Club de la sécurité de l'information français

CLUSIF

Quelle organisation pour la crise, en particulier cyber ?

Damien LACHIVER, WAVESTONE
Animateur au sein de la Cellule d'Animation

Qu'est-ce qu'une crise ?

- Une crise est une situation de trouble, due à une rupture d'équilibre et dont l'issue est déterminante pour l'individu ou la société Dictionnaire ATTILF/CNRS

- Une crise est…
  - Une situation soudaine, souvent brutale, inattendue
  - Aux conséquences potentiellement très grave pour l'entreprise
  - Et pour laquelle les mécanismes et réactions habituels sont inadaptés

- Avec des origines extrêmement variées

- **Naturelles**
  - Inondations, tempêtes, grands froids, épidémies…

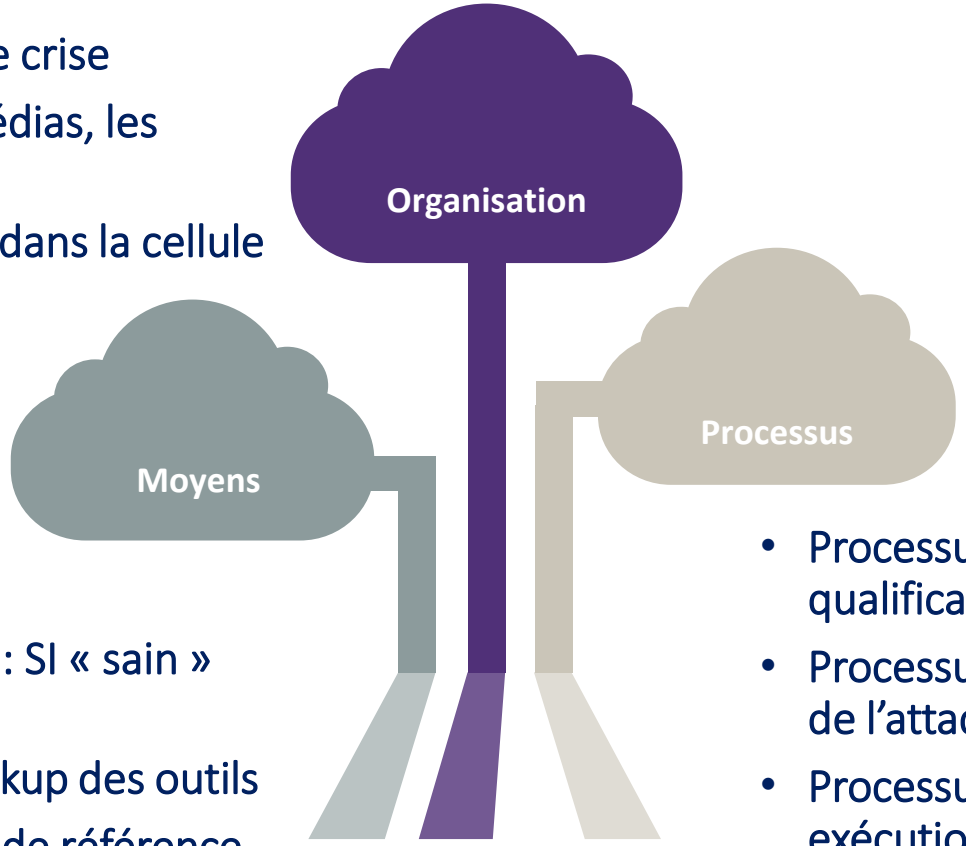
- **Environnementales**
  - Incendies, explosions liées à des sites à risques…

- **Humaines**
  - Défaillance de processus, erreur humaine, malveillance, attentat…

- **Technologiques**
  - Panne informatique, défaillance matérielle, virus, cyber-attaque…

Quels dispositifs pour y répondre ?

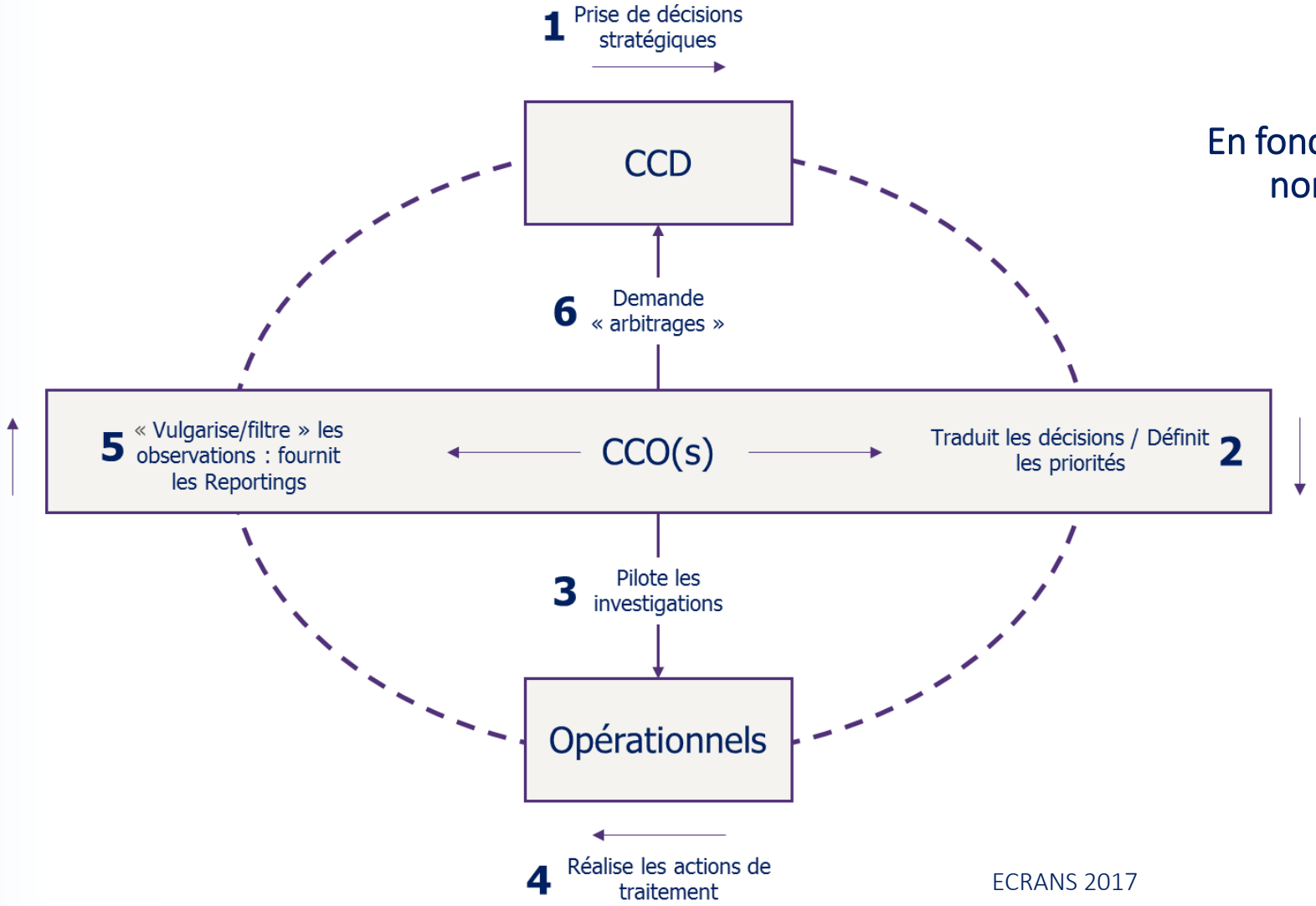
- Prise de décisions
- Organisation de la cellule de crise
- Communication avec les médias, les partenaires, les clients…
- Inclusion des acteurs cyber dans la cellule de crise



- Moyens de communication : SI « sain » de crise
- Moyens de traitement : backup des outils
- Informations et documents de référence

- Processus de déclenchement : qualification de l'incident cyber
- Processus de traitement : compréhension de l'attaque et préparation de la défense
- Processus de réaction : planification et exécution du plan de défense

Quelle organisation pour gérer une crise ?



En fonction de la taille de l'organisation, le nombre et le type de cellules peut fortement varier

Quels rôles propres au fonctionnement d'une cellule de crise ?

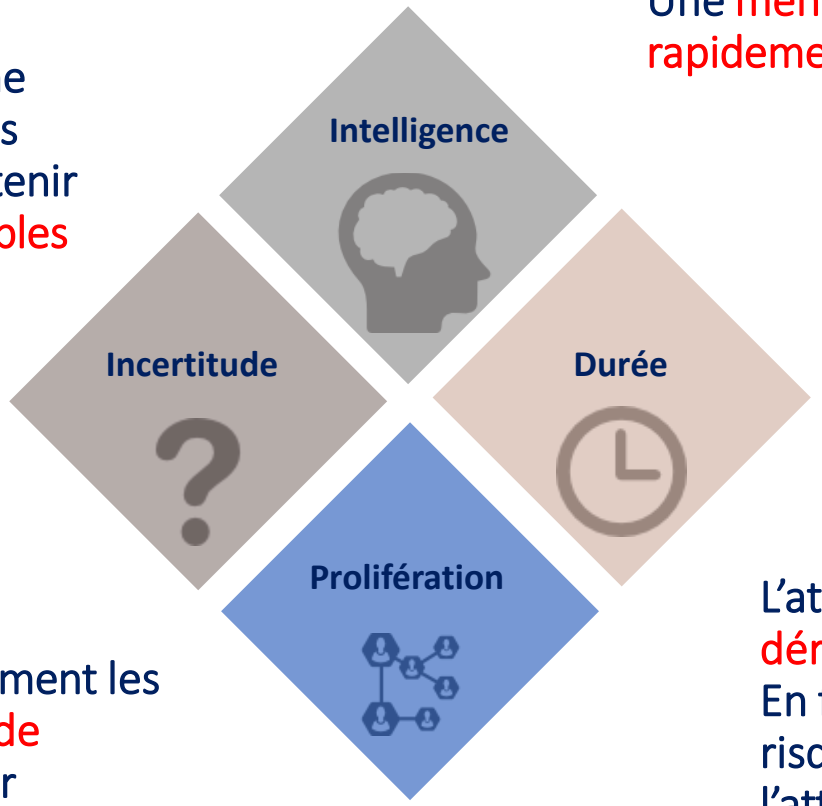
- Directeur de crise
  - Piloter la cellule et la réponse à la crise
  - Réaliser les arbitrages lorsque cela est nécessaire
  - Donner le rythme de la cellule
  - Faire le lien avec les autres parties prenantes de l'organisation

- PMO
  - Produire la main courante pour garder une traçabilité des actions et décisions
  - Formaliser les points de situations et plans d'action et les diffuser à ses homologues

- Conseiller de crise
  - Apporter un point de vue d'expert à la cellule
  - Prendre de la hauteur sur les évènements unitaires
  - Anticiper les évènements à venir

Quelles spécificités à prendre en compte pour les crises cyber ?

Face à la complexité d'un système d'information et à la diversité des menaces, il est très difficile d'obtenir rapidement des informations fiables sur l'attaque en cours et les motivations de l'attaquant



Une menace intelligente qui peut s'adapter rapidement aux réactions de l'organisation

Les attaquants utilisent généralement les réseaux et les nouveaux canaux de communication pour se propager largement au sein d'une organisation

L'attaquant, en général bien préparé, déroule un plan d'attaque très rapidement. En face, si l'entreprise est peu préparée, elle risque de répondre trop tardivement à l'attaquant et d'être dépassée par la menace

Quel bilan pour l'exercice ECRANS 2017 ?

- Des forces portées par de bons réflexes de gestion de crise et de connaissances cyber…

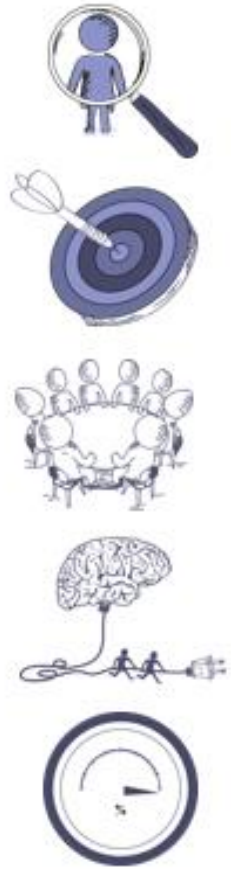
  - Les cellules se sont immédiatement organisées
  - Les participants ont définis clairement et respecté leurs périmètres de responsabilité
  - De bons réflexes en temps de crise sont partagés au sein des cellules : vérifier les identités, ne pas communiquer sans validation…

- Et des pistes d'amélioration pour corriger quelques points

  - Un manque de recul sur la situation globale et d'anticipation notamment en l'absence de partage centralisé de l'information au sein des cellules
  - Une désorganisation ponctuelle quand le responsable de la cellule doit s'absenter
  - Un manque de structure dans la prise de décision qui nuit à la prise en compte des aspects métiers

Les bons réflexes à respecter dans une crise cyber

1. Identifier Directeur, PMO et conseiller (et leurs backups !) et organiser la logistique de crise
2. Structurer, tracer et partager les décisions au sein de la cellule
3. Prendre le temps d'identifier les impacts de décisions
4. Prendre du recul et se mettre dans la peau de l'attaquant
5. Maitriser sa communication et rester discret sur la stratégie de défense



Se préparer et s'organiser en amont !

1. Formaliser et organiser		Définir et formaliser le processus et l'organisation de gestion de crise cyber du Groupe et des filiales
2. Monter en expertise		Identifier et impliquer des professionnels experts de la gestion de crise et du cyber
3. Tester les dispositifs		Tenir régulièrement des exercices de gestion de crise