De la Menace à la Résilience : Un programme de réponse aux incidents stratégique et opérationnel

WHOAMI

Patrick Pilotte

https://www.linkedin.com/in/ppilotte/

- Expert chevronné en cybersécurité avec plus de 20 ans d'expérience en administration de serveurs et en sécurité informatique.
- Gestionnaire de la sécurité de l’information, responsable de la sécurisation des infrastructures critiques.
- Détenteur de la certification Certified Incident Responder (eCIR).
- Formateur et animateur d’ateliers reconnus, notamment à ITSEC et SecTor.
- Passionné par le transfert de connaissances et la formation des professionnels en cybersécurité.

WHOAMI

- Spécialiste en sécurité opérationnelle avec près de 10 ans d’expérience en TI.
- Analyste en sécurité chez Devolutions, responsable de la surveillance et de la réponse aux menaces en environnement de production.
- Actuellement en formation spécialisée en cybersécurité et analyse opérationnelle à Polytechnique Montréal.
- Expérience concrète en détection, réponse aux incidents et en durcissement d’environnements Microsoft 365 et Linux.
- Impliqué dans la gestion forensic et la reprise d’opérations lors d’au moins cinq incidents de sécurité majeurs.

Michaël Grenier-Doucet

https://www.linkedin.com/in/michaël-grenier-doucet-1696abb6/

Objectif de l’atelier

🧠 **Comprendre**

Les fondations d’un programme de réponse aux incidents (IRP) stratégique et opérationnel

⚠️ **Identifier**

Les menaces actuelles et leur impact sur la continuité et la résilience

📐 **Structurer**

Un plan de réponse cohérent, aligné avec la gouvernance de ton organisation

🤝 **Collaborer**

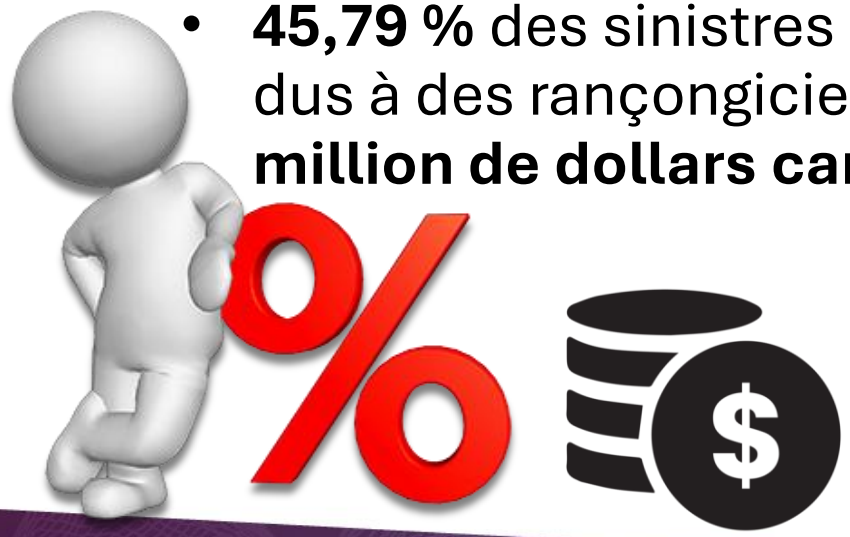
Partager des expériences et repartir avec des actions concrètes à implanter

💼 **Outils**

Partage d’outils pour démarrer ou améliorer votre gestion d’incident

Pourquoi investir dans la réponse aux incidents?

- **56 %** des entreprises canadiennes ont été touchées par une cyberattaque réussie en 2024. – Rapport sur l'état de la cybersécurité au Canada, Terranova Security + Cybereco, 2024
- Les dépenses totales engagées pour le rétablissement des activités à la suite d'incidents de cybersécurité ont doublé, passant de **600 millions de dollars en 2021** à **1,2 milliard de dollars en 2023**. – Statistique Canada
- **45,79 %** des sinistres liés à la cybersécurité dans les PME canadiennes sont dus à des rançongiciels, avec un coût moyen par incident d'environ **1,34 million de dollars canadiens.** – Gascon & Associées S.E.N.C.R.L.



