Utilisation de connaissances de cybersécurité pour une meilleure quantification en cyber assurance.

Nicolas Rosal

Institut
4, rue Chauveau-L
www.institutdesact

Sommaire

EXIOM

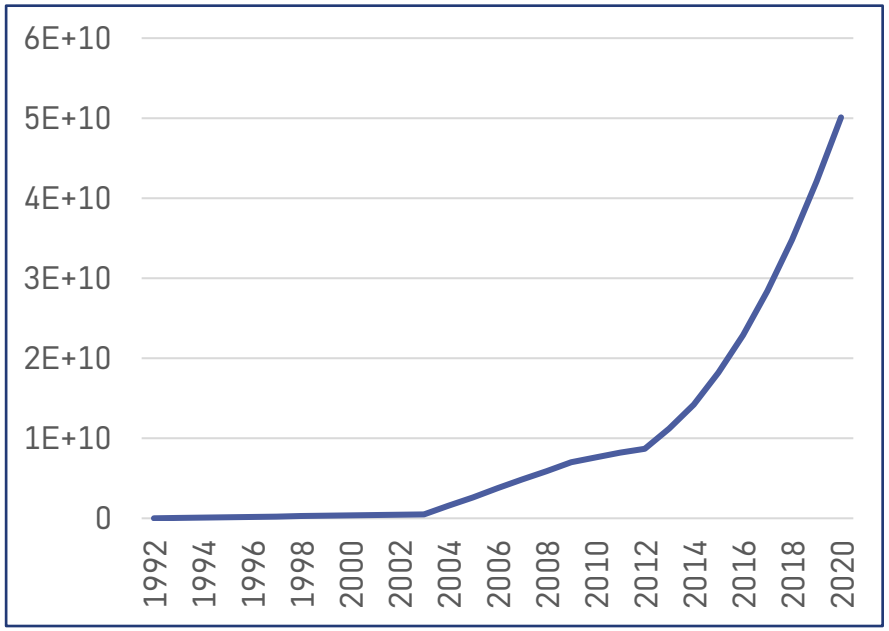
1 Contexte & Objectifs

EXIOM

CONTEXTE – LE RISQUE CYBER, UN RISQUE CROISSANT

Un premier parallèle.

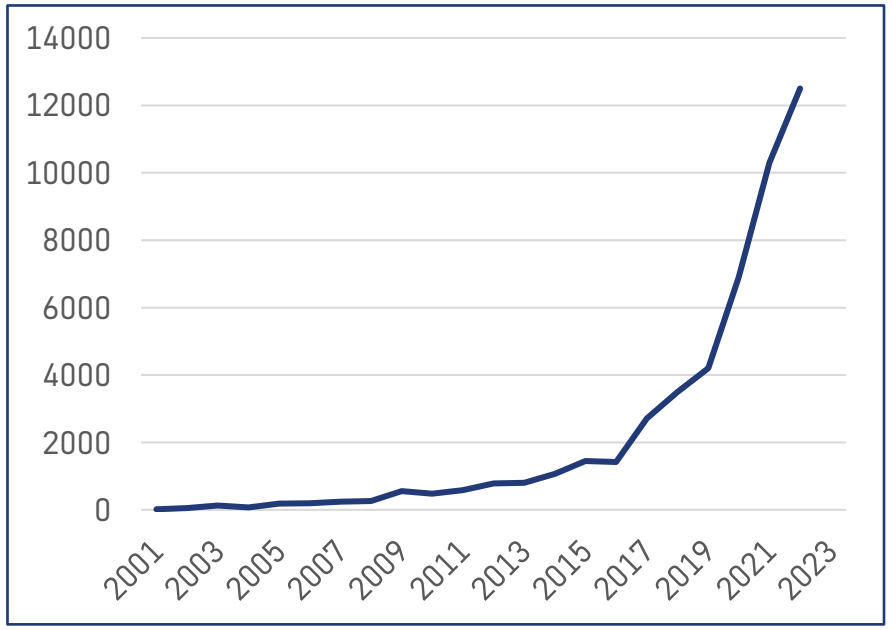
Nombre d'appareils connectés dans le monde



Plus de surface d'attaque

Plus de menace

Dommages rapportés à l'IC3 causés par le cybercrime aux Etats-Unis (en M$)



CONTEXTE – LE RISQUE CYBER, UN RISQUE CROISSANT

Le risque cyber : de quoi parle-t-on?

Le risque cyber est défini comme étant *risque opérationnel portant sur la **confidentialité**, l'**intégrité** ou la **disponibilité** des données et systèmes d'informations.*

La **confidentialité** désigne la protection des données contre tout accès non autorisé pour garantir leur caractère privé.

L'**intégrité** désigne la garantie que les données sont exactes, complètes et non modifiées de manière non autorisée.

La **disponibilité** désigne le fait que les données et les systèmes restent accessibles aux utilisateurs autorisés lorsqu'ils en ont besoin.

Un risque qui inquiète

1e Risque selon France Assureur depuis 2017.

Un impact global

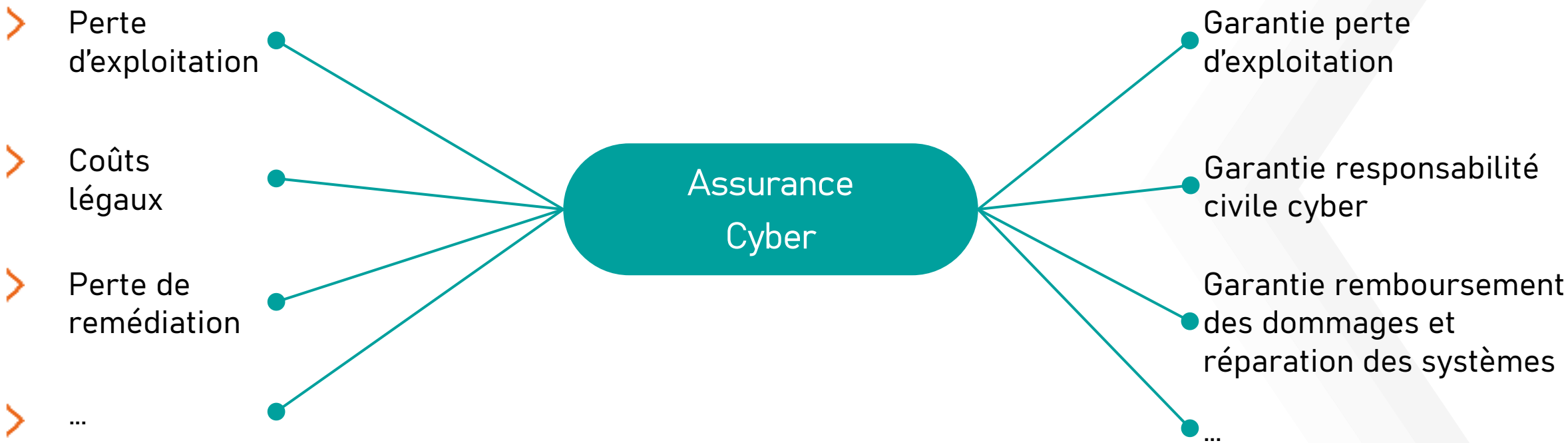
45% Des entreprises sondées par le Césin ont subi au moins une cyberattaque en 2022.

Une Diversité de coûts

+ 6 Types de coûts différents dont les coûts financiers, les coûts opérationnels, ...

CONTEXTE – L'ASSURANCE CYBER, UNE SOLUTION EN DÉVELOPPEMENT

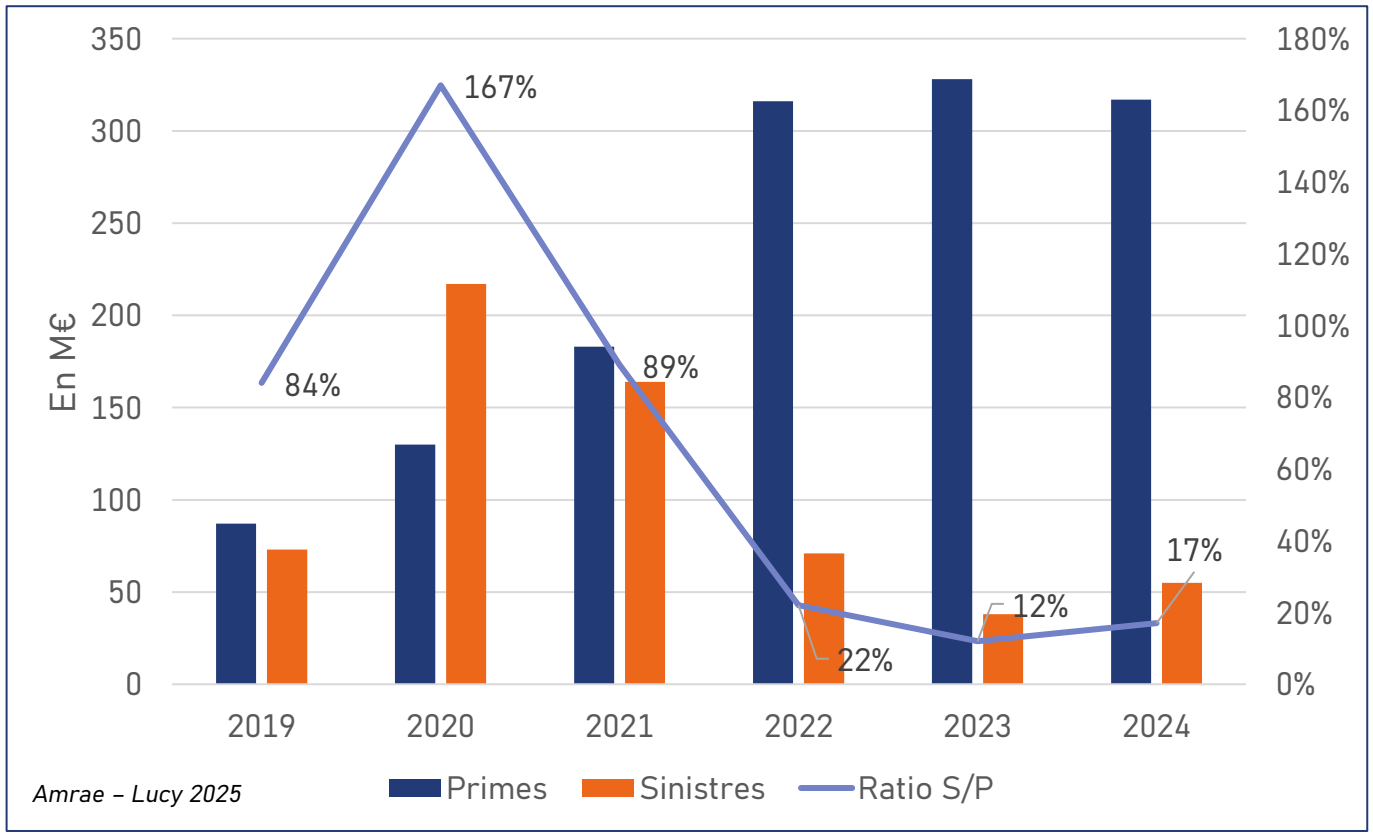
L'assurance cyber, une protection étendue aux différents coûts.



