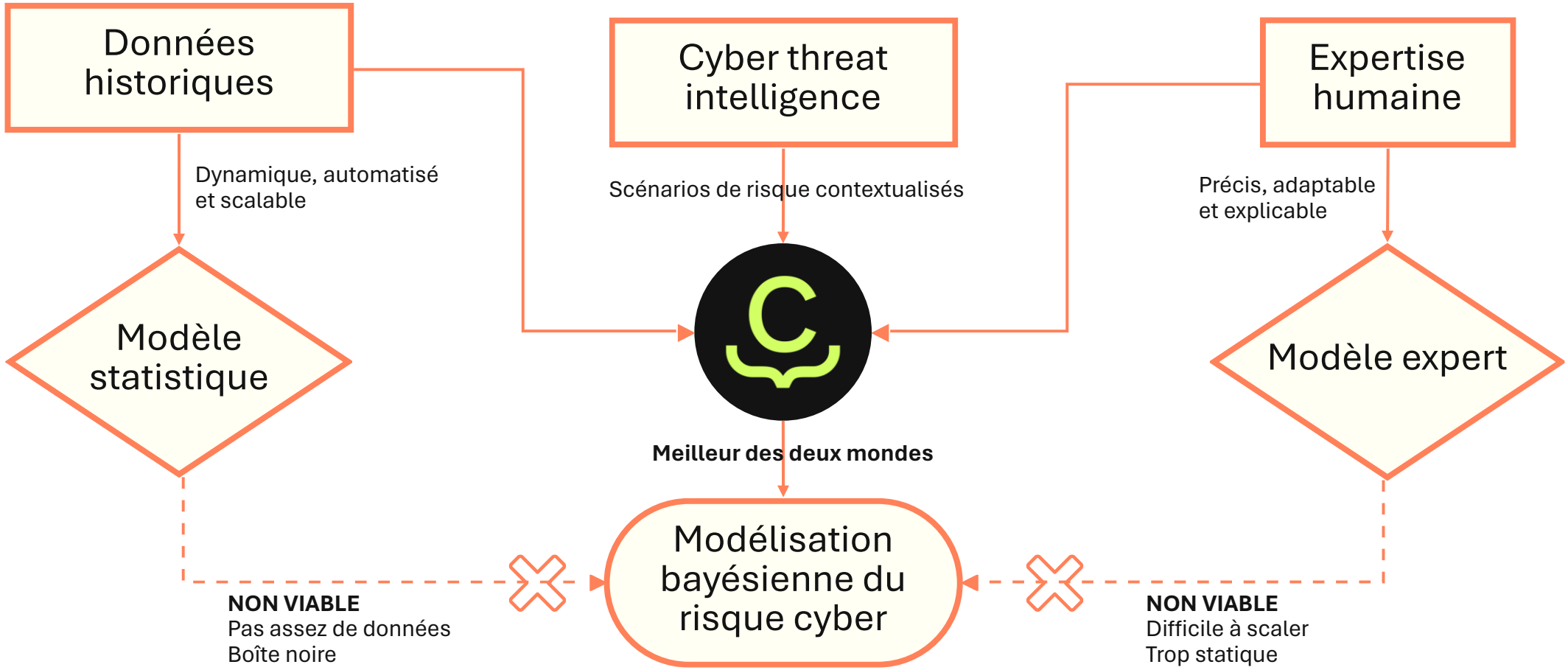
Cohérence, homogénéité et **anticipation**

Fréquence de ciblage	Chances de succès de l'attaque	Impacts financiers	ROI de la sécurité et de l'assurance
➢ **Pondérer les attaquants** pertinents en fonction de leur victimologie	➢ Simulation des **probabilités de propagation** des attaquants pertinents	➢ La propagation déclenche certains **types de pertes financières**	➢ **Simulations "What if"** pour calculer le **ROI** des solutions de sécurité et d'assurance
➢ Anticiper l'intensité de la menace et la **fréquence de ciblage**	➢ **Confrontation des modes opératoires** offensifs et défensifs (théorie des jeux)	➢ Les impacts dépendent de **quels actifs IT sont compromis**	➢ Génération de **recommandations d'investissement**

La « Threat Intelligence »

Entraîner une IA explicable

L'approche bayésienne de Citalid citée dans le **rapport de la DG Trésor** sur l'assurance cyber



