

A large, stylized illustration of bamboo stalks and leaves, rendered in various shades of green, occupies the left side of the slide and extends diagonally towards the center.

WAVESTONE

CYBER-RÉSILIENCE

Plier pour ne pas rompre

CLUSIR Côte d'Azur

06/02/2017

Nicolas VAN-TIEGHEM

nicolas.van-tiegheem@wavestone.com

+33 (0)6 61 64 69 23





Dans un monde où la capacité à se transformer est la clé du succès, nous éclairons et guidons nos clients dans leurs décisions les plus stratégiques



Des clients leaders
dans leur secteur



2,500 collaborateurs
sur 4 continents



Parmi les leaders du conseil
indépendant en Europe,
n°1 en France

Paris | Londres | New York | Hong Kong | Singapour* | Dubaï*
Bruxelles | Luxembourg | Genève | Casablanca
Lyon | Marseille | Nantes

Une capacité unique à combiner expertise sectorielle, connaissance des fonctions de l'entreprise et maîtrise des technologies

FONCTIONS

Stratégie

Management et financement
de l'innovation

Marketing, ventes &
expérience client

People & change

Finance & performance

Operations & logistique

SECTEURS

Banque & assurance

Télécoms & média

Biens de consommation &
distribution

Industrie

Énergie & utilities

Transport & voyages

Immobilier

Secteur public & institutions
internationales

TECHNOLOGIES

Stratégie digitale & SI

Technologies digitales &
émergentes

Architecture SI & data

 **Cybersécurité &
confiance numérique**

Des assets Wavestone exclusifs pour enrichir la valeur de nos prestations



R&K CENTER

Fournir les bonnes informations pour éclairer les décisions



CREADESK

Booster la créativité et générer de nouvelles idées



SHAKE UP

Construire et animer un écosystème d'open-innovation créateur de valeur pour nos clients



THE FAKTORY

Transformer les concepts en réalité tangible



**MACHINE LEARNING
& DATA LAB**

Créer de la valeur à partir des données



Réussir sa transformation numérique grâce à la **confiance numérique**



400+
Consultants
& Experts



1,000+
Missions par an
dans plus de
20 pays



Nos clients
COMEX, Métier,
CDO, CIO, CISO, BCM



UNE EXPERTISE EPROUVEE

- / Stratégie et Conformité
- / Transformation métier sécurisée
- / Architecture et programme sécurité
- / Identité, Fraude et Services de Confiance
- / Tests d'intrusion & Réponse à incident
- / Continuité d'Activité & Résilience
- / SI Industriel



NOS DIFFERENCIEATEURS

- / Connaissance des risques métier
- / Méthodologie AMT pour les schémas directeurs
- / Radars Innovation et Start-ups
- / CERT-W
- / Bug Bounty by Wavestone



WAVESTONE MEDITERRANEE



PACA et Occitanie



4M€ de CA



Expertises de proximité

FDJ | Notariat | RTM | Tisséo | Ministère de l'environnement | EPF PACA
Toulon Provence Métropole | CD83 | GPMM | CHU Toulouse | APMH
Ville de Marseille | Région PACA | SDIS13 | Solimut | Groupe SNI | ...

La résilience, c'est la capacité à revenir dans un état initial après une altération

La résilience au cœur de la continuité d'activité



**Dispositifs de
continuité**



Gestion de crise

Mais l'évolution des menaces cyber
nécessite de **repenser cette résilience**

Objectifs des cyber-attaques

Destruction

Destruction
(massive) de
données

Destruction
(massive) de
postes de
travail

Destruction
(massive) de
serveurs

Utilisation des
canaux de
communication

Atteinte délibérée à l'image

Gain financier / stratégique

Vol de données
clients ou
confidentielles

Modification de
données ou de
paramètres
applicatifs

Transactions /
virements
frauduleux /
rançons

2012



30.000 PC

2013



48.000 PC

2014/2015

75% serveurs



100% PC

2015



12h

2015



2013



>100 PC



2013

2013-2014

> 100m \$



Carbanak

2015



2015



2016



2016



2015



2016



1 site = perte d'image

1 poste = 10 jours

Objectifs des cyber-attaques

Destruction

Atteinte délibérée à l'image

Destruction
(massive) de
données

Destruction
(massive) de
serveurs

Utilisation des
canaux de
communication

Des PCI construits pour la
haute disponibilité et/ou avec un
partage des infrastructures

→ Des **systèmes vulnérables** face
aux menaces actuelles

Gain financier / stratégique

Vol de données
clients ou
confidentielles

Transactions /
virements
frauduleux /
rançons

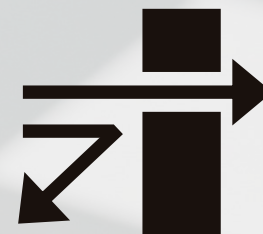
Des scénarios souvent pris en compte (équipe
fraude, gestion des risques...)...

...mais sans intégrer **la perte de confiance
dans le SI générée par les attaques
cyber**

Une cyber-menace est une menace atypique



Une intelligence humaine capable de réagir et de s'adapter



Des actions de défense qui peuvent impacter l'entreprise

Une véritable partie d'échec entre l'entreprise et l'attaquant



Rejouons une partie

Gestion d'une crise cyber chez un grand compte



Interne : 1



CERT 



Jeudi :

Contact en urgence de Wavestone par le RSSI
Mobilisation d'un **first-responder**

3 jours

Mobilisation

Traitement de la crise

Surveillance

Gestion d'une crise cyber chez un grand compte



Interne : 5
Externe : 1



Vendredi :

Découverte d'un malware ciblant spécifiquement
des données métiers critiques

**L'étendue de la compromission semble
large**

3 jours

Mobilisation

Traitement de la crise

Surveillance

Gestion d'une crise cyber chez un grand compte



Interne : 10
Externe : 4



Découverte d'un vol
massif de données



Samedi:

Mobilisation de la **cellule de crise** DG, avec le support de Wavestone et d'avocats
Bascule sur un système de **messaging externe**