CONTEXTE – L'ASSURANCE CYBER, UNE SOLUTION EN DÉVELOPPEMENT

Evolution du marché français de la cyber-assurance

Un marché en croissance mais toujours instable



Amrae – Lucy 2025

- Une croissance annuelle du volume des primes **(+277% en 4 ans).**
- Une diminution des montants de sinistre depuis 2020 en partie du fait du hardmarket.
- Un S/P très instable.

CONTEXTE – L'ASSURANCE CYBER, DES DÉFIS STRUCTURANTS.

Un marché jeune et en développement qui fait face à des défis structurants.

Trois grandes problématiques de l'assurance cyber

1 UNE PÉNURIE DE DONNÉES DE SINISTRES DE QUALITÉ

- Faible maturité des assureurs.
- Réticence à partager des données.
- Entraine une modélisation complexe.

- Trouver **d'autres sources de données**.

2 UNE ÉVOLUTIVITÉ DU RISQUE

- Un risque fortement dépendant de facteurs évoluant dans le temps.

UN CARACTÈRE SYSTÉMIQUE DU RISQUE

- Une fréquence difficile à appréhender (systémique).

- Nécessité d'une quantification **dynamique** et **plus explicative** du risque.

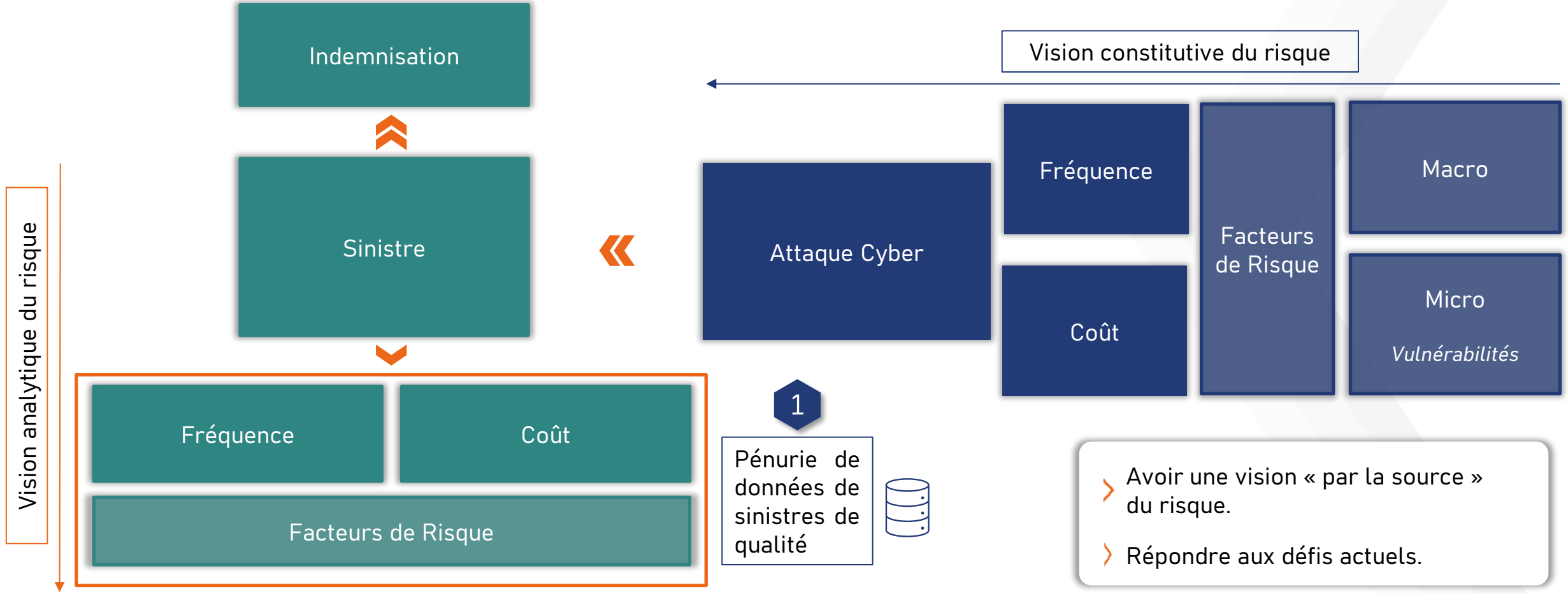
3 UNE FAIBLE PÉNÉTRATION DU MARCHÉ DES PME

- Marché encore concentré sur les grandes structures.
- Secteur des PME encore très vulnérable.

- **Proposer des services adaptés** aux PME pour **augmenter l'attractivité** et **diminuer le risque** de ces structures.

Contexte – Surmonter les difficultés techniques.

Un marché jeune et en développement qui fait face à des défis structurants.



CONTEXTE – LA CYBERSÉCURITÉ, UN PUIT DE CONNAISSANCES.

Que peut apporter la cybersécurité pour l'assurance cyber ?

Des connaissances sur les failles techniques

- **Bases de données recensant les vulnérabilités (CVE, KEV,…).**
- Conseils sur la mitigation de la faille.

Des connaissances sur la menace

- *« Cyber Threat Intelligence ».*
- ***Méthodologies d'attaque*** *(Matrice Att&ck).*

Des méthodes pour quantifier l'exploitabilité

- Différentes **métriques** permettant de juger de la dangerosité d'une faille : CVSS, EPSS.

Une connaissance en général plus **« constitutionnelle »** du risque, à une échelle **micro**.

Objectifs – La Problématique.

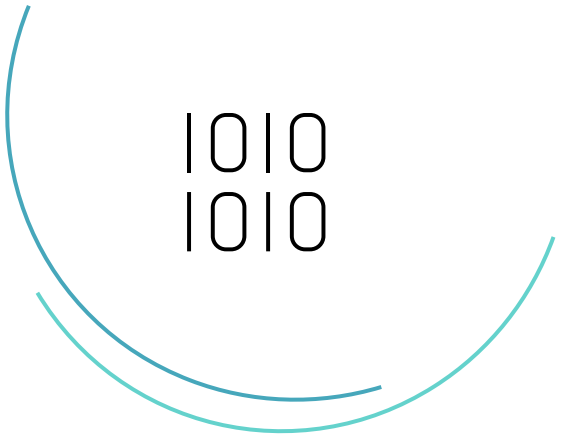
Comment combiner cybersécurité et cyber assurance?

Des enjeux

Objectifs – La Problématique.

Comment combiner cybersécurité et cyber assurance?

Des enjeux

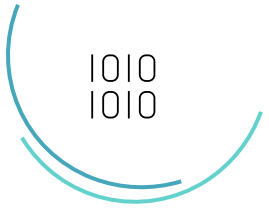


Des connaissances exploitables

Objectifs – La Problématique.

Comment combiner cybersécurité et cyber assurance?

Des enjeux



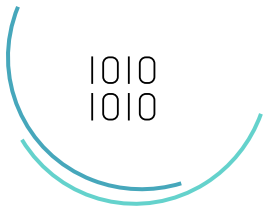
Des connaissances exploitables

Comment utiliser les **connaissances de cybersécurité** pour une **quantification dynamique** du risque cyber en assurance ?

Objectifs – La Problématique.

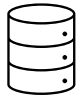
Comment combiner cybersécurité et cyber assurance?

Des enjeux



Des connaissances exploitables

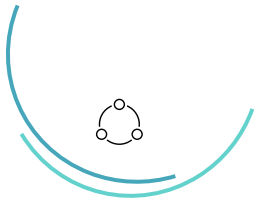
Comment utiliser les **connaissances de cybersécurité** pour une **quantification dynamique** du risque cyber en assurance ?



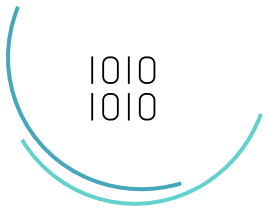
Qui pourra utiliser d'autres types de **données explicatives du risque**.

Objectifs – La Problématique.

Comment combiner cybersécurité et cyber assurance?



Des enjeux



Des connaissances exploitables

Comment utiliser les **connaissances de cybersécurité** pour une **quantification dynamique** du risque cyber en assurance ?

Qui pourra utiliser d'autres types de **données explicatives du risque**.

Qui pourra permettre de répondre à la problématique des PME **de besoin de prévention**.

2 Modèle de cyberassurance dynamique et graphique

Institut des ACTUAIRES EXIOM

Modèle – La Problématique.

Quelles questions se poser pour la modélisation?

Comment utiliser les **connaissances de cybersécurité** pour une **quantification dynamique** du risque cyber en assurance ?

Modèle – La Problématique.

Quelles questions se poser pour la modélisation?

Comment utiliser les **connaissances de cybersécurité** pour une **quantification dynamique** du risque cyber en assurance ?

connaissances de cybersécurité

- Trouver une modélisation pouvant être adaptée à l'échelle **micro** de la connaissance en cybersécurité.

Modèle – La Problématique.

Quelles questions se poser pour la modélisation?

Comment utiliser les **connaissances de cybersécurité** pour une **quantification dynamique** du risque cyber en assurance ?

connaissances de cybersécurité

- Trouver une modélisation pouvant être adaptée à l'échelle **micro** de la connaissance en cybersécurité.

quantification dynamique

- Trouver une modélisation **évoluant** avec le **risque actuelle** (en fonction des menaces) grâce à des **connaissances structurelles**.

Modèle – La Problématique.

Quelles questions se poser pour la modélisation?

Comment utiliser les **connaissances de cybersécurité** pour une **quantification dynamique** du risque cyber en assurance ?

- Utilisation du papier **Quantification of Cyber Risk for Actuaries An Economic-Functional Approach** – SOA - Unal Tatar, comme brique technique principale.
- Transformation des notions du papier pour l'appliquer avec une vision stochastique.

Modèle – Une vision cyber économique.

Comment le papier propose-t-il d'évaluer une perte cyber?

Ce framework propose **d'estimer le coût d'une attaque en deux temps** :

Modéliser l'attaque sur les actifs de l'entreprise

- Graphe Bayésien d'Attaque

Transposer le coût en terme « physique » et « informatique » en coût économique pour l'entreprise

- Graphe d'Impact

L'attention de la modélisation n'est alors plus portée sur la modélisation **d'un sinistre** mais bien celle **d'une attaque** ce qui permet d'utiliser des **connaissances de cybersécurité**.

