Vers une gestion durable des riques : Comment le risque cyber systémique redéfinit-il les stratégies en assurances ?

Alexandre ANDREINI
Chief Risk Officer
Stoïk

Antoine CHANH
Senior Manager
Modeling & Risk P&C
Addactis

Geoffrey BARD
Consultant
Modeling & Risk P&C
Addactis

SOMMAIRE

Introduction au **risque Cyber** et **contexte actuel**

Présentation du risque Cyber
Évolution du cadre législatif
Implications pour les assurances

Le risque Cyber

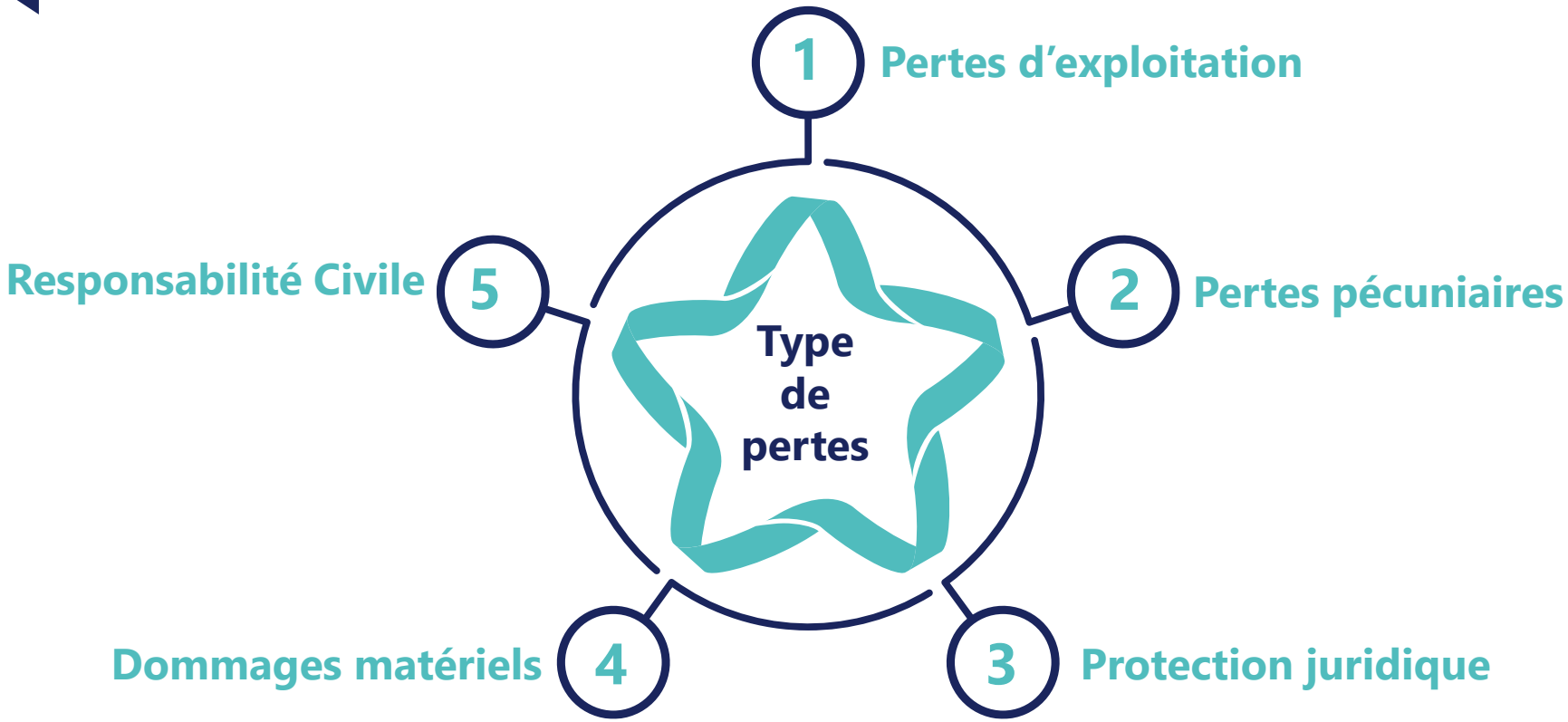
Le risque Cyber

Au sens strict :

Atteinte à des systèmes informatiques réalisée dans **un but malveillant** caractérisée par une **origine immatérielle.**

Au sens retenu par les assureurs :

Défaillance de systèmes informatiques entraînant **des pertes financières** ou **une atteinte à la réputation**.