Plan de la présentation

- Etats des lieux de l'assurance cyber
- La « Threat Intelligence »
- **Contexte de l'étude**
- Focus sur la modélisation
- Diversification et optimisation du portefeuille
- Résultats empiriques
- Conclusion

Contexte de l'étude

Défaillances de cloud

- La défaillance de cloud est un exemple de défaillance d'infrastructure critique.
- L'usage du cloud est essentiellement :
  - stockage de données
  - data processing
- Essentiellement deux types de solutions cloud :
  - private cloud: un fournisseur (Amazon, Google…) a une technologie utilisée pour construire un serveur spécifique chez une client.
  - public cloud: un seul serveur garde les données de plusieurs utilisateurs et est localisé chez le fournisseur.
- Le cloud publique est plus susceptible de genérer un événement systémique…
- … mais le cloud privé le peut aussi, car utilise des technologies partagées.

Contexte de l'étude

Exemples d'incidents

- Deux exemples récents en France:
  - **OVH** à Strasbourg (2021) : un incendie détruit les serveurs. Des serveurs de back-up (situés au même endroit) brûlent également. Plus de 400K de dommages aux tiers payés par OVH.
  - **Google** (Août 2023) : une inondation dans un entrepôt de données Google génère une interruption de certains services web impactant une part significative du territoire.

- Exemple criminel : **CloudNordic (ransomware attack)**
- **Cloud et Assurance :** est-ce que l'assurance du fournisseur doit payer, ou est-ce celle de la victime ?
- Amazon a également développé des partenariats en assurance, couplés avec ses offres cloud aux US.


TECH MONITOR 30
PROUDLY CELEBRATING 30 YEARS OF INDEPENDENT IT JOURNALISM

ctions | Cybersecurity | Digital economy | Hardware | Leadership | Events

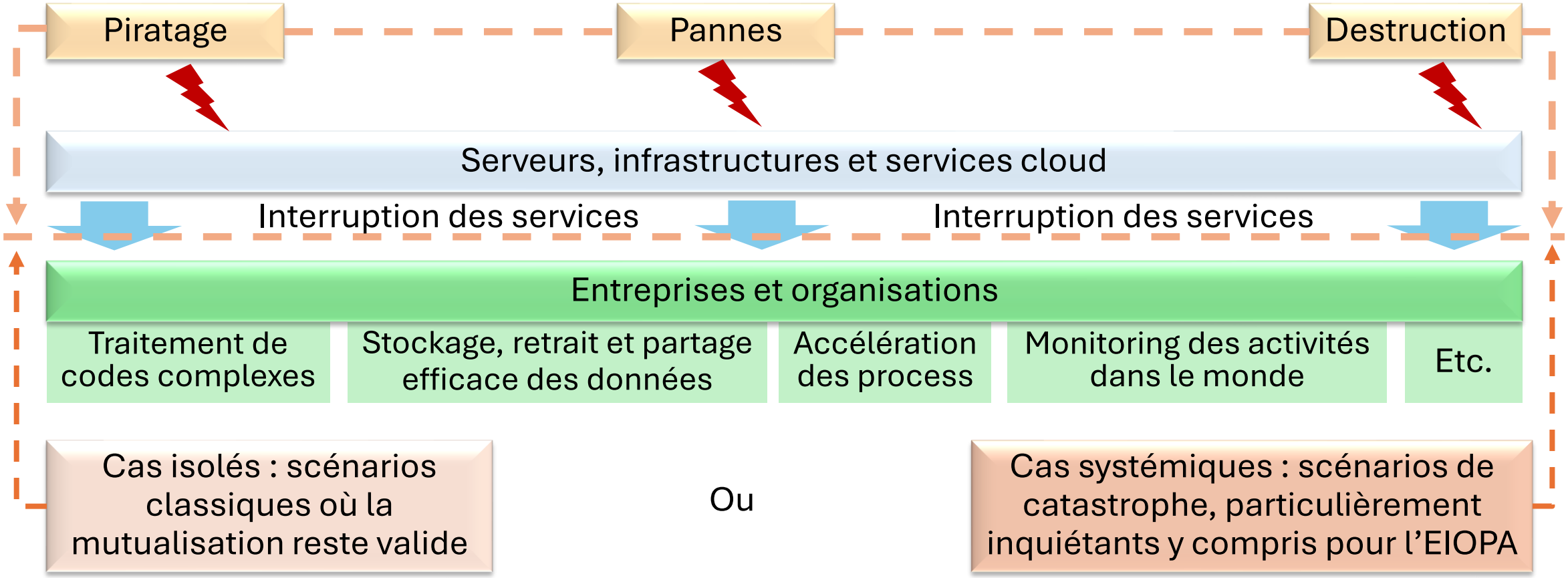
TECHNOLOGY > CYBERSECURITY | August 25, 2023