Modèle – Une vision cyber économique

Modéliser l'attaque sur les actifs de l'entreprise

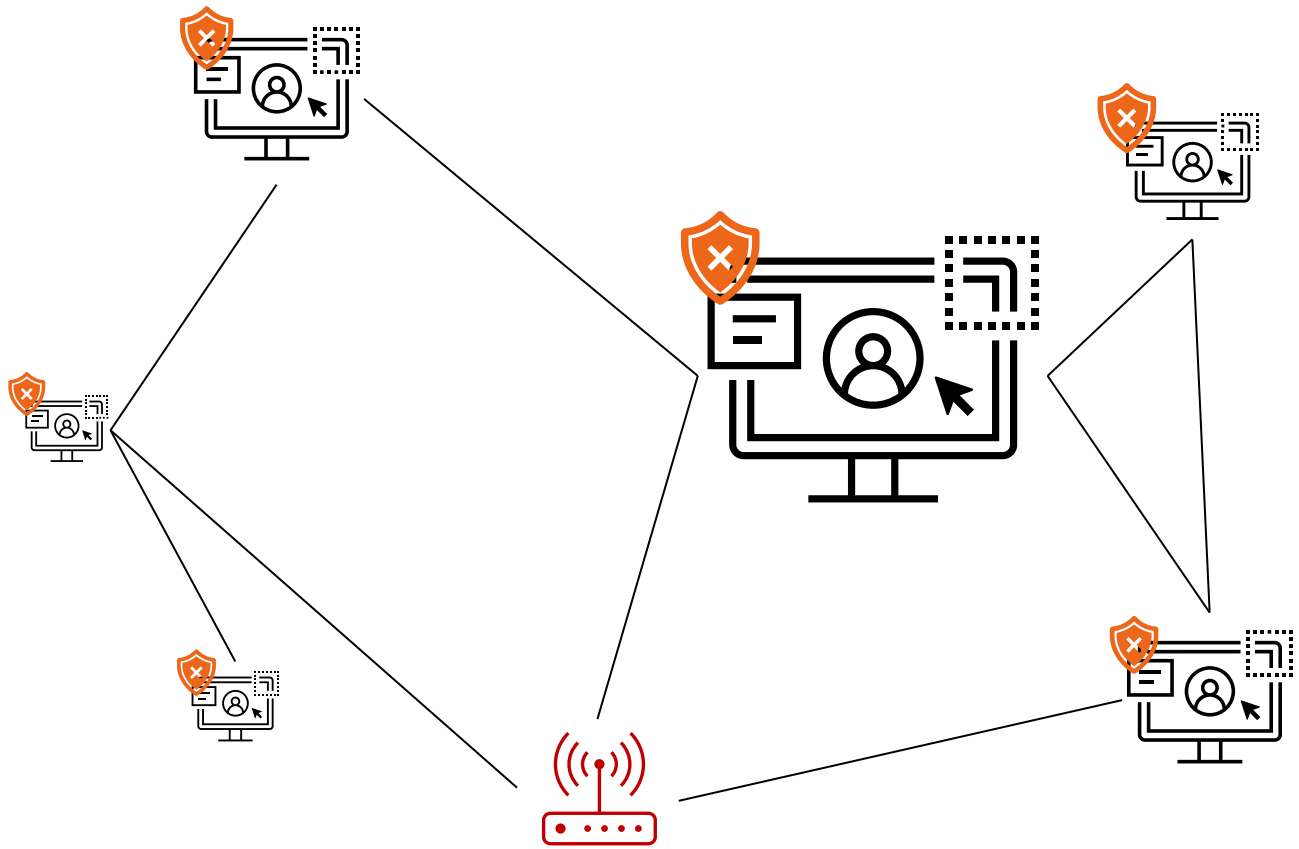
- Graphe Bayésien d'Attaque

Transposer le coût en terme « physique » et « informatique » en coût économique pour l'entreprise

- Graphe d'Impact

Modèle – Graphe Bayesien d'attaque, structurer la dépendance.

Modéliser l'attaque sur les actifs de l'entreprise

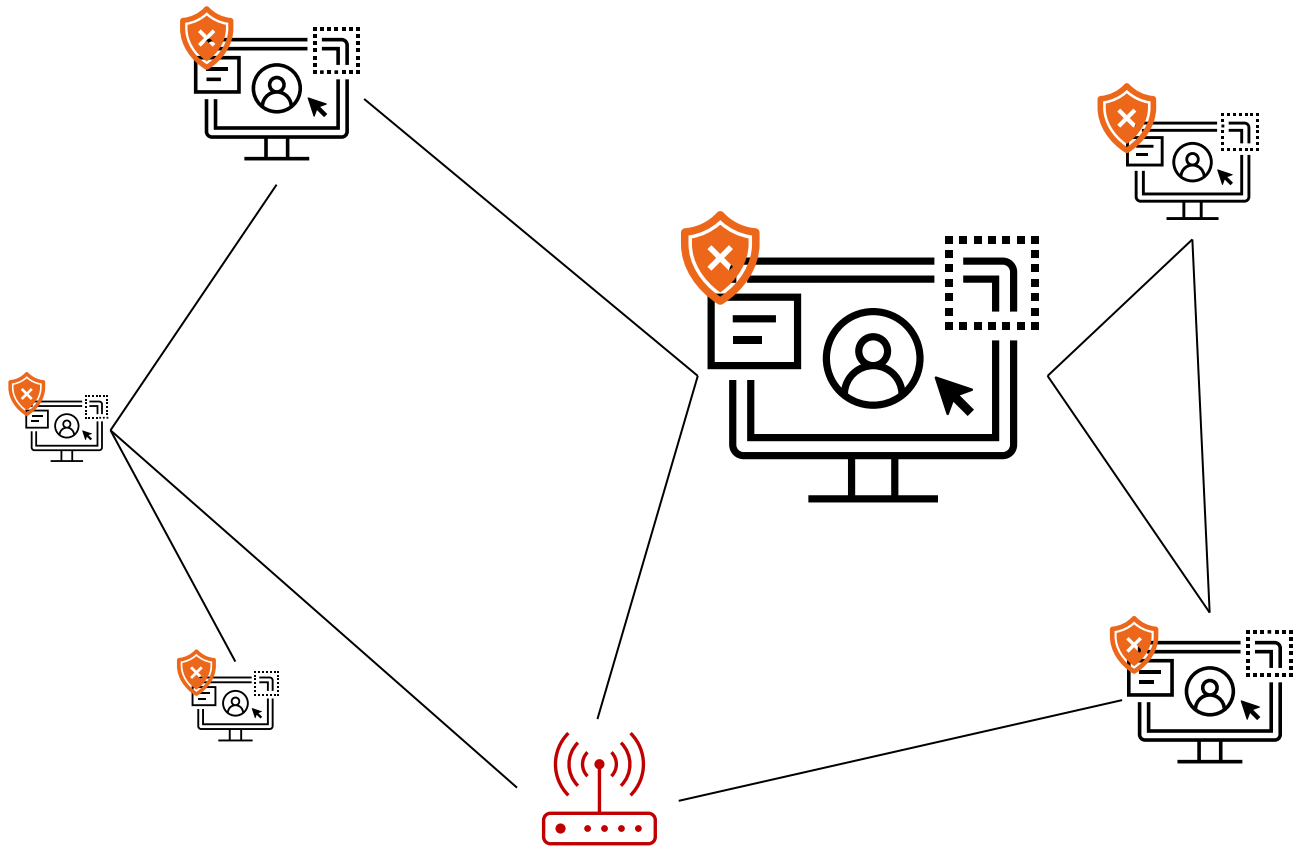


- Une entreprise est composée de plusieurs **actifs** (ordinateur, serveur, …).
- Chaque actif a des **vulnérabilités**.
- Les actifs de l'entreprise sont organisés en **réseau(x)**.
- **L'attaquant se déplacera sur le réseau** à partir d'un **point d'entré** en exploitant les vulnérabilités.

Institut des ACTUAIRES EXIOM

Modèle – Graphe Bayesien d'attaque, structurer la dépendance.

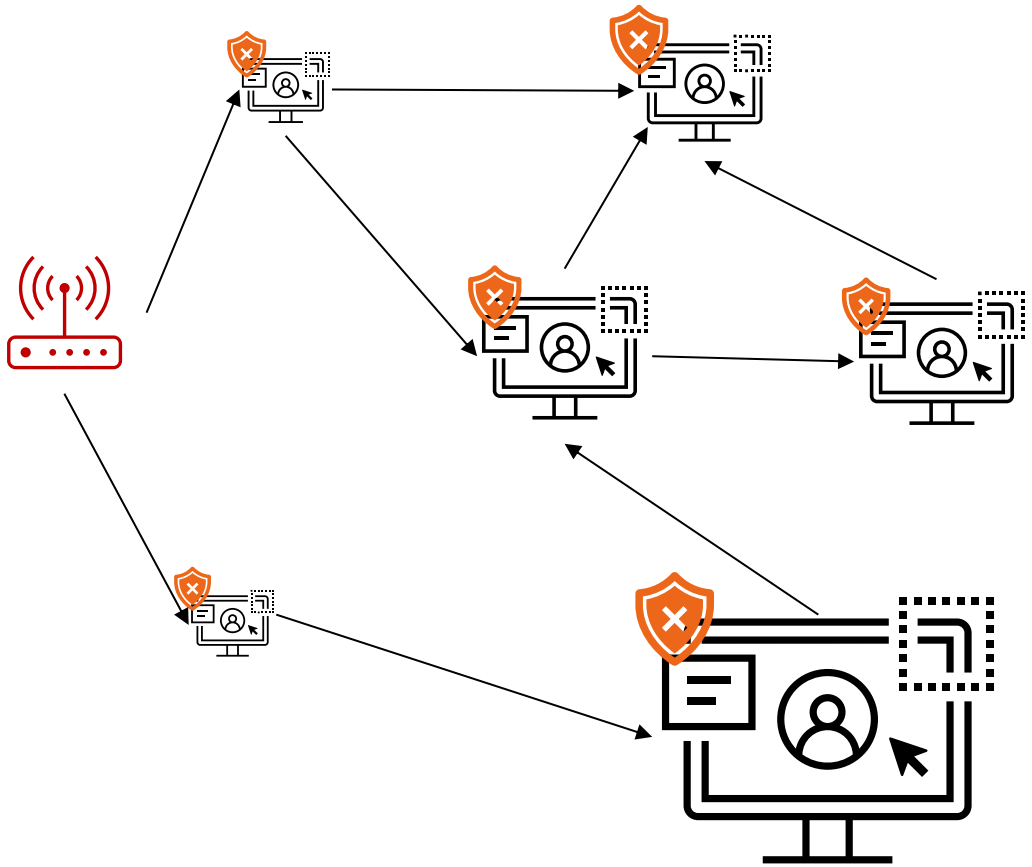
Modéliser l'attaque sur les actifs de l'entreprise



- Une fois ce réseau construit, l'objectif est de comprendre comment l'attaquant peut se déplacer.