3 jours

Mobilisation

Traitement de la crise

Surveillance

Gestion d'une crise cyber chez un grand compte



Interne : 15
Externe : 5



Gestion d'une crise cyber chez un grand compte



Interne : 25
Externe : 10



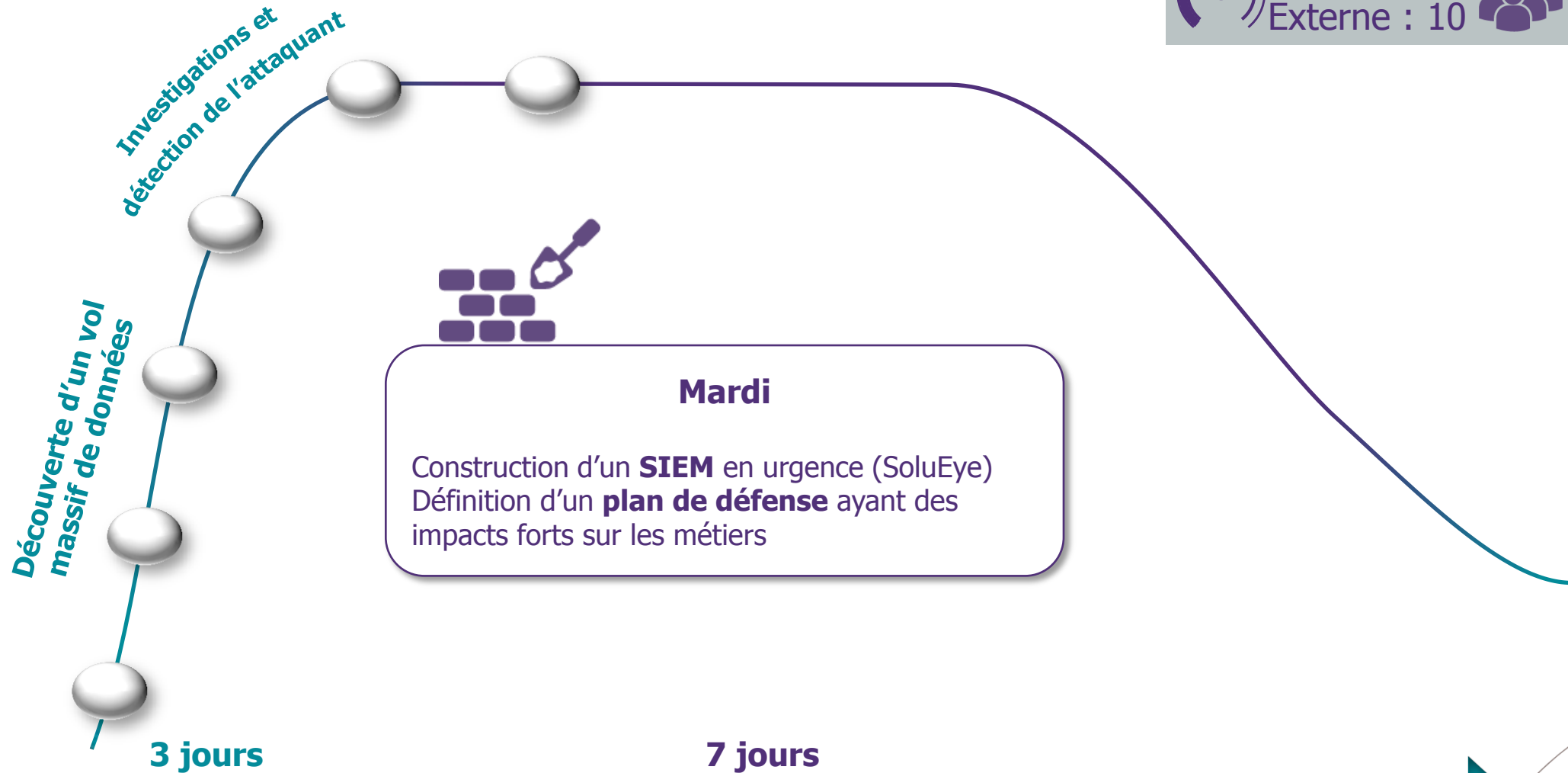
Mobilisation

Traitement de la crise

Surveillance

Gestion d'une crise cyber chez un grand compte

Interne : 25
Externe : 10



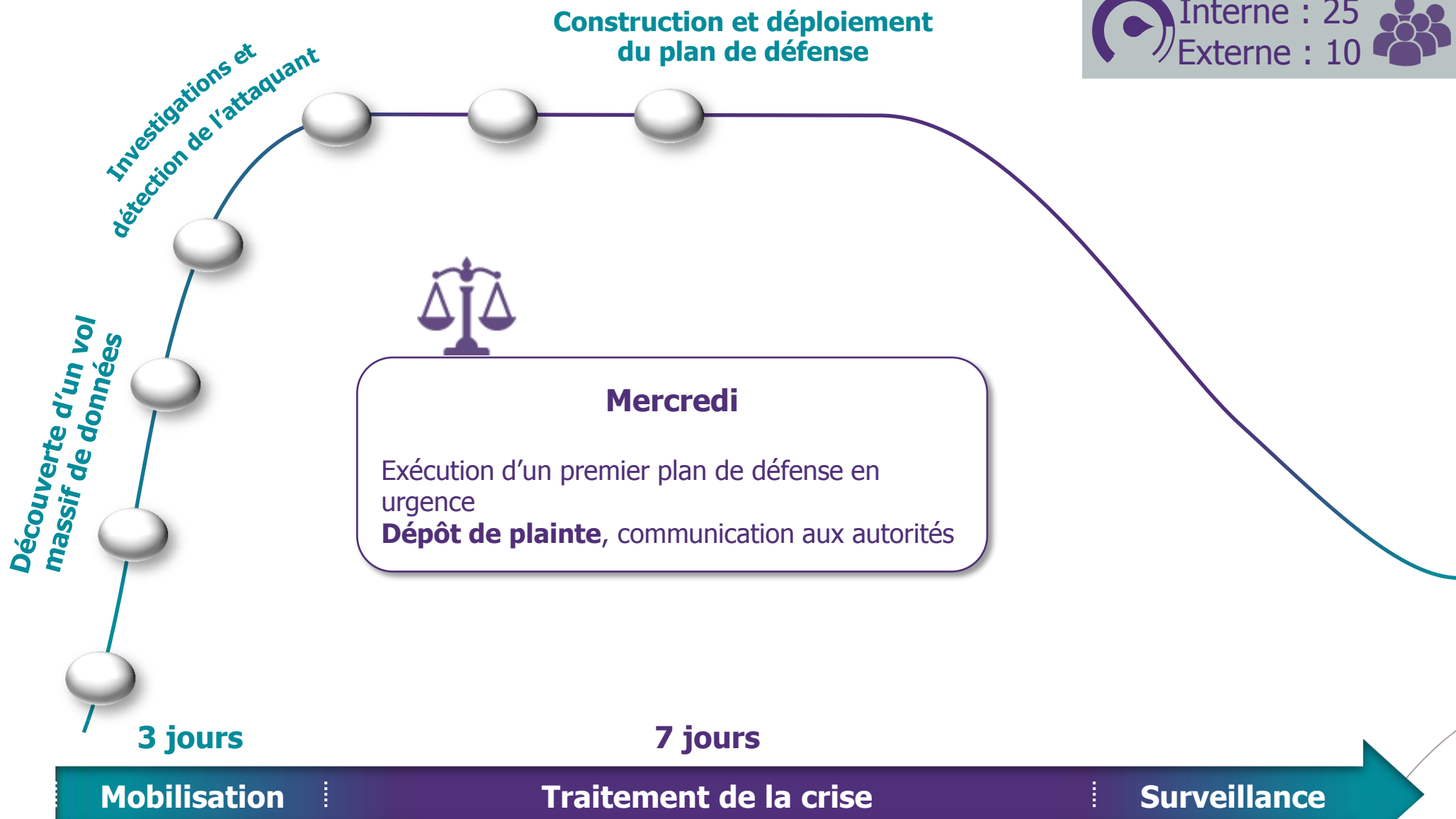
Mobilisation

Traitement de la crise

Surveillance

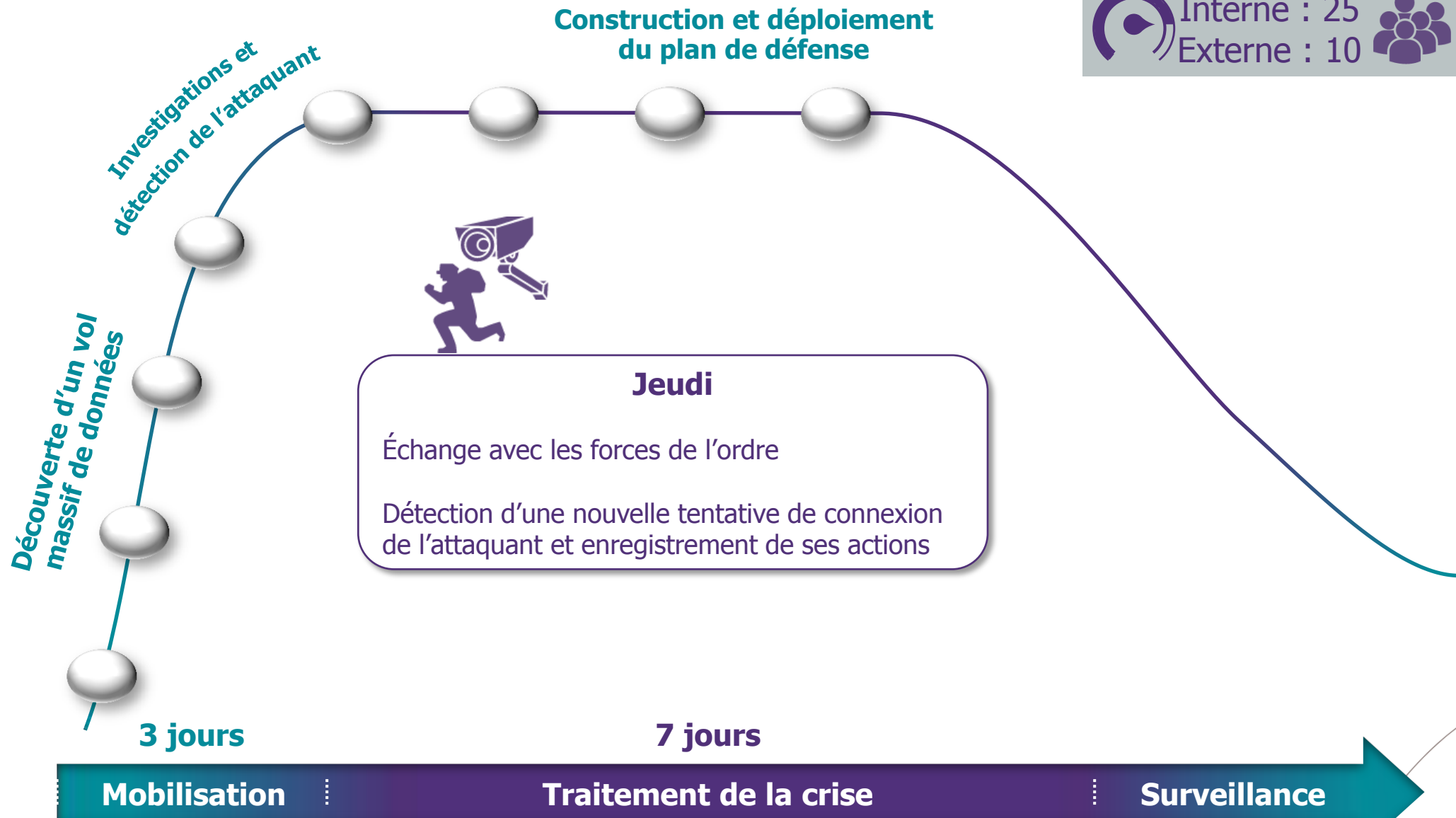
Gestion d'une crise cyber chez un grand compte

 Interne : 25
Externe : 10 



Gestion d'une crise cyber chez un grand compte

 Interne : 25
Externe : 10 



Gestion d'une crise cyber chez un grand compte

 Interne : 15
Externe : 5 



Gestion d'une crise cyber chez un grand compte

 Interne : 15
Externe : 5 



Gestion d'une crise cyber chez un grand compte



Interne : 5
Externe : 2



De nombreuses frustrations mais aussi des points forts

Points forts

Compréhension et mobilisation de la **direction générale** et des métiers

Organisation de gestion de crise bien rodée, mais neuve sur le sujet « cyber »

Perte d'efficacité durant la crise

Absence de traces et capacités d'investigation simple (recherche de marqueurs...)

