2025

citalid

Piloter son risque cyber : les fondamentaux de la *quantification financière*

Le pouvoir caché de la cyber threat intelligence

Sapere aude – Osez savoir

Dare to know - Sapere aude

A propos

Citalid, leader européen de la quantification du risque cyber (CRQ)

Premier pure-player CRQ européen

CLIENTS

100+ Clients
35% du **CAC40**

Entreprises & Gestionnaires de Portefeuille

MARCHE

Siège en France, présence en DE, BE, CH, JD, USA, CA

Industrie, Transports, Banque & Finance, Luxe & Retail, Assurance, Santé.

TECHNO

Ancrée à l'ANSSI

Brevets européens & soutien du gouvernement

CITALID

Trusted by 100+ Enterprises Across the Globe

GENERALI

Allianz

FRESENIUS

FRANCE ASSUREURS

Lagardère

ALSTOM

Recognized by

Gartner

FORRESTER®

Innovation Championship by ZURICH

INSURTECH HUB MUNICH

SOLUTION

La plateforme de CRQ #1 pour la chaine de valeur du risque

Un partenaire de confiance pour les assurés, courtiers, assureurs et réassureurs.

Citalid Core

Permettre aux experts de la cybersécurité et à leur direction de prendre les bonnes décisions en matière de risques cyber, renforçant à la fois leur posture en cybersécurité et leur solidité financière.

Citalid Engine

Le moteur CRQ le plus transparent, alliant nativement données de Cyber Threat Intelligence et cyber-économie pour une vision réelle du risque cyber.

Citalid Portfolio

Offrir aux gestionnaires de portefeuilles – tels que les courtiers, (ré)assureurs, banquiers et MSSP – des insights exploitables sur l'exposition aux risques de leurs clients et prospects, ouvrant ainsi de nouvelles opportunités commerciales.

Risk quantification is *not just* about *math.*

It is about helping your organization make the right *business decisions*.

Graeme Keith

(Københavns Universitet - University of Copenhagen)

POURQUOI

Quand le *COMEX* s'en mêle, le qualitatif n'est plus une option

Comment justifier une **décision d'investissement** et calculer un **ROI** avec des échelles **arbitraires** ?

	Fréquence	Impact
Rançongiciel	Élevée - 4/5	Faible - 2/5
Fuite de données	Moyenne - 3/5	Moyen - 3/5
Espionnage	Faible - 2/5	Élevé - 4/5
Sabotage	Très faible - 1/5	Très élevé - 5/5

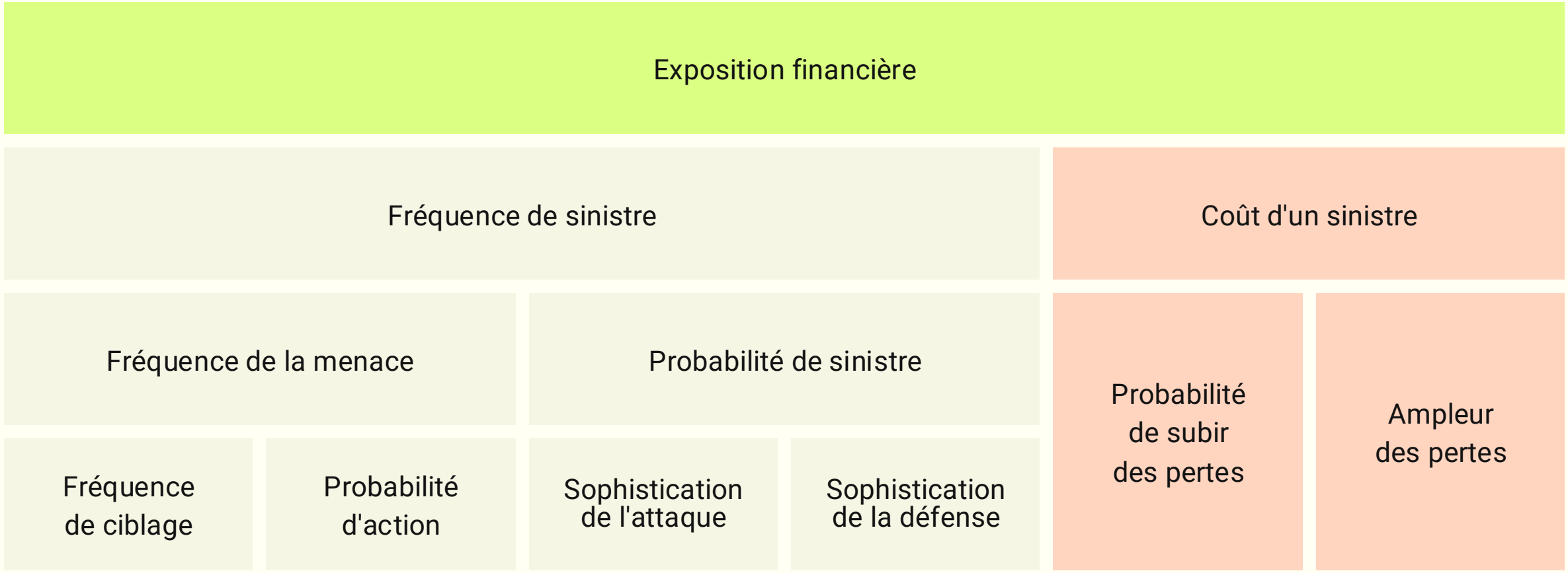
Combien cela risque-t-il de me **coûter** ? Avec quelle **probabilité** ?

De combien réduit-on notre exposition si nous **investissons** dans cette solution ?