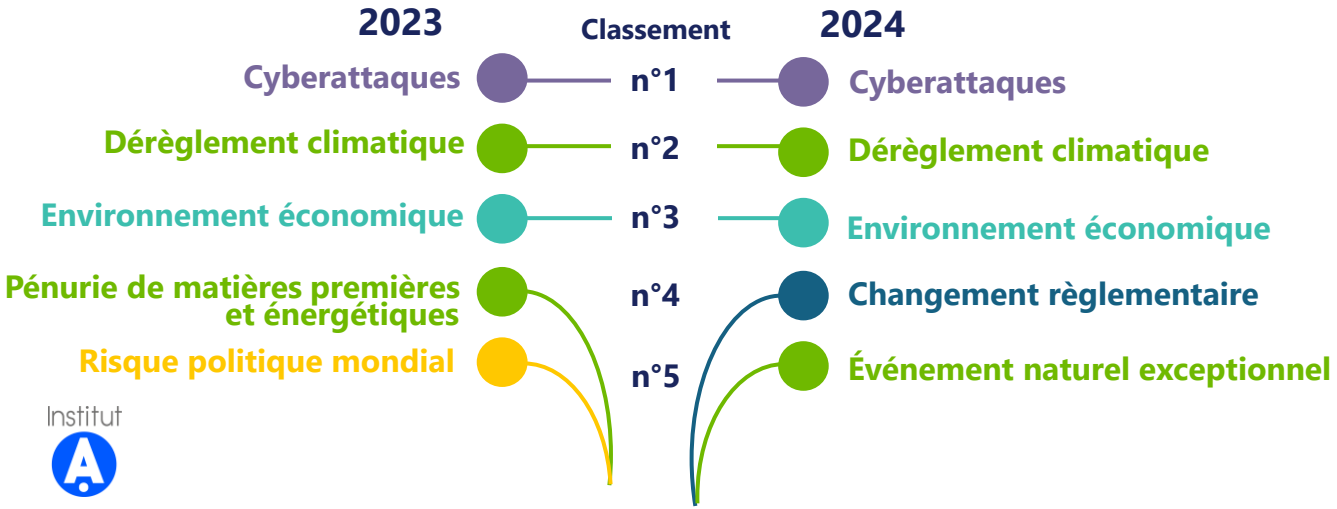


Le risque Cyber

Baromètre France 2023

Enquête réalisée par OpinionWay auprès de 456 grandes entreprises en 2023

Cartographie des risques de France Assureurs

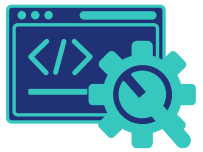


Institut

Contexte économique favorable aux attaques

Pression concurrentielle

La sécurité est difficile à promouvoir



Un monde de plus en plus interconnecté

Les enjeux réglementaires et actualités

23e CONGRÈS DES ACTUAIRES

RGPD
25 mai 2018

La sanction est dissuasive : jusqu'à 20 millions d'euros Ou 4% du chiffre d'affaires mondial.

Miris
11 avril 2022

BASF, Michelin, Airbus ont créé leur propre captive : **Car difficulté à s'assurer au juste prix**

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
25 janvier 2023

LOI LOPMI :
Obligation de porter plainte dans les 72h dans le cadre d'une attaque Cyber

DORA
2025

Réglementation européenne sur **la résilience opérationnelle numérique**

Communiqué de l'ACPR sur la distribution des garanties contre les risques cyber : **une de ses priorités de contrôle**

ACPR BANQUE DE FRANCE
12 novembre 2019

Le risque cyber rentre dans le code des assurances.

CODE DES ASSURANCES DALOZ
1er janvier 2023

Nombreuses publications de l'EIOPA sur le risque Cyber

eiopa EUROPEAN INSURANCE AND OCCUPATIONAL PENSIONS AUTHORITY
10 mai 2023

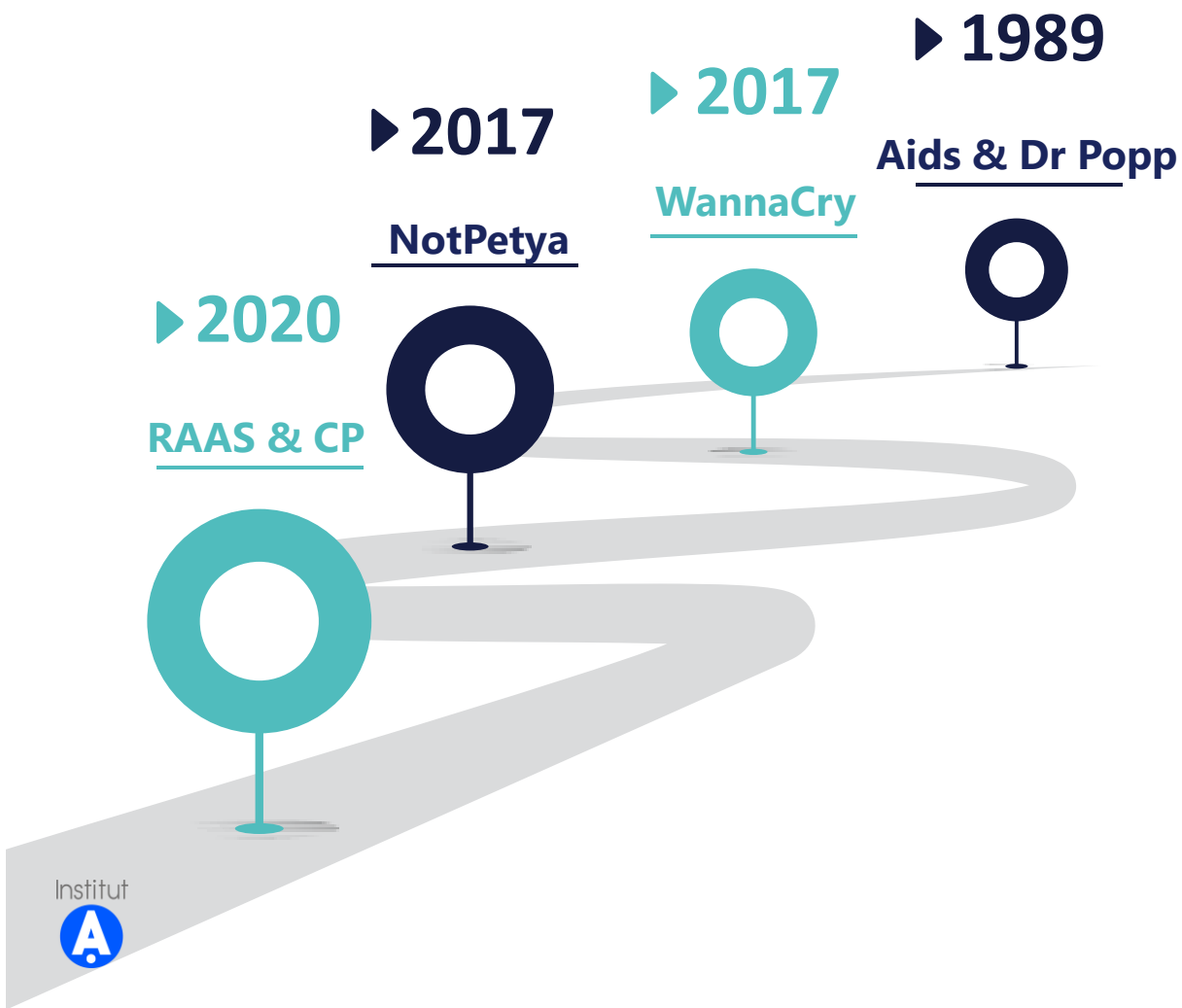
Blog Addactis : Cyber : les exigences de l'EIOPA (addactis.com)