Absence d'outillage de gestion de crise « de confiance » (messaging, échange de fichiers...)

Difficulté à faire tourner les équipes (compétences rares, envie de rester)

**Gestion
de crise**

Difficultés majeures pendant la crise

Impossibilité d'isoler les applications métiers critiques pour assurer leur continuité

Incapacité à utiliser les systèmes de secours car potentiellement compromis

Incapacité à utiliser les sauvegardes vu l'antériorité de l'attaque

**Dispositif
de
continuité**



Comment renforcer ma cyber-résilience ?

Zoom sur 2 principaux axes

1 Faire évoluer sa gestion de crise

2 Réinventer ses dispositifs de continuité

Et de toutes ces actions, lesquelles prioriser en fonction de leur complexité ?



Zoom sur 2 principaux axes

1

Faire évoluer sa gestion de crise

2

Réinventer ses dispositifs de continuité

Et de toutes ces actions, lesquelles prioriser en fonction de leur complexité ?

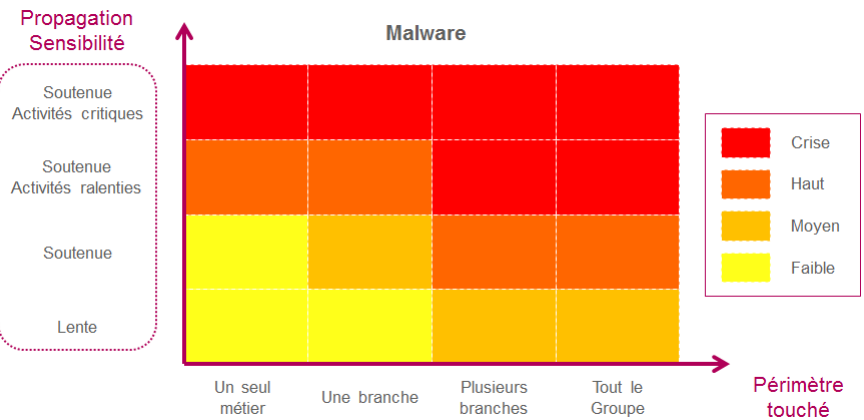


Faire évoluer sa gestion de crise

● Organisation de la cellule

- Savoir identifier et qualifier une crise cyber

Matrice de qualification

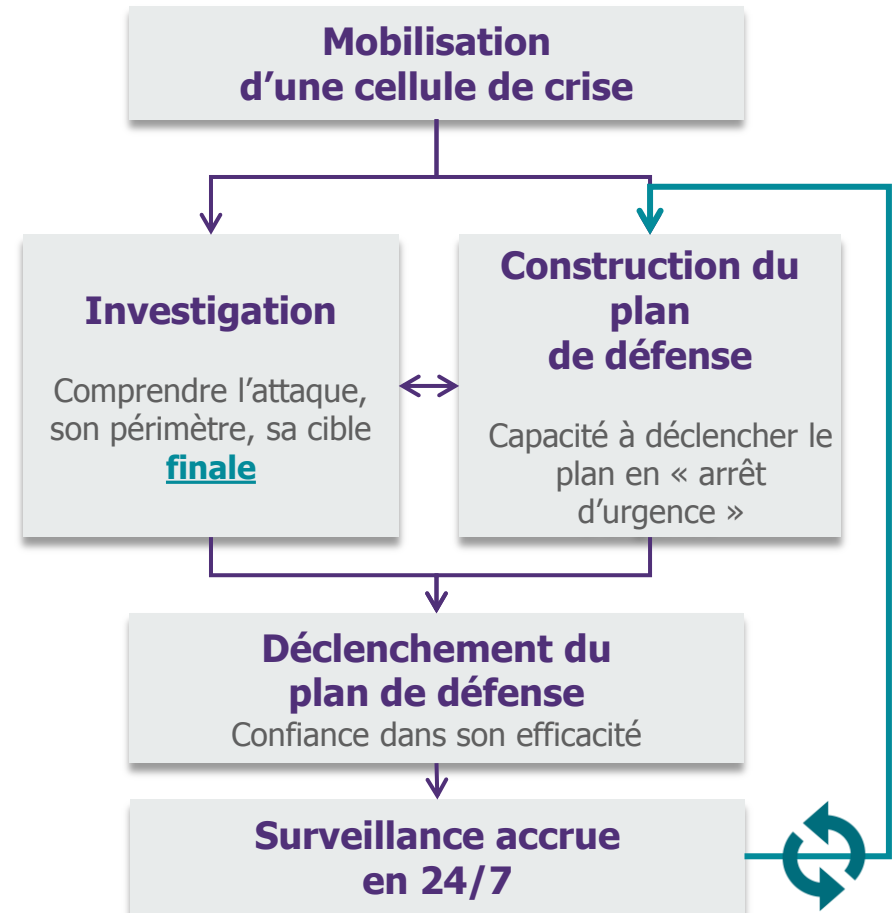


Faire évoluer sa gestion de crise

● Organisation de la cellule

- Savoir identifier et qualifier une crise cyber
- Adopter un processus spécifique pour la gestion de crise cyber