SOLUTION

Méthodologie *openFAIR* : Factor Analysis of Information Risk

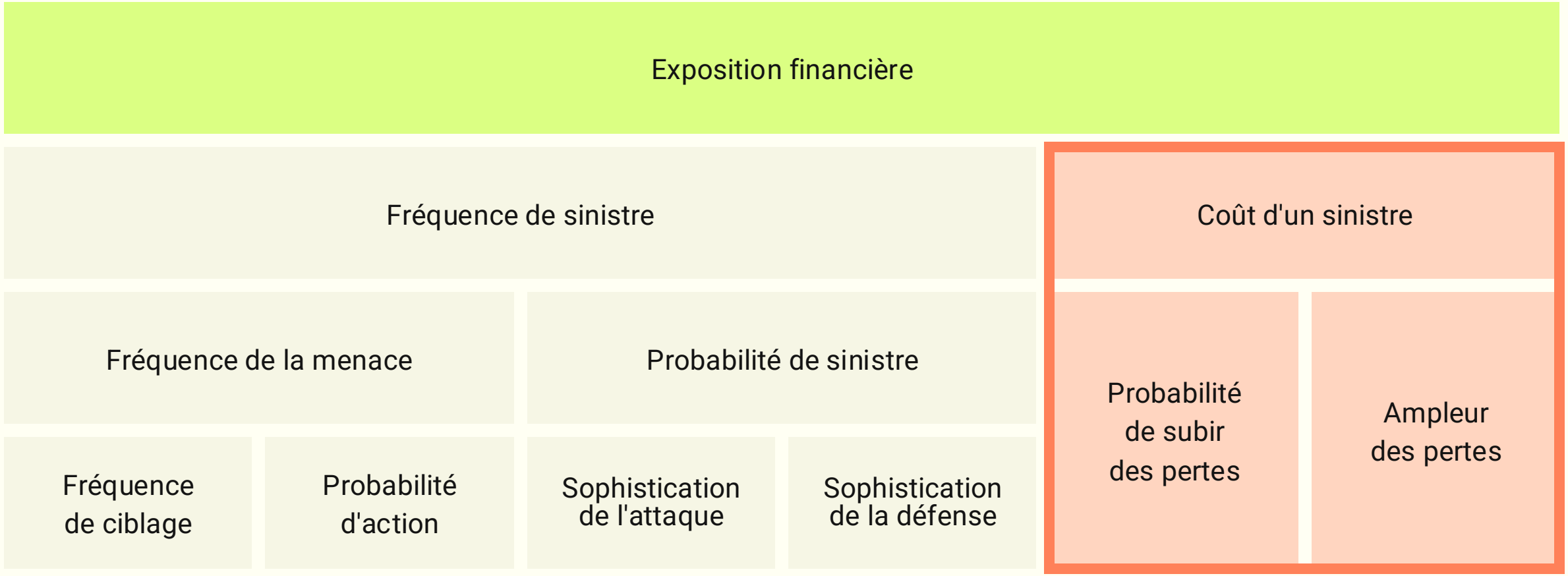
18 ans d'existance, standard de fait



SOLUTION

Quid de *l'amplitude* du sinistre?

Méthodologie **FAIR** : Factor Analysis of Information Risk

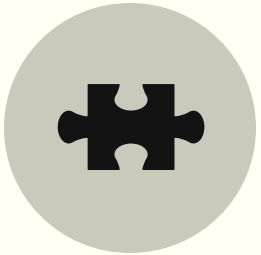


PROBLEME

Les données sur le risque cyber manquent cruellement.

Nouveauté

Trop peu de données **historiques**

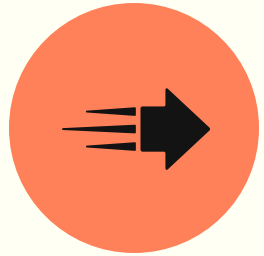


Complexité

Compréhension et modélisation difficiles

Sensibilité

Frein au **partage** des données



Dynamisme

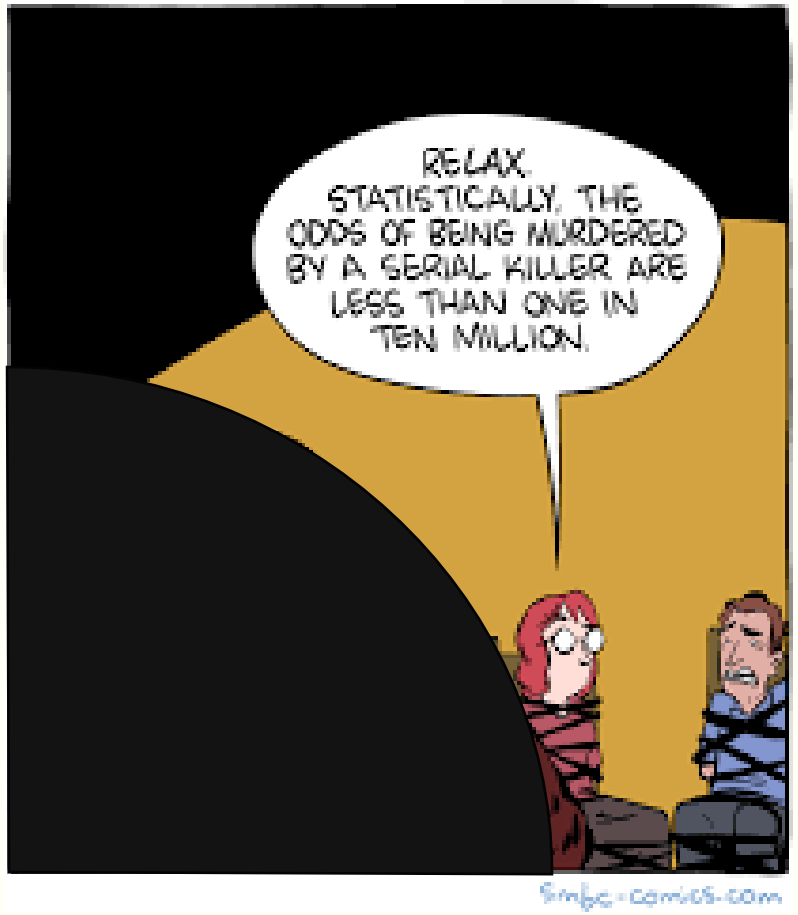
Durée de pertinence des données trop courte

SOLUTION

Une approche bayésienne

Probabilité conditionnée à des données de contexte :

La probabilité d'être assassiné par un serial killer est inférieure à 1 sur 10 millions



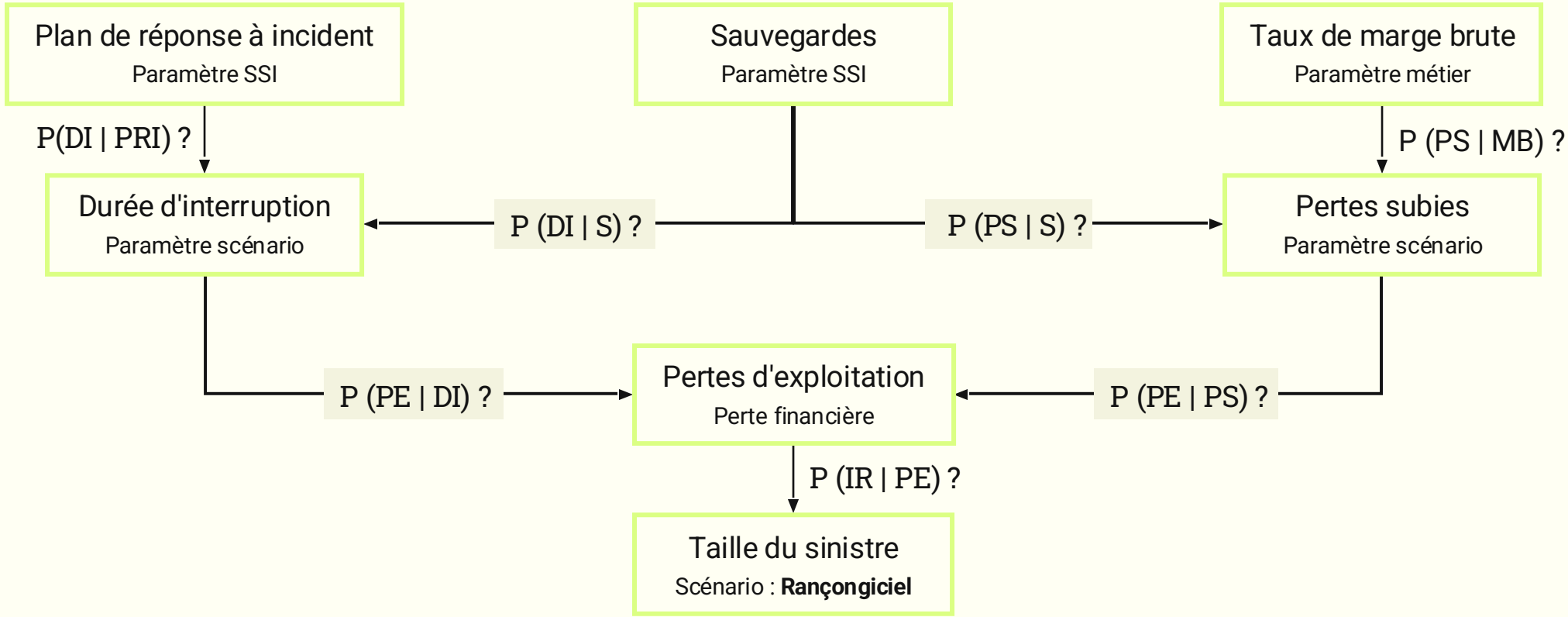
SOLUTION

Qu'est-ce qu'une approche bayésienne ?