Devastating ransomware attack hits Danish cloud hosting companies CloudNordic and AzeroCloud

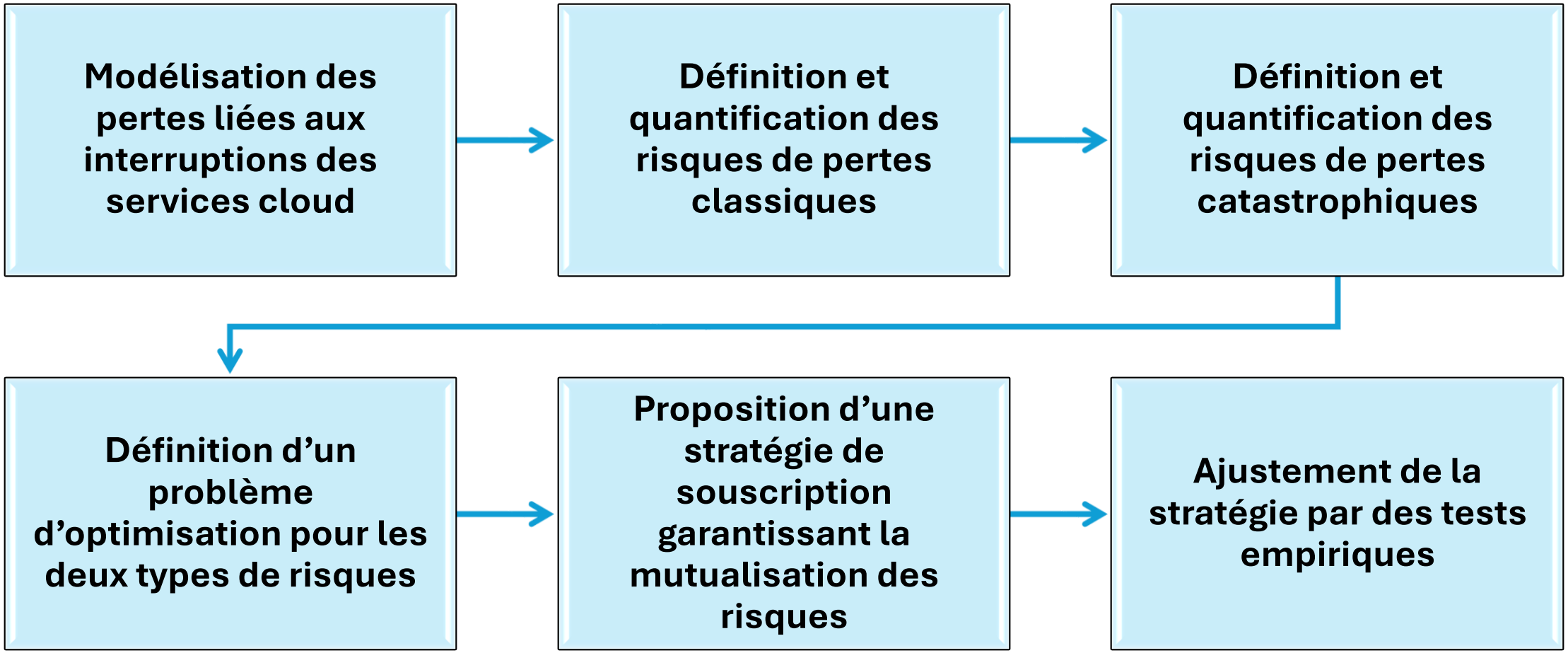
A ransomware attack on the Danish hosting sites saw its back-ups encrypted and both firms lose access to all of their customers' data.