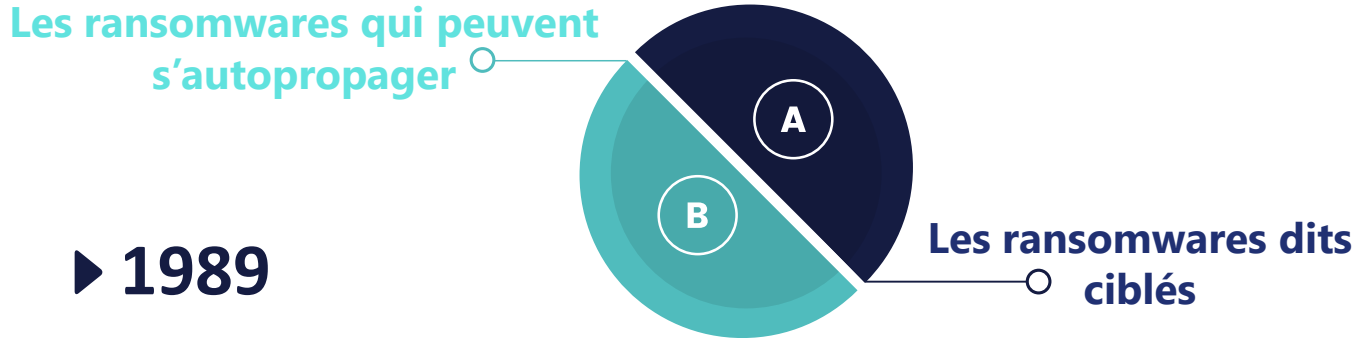
Institut Actuaires

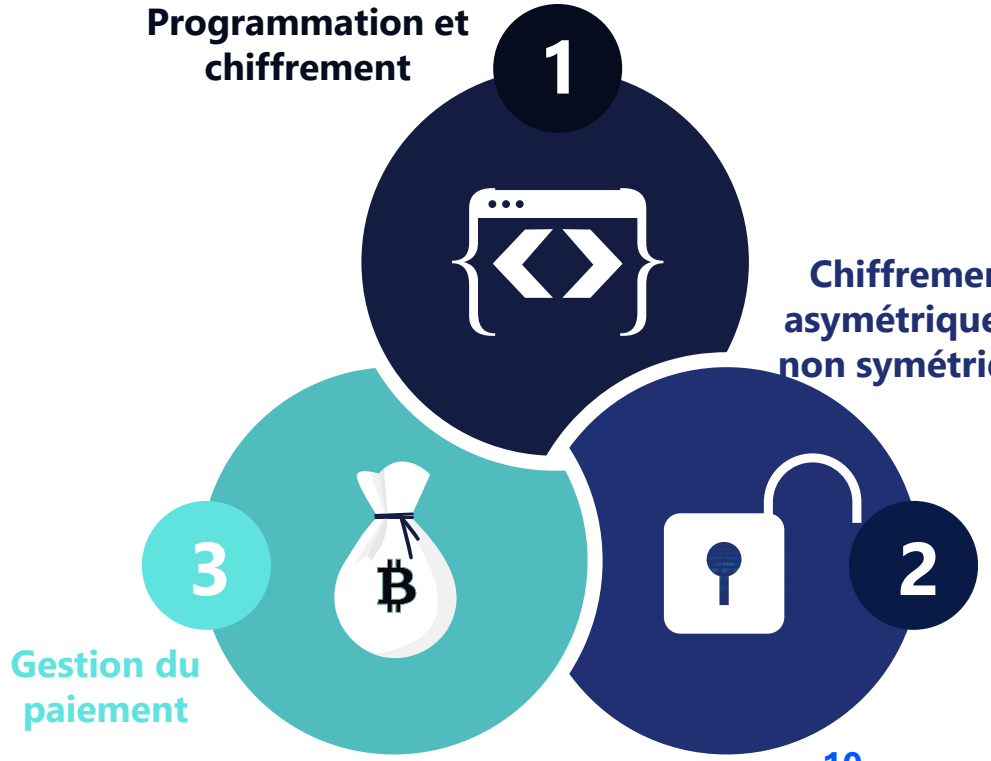
Modélisation du risque systémique

Limites des approches actuarielles classiques
Exploration des structures de dépendances
Application des modèles épidémiologiques et de réseaux épidémiques