Création du modèle a priori	Calibration du modèle	Mise à jour du modèle
Avec des experts du domaine	Avec les données initialement à disposition	Dès que de nouvelles données sont disponibles

SOLUTION

Un exemple simplifié et non-exhaustif de modèle “a priori”



SOLUTION

Articuler les intelligences humaine et logicielle

Modèle de croyance a priori

Calibration par les données

Expertise Citalid

Templates

Expertise client

Interviews

Données Citalid

Base de données

Données client

Hétérogènes

OSINT

SSI

Métier

CTI

Finance

Contexte

SOLUTION

Avantages de cette approche

Les meilleures anticipations s’adaptent en trouvant l'équilibre optimal entre sous- et sur-réaction aux nouvelles données.

Fonctionne avec peu de données

S'améliore à mesure que les données affluent

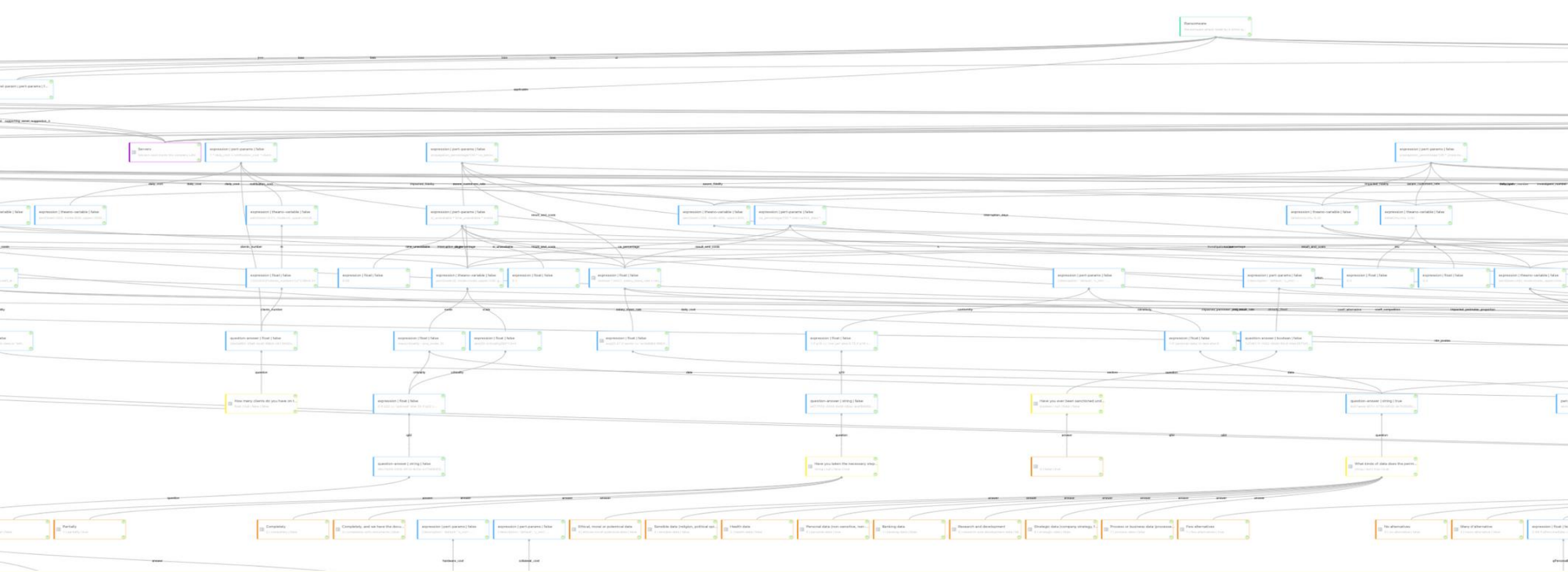
Évolue à mesure que les données changent

Cf. **Good Judgment Project**, **Philip Tetlock** :

*“Superforecasters aren’t perfect **Bayesian** predictors, but they are much better than most of us.”*

SOLUTION

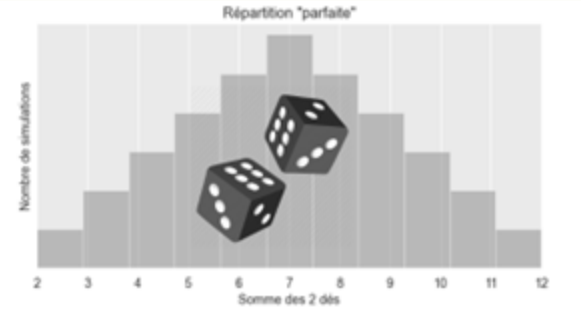
Nos templates de scénarios ressemblent plutôt à ça !

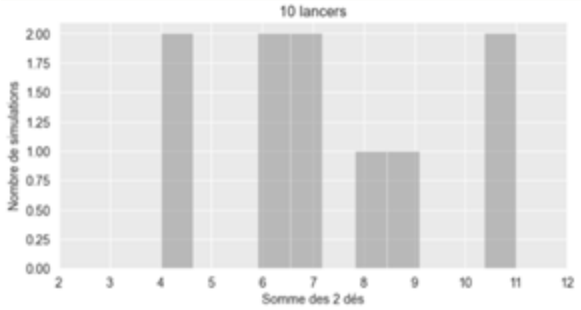


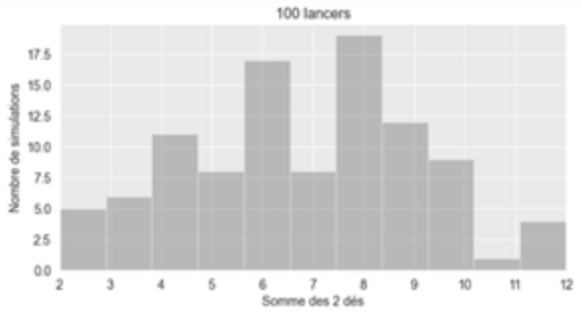
SOLUTION

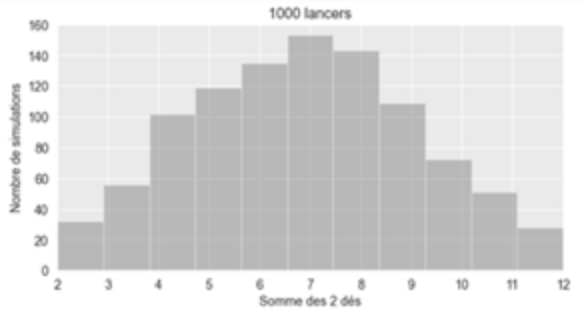
Comment résoudre un problème aussi complexe ?