Modèle – Graphe Bayesien d'attaque, structurer la dépendance.

Modéliser l'attaque sur les actifs de l'entreprise

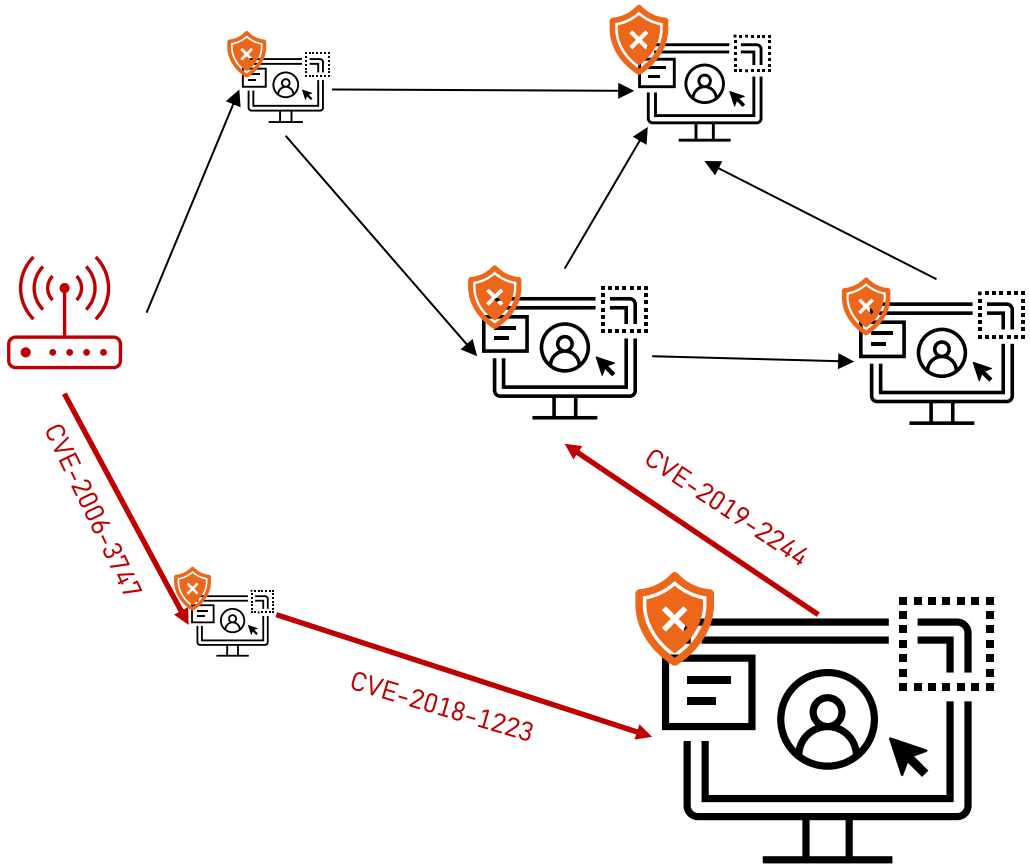


- Une fois ce réseau construit, l'objectif est de comprendre comment l'attaquant peut se déplacer.

- Ce nouveau graphe orienté s'appelle le **Graphe d'Attaque**.

Modèle – Graphe Bayesien d'attaque, structurer la dépendance.

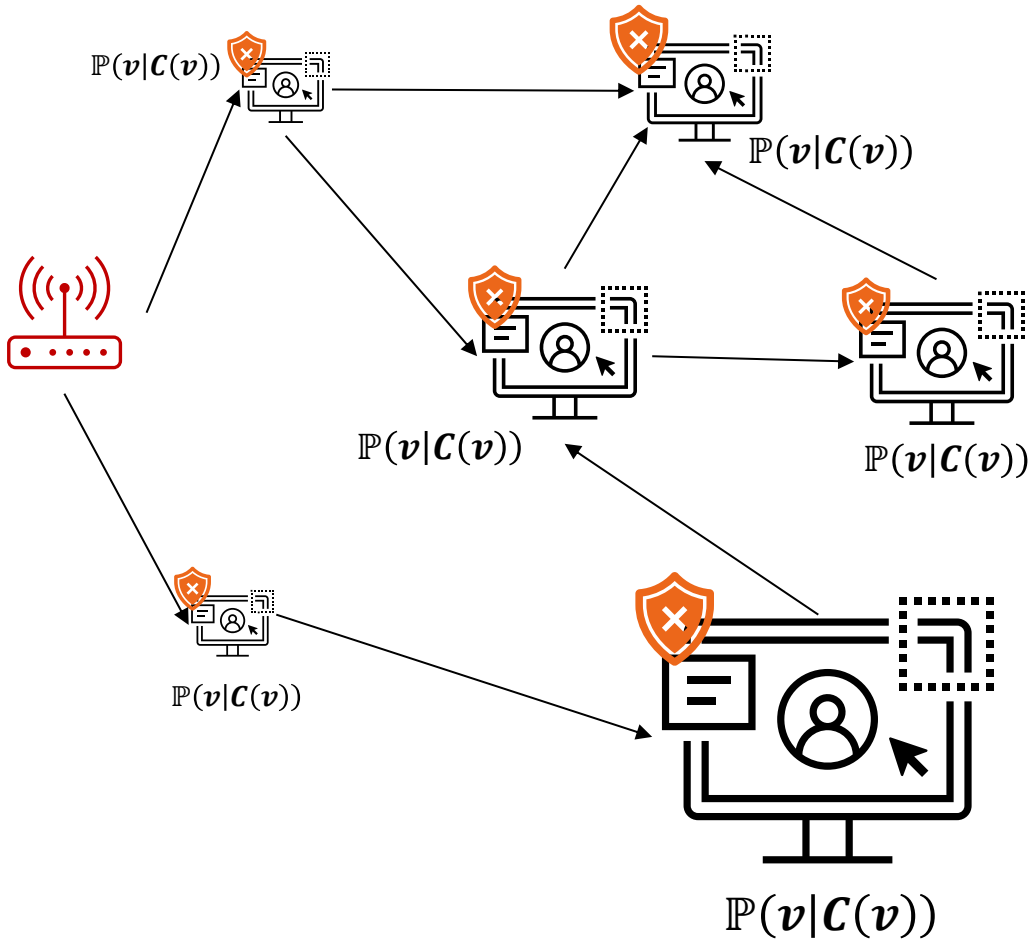
Modéliser l'attaque sur les actifs de l'entreprise



- Une fois ce réseau construit, l'objectif est de comprendre comment l'attaquant peut se déplacer.
- Ce nouveau graphe orienté s'appelle le **Graphe d'Attaque**.
- Il représente **le(s) chemin(s) que peut emprunter l'attaquant**.
- Assimilable à un graphe $G=(V,E)$ où chaque $v \in V$ est un actif et chaque $e \in E$ est une vulnérabilité.

Modèle – Graphe Bayesien d'attaque, structurer la dépendance.

Modéliser l'attaque sur les actifs de l'entreprise

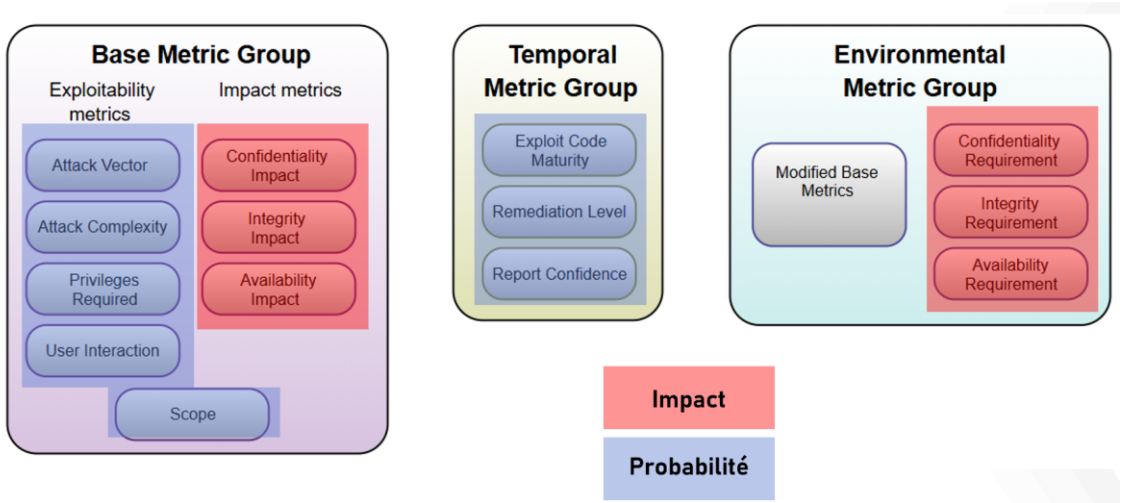


- Enfin, sur ce graphe est créée **une structure de probabilité.**
- Cette probabilité conditionnelle est déterminée **à partir des vulnérabilités** de chaque actif et évaluée **grâce au score CVSS** de la **base CVE**.
- Ce nouveau graphe orienté s'appelle le **Graphe d'Attaque Bayesien**.
- Permet d'avoir la **probabilité de « saut »** d'un attaquant **sachant les privilèges** précédemment capturés.

Modèle – Graphe Bayesien d'attaque, estimer la probabilité.

Modéliser l'attaque sur les actifs de l'entreprise

- Créer une **structure de probabilité** autour du graphe d'attaque.
- Soit le graphe d'attaque $G = (V, E)$. Nous voulons **pondérer les arêtes (les vulnérabilités) par leur probabilité d'exploitation.** En d'autres termes, nous voulons pour chaque $e \in E$, $p(e)$.
- **score CVSS 3.1 :**



- Chaque **métrique de probabilité a un score.**

Métrique	Valeur Métrique	Valeur Numérique
Attack Vector / Modified Attack Vector	Network	0.85
	Adjacent	0.62
	Local	0.55
	Physical	0.2

- Le papier propose ensuite de poser pour une vulnérabilité e :

$$p(e) = K \times \prod ValeurNumérique_{Métrique\ de\ proba.}$$

Avec $K = 2.1$ pour $p(e) \in [0; 1]$

- Exemple avec la vulnérabilité CVE-2018-1223 :
  Vecteur de métriques : CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
  D'où : $p(e) = 2{,}1 \times 0{,}85 \times 0{,}77 \times 0{,}62 \times 0{,}85 = 0{,}72$

Institut des ACTUAIRES EXIOM

Modèle – Une vision cyber économique

Comment le papier propose-t-il d'évaluer une perte cyber?