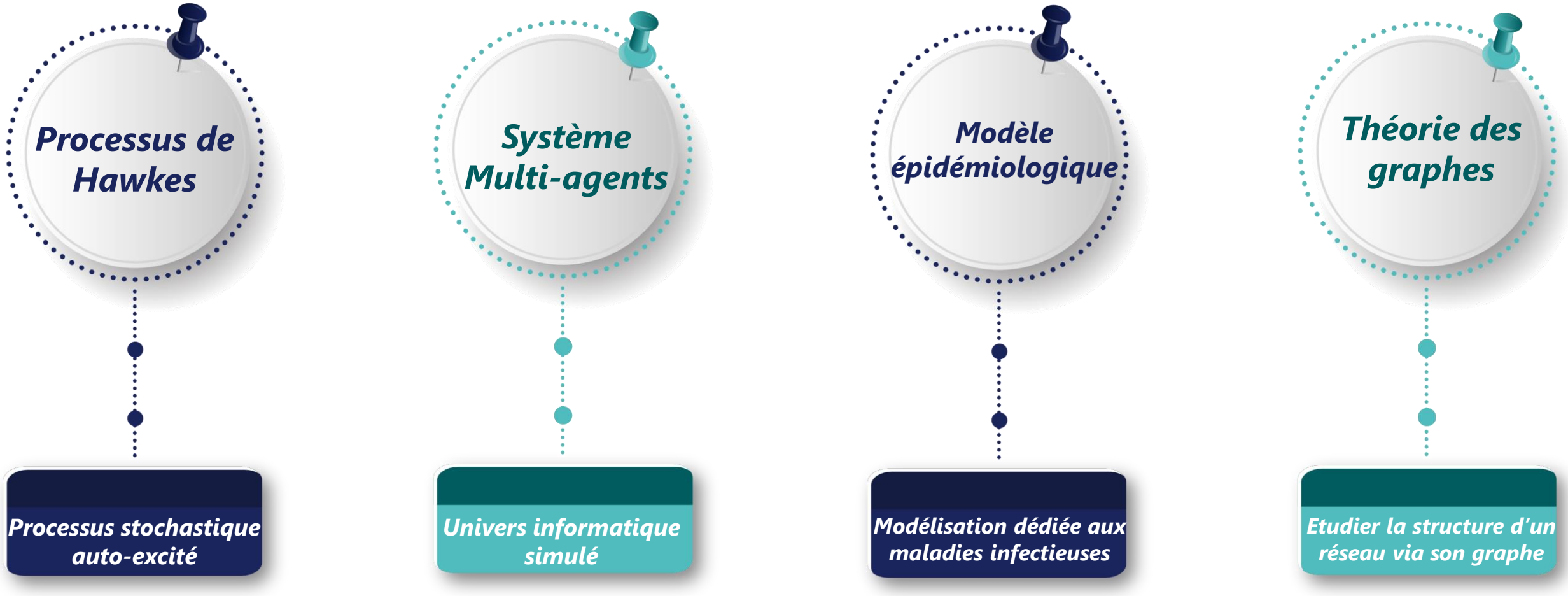
Ransomware : histoire et fonctionnement







Rançongiciel : Choix et justification de la modélisation

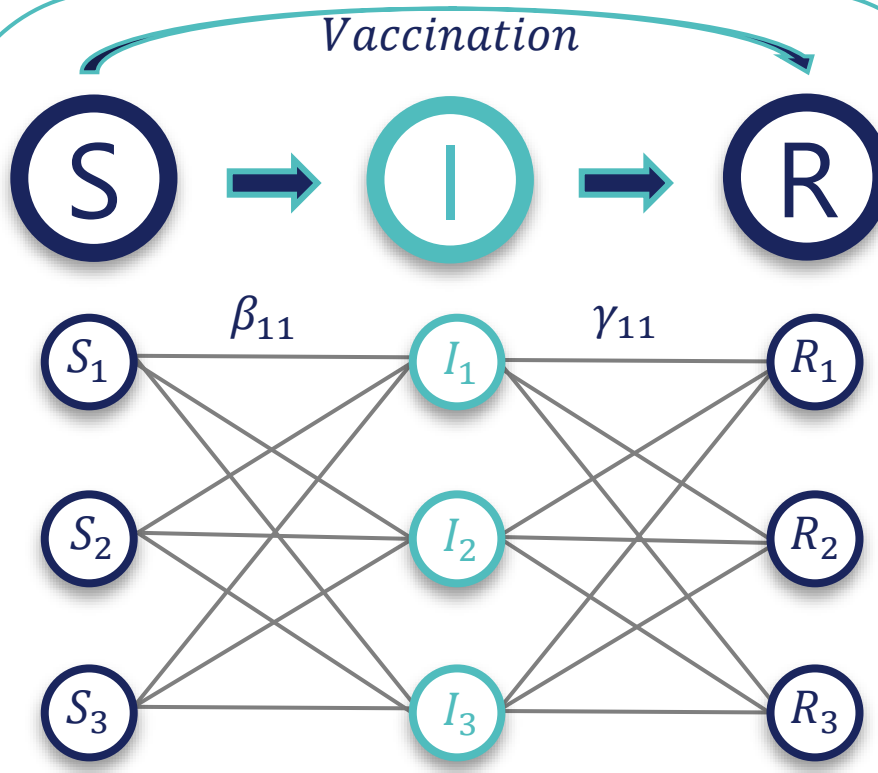


- La **modélisation** est basée sur l'approche du **modèle collectif** mais avec une **structure** de **dépendance** pour identifier les assurés concernés.

Exemple de modélisation d'un processus de diffusion

Le modèle SIR simple à un modèle SIR multi-groupes

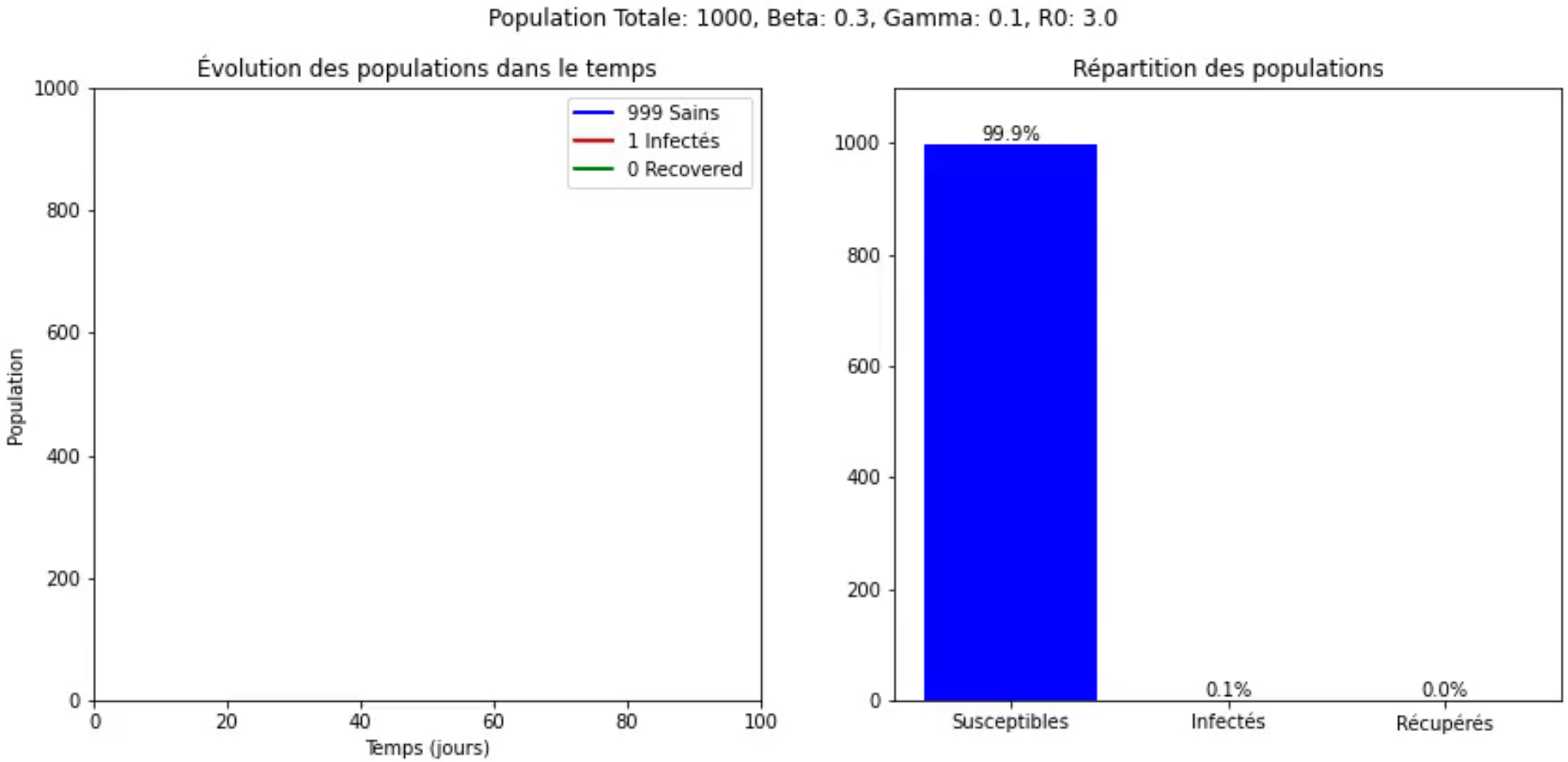
Taux de reproduction $R_0 = \frac{\beta}{\gamma}$