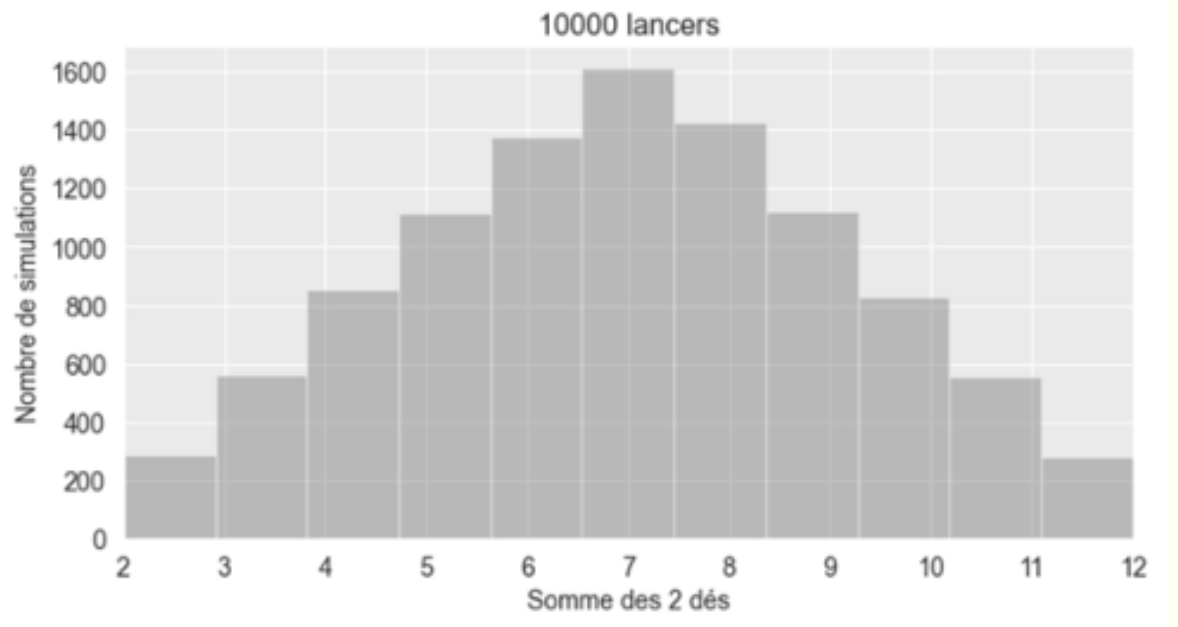
Simulations de *Monte-Carlo*











SOLUTION

Le résultat est une *distribution de probabilité*

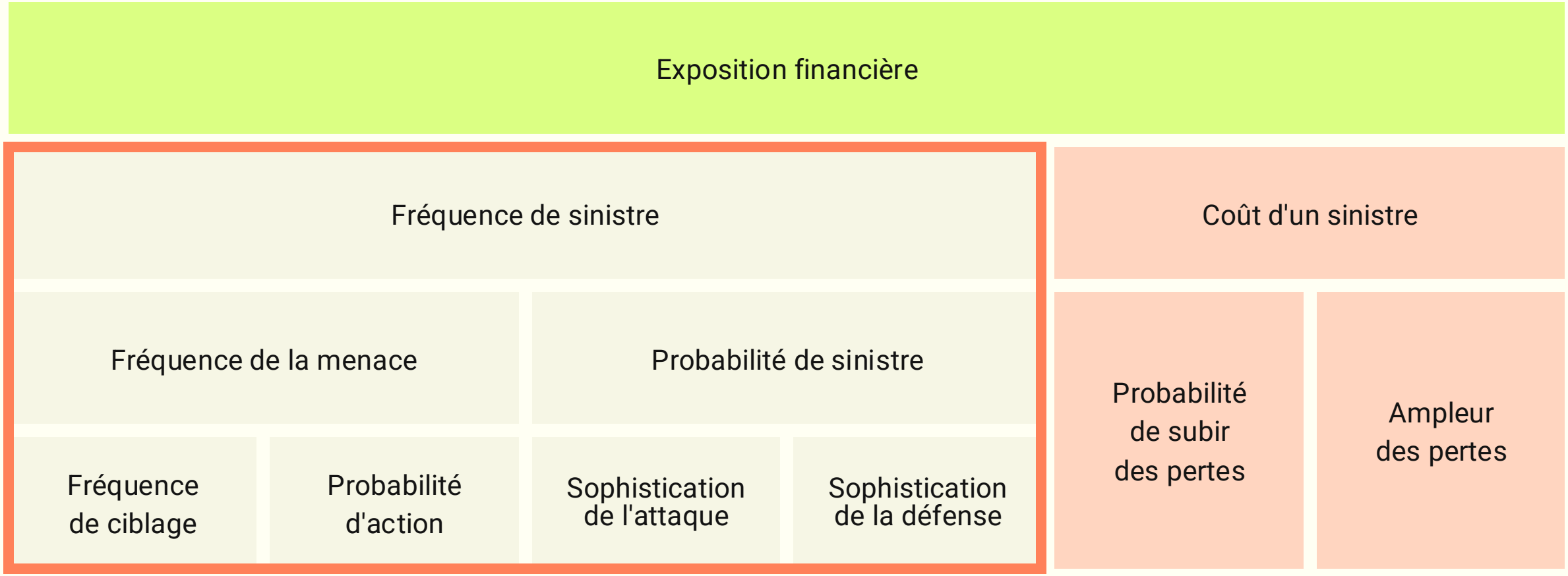
L'incertitude est **inhérente** au risque cyber, il faut la **restituer aux décideurs.**

	Minimum	Plus probable	Maximum	Confiance	Probabilité
Interruption de productivité	210000	4100000	12500000	Moyenne	1
Perte de clientèle	7000	150000	2000000	Faible	1
Coûts des actions correctives	66000	90000	110000	Élevée	100%
Coûts d'investigation	0	45000	160000	Élevée	1
Notifications légales	5000	7000	25000	Moyenne	100%
Gestion de crise	1000	7000	25000	Moyenne	100%

SOLUTION

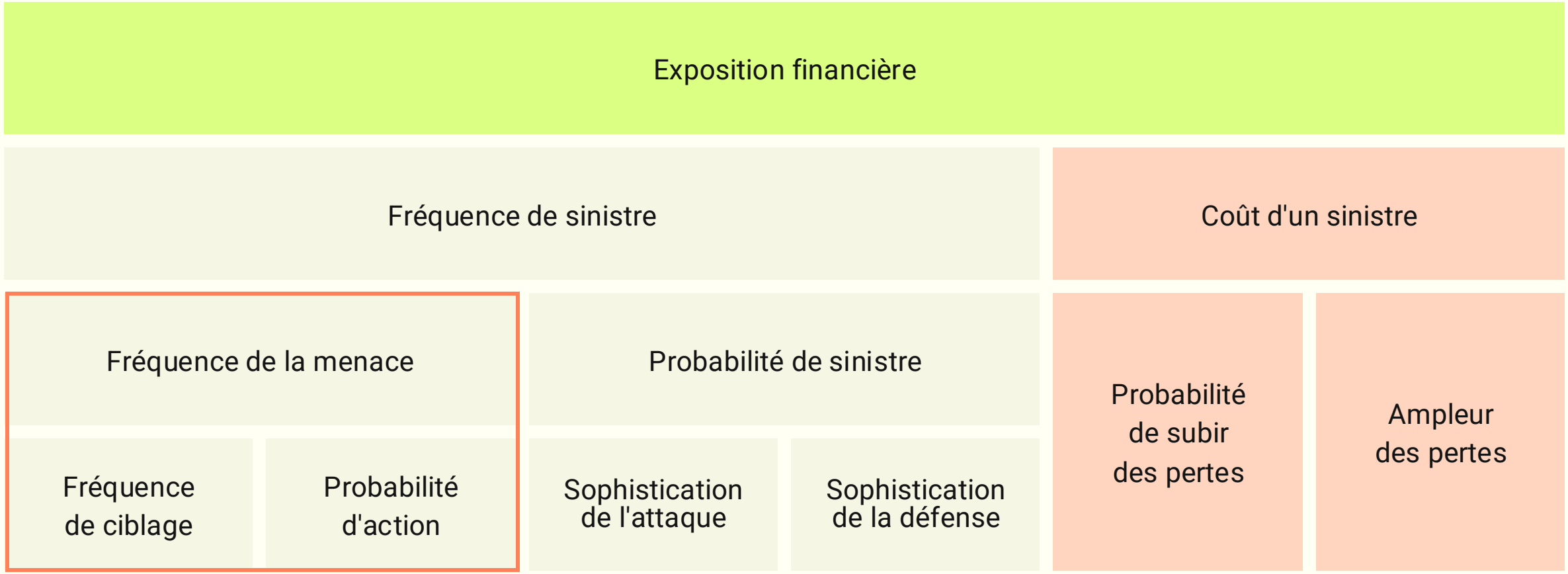
Quid de la *fréquence* de sinistre?