Modéliser l'attaque sur les actifs de l'entreprise

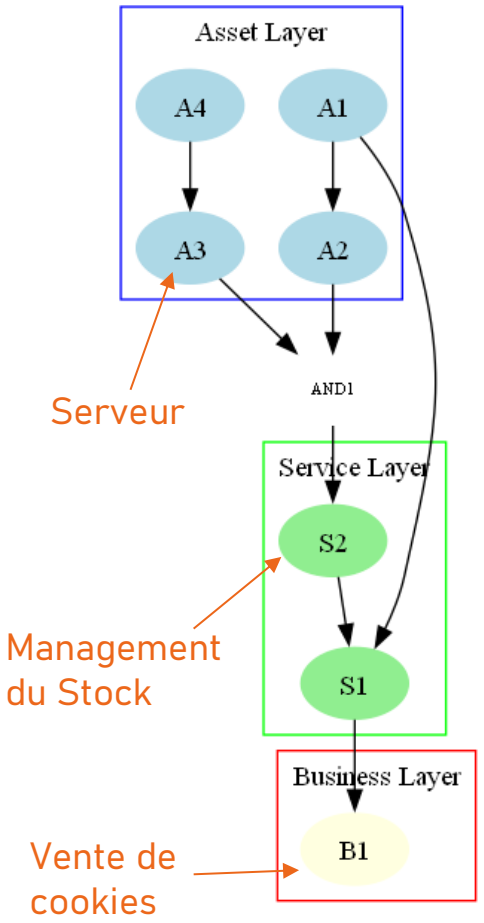
- Graphe Bayésien d'Attaque

Transposer le coût en terme « physique » et « informatique » en coût économique pour l'entreprise

- **Graphe d'Impact**

Modèle – Graphe d'impact, perte d'opérabilité en perte économique

Transposer le coût en terme « physique » et « informatique » en coût économique pour l'entreprise



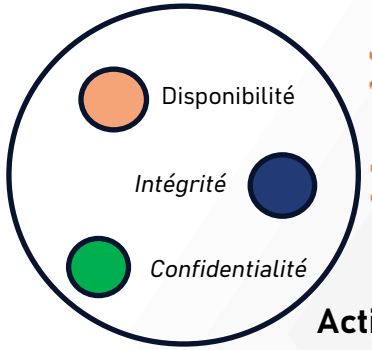
Le Graphe d'Impact

- Représente **les dépendances opérationnelles** dans une entreprise.
- Trois couches :
  - **Actifs :** serveurs, ordinateurs, …
  - **Services :** permet la création de tâches
  - **Business :** l'objectif de l'entreprise

Les pertes à l'échelle des Actifs

- Métriques CVSS 3.1
- Représentent **l'impact**
- Opérabilité des actifs calculés à partir de la métrique

L'application du graphe au cyber



- Chaque nœud est **divisé en 3**
- **Les trois piliers**

Actif/Service/Business

La propagation de la perte d'opérabilité

- Chaque lien dispose de deux paramètres α et β qui représentent la force du lien.
- La **perte d'opérabilité peut être remontée** pour chaque sous-nœud jusqu'au business.
- La **perte économique est enfin calculée** au niveau du business (selon les méthodes propres au modèle).

FDNA

EXIOM

Modèle – Application stochastique à la perte d'exploitation.

Notre modélisation – comment appliquer ces idées à la quantification dynamique de la perte d'exploitation ?

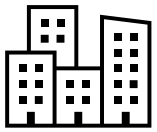
Modéliser l'attaque sur les actifs de l'entreprise

+

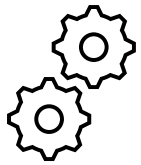
Transposer le coût en terme « physique » et « informatique » en coût économique pour l'entreprise

Framework du papier

Entreprise

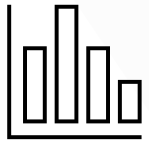


- Graphe d'Attaque
- Graphe d'Impact



Modèle perte d'exploitation

- Multiples simulations d'attaque.
- Stochastique pour avoir une répartition du risque.
- Qui suit la méthodologie d'une attaque.

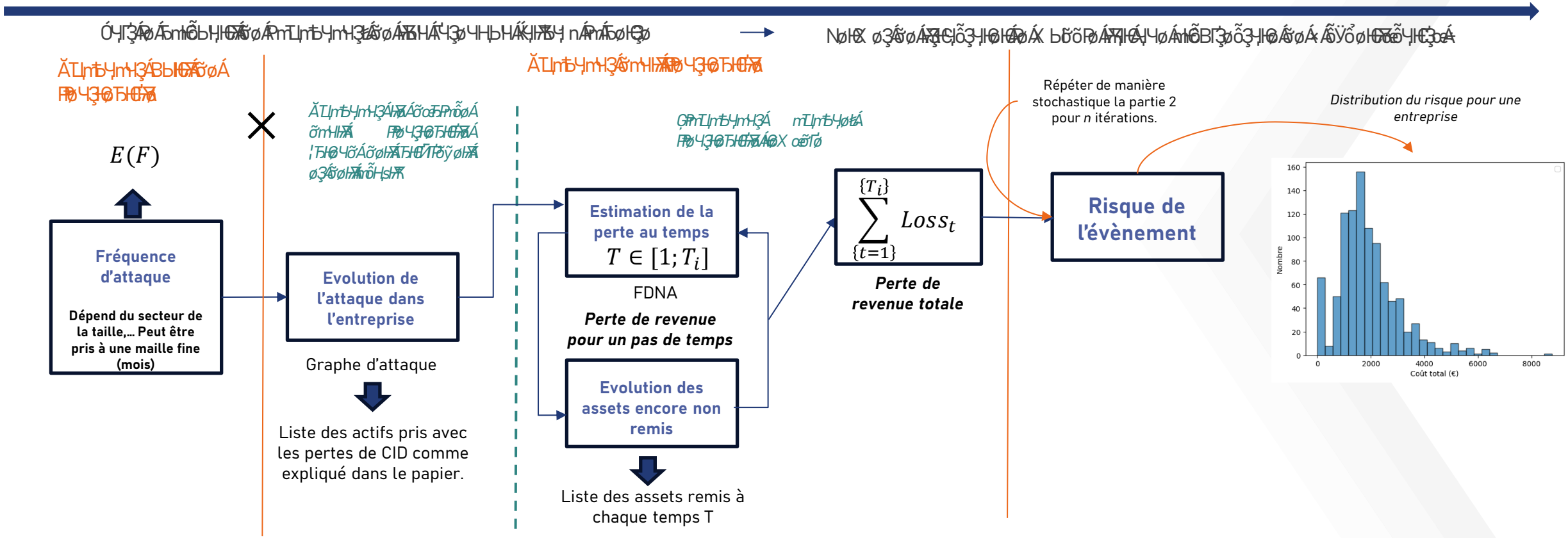


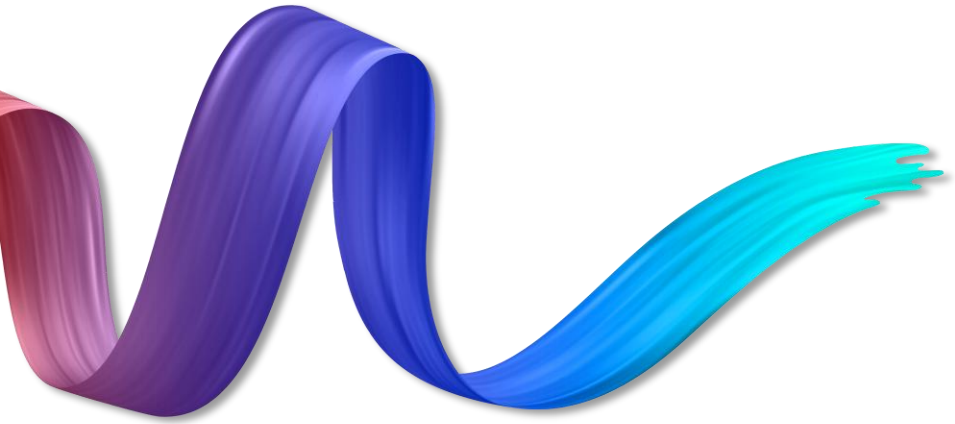
Distribution du risque

Institut des ACTUAIRES EXIOM

Modèle – Application stochastique à la perte d'exploitation.

Architecture du Modèle





3 Applications à un portefeuille

Institut des ACTUAIRES EXIOM

APPLICATION – CRÉATION DU PORTEFEUILLE FICTIF.

- Limite l'étude à des **PME**: secteur vulnérable, ayant besoin de prévention et donc d'une visibilité plus fine sur le risque.
- En entrée du modèle
  - **Graphe d'attaque**
  - **Graphe d'impact**
  - **Chiffre d'Affaires** par business

  Savoir comment récupérer ces différentes informations dans un cas réel.
- Objectif de **créer un portefeuille fictif cohérent** pour étudier les résultats et le comportement du modèle.

1 **OBTENIR DES TAILLES COHERENTES D'ENTREPRISES ET CA**

2 **CRÉER UN RESEAU ET UN GRAPHE D'ATTAQUE REALISTE**

3 **CRÉER UN GRAPHE D'IMPACT COHERENT**

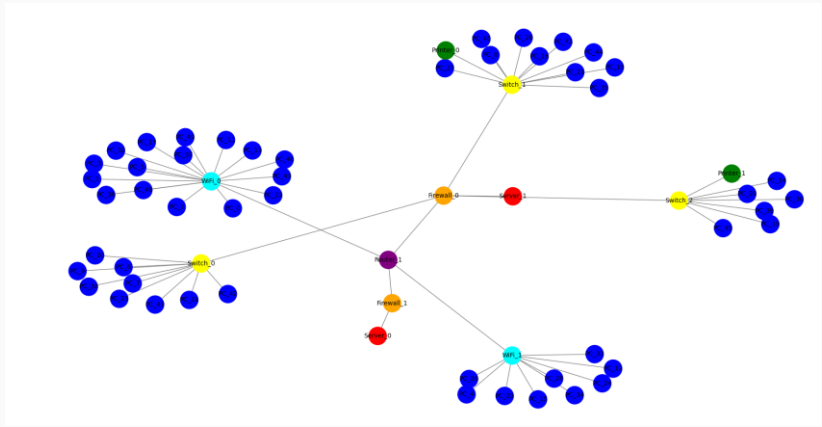
- Récupérer les informations sur le site de l'INSEE

APPLICATION – CRÉATION DU PORTEFEUILLE FICTIF.

2

CRÉER UN RESEAU ET UN GRAPHE D'ATTAQUE REALISTE

Création du Réseau



Catégorie	Actifs
Actifs de Réseaux	Firewall, routeur, switch, routeur wifi
Actifs Terminaux	Ordinateur (PC), serveur (de données et web)

- **Génération aléatoire du réseau** pour chaque entreprise.
- Chaque type d'actif suit des lois pour le nombre.