Régi par un système d'équations différentielles :

$$\frac{\partial S}{\partial t} = -\beta S(t)I(t) \qquad \frac{\partial I}{\partial t} = \beta S(t)I(t) - \gamma I(t) \qquad \frac{\partial R}{\partial t} = \gamma I(t)$$

Exemple de modélisation d'un processus de diffusion



Modélisation des effets d'une attaque sur un portefeuille

Mesures, coûts, comportements et variable de durée

Mesures

$N_t = \sum_{J=1}^{n} \delta_j \, 1_{T_j \le t}$: Nombre cumulé d'infectés

$R_t = \sum_{J=1}^{n} \delta_j \, 1_{T_j + U_j \le t}$: Nombre d'infectés guéris avant t

$J_t = N_t - R_t$: Nombre d'infectés à l'instant t

Coûts

$C_1 = C \lim_{t \to +\infty} N_t$: Coût financier

$C_2 = 1_{sup\, t} J_t > K$: Coût de saturation

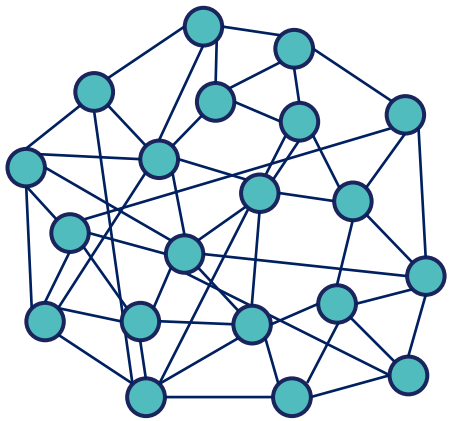
$C_3 = \int_0^{t_d} \phi\left(\frac{J_t}{n}\right) dt$: Coût de capacité

Comportements des assurés :

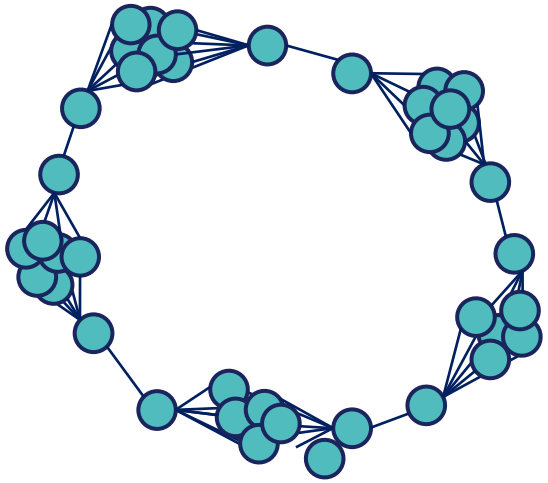
- $\lambda_C^{(1)} = c_1 1_{t \ge \tau_1}$: Réaction lambda
- $\lambda_2^{(c)} = c_2 \left(t - \tau_2 + \frac{1}{2}\right)^{-\alpha_2} 1_{t \ge \tau_2}$: Réaction qui diminue.
- $\lambda_3^{(c)} = c_3 (t - \tau_3)^{\alpha 3} 1_{t \ge \tau_3}$: Réaction rapide.

Analyse de la topologie du réseau d'un portefeuille d'assurés

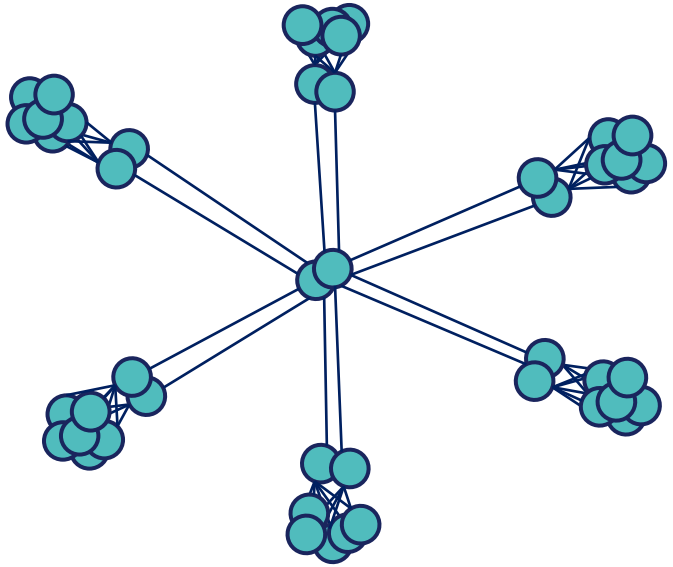
L'analyse spectrale fournit des informations sur **la topologie du réseau** et **ses interections**