Méthodologie **FAIR** : Factor Analysis of Information Risk



SOLUTION

Etape 1 : évaluer la probabilité de sinistre



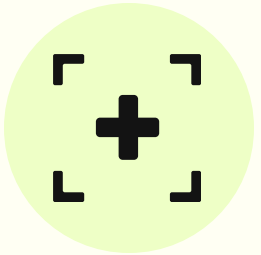
De l'importance de la Cyber Threat Intelligence

Typologie de menace

- Crime organisé
- Criminel

Exemple d'acteurs

- Maze
- Sodinokibi
- Ryuk
- Phobos



Motivations

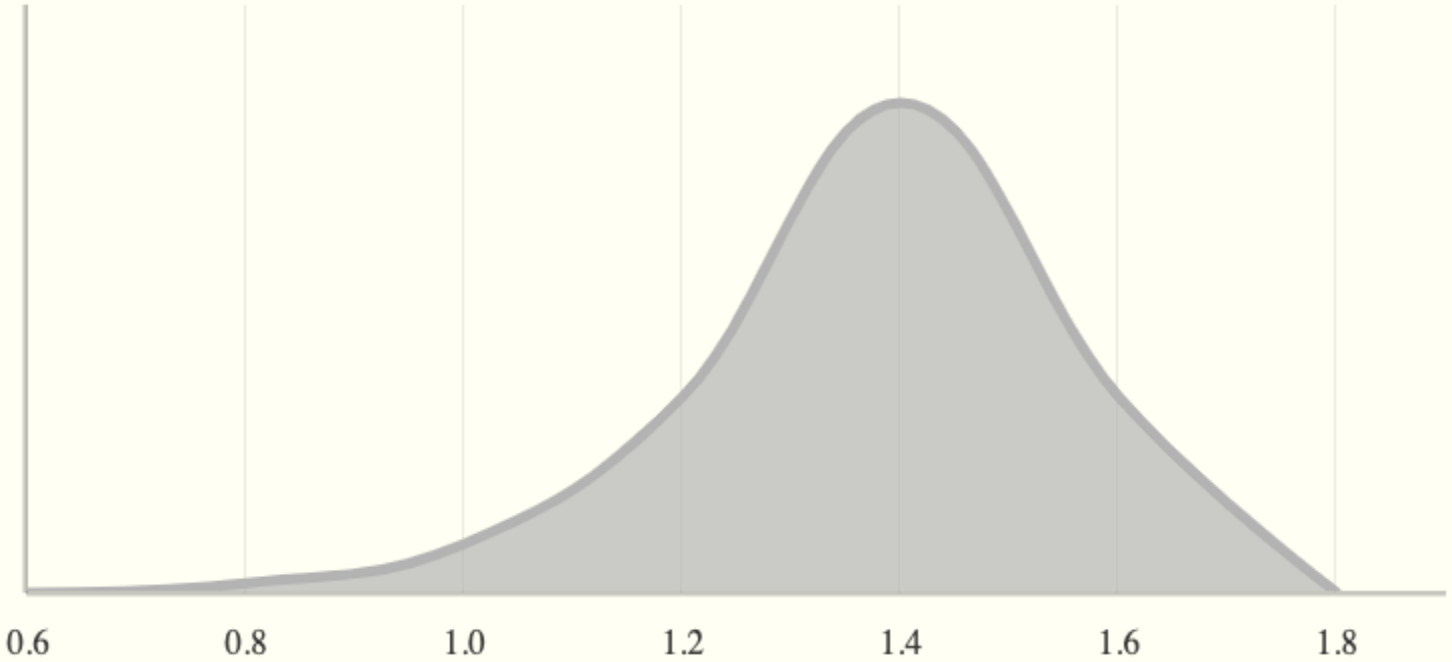
- Argent

Actifs ciblés

- Tous les fichiers hébergés sur le SI