Création du Graphe d'Attaque

Actif	Types de Programmes
Ordinateur (PC)	Système d'Exploitation
	Navigateur Internet
	Antivirus
	Logiciel de Partage d'Information
	Logiciel de Productivité
	Logiciel de Communication

- Chaque type d'actif a plusieurs types de logiciel

Type de Programme	Programmes	Part de marché
Système d'Exploitation	Windows	75,51%
	Mac OS	15,06%
	Linux	3,16%
	Chrome OS	1,23%
	Autre	5,02%

- Chaque type de logiciel a des logiciels avec une part de marché

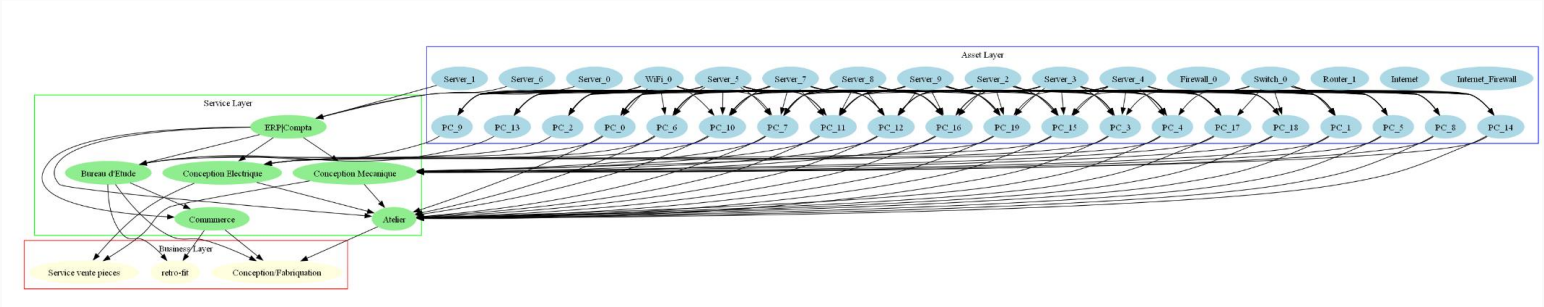
- Chaque logiciel a des failles : **Bibliothèque de failles**
- Chaque actif reçoit aléatoirement un logiciel par type de logiciel.
- Des failles sont ensuite données de manière aléatoire pour **obtenir le graphe d'attaque**.

APPLICATION – CRÉATION DU PORTEFEUILLE FICTIF.

3

CRÉER UN GRAPHE D'IMPACT COHERENT

- Les graphes d'impact restent un sujet très théorique. **Peu d'applications dans le monde réel.**
- **Questionnaires** sont un des moyens proposés pour obtenir un graphe d'impact.
- Des entretiens ont été menés pour mettre en application et avoir une idée de l'avis des PME.
- A permis de mettre en lumière la **spécificité d'un graphe d'impact à l'entreprise étudiée.**



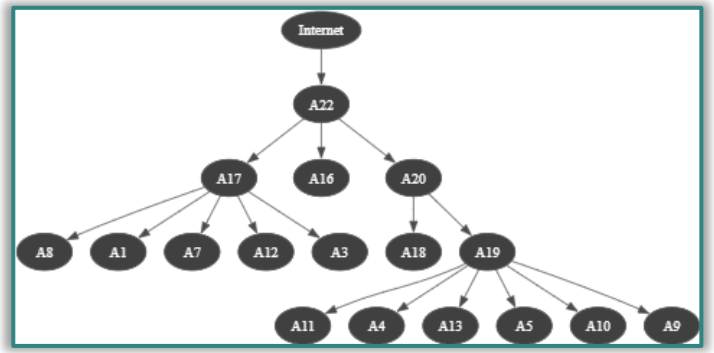
- Choix d'avoir **deux types de graphes d'impact** : un pour le secteur industriel et un pour le commerce en ligne.

Application – Résultat du modèle et sensibilité.

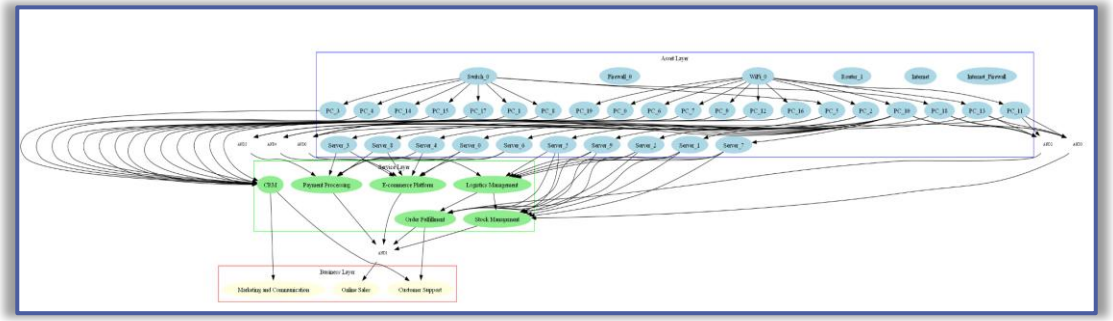
Comment se présentent les résultats au niveau d'une entreprise?

Entreprise ENT0Com

- Graphe d'Attaque



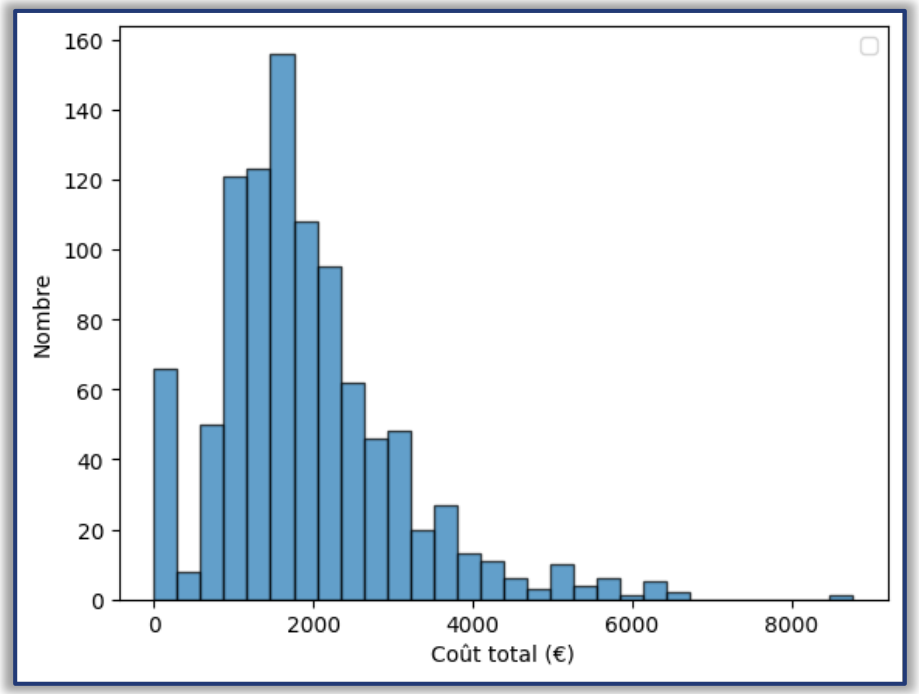
- Graphe d'Impact



Modèle perte d'exploitation

- n simulations (attaques indépendantes).

Distribution des coûts



- Valeur moyenne de 1904 € soit 1% du CA.

Application – Résultat du modèle et sensibilité.

Sensibilité par rapport à ρ.

Impact du graphe d'attaque sur les résultats du modèle.

Dynamisme du modèle par l'introduction d'un nouveau contexte.

Application – Résultat du modèle et sensibilité.

Sensibilité par rapport à ρ.

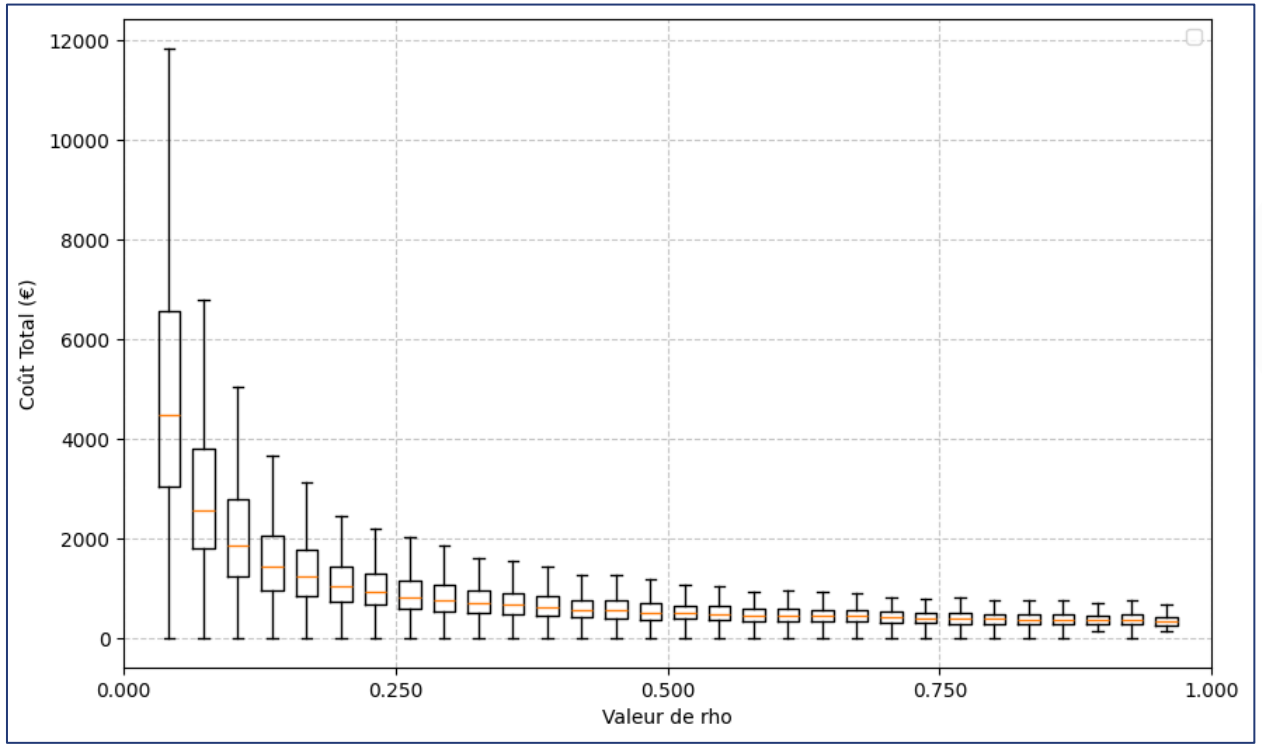
Impact du graphe d'attaque sur les résultats du modèle.