«L'avenir ne se prévoit pas, il se prépare. »
Maurice Blondel, Philosophe
1861 / 1949

Pourquoi un programme IRP est essentiel

- **Réduire** l'impact des incidents
  - Financier (pertes, interruption)
  - Légal (amendes, poursuites)
  - Réputationnel (perte de confiance)
- **Renforcer** la résilience organisationnelle
  - Capacité de réponse rapide
  - Adaptabilité aux menaces changeantes
  - Culture de gestion de risques
- **Se conformer** aux exigences (ex: RGPD, ISO)
  - Exigences clients et partenaires
  - Réponses aux audits et certifications

Executive Summary | Maturité CIS /CSC

Réactif

Stratégique

Niveau 1 – Basique

L'attention en matière de sécurité est au niveau tactique. Les risques liés à un incident de cybersécurité sont graves.

Niveau 2 – Standardisé

L'attention en matière de sécurité est au niveau proactif. Les risques liés à un incident de cybersécurité sont significatifs.

Niveau 3 – Rationalisé

L'attention en matière de sécurité est au niveau opérationnel. Les risques liés à un incident de cybersécurité sont modérés.

Niveau 4 – Dynamique

L'attention en matière de sécurité est au niveau stratégique. Les risques liés à un incident de cybersécurité sont mineurs.

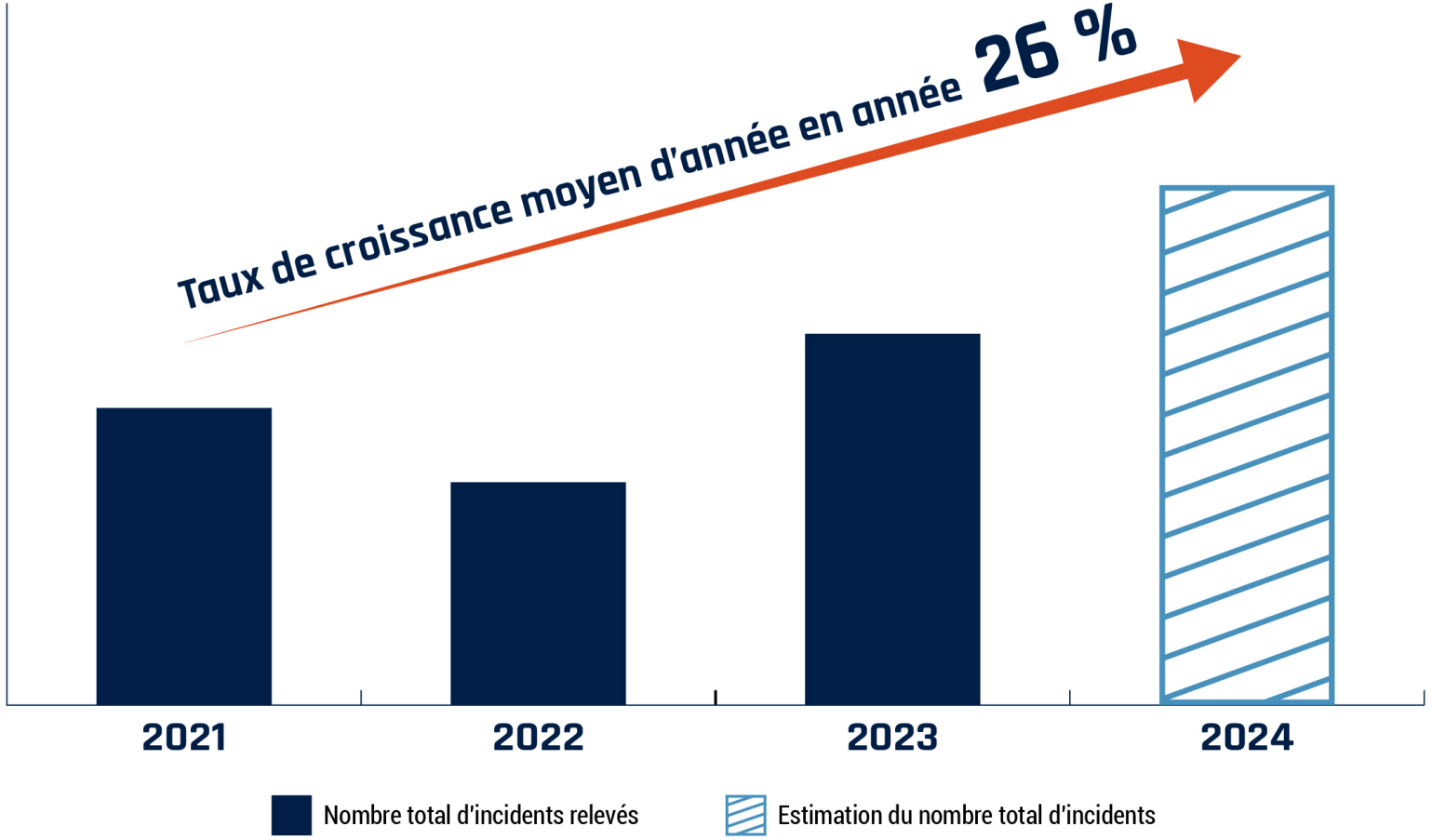
Que pouvons nous considérer comme un incident