Définissez votre “*modèle expert*” et ses paramètres

Faites *évoluer votre modèle* avec les données à disposition

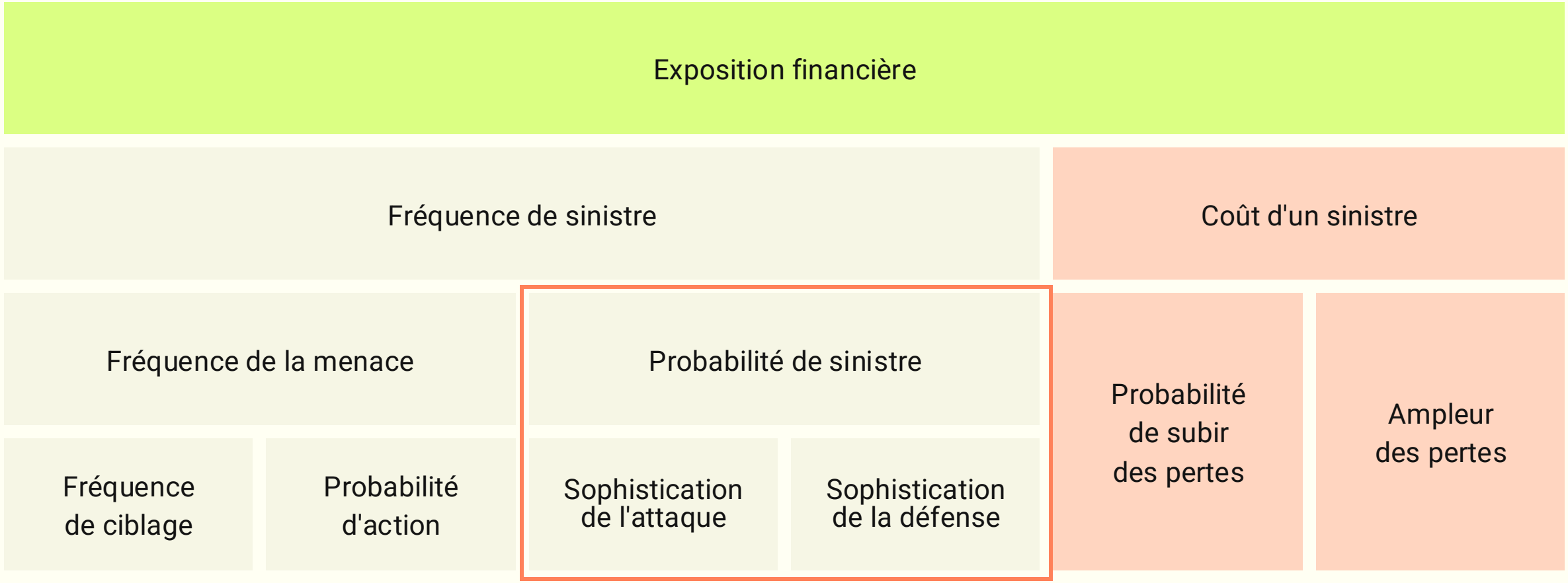


Fréquence de ciblage annuelle

Ex : https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-001

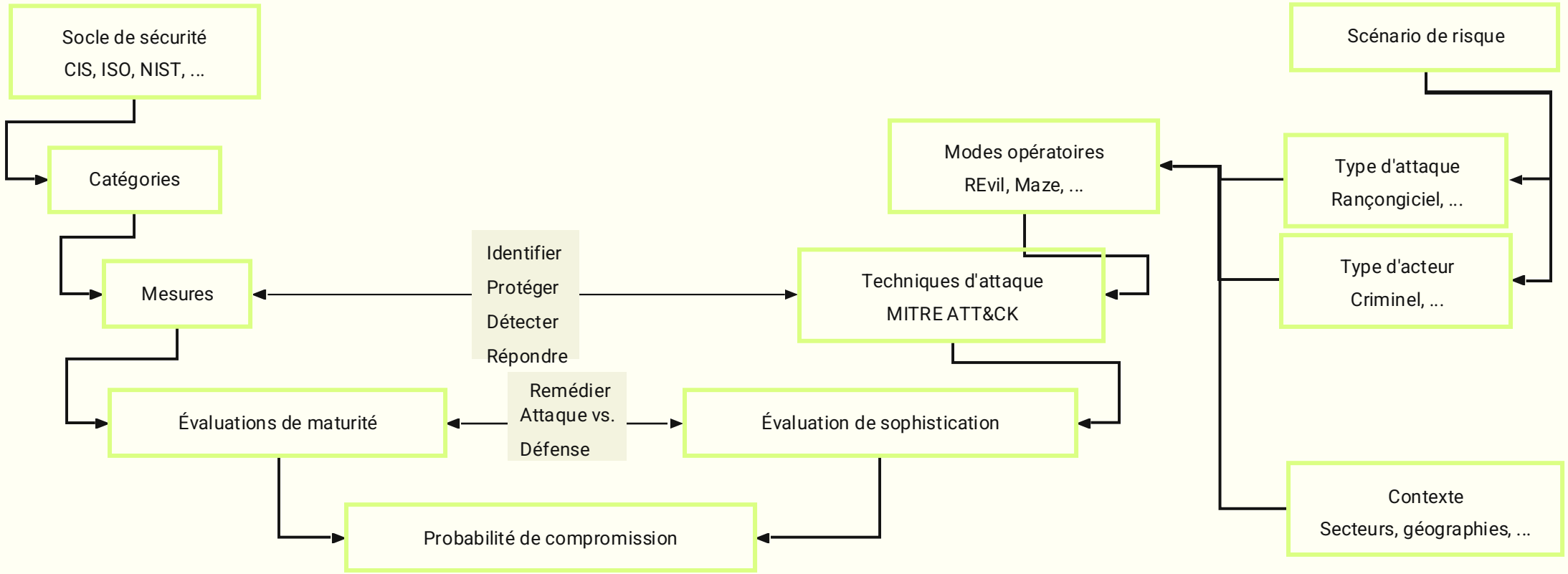
SOLUTION

Etape 2 : évaluer la probabilité de sinistre



SOLUTION

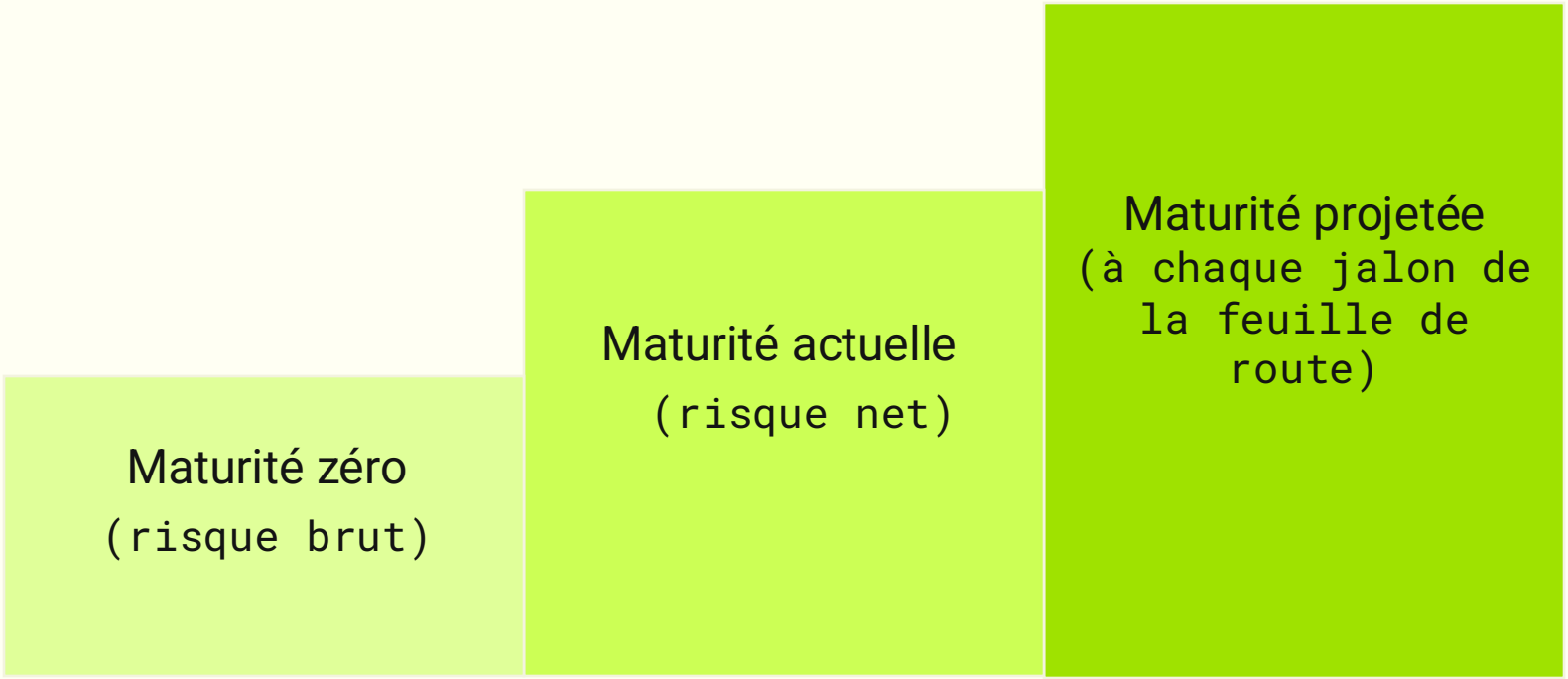
Un moteur de simution de “pentest théorique” unique au monde (brevet déposé)