Dynamisme du modèle par l'introduction d'un nouveau contexte.

Application – Résultat du modèle et sensibilité.

Sensibilité par rapport à ρ – un choix de grande importance.

- Le choix de la probabilité de remédiation à chaque temps ρ est fondamental.



Cout total, toutes choses égales par ailleurs de ENTOCom en fonction de ρ

Application – Résultat du modèle et sensibilité.

Sensibilité par rapport à ρ.

Impact du graphe d'attaque sur les résultats du modèle.

Dynamisme du modèle par l'introduction d'un nouveau contexte.

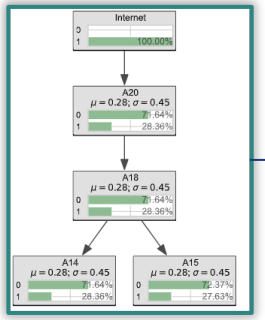
Application – Des résultats sur le graphe d'attaque.

Des résultats intéressants sur l'impact du graphe d'attaque.

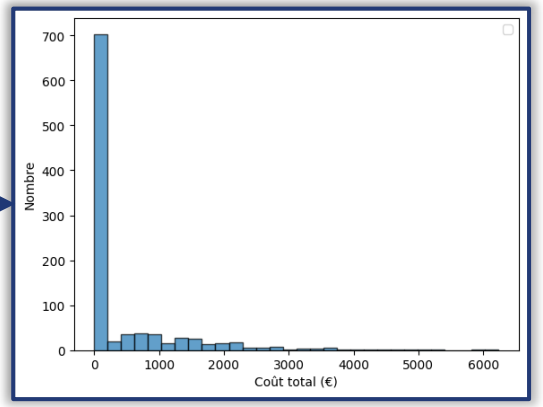
- Choix de différentes entreprises avec un CA similaire et un graphe d'impact similaire mais avec un graphe d'attaque différent.

Entreprise ENT15Com

Graphe d'Attaque



Distribution des coûts



- Graphe d'attaque **peu développé** (peu de surface d'attaque) se traduit par de **faibles coûts.**

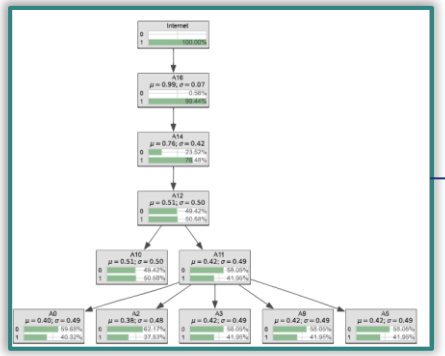
Application – Des résultats sur le graphe d'attaque.

Des résultats intéressants sur l'impact du graphe d'attaque.

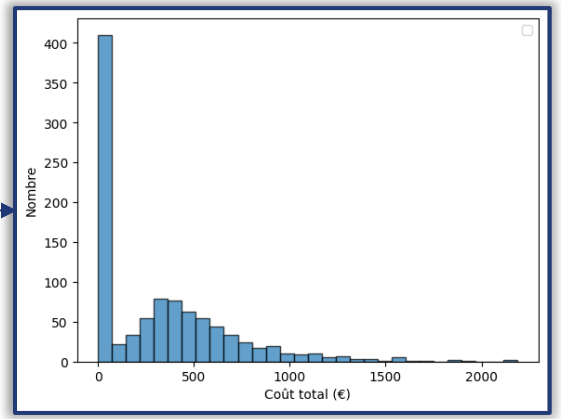
- Choix de différentes entreprises avec un CA similaire et un graphe d'impact similaire mais avec un graphe d'attaque différent.

Entreprise ENT20Com

Graphe d'Attaque



Distribution des coûts



- Graphe d'attaque **développé mais en longueur** se traduit par une **forte proportion de coûts nuls**.

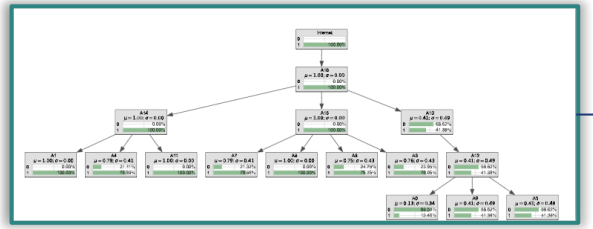
Application – Des résultats sur le graphe d'attaque.

Des résultats intéressants sur l'impact du graphe d'attaque.

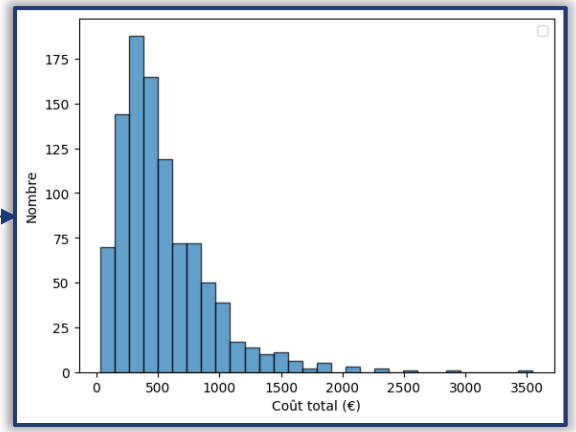
- Choix de différentes entreprises avec un CA similaire et un graphe d'impact similaire mais avec un graphe d'attaque différent.

Entreprise ENT26Com

Graphe d'Attaque



Distribution des coûts



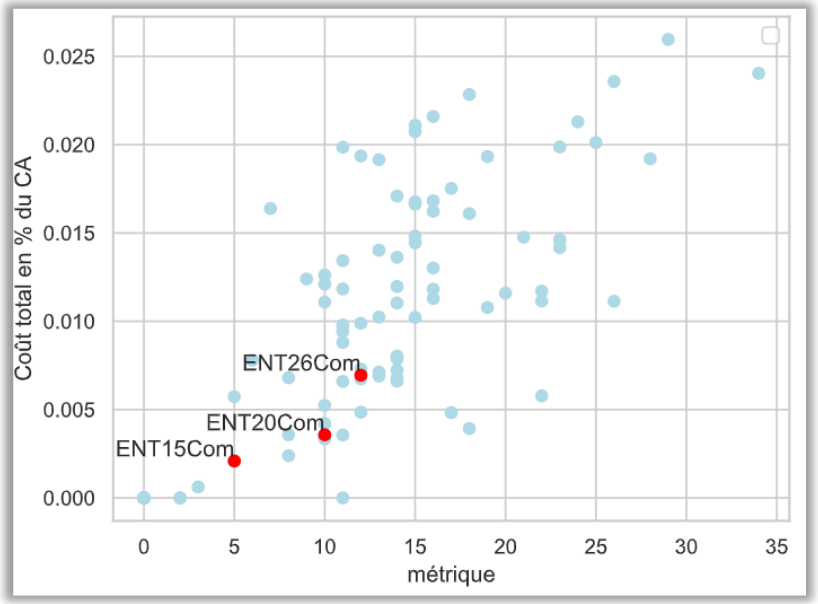
- Graphe d'attaque **développé** se traduit par une **distribution développée des coûts**.

Application – Des résultats sur le graphe d'attaque.

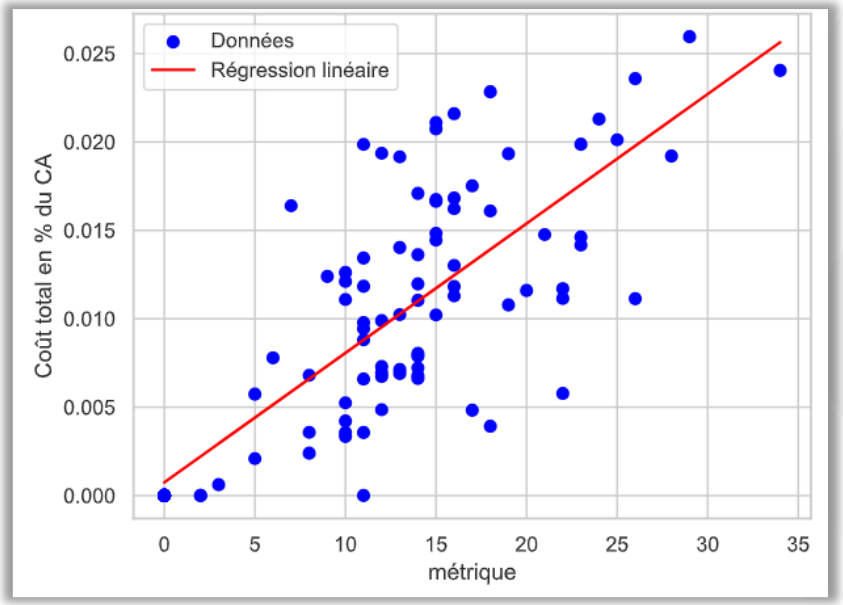
Vérifier cet impact au niveau du portefeuille.

- Impact de la complexité du graphe d'attaque sur les coûts est vérifiable au niveau du portefeuille.

Coût moyen en fonction de la complexité du graphe



Régression linéaire multiple



- De bons résultats de régression linéaire multiple (différentes notions de complexité).

- Rappelle la notion de cybersécurité de **propagation latérale**.
- Si cette propriété continue à être vraie sur un vrai graphe d'attaque : possibilité pour l'assureur de rapidement approximer le risque d'un assuré.

Institut des ACTUAIRES EXIOM

Application – Résultat du modèle et sensibilité.

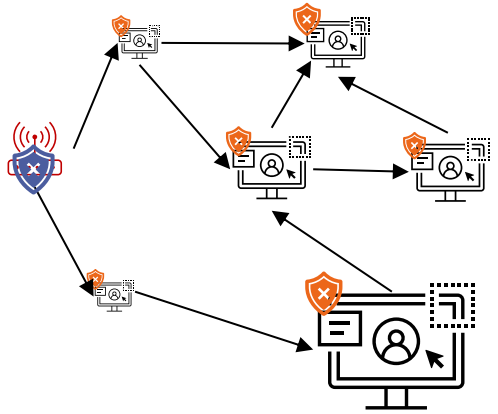
Sensibilité par rapport à ρ.

Impact du graphe d'attaque sur les résultats du modèle.

Dynamisme du modèle par l'introduction d'un nouveau contexte.

Application – Dynamisme et adaptabilité du modèle.

Que se passe-t-il lorsqu'une nouvelle faille apparaît dans les systèmes ?