Homogeneous



Clustered



Star

Application découlant de la topologie d'un portefeuille

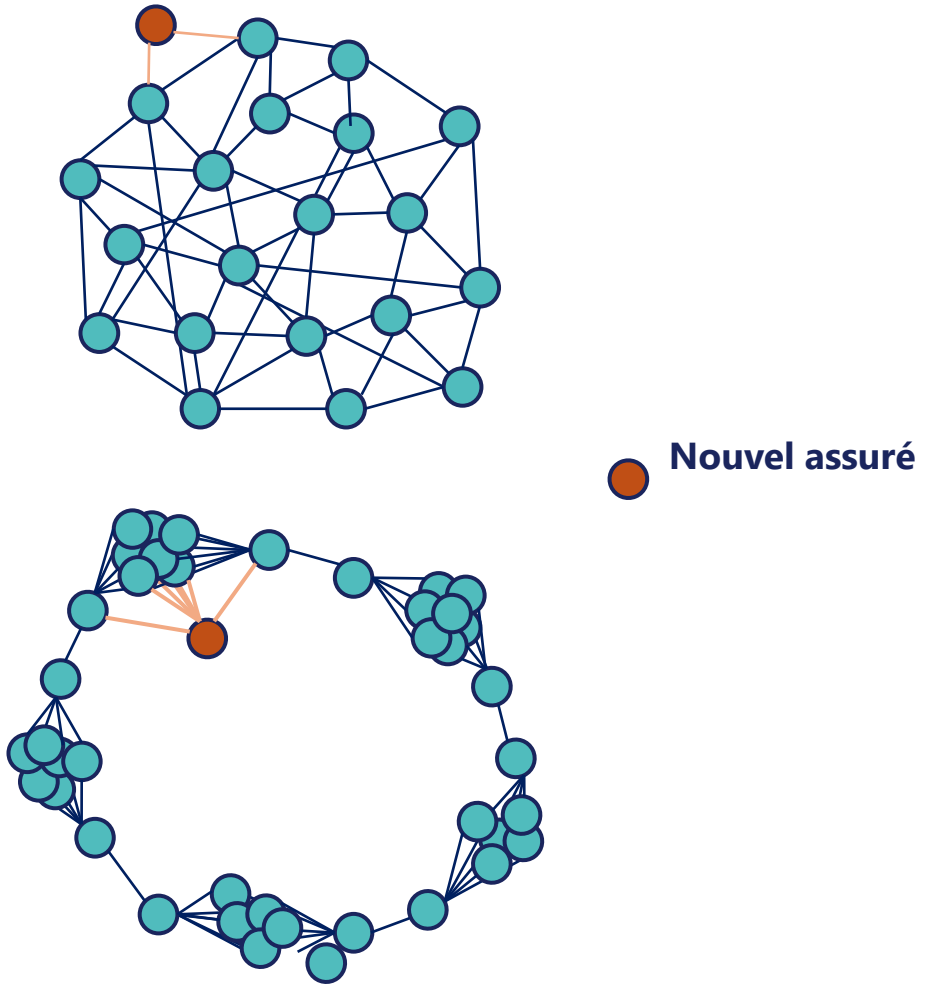
La mesure de dépendance des portefeuilles

- **Objectif :** Montrer que la prime d'un même assuré est différente selon le portefeuille dans lequel il se trouve

- Évaluer la **prime pure** dans une perspective de **tarification.**

La prime d'un assuré pourrait donc **dépendre** de :

$$\textbf{Prime Pure} = \alpha_{DCP} \times \beta_{Secteur\ d'activité} \times \gamma_{Zone} \times \textbf{Mesure de dépendance}$$



Les bases de données du Cyber

Privacy Rights Clearinghouse

Vocabulary For Event Recording and Incident Sharing

Toutes les transactions réalisées entre **janvier 2009 et février 2018**

Sophos a réalisé une enquête auprès de **5 000 DSI** pour connaître leurs expériences en matière de **ransomwares**.

Calibration des données

1

Paramétrage du taux de transmission et du taux de guérison

$R_0 = 1.04$

- Utilisation du Bitcoin de *WannaCry* pour estimer β
- Le taux de guérison y est probabilisé selon 3 lois :
  1. ***Loi exponentielle*** : réaction lente.
  2. ***Loi de Weibull*** : *réaction lambda*
  3. ***Loi Log Normal*** : *réaction rapide*
- Paramètres des lois basés sur le nombre d'entreprises assurées

2

Construction de la matrice de proximité des secteurs

$$B = \begin{bmatrix} x & \cdots & y \\ \vdots & \ddots & \vdots \\ w & \cdots & z \end{bmatrix}$$

- La matrice B est le taux de proximité des secteurs d'activité avec $B' = \beta \times B$
- Le coefficient B_{ij} représente le taux de proximité entre le secteur d'activité n°i et le n°j.

3

Estimation des coûts

- Définition d'un **coût** pour chaque secteur d'activité
- Définition du **coût pays.**
- **Multiplication** des 2 **coûts** pour obtenir le **coût moyen** de remédiation d'une attaque par rançongiciel.

4

Création des portefeuilles

- Taille des portefeuilles est de **10000 entreprises**
  1. ***Portefeuille A*** : Il s'agit d'une sous-sélection de la population globale
  2. ***Portefeuille B*** : Répresentatif de la proportion des pays, mais secteurs d'activité uniforme.
  3. ***Portefeuille C*** : *Séléction choisie minutieusement*

Modélisation d'un rançongiciel au sein de 3 portefeuilles

Simulations et résultats

Scénario

Le **taux de guérison** est celle de la loi **exponentielle** : les **entreprises** réagissent **généralement lentement**.