By Claudia Glover

Contexte de l'étude



Méthodologie de l'étude



Plan de la présentation

- Etats des lieux de l'assurance cyber
- La « Threat Intelligence »
- Contexte de l'étude
- **Focus sur la modélisation**
- Diversification et optimisation du portefeuille
- Résultats empiriques
- Conclusion

Focus sur la modélisation

Définition de la perte du portefeuille

Supposons qu'il existe d **fournisseurs** de services cloud et n **assurés** dans le portefeuille.

Soit $\delta_{i,j}$ **l'indicatrice indiquant qu'un assuré** i **a souffert d'une interruption du fournisseur** j. La perte au niveau du portefeuille est donnée par :

$$\mathfrak{L} = \sum_{i=1}^{n} \sum_{j=1}^{d} \delta_{i,j} \omega_{i,j} \tau_i \boldsymbol{L_i^{(j)}}$$

Où :

- $\boldsymbol{\omega_{i,j}}$ est l'exposition de l'assuré $\boldsymbol{i}$ au fournisseur j $\left(\sum_{j=1}^{d} \omega_{i,j} = 1\right)$;
- $\boldsymbol{\tau_i}$ est le chiffre d'affaires de l'assuré $\boldsymbol{i}$;
- $\boldsymbol{L_i^{(j)}}$ est le coût unitaire de la perte de l'assuré $\boldsymbol{i}$ à la suite de l'interruption du fournisseur $\boldsymbol{j}$;

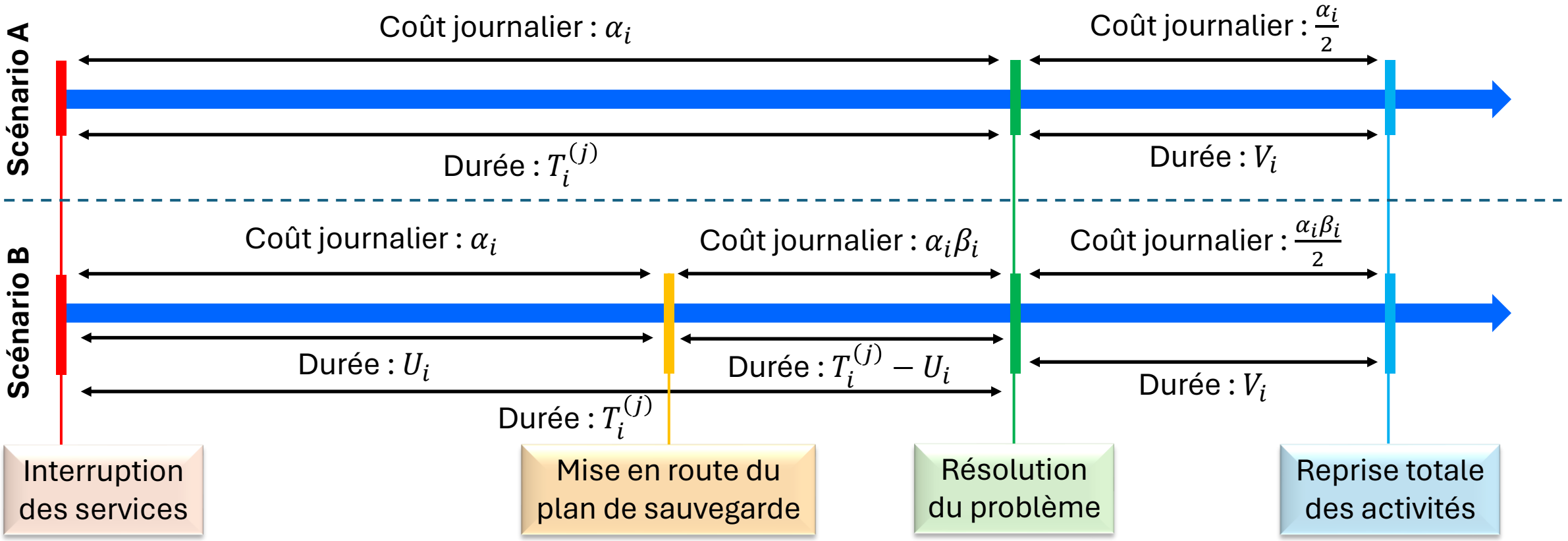
NB : $\boldsymbol{\delta_{i,j}}$ **peut être stochastique (régime standard) ou égale à 1 (régime stressé)**