SOLUTION

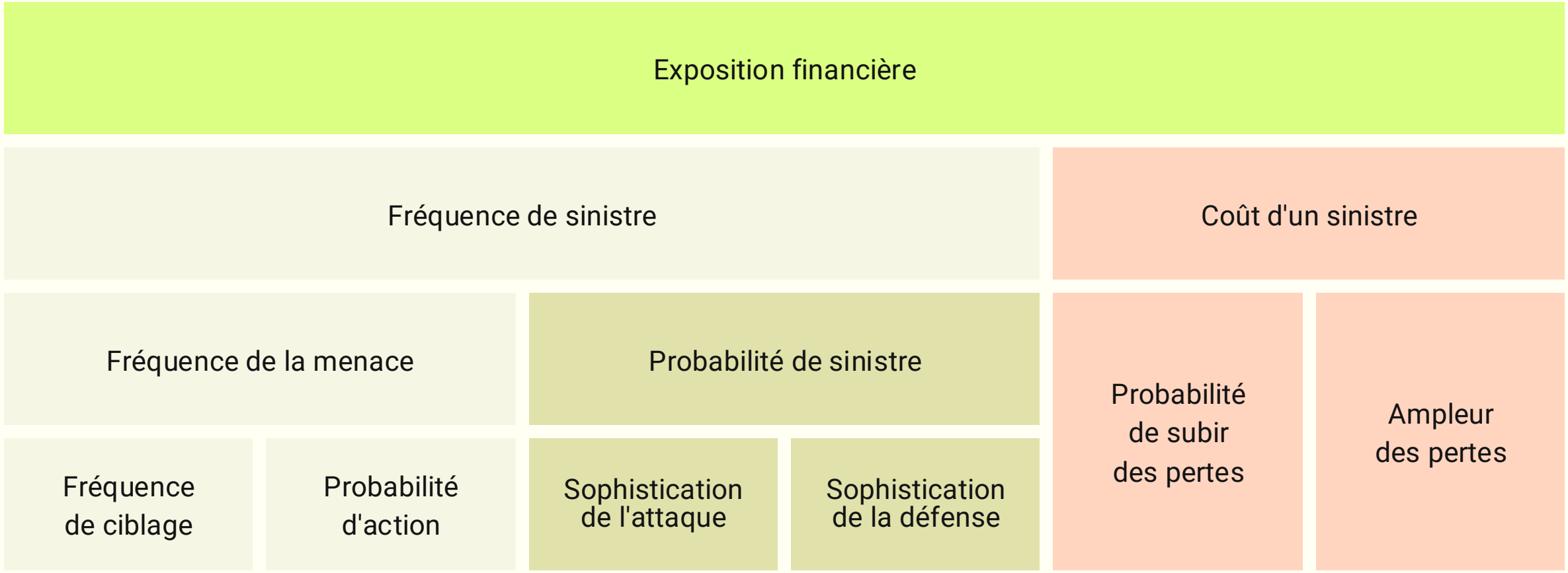
Confronter *plusieurs niveaux de maturité défensive* à un seul scénario

La mise en correspondance entre les **scénarios** et les **mesures défensives** peut être effectuée et **dynamiquement** mise à jour grâce aux **données sur les menaces**



SOLUTION

Il ne reste plus qu'à anticiper et agir



DASHBOARD

Exemple de tableau de bord du risque rançongiciel

Valeurs nettes calculées sur une base annuelle en utilisant le profil de défense actuel

Fréquence moyenne des ciblages/ tentatives d'attaques par an

1.47

Chances de succès de l'attaquant

62%

Pertes financières moyennes subies lorsque l'attaque réussit

€4.3M

Exposition annuelle moyenne sur la base de la fréquence et de l'impact

€3.9M

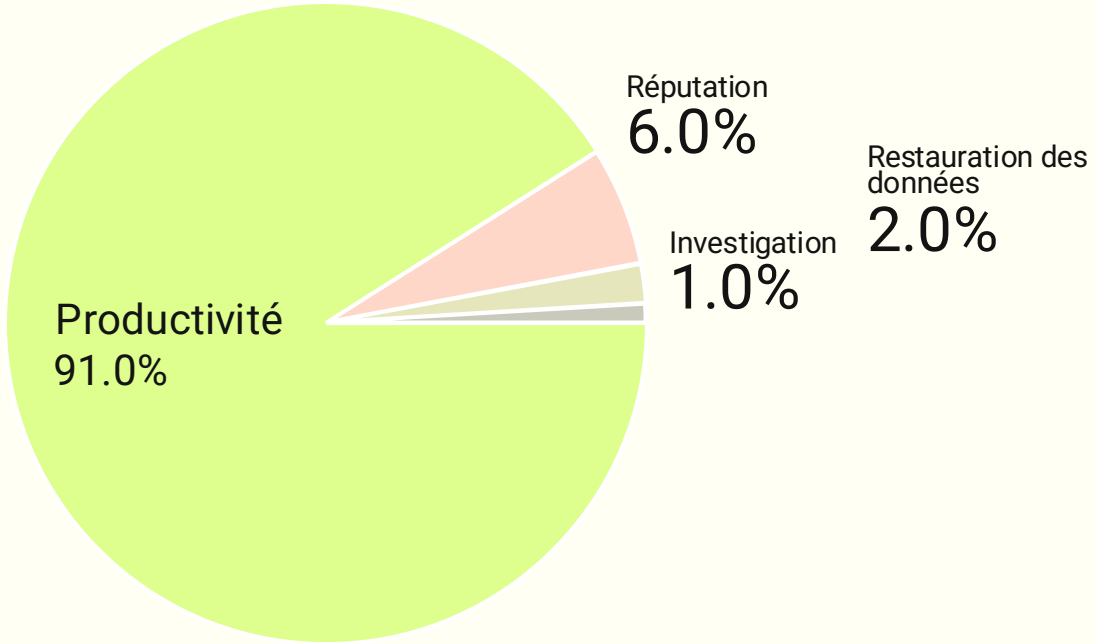
Pertes financières maximales subies lors de la pire année simulée