La **durée** de l'épidémie est supposée à **60 jours**

Le **premier infecté** est **unique** (un seul patient zéro) et est **aléatoire**

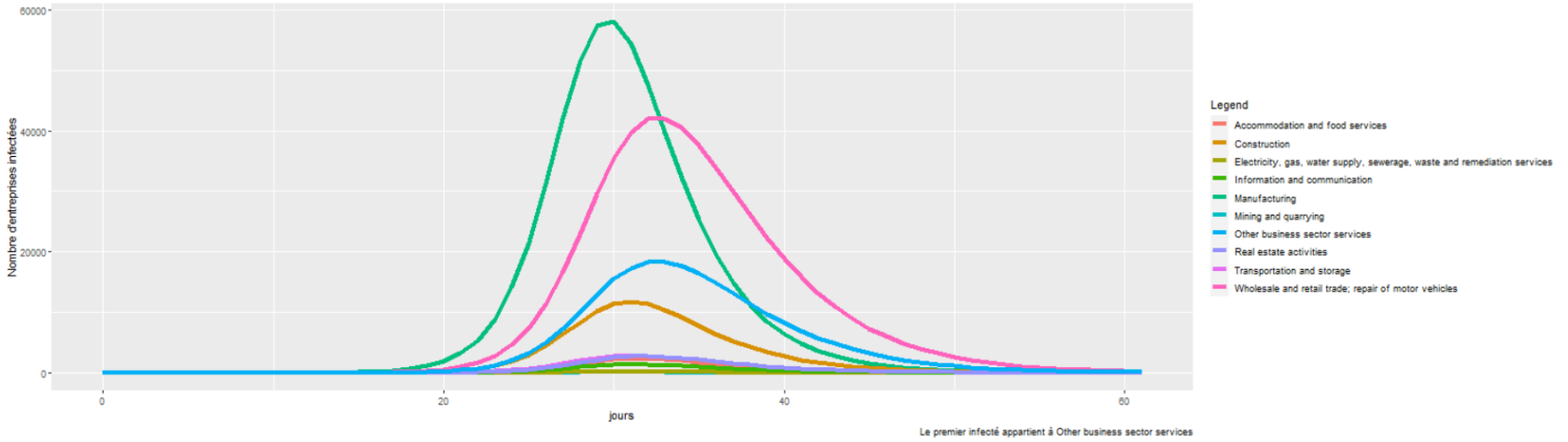


Fig *: Évolution du nombre d'entreprises infectées pour chaque secteur d'activités*

	Portefeuille A	Portefeuille B	Portefeuille C
Min	0,00 €	0,00 €	0,00 €
Moyenne	1 061,52 €	1 187,39 €	297,12 €
Mediane	1 086,19 €	1 012,82 €	287,50 €
Ecart-type	642,68 €	893,73 €	200,34 €
SCR	1 987,01 €	3 691,04 €	795,05 €
Max	2 160,83 €	5 953,35 €	832,88 €

Fig *: Détaille des différentes informations en termes de coût totales des sinistres sur les 50000 simulations réalisées. Le coût est exprimé en millions.*

Modélisation pratique de l'impact d'un événement systémique

Scan externes et données techniques apportées

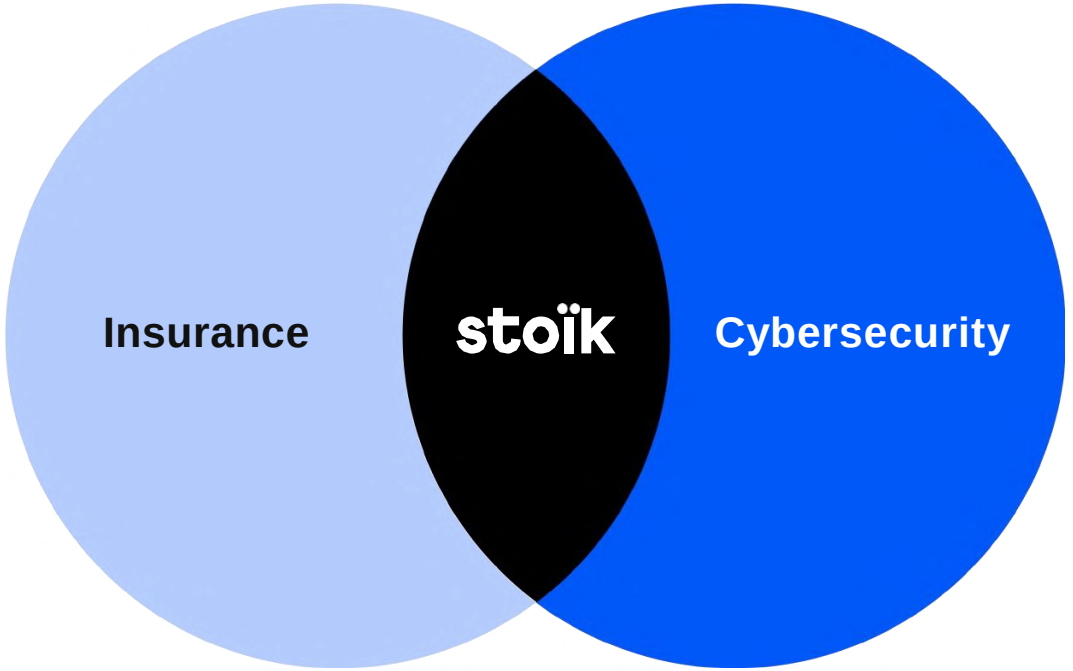
Événement systémique lié à une vulnérabilité vs événement systémique lié à un hébergeur partagé

Modélisation de la sévérité pour une entreprise donnée

Calcul de choc sur un portefeuille

Stoïk

Appréhension pratique du risque systémique



Composante systémique

Les sinistres ne sont pas tous indépendants : ils peuvent être corrélés entre eux.

Les **entreprises d'hébergement ou les MSP** peuvent héberger ou avoir accès aux SI de nombreuses entreprises.