Focus sur la modélisation

Modélisation de la perte d'un assuré $\left(L_i^{(j)}\right)$

Scénario A : L'assuré i ne possède pas de plan de sauvegarde

Scénario B : L'assuré i possède un plan de sauvegarde d'efficacité $1 - \beta_i \in [0,1]$



Focus sur la modélisation

Modélisation de la perte d'un assuré $\left(L_i^{(j)}\right)$

Scénario A : L'assuré i ne possède pas de plan de sauvegarde

Scénario B : L'assuré i possède un plan de sauvegarde d'efficacité $1-\beta_i \in [0,1]$

$$L_i^{(j)} = \alpha_i \left(T_i^{(j)} - \left(T_i^{(j)} - U_i \right)_+ (1-\beta_i) \right) + \frac{\alpha_i \left\{ 1-(1-\beta_i)\epsilon_i^{(j)} \right\} V_i}{2}$$

Où :

- $\epsilon_i^{(j)} = 1_{U_i \leq T_i^{(j)}}$ est l'indicatrice de la mise en route d'u plan de sauvegarde
- Toutes les variables sont aléatoires
- Nous supposons que le vecteur $(U_i, V_i, \alpha_i, \beta_i)_{1 \leq i \leq n}$ **est i.i.d** et indépendant de $T_i^{(j)}$

Focus sur la modélisation

Mesure de risque en régime standard

Il s'agit du régime classique où le principe de mutualisation est valide **($\delta_{i,j}$ est stochastique)**

Pour ce régime, nous choisissons **la variance du portefeuille $\mathfrak{V}$** comme mesure de risque

$$\mathfrak{V} = Var(\mathfrak{L}) = \bar{\omega}'\Sigma\bar{\omega}$$

Où :

$$\Sigma_{j,k} = Cov\left(\delta_{i_1,j}L^{(j)}_{i_1,j}, \delta_{i_2,j}L^{(k)}_{i_2,k}\right)$$

$$\bar{\omega}_j = \sum_{i=1}^{n} \omega_{i,j}\tau_i$$

Focus sur la modélisation

Mesure de risques en régime stressé ou de catastrophe

Les risques sont systémiques et le principe de mutualisation n'est plus valide **($\delta_{i,j} = 1$)**

La mesure de risque choisie est :

$$\mu(\overline{\omega}) = m'\overline{\omega}$$

Soit

$$L^{(j)} = \sum_{i=1}^{n} \omega_{i,j}\tau_i L_i^{(j)}$$

Alors $\boldsymbol{m}$ peut être :

- **La moyenne de $L^{(j)}$**
- **La Value-at-Risk (VaR) d'ordre γ de $L^{(j)}$**
- **La Conditional Tail Expectation (CTE) d'ordre γ de $L^{(j)}$**

Plan de la présentation

- Etats des lieux de l'assurance cyber
- La « Threat Intelligence »
- Contexte de l'étude
- Focus sur la modélisation
- **Diversification et optimisation du portefeuille**
- Résultats empiriques
- Conclusion

Diversification et optimisation du portefeuille

Objectif de l'optimisation

Trouver la meilleure configuration en fonction des $\bar{\omega}$ permettant d'atteindre un niveau optimal de diversification en régime standard et en régime stressé.

Le problème d'optimisation est :

$$\min_{\bar{\omega}} \frac{1}{2}\bar{\omega}'\Sigma\bar{\omega} + \lambda m'\bar{\omega}$$
$$s.c.\,\bar{\pi}'\bar{\omega} = \rho,$$
$$\bar{\omega} \geq 0$$
$$\sum_{j=1}^{d} \bar{\omega}_j = \mathrm{W}$$