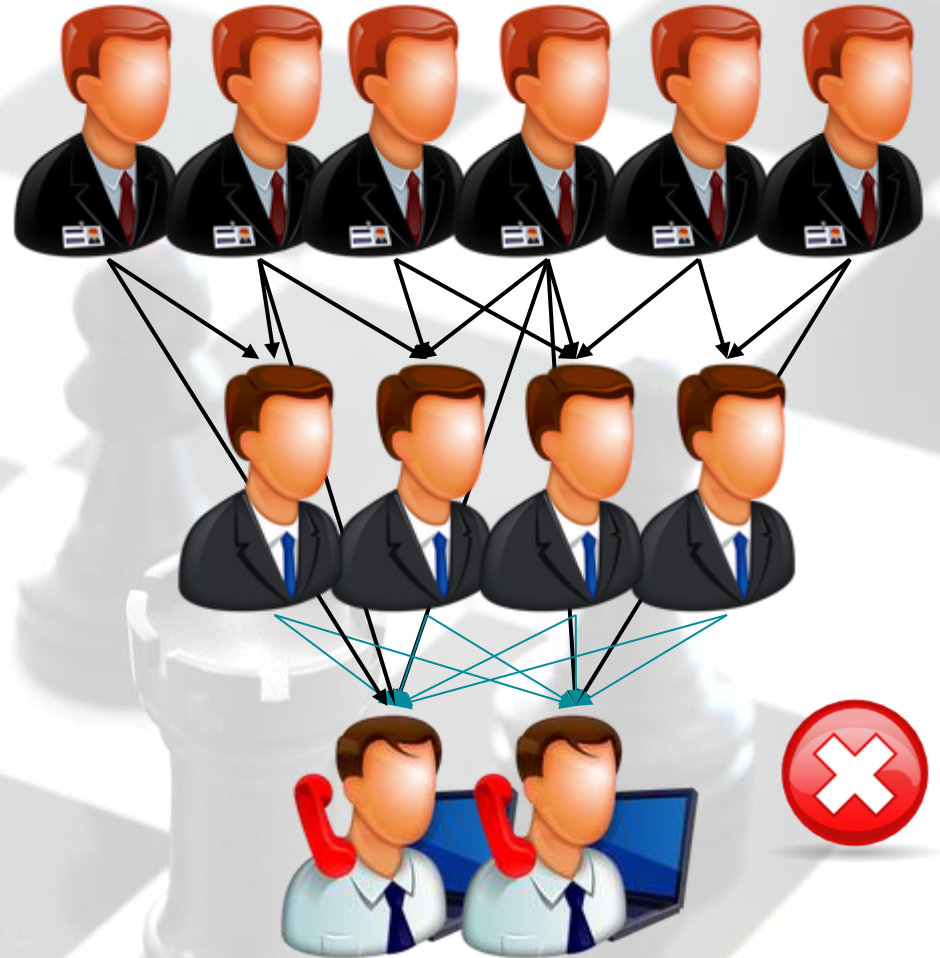
Méthodologie de gestion d'une crise cyber



Faire évoluer sa gestion de crise

● Organisation de la cellule

- Savoir identifier et qualifier une crise cyber
- Adopter un processus spécifique pour la gestion de crise cyber
- Éviter la **pyramide inversée**



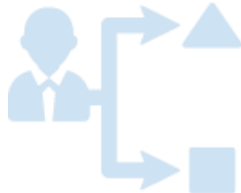
Faire évoluer sa gestion de crise

● Organisation de la cellule



Qualifier

Investigation
Plan de défense



Pyramide
inversée

● Interactions externes

- **Obligation de notification ou d'information** aux autorités voire aux clients (OIV, Télécoms, LIL, ANSSI)
- Savoir **communiquer** sur l'attaque en externe comme en interne avec ses collaborateurs

Faire évoluer sa gestion de crise

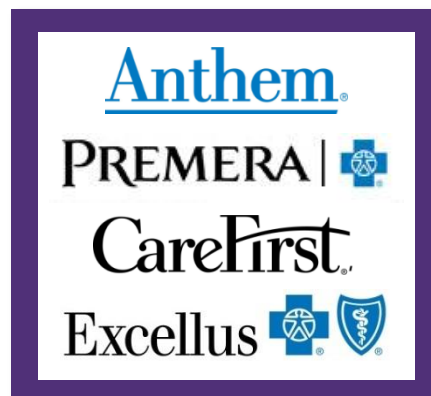
● Organisation de la cellule



● Interactions externes

- **Obligation de notification ou d'information** aux autorités voire aux clients (OIV, Télécoms, LIL, ANSSI)
- Savoir **communiquer** sur l'attaque en externe comme en interne avec ses collaborateurs

Une attaque ne vient jamais seule !



Et certains l'ont
déjà compris ...



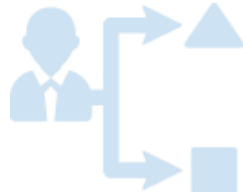
Faire évoluer sa gestion de crise

● Organisation de la cellule



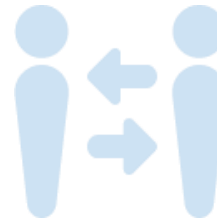
Qualifier

Investigation
Plan de défense



Pyramide
inversée

● Interactions externes



Partage

Notifications



Autorités

● Expertise et outils

- Postes de travail et moyens de communication de crise **sains** (MI6)

Poste de travail / Outils de communication...



Mails, image de référentiel documentaires,...

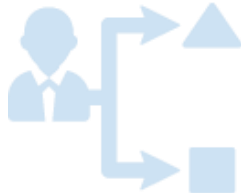
Faire évoluer sa gestion de crise

Organisation de la cellule



Qualifier

Investigation
Plan de défense



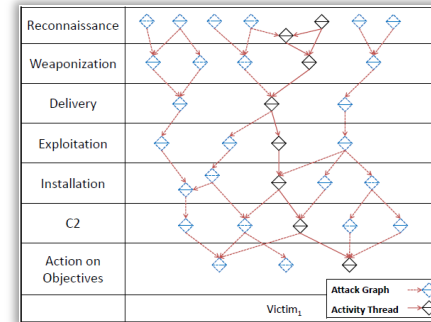
Pyramide
inversée



Expertise et outils

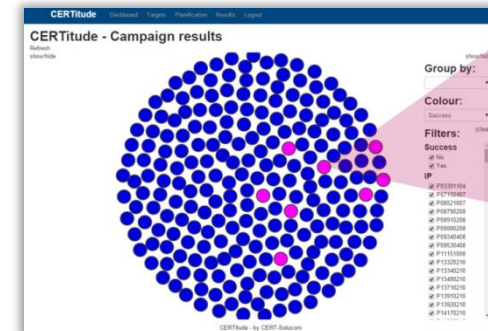
- Postes de travail et moyens de communication de crise **sains** (MI6)
- Compétences **forensics** et **méthodes** de réponse technique

Pilotage des investigations



Diamond Model : Graphe activity-attack

Cartographie de l'attaque



CERTitude

Investigation technique à large échelle

Faire évoluer sa gestion de crise

Organisation de la cellule



Construction du plan de défense

Phase	Detect	Deny	Disrupt	Degrade	Deceive
Reconnaissance	Web analytics	Firewall ACL			
Weaponization	NIDS	NIPS			
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing	
Exploitation	HIDS	Patch	DEP		
Installation	HIDS	"chroot" jail	AV		
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect
Actions on Objectives	Audit log			Quality of Service	Honeypot

Kill Chain Model

- Éradiquer les modes opératoires connus ou supposés
- Anticiper une résurgence

Clean & Restart

- Assainir à minima l'infrastructure et les applications métiers
- Prioriser les périmètres à maintenir en activité ou à redémarrer

Expertise et outils

- Postes de travail et moyens de communication de crise **sains** (MI6)
- Compétences **forensics** et **méthodes** de réponse technique
- Identifier des **marqueurs d'attaques** sur le SI et savoir utiliser la **threat-intelligence**
- Construire et déployer un **plan de défense** incluant la **défense active**

Zoom sur 2 principaux axes

1 Faire évoluer sa gestion de crise

2 Réinventer ses dispositifs de continuité

Et de toutes ces actions, lesquelles prioriser en fonction de leur complexité ?



Réinventer ses dispositifs de continuité

● Stratégies de continuité des activités critiques

- Évaluer les stratégies de secours des **systèmes critiques** face à la menace cyber
- Définir des **nouvelles mesures palliatives** avec les **métiers** et leurs **partenaires**

Réinventer ses dispositifs de continuité

● Stratégies de continuité des activités critiques



Identifier les processus critiques

Mesures palliatives



● Repenser son plan de reprise utilisateur

- Construire un **système alternatif** utilisable sur une clé USB
- Disposer de **matériel disponible** chez les fournisseurs/constructeurs
- Disposer de **bancs de remasteration** rapide
- **Virtualiser** les environnements de travail

Réinventer ses dispositifs de continuité

● Stratégies de continuité des activités critiques



Identifier les processus critiques

Mesures palliatives



● Repenser son plan de reprise utilisateur



Système alternatif

Banc de remasterisation



Virtulisation

Revoir son PCI

- Utiliser le matériel du SI de secours pour **accélérer la reconstruction**

Réinventer ses dispositifs de continuité

Stratégies de continuité



Identifier les processus critiques

Mesures palliatives



Repenser son plan de reprise utilisateur



Système alternatif

Banc de remasterisation



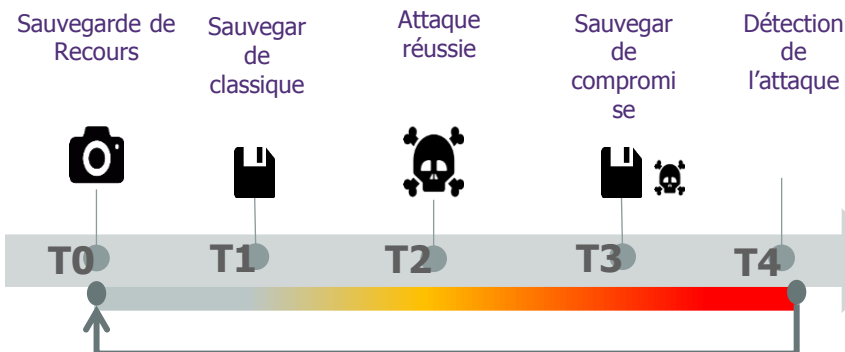
Virtualisation

Revoir son PCI

- Utiliser le matériel du SI de secours pour **accélérer la reconstruction**
- Repenser les **sauvegardes**

Sauvegardes de recours intégrées

Golden point



Réinventer ses dispositifs de continuité

Stratégies de continuité des activités critiques



Identifier les processus critiques

Mesures palliatives



Repenser son plan de reprise utilisateur



Système alternatif

Banc de remasterisation



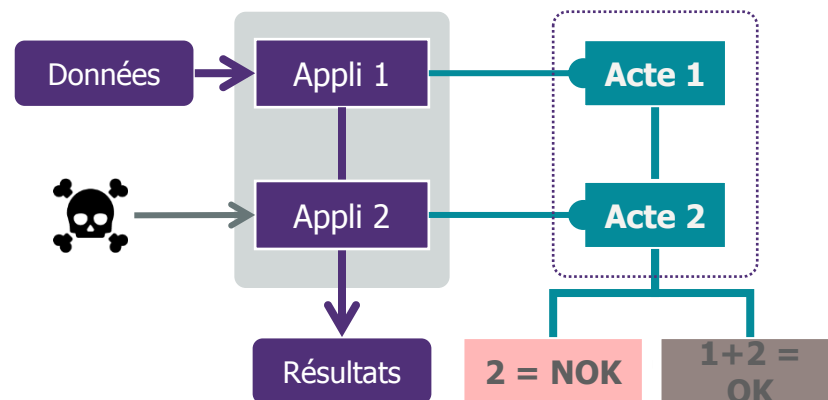
Virtualisation

Revoir son PCI

- Utiliser le matériel du SI de secours pour **accélérer la reconstruction**
- Repenser les **sauvegardes**
- Mettre en place des **contrôles fonctionnels d'intégrité**

Contrôles fonctionnels d'intégrité

Multi-level controls



Réinventer ses dispositifs de continuité

● Stratégies de continuité des activités critiques



Identifier les processus critiques

Mesures palliatives



● Repenser son plan de reprise utilisateur



Système alternatif

Banc de remasterisation



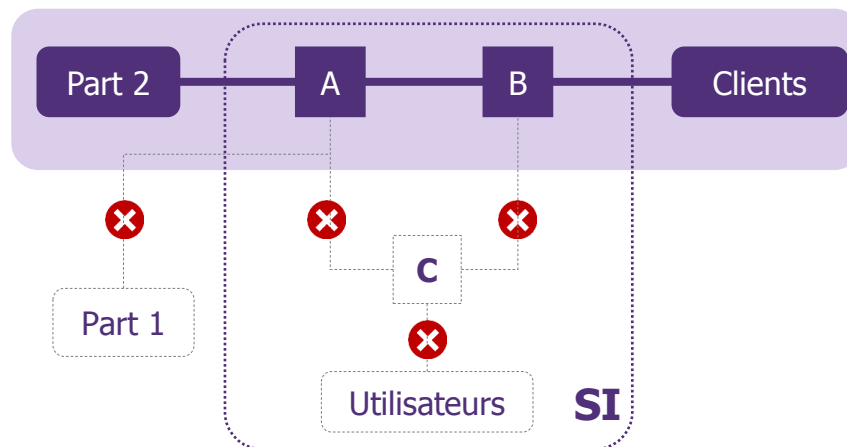
Virtulisation

Revoir son PCI

- Utiliser le matériel du SI de secours pour **accélérer la reconstruction**
- Repenser les **sauvegardes**
- Mettre en place des **contrôles fonctionnels d'intégrité**
- Prévoir une **isolation des systèmes sensibles**

● Isolation des systèmes sensibles

Floodgate



Réinventer ses dispositifs de continuité

Stratégies de continuité des activités critiques



Identifier les processus critiques

Mesures palliatives



Repenser son plan de reprise utilisateur



Système alternatif

Banc de remasterisation



Virtulisation

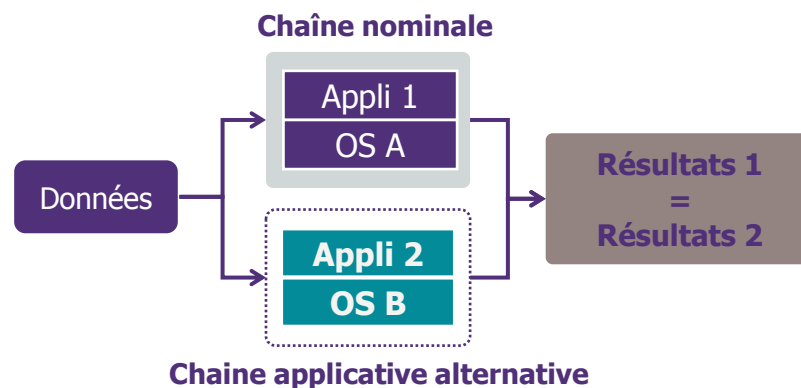
Revoir son PCI

- Utiliser le matériel du SI de secours pour **accélérer la reconstruction**
- Repenser les **sauvegardes**
- Mettre en place des **contrôles fonctionnels d'intégrité**
- Prévoir une **isolation des systèmes sensibles**
- Mettre en œuvre des **chaînes applicatives alternatives**

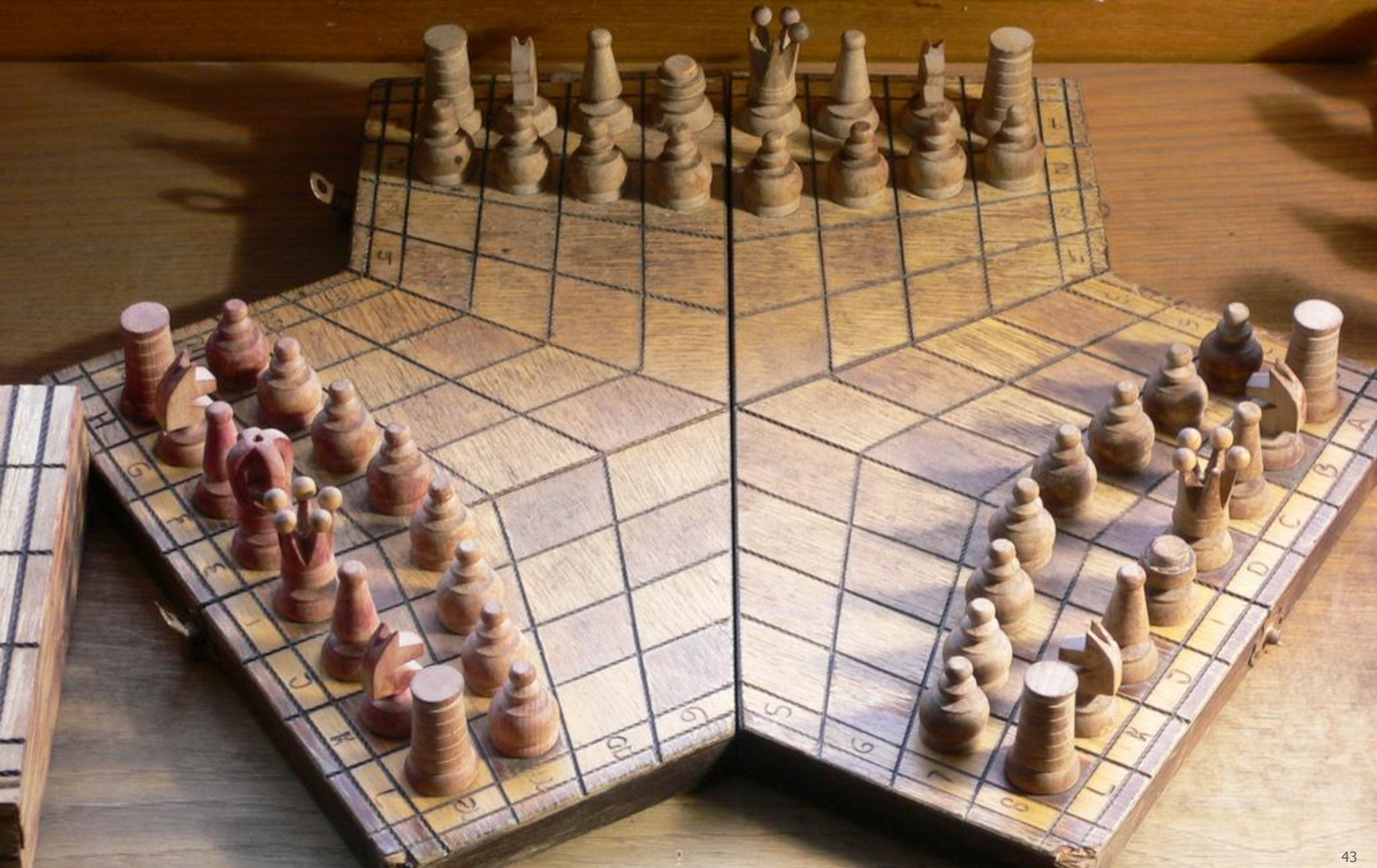


Chaîne applicative alternative

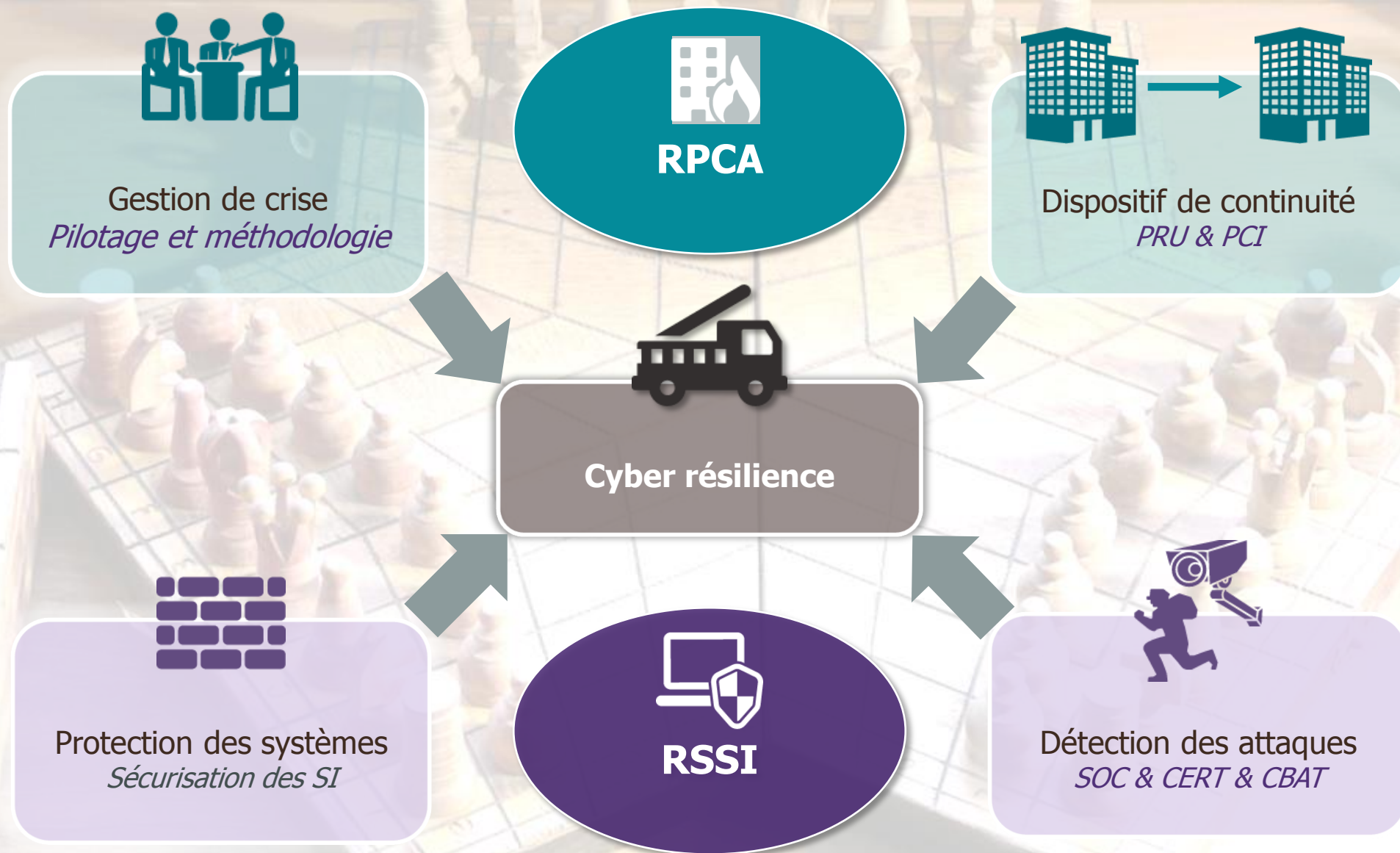
Non-similar facility



Deux cerveaux valent mieux qu'un



La cyber-résilience s'appuie sur les bases de la sécurité



Opérer un rapprochement entre les filières traditionnelles

Concevoir une **stratégie commune**
et **mutualiser** les moyens



Réaliser un **exercice de crise cyber** et un **audit red team** pour évaluer concrètement votre préparation et vos vulnérabilités

WAVESTONE

Nicolas VAN-TIEGHEM

Consultant sénior



M +33 (0)6 61 64 69 23

nicolas.van-tieghem@wavestone.com

Sandra COURPASSON

Manager

Responsable de l'offre cyber-sécurité



M +33 (0)6 75 07 31 39

sandra.courpasson@wavestone.com

Nathalie MELI

Directrice Bureau Marseille



M +33 (0)6 73 19 44 84

Nathalie.meli@wavestone.com

wavestone.com
[@wavestone_](#)

PARIS

LONDON

NEW YORK

HONG KONG

SINGAPORE *

DUBAI *

BRUSSELS

LUXEMBOURG

GENEVA

CASABLANCA

LYON

MARSEILLE

NANTES

**partenaires stratégiques*

WAVESTONE