€46.2M

ASSURANCE

Répartition des pertes à couvrir par *l'assurance*

Répartition moyenne de **toutes les pertes** subies pour chaque **incident**

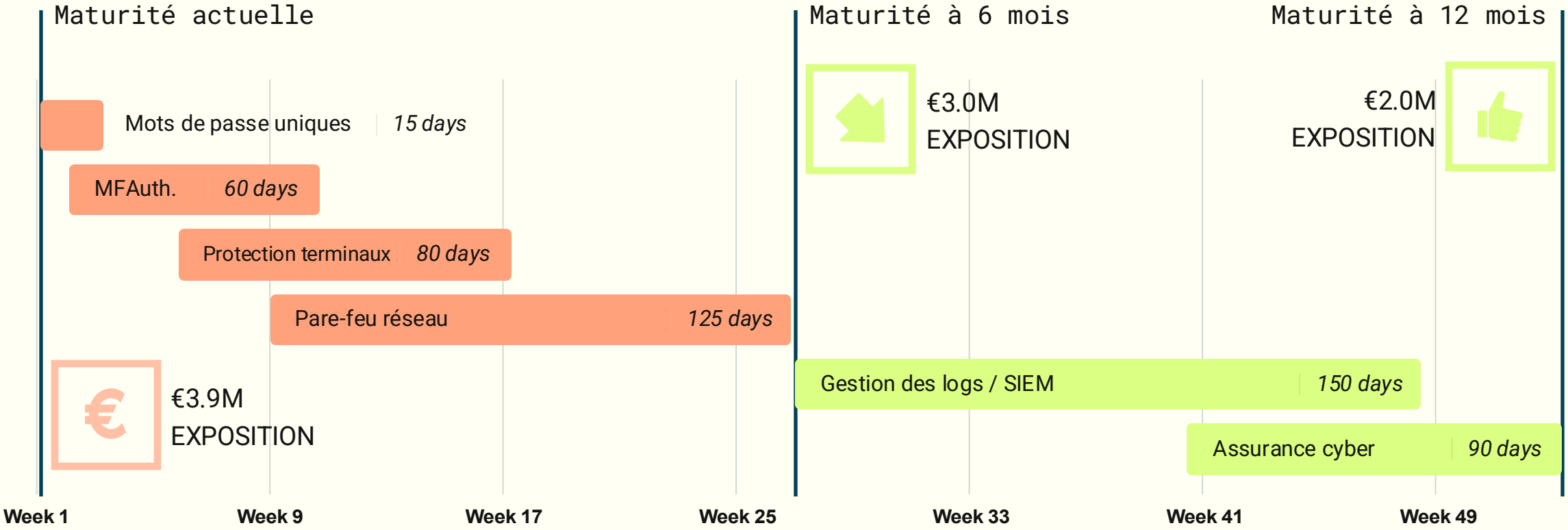


Vous pouvez déterminer la **pertinence** de votre **police d'assurance** en simulant son **impact / niveau de couverture** sur le risque de votre organisation

ROADMAP

Concevez votre feuille de route en *optimisant vos investissements*

Simulez la **réduction de votre exposition** associée aux recommandations **générées**



TAKEWAY

Seule la *quantification du risque* cyber permet un pilotage *proactif* et optimal des investissements de *sécurité* et d'*assurance.*

CONCLUSION

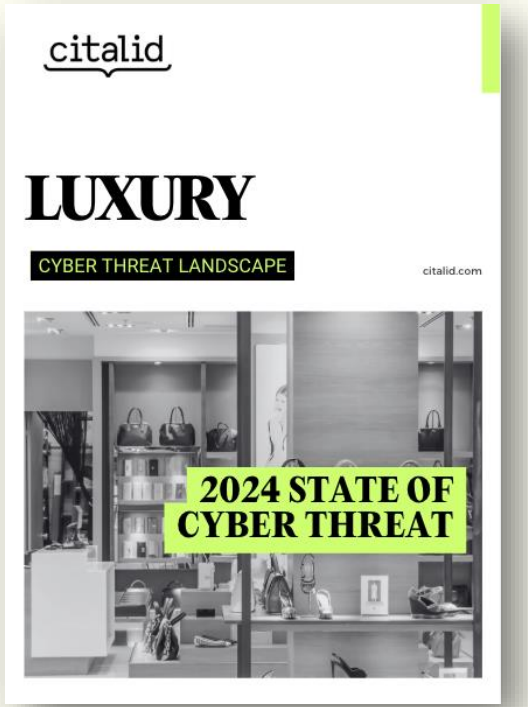
CRQ : des bénéfices multiples

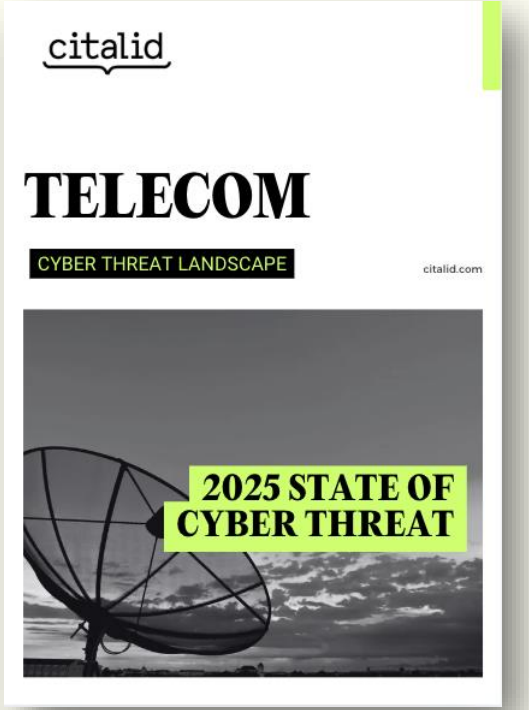
1	Alignement Stratégique	Gouvernance & Prise de décision stratégique
2	Optimisation Budgétaire	Priorisation des investissements de sécurité
3	Efficacité	Réduction du temps passé à justifier des décisions cyber
4	Risque partagé	Résilience cyber renforcée
5	Communication Impactante	Discussions facilitées avec les parties prenantes

CONTENU

Gardez un coup d'avance sur la menace

Accédez à notre hub de ressources CTI

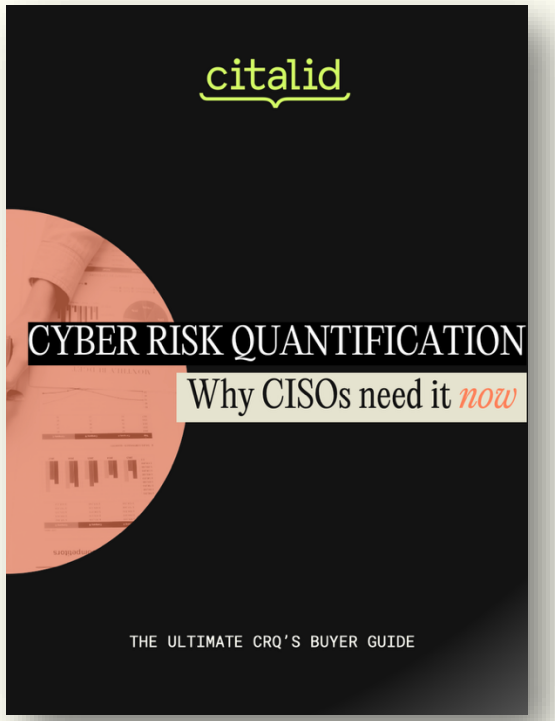


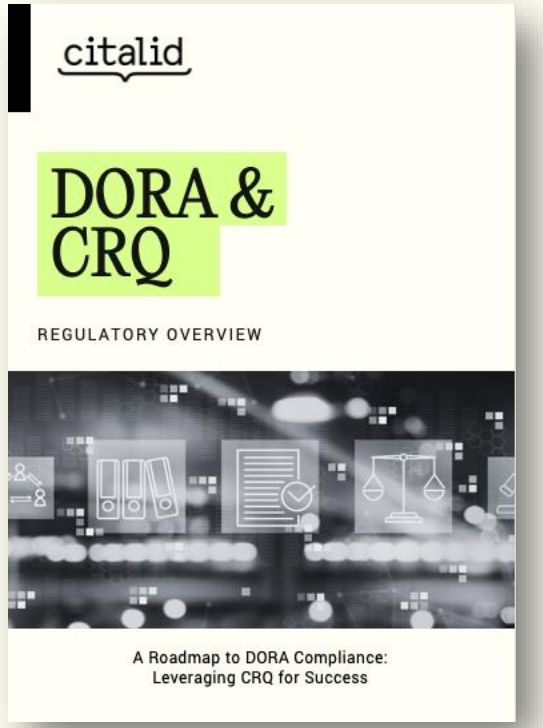


CONTENU

Contenus Risque cyber, Assurance, Conformité...

Recevez notre newsletter





Merci

Julien Chamonal
Chief Revenue Officer

julien@citalid.com