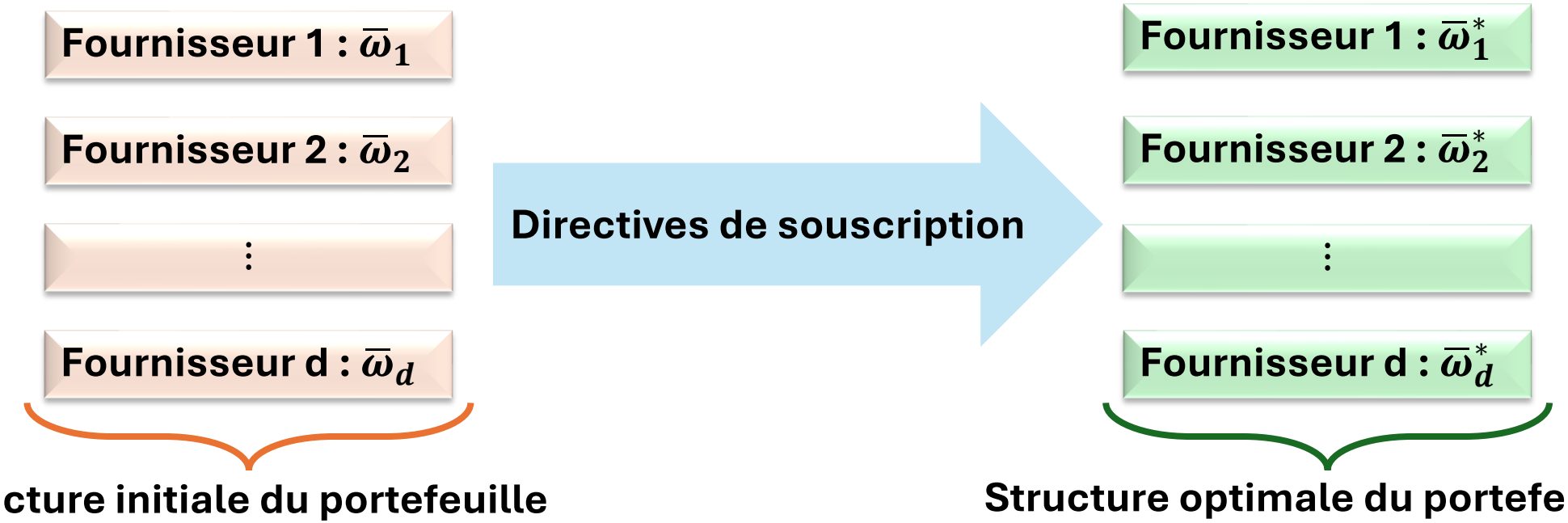
Où :

- $\boldsymbol{W}$ est l'exposition totale et
- $\boldsymbol{\rho}$ la perte moyenne espérée