Un Incident est déclaré comme tel lorsque l'un ou plusieurs des critères suivants survient ou est suspecté:

- **Confidentialité:** Les informations sensibles ne sont accessibles qu'à ceux qui ont le droit de les consulter.
- **Intégrité:** L'information est fiable et inchangée par rapport à son état d'origine.
- **Disponibilité:** Les informations sont facilement disponibles pour les utilisateurs autorisés quand ils en ont besoin.

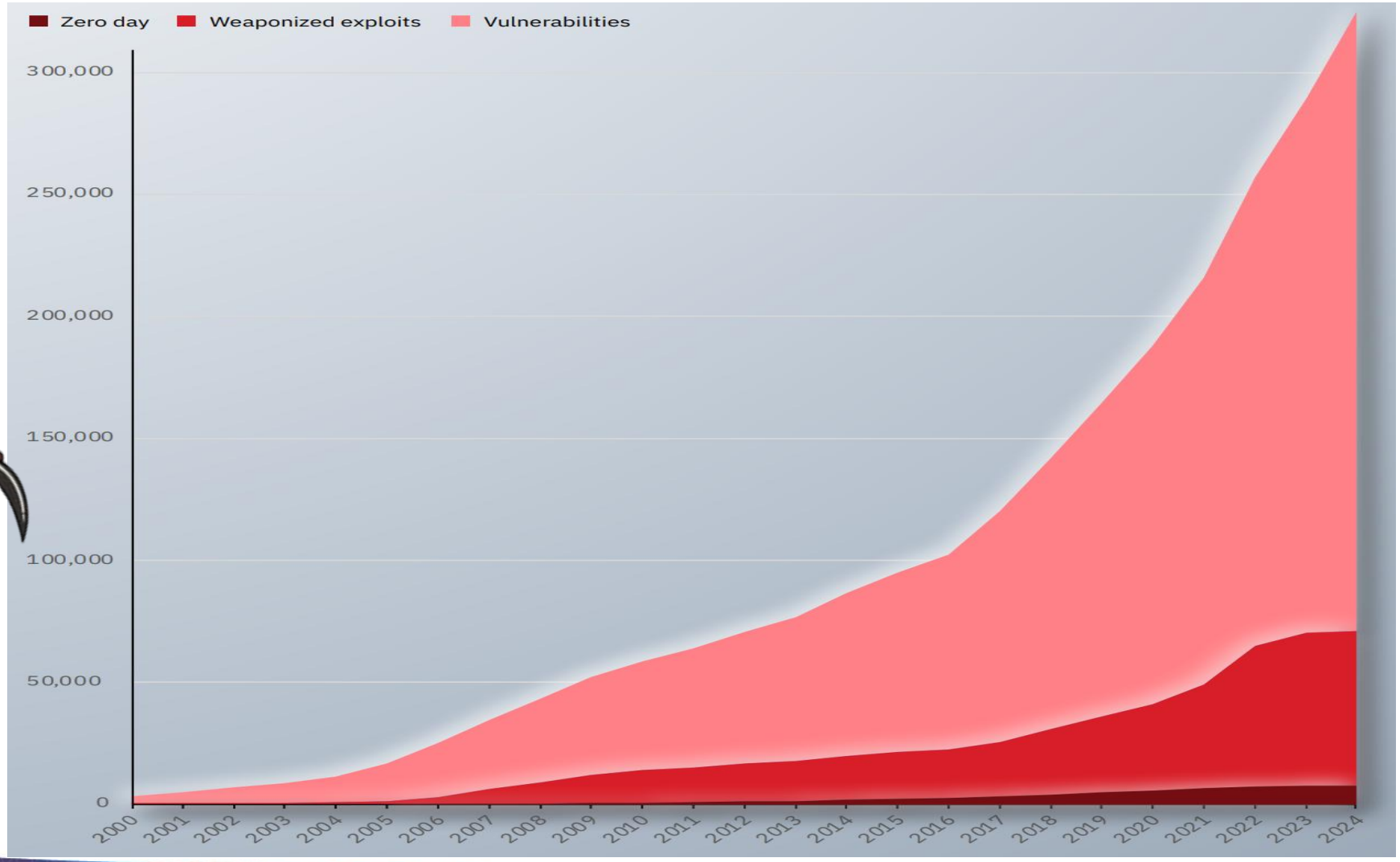
Les menaces actuelles et leur impact

Croissance relative depuis 2021 du nombre d’incidents liés à des rançongiciels au Canada connus du Centre pour la cybersécurité