Une **vulnérabilité systémique** affectant plusieurs entreprises en même temps (même cyberattaquant ou non).

Focus sur la composante vulnérabilités

Technologies largement répandues

Certains technologies peuvent être partagées par de nombreux assurés (OS, VPN, E-commerce).

Fréquemment, une vulnérabilité critique impacte l'une de ces technologies.

Exemples : NotPetya, ESXI (23), Citrix (23), Fortinet (23), PaloAlto (24).

Technologie	Assurés concernés
Citrix	>40
Fortinet	>176
Wordpress	>625

Spécificités

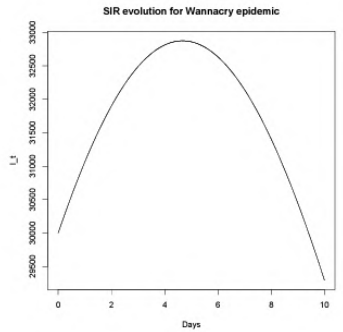
- Patch ou mesures de limitation du risque disponibles quelques heures la parution
- Contamination rapide (généralement 1ou 2 jours avant d'atteindre son plein).
- Des vulnérabilités passées peuvent être exploitées de manière massive bien après leur publication (ESXiArgs, NotPetya).

Timeline WannaCry / NotPetya

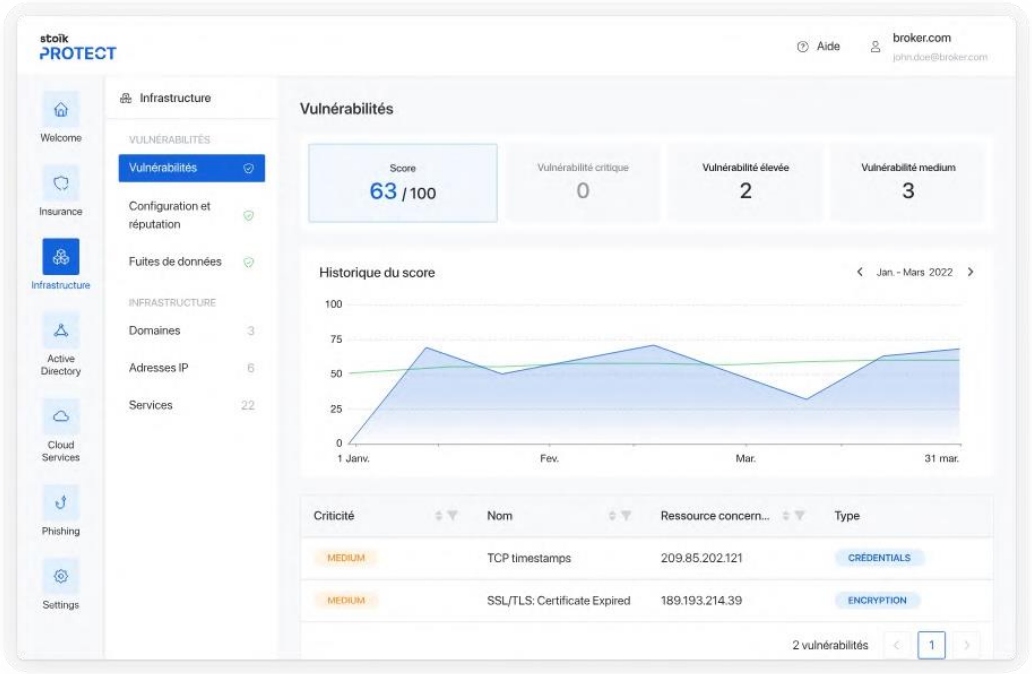
- Microsoft a publié un correctif pour la vulnérabilité EternalBlue en mars 2017.
- Le 12 mai 2017 : Les premiers signes de WannaCry sont apparus en Asie vers 07h00 UTC. En une journée, plus de 200 000 ordinateurs dans 150 pays ont été détruits par le ransomware. La rançon demandée était de 300 €.
- Le 13 mai 2017 :Nouvelle mise à jour de sécurité pour Windows XP, Windows 8 et Windows Server 2003.
- NotPetya commence le 27 juin et avait impacté au moins 2 000 organisations au 28 juin 2017, avec des conséquences financières plus élevées.

Vue CERT et différences par rapport à aujourd'hui

- Equipes CERT furent débordées. Priorité accordée aux entreprises ayant un abonnement CERT.
- Depuis, renforcement des relations entre CERT qui entrainerait une meilleure communication, le partage d'IoC et de l'investigation commune.



Scan externe & calcul de choc



Un audit hebdomadaire de la surface externe du système d'information lancé automatiquement pour détecter les failles de sécurité et les technologies utilisées

domaines →sous-domaines →ip →services + vulnérabilités

techno	Limit (M€)	Estimated Loss (M€)
openvpn	2.25	0.009805
sonicwall-sslvpn-panel	5.50	0.061668
citrix-vpn-detect	3.50	0.112586
ciscovpn	5.10	0.598197
microsoft-exchange	104.35	1.920781
drupal-detect	44.00	2.386368
fortinet-fortigate	64.85	2.568296
cpe:/o:microsoft:windows	350.45	10.211999
Pure-FTPd	404.50	10.754185
wordpress-detect	445.55	12.577808
OpenSSH	678.10	18.026508

Application Stoïk

Comment réduire ce risque et limiter l'exposition du portefeuille ?

Procédure de notification
Biaiser le portefeuille par le pricing
Priorisation des incidents

Mécanismes d'appréhension

Pour l'assureur

1 Sous-limitation du transfert de risque

Mauvaise visibilité côté assuré : son indemnisation dépend de si d'autres entreprises sont touchées. Les vulnérabilités étant globalement utilisées contre plusieurs entreprises, les modalités de prise en charge ne sont pas claires.

2 Notification proactive et priorisation

- Notification des vulnérabilités et aide à la mise en place des patchs.
- Priorisation des incidents par sévérité

Intérêts et inconvénients de l'approche

- Bonne visibilité côté assuré sur la couverture en cas d'incident.
- Pertinence dépend de la bonne réactivité des assurés.

Conclusion