Diversification et optimisation du portefeuille

Résultats de l'optimisation

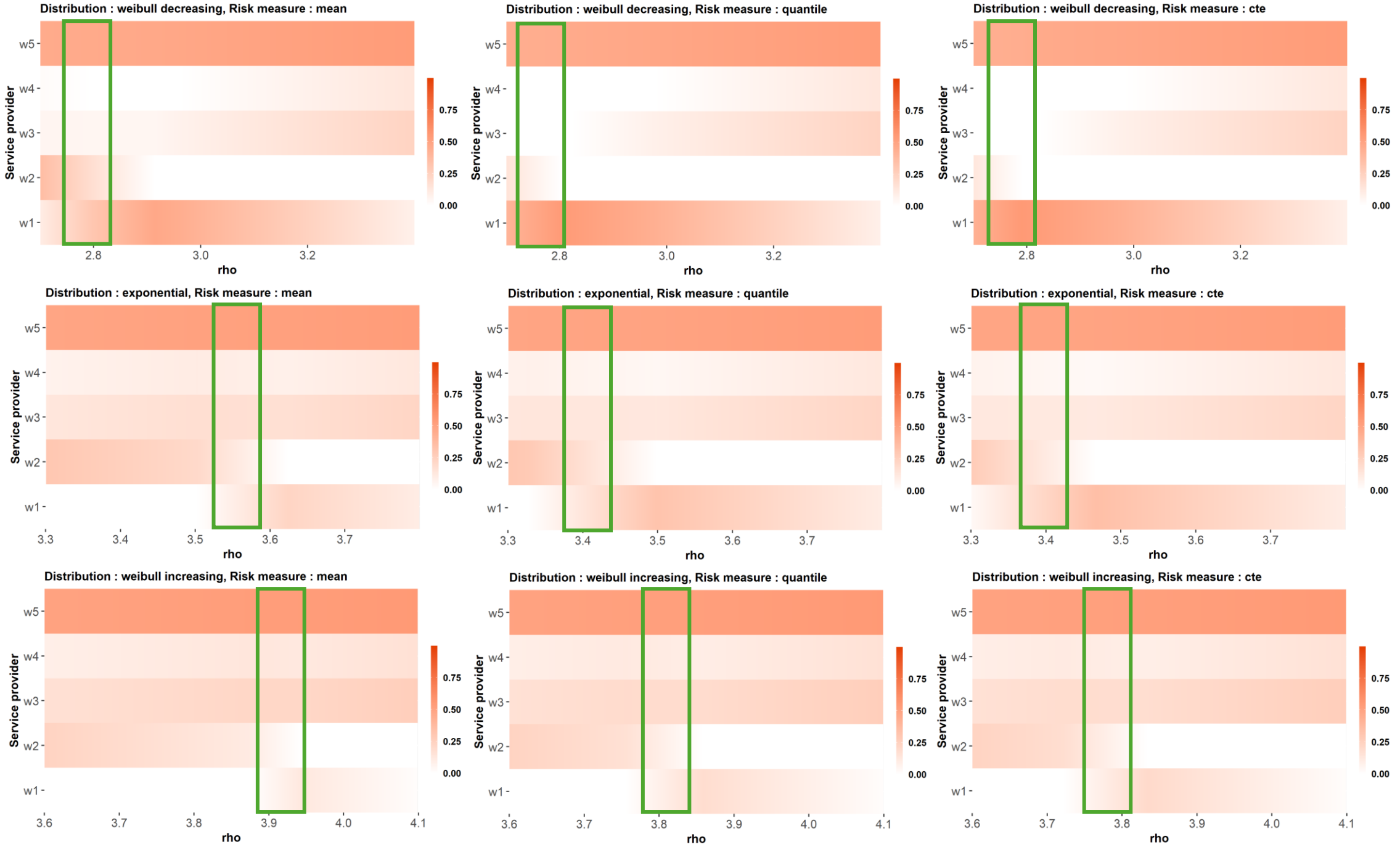
Les valeurs optimales $(\bar{\omega}_1^*, \bar{\omega}_2^*, \dots, \bar{\omega}_d^*)$ qui assurent une diversification et minimisent les risques de perte dans les deux régimes.



Plan de la présentation

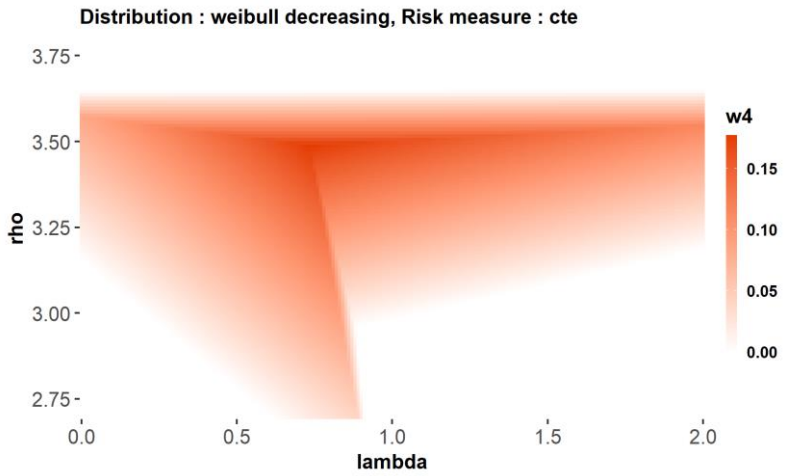
- Etats des lieux de l'assurance cyber
- La « Threat Intelligence »
- Contexte de l'étude
- Focus sur la modélisation
- Diversification et optimisation du portefeuille
- **Résultats empiriques**
- Conclusion

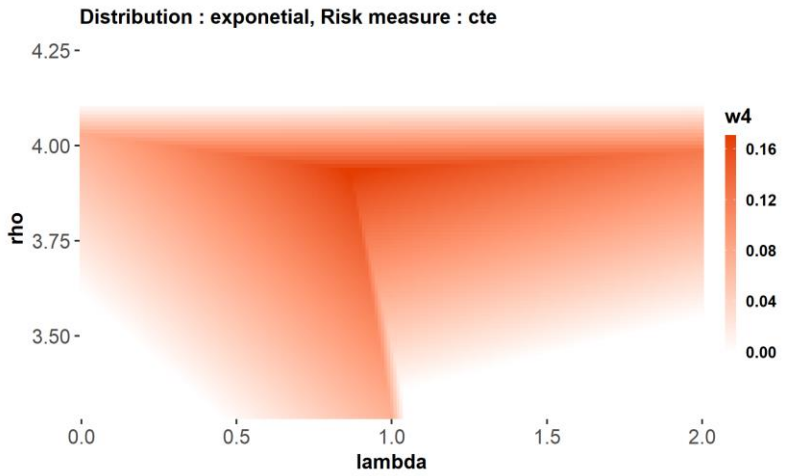
Résultats empiriques

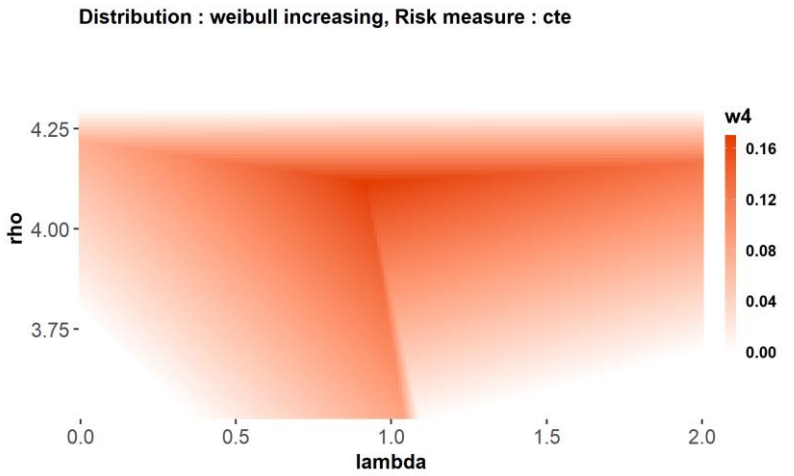


Résultats empiriques

Focus sur $\bar{\omega}_4$ et sur la CTE comme mesure de risque







- Les trois distributions ont des comportements similaires mais avec des décalages sur λ
- Nous observons ici une interaction entre ρ, λ et $\bar{\omega}_4^*$ **(idem pour tous les $\bar{\omega}^*$).**
- Question résultante : **Sur quel critère choisir une valeur de λ en pratique ?**

Plan de la présentation

- Etats des lieux de l'assurance cyber
- La « Threat Intelligence »
- Contexte de l'étude
- Focus sur la modélisation
- Diversification et optimisation du portefeuille
- Résultats empiriques
- **Conclusion**

Conclusion

- L'interruption des services de cloud est l'un des scénarios les plus préoccupants en gestion de risque cyber collectif.

- Notre étude, basée sur les travaux de Lloyd's (2018), propose une méthodologie pour la quantification et la gestion de ces risques dans des scénarios classiques et extrêmes. Un guide pour les souscripteurs.

- L'application de cette méthodologie nécessite une compréhension approfondie du contexte de l'assureur et des caractéristiques de ses assurés.

- Notre méthodologie pourrait également s'appliquer à d'autres risques de même nature, tels que les risques d'approvisionnement (supply chain risk).

Conclusion

- Cyber = risque en évolution.
- De par sa nature humaine, nécessité de comprendre les motivations, les évolutions, les modes opératoires des hackers (threat intelligence).
- Scénarios de crise cyber : difficulté pour projeter un événement qui ne s'est, de fait jamais réalisé.
- Formalisation de ces scénarios : permet de cibler les quantités à modéliser, ce qui s'effectue en mixant données et expertise (bayésien).
- Importance de déduire ce ces scénarios des leviers d'action pour augmenter la diversification, la prévention.

Conclusion

Un programme de R&D ambitieux

Citalid & **l'Institut Europlace de Finance (EIF) Louis Bachelier** joignent leurs forces

- **Interdépendance** entre les risques, **démutualisation** (systémique)
- Analyse et extrapolation des **queues de distributions** (sévérité)
- Construction de **mesures d'exposition** et de diversification des portefeuilles par scénario

Merci pour votre aimable attention