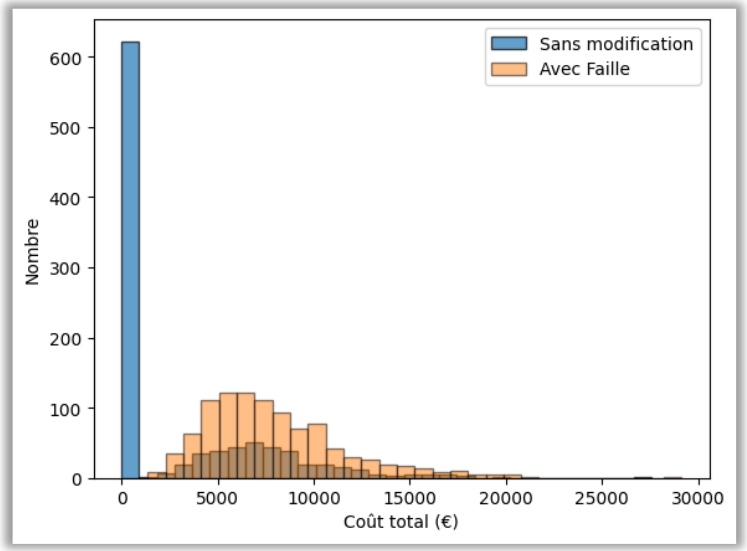


- Création de la **faille fictive** CVE-0000-00000 présente sur 67,59% des firewalls.
- Changements appliqués au graphe d'attaque.

Modèle perte d'exploitation

Observation de l'évolution des coûts sur le portefeuille.

Au niveau d'une entreprise



- Certaines entreprises ont une évolution forte de la répartition du coût.

Au niveau du portefeuille

Nom	Augmentation (%)
ENT62Ind	inf %
ENT79Com	172.859441 %
ENT88Ind	169.682549 %
ENT53Com	98.003952 %
ENT97Ind	51.494563 %

- Le coût moyen **augmente au niveau du portefeuille de 7,34%.**

Conclusion – Qu'est-ce que ce modèle apporte ?

Une quantification proche du risque

- Avec une connaissance de $\mathbb{E}(F)$, **l'assureur pourrait calculer le risque de l'assuré de manière plus fréquente.**
- Peut servir à suivre ses assurés voir **à terme être intégré dans la tarification**.

Une possibilité de prévention

- L'assureur **observe les changements de risque** avant qu'un sinistre ne se produise par l'aspect dynamique du graphe d'attaque bayésiannisé. Il peut ainsi **proposer de l'aide aux entreprises en ayant le plus besoin**.

Une applicabilité pour des stress tests

- L'assureur **peut tester des scénarios** (Perte systémique – Type Serveur Amazon attaqué) et **regarder l'impact sur son portefeuille.**

Répond à la problématique posée en proposant une méthodologie

Conclusion – Qu'est-ce que ce modèle apporte ?

Une quantification proche du risque

- Avec une connaissance de $\mathbb{E}(F)$, **l'assureur pourrait calculer le risque de l'assuré de manière plus fréquente.**
- Peut servir à suivre ses assurés voir **à terme être intégré dans la tarification**.

Une possibilité de prévention

- L'assureur **observe les changements de risque** avant qu'un sinistre ne se produise par l'aspect dynamique du graphe d'attaque bayésiannisé. Il peut ainsi **proposer de l'aide aux entreprises en ayant le plus besoin**.

Une applicabilité pour des stress tests

- L'assureur **peut tester des scénarios** (Perte systémique – Type Serveur Amazon attaqué) et **regarder l'impact sur son portefeuille.**

Répond à la problématique posée en proposant une méthodologie

Dynamique

Conclusion – Qu'est-ce que ce modèle apporte ?

Une quantification proche du risque

- Avec une connaissance de $\mathbb{E}(F)$, **l'assureur pourrait calculer le risque de l'assuré de manière plus fréquente.**
- Peut servir à suivre ses assurés voir **à terme être intégré dans la tarification**.

Une possibilité de prévention

- L'assureur **observe les changements de risque** avant qu'un sinistre ne se produise par l'aspect dynamique **du graphe d'attaque bayésiannisé**. Il peut ainsi **proposer de l'aide aux entreprises en ayant le plus besoin**.

Une applicabilité pour des stress tests

- L'assureur **peut tester des scénarios** (Perte systémique – Type Serveur Amazon attaqué) et **regarder l'impact sur son portefeuille.**

Répond à la problématique posée en proposant une méthodologie

Dynamique

Grâce aux connaissances de cybersécurité

Conclusion – Qu'est-ce que ce modèle apporte ?

Une quantification proche du risque

- Avec une connaissance de $\mathbb{E}(F)$, **l'assureur pourrait calculer le risque de l'assuré de manière plus fréquente**.
- Peut servir à suivre ses assurés voir **à terme être intégré dans la tarification**.

Une possibilité de prévention

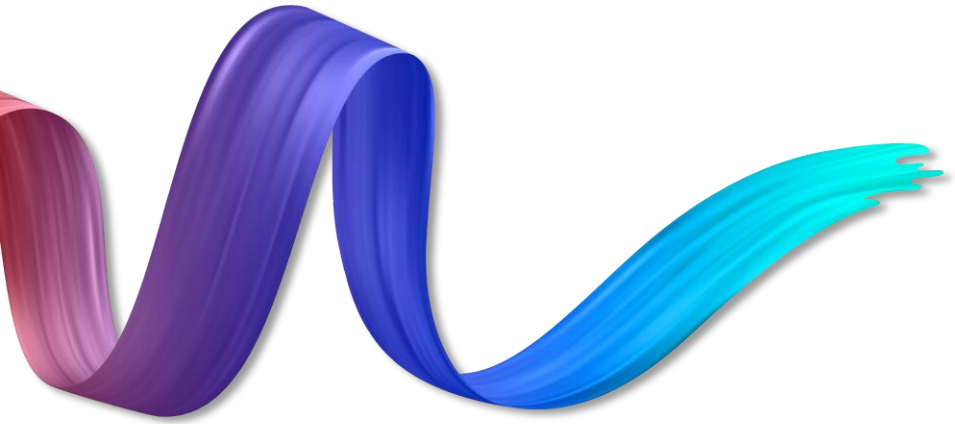
- L'assureur **observe les changements de risque** avant qu'un sinistre ne se produise par l'aspect dynamique du graphe d'attaque bayésiannisé. Il peut ainsi **proposer de l'aide aux entreprises en ayant le plus besoin**.

Une applicabilité pour des stress tests

- L'assureur **peut tester des scénarios** (Perte systémique – Type Serveur Amazon attaqué) et **regarder l'impact sur son portefeuille.**

Répond à la problématique posée en proposant une méthodologie

- Dynamique
- Grâce aux connaissances de cybersécurité
- Qui répond au besoin de prévention



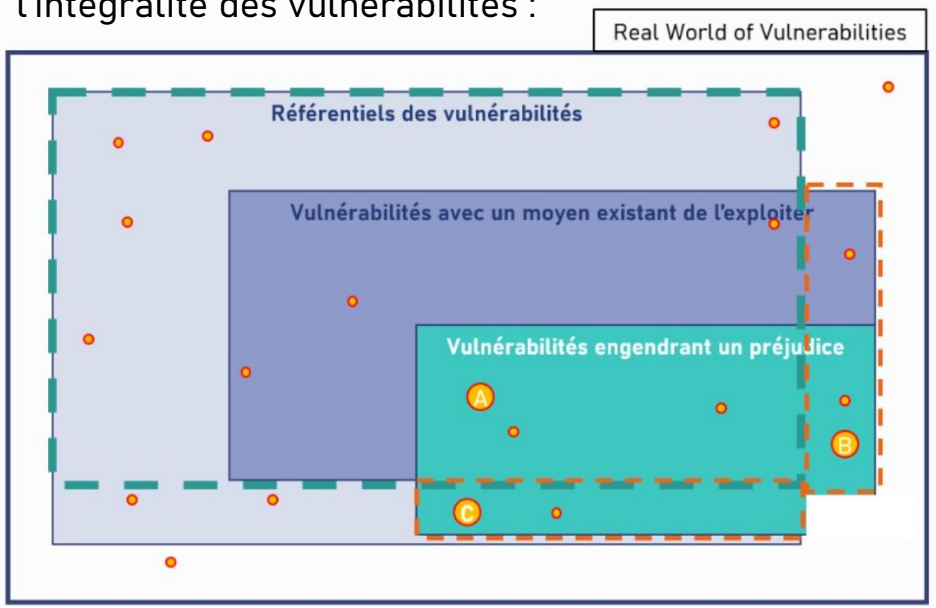
4 Limites et Ouverture

EXIOM

Limites et Ouvertures

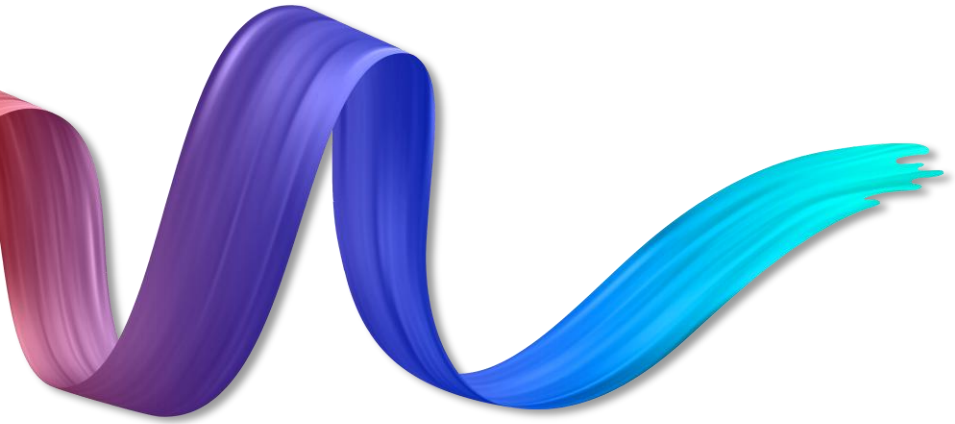
Limites

- **Peu d'informations sur** $\mathbb{E}(F)$, les résultats restent sur le coût.
- La création de la base fictive induit beaucoup d'hypothèses qui jouent sur le réalisme des résultats.
- Certains paramètres comme ρ ou la loi des $p(e)$ sont à étudier de manière approfondie avant de quelconques conclusions.
- Les vulnérabilités présentes sur CVE ne constituent pas l'intégralité des vulnérabilités :



Ouvertures

- **Des études sur** $\mathbb{E}(F)$**,** la fréquence d'attaque, peuvent être mené. Celle-ci diffère légèrement de la fréquence de sinistre et plus de sources peuvent exister grâce à la ***Threat-Intelligence***.
- Les **données historiques** même biaisées pourraient servir de première **calibration** des paramètres ρ et $p(e)$.
- Les **vulnérabilités humaines** pourraient être ajoutées au modèle.
- Des **modèles bilatéraux** tenant compte de l'agissement actif de l'entreprise pourrait aussi être pris en compte.



Merci pour votre attention !!

Institut des ACTUAIRES EXIOM