Centre canadien pour la cybersécurité. Évaluation des cybermenaces nationales 2025-2026

Croissance des vulnérabilités, des exploits et des failles zero-day



IBM X-Force 2025 Threat Intelligence Index

Identifier L’impact d’un incident

Niveau de sévérité	Performance	Réputation / Image	Opérations / Capital Humain	Finances
Critique	Rend impossible l’atteinte de l’objectif Met la survie de l’entreprise en péril Touche plus de 35% des effectifs de l’entreprise	Impact irréversible ou à très long terme sur notre réputation, notre croissance, et la confiance de nos clients et partenaires Effets irréversibles ou à long terme, malgré la mise en place de mesures correctives Touche plus de 35% des clients de l’entreprise	Impact irréversible ou à très long terme sur notre capacité à opérer ou à maintenir la disponibilité de nos produits, ou notre capacité à conserver ou attirer des employés de talent	Plus de 10M$ en pertes ou dommages, ou dommages très élevés difficilement quantifiables

Bâtir un plan d’intervention

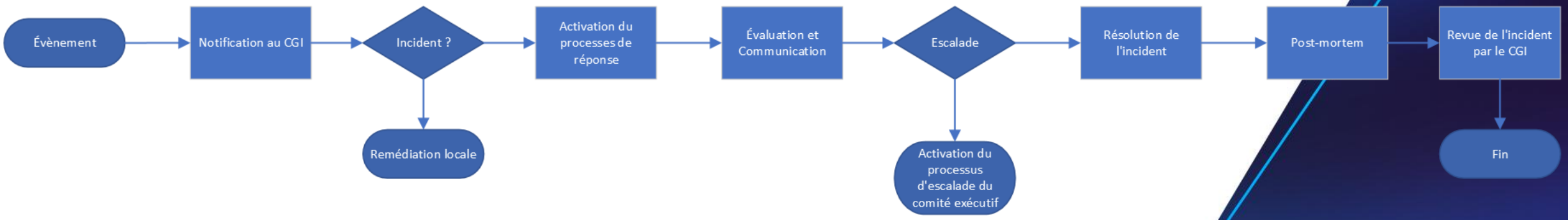
Avant	Pendant	Après
1. Définir les rôles et responsabilités 2. Documenter les politiques et procédures 3. Former les équipes et sensibiliser les utilisateurs 4. Mettre en place les outils de détection et de communication	1. Détection : identifier rapidement l’événement 2. Analyse : comprendre la portée et les causes 3. Containment : isoler et limiter la propagation 4. Éradication : supprimer la menace 5. Rétablissement : restaurer les systèmes affectés	1. Conduire un post-mortem 2. Identifier les améliorations possibles 3. Mettre à jour les playbooks et politiques 4. Communiquer les leçons apprises aux parties prenantes

Un plan de réponse n’est utile que s’il est compris, appliqué et évolutif.

Définir les rôles et responsabilités

- Comité de gestion d’incident
- Gestionnaire d’incident
- Équipe de réponse
  - Administrateur système
  - Analyste en sécurité
  - Chasseur de menace
  - Spécialiste forensic
  - Spécialiste réseau
  - Partenaire externe
  - Etc.
- Affaires légales
- Communications

Processus



- **Évènement** détecté dans l'environnement
- **Notification** au CGI (Comité de gestion d'incident)
- **Vérification** : Incident ou faux positif ?
- **Évaluation** & Communication auprès des parties prenantes
- **Escalade** si impact critique → Comité exécutif activé
- **Résolution** de l'incident (technique ou organisationnelle)
- **Post-mortem** pour tirer des leçons
- **Revue** par le CGI pour mise à jour des politiques et plans

Transformer les incidents en leviers

Résumé de l'incident : nature, moment, contexte

Chronologie : déroulement précis des événements

Impact : systèmes affectés, pertes, implications métier

Détection : comment l'incident a été découvert

Réponse : actions entreprises, coordination des équipes

Récupération : restauration des services et vérifications

Cause profonde : analyse RCA (Root Cause Analysis)

Enseignements : ce que l'on a appris

Actions correctives : techniques, organisationnelles, humaines

Les 5 règles pour une analyse post mortem sans blâme, efficace et efficient.

1. Être planifiée le plus tôt possible après la phase de RÉCUPÉRATION
2. Inclure les participants directs ayant participés au traitement de l'incident
3. Inclure, de façon facultative, les membres de la direction pertinents
4. Identifier des actions correctives réalisables à court terme et proportionelles à l'impact de l'incident
5. Formuler une action corrective autrement que d'une manière qui suppose qu'un individu ou une équipe fera mieux la prochaine fois.

Passer à la résilience

🛡️ **Anticiper**

Cela réduit la probabilité et la gravité des incidents.

🪲 **Résister**

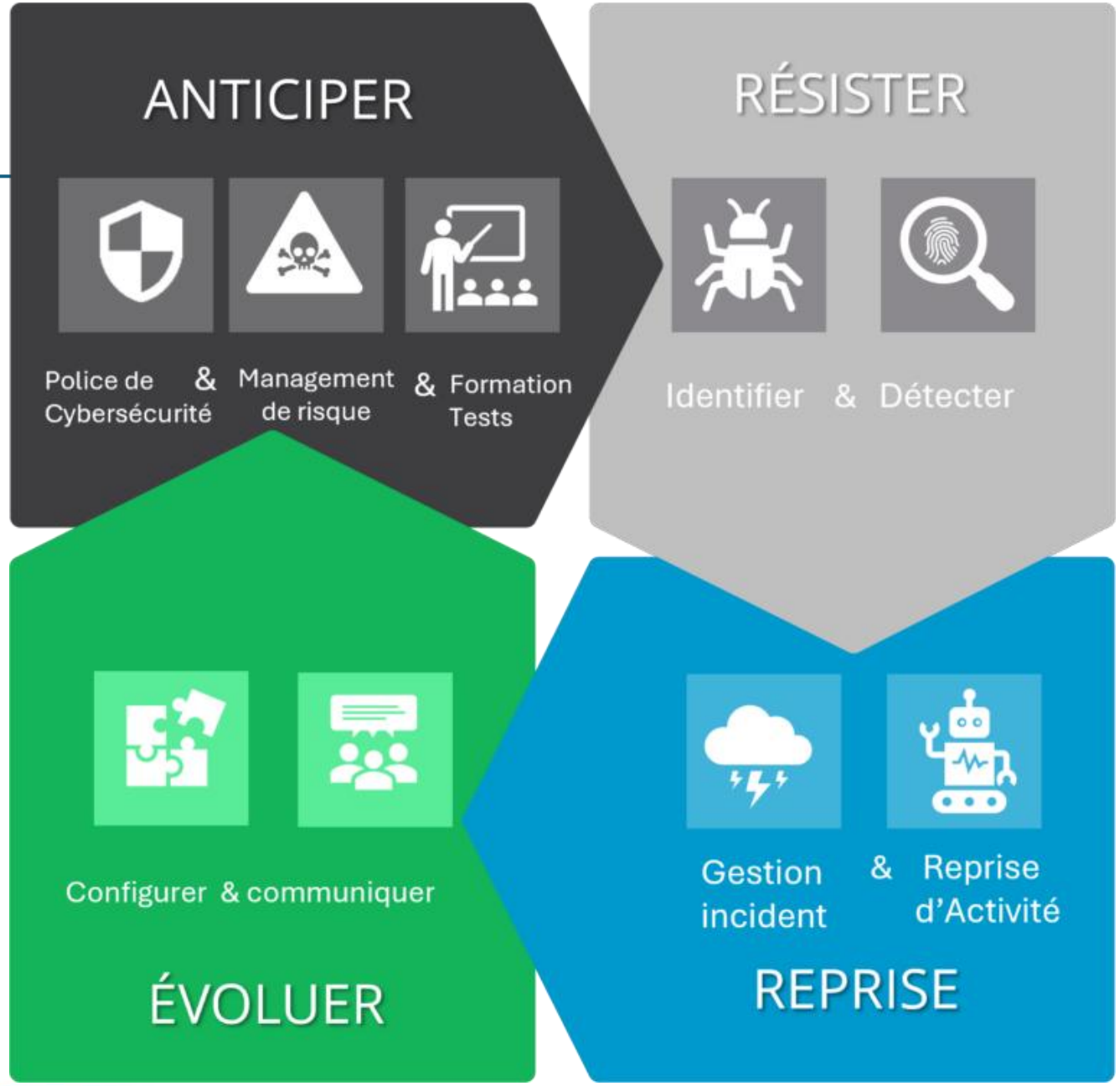
La vitesse de détection est clé dans le MTTR.

🌩️ **Reprise**

Cela démontre la maturité du programme IRP.

📈 **Évoluer**

Une organisation résiliente apprend, s’adapte et s’améliore en continu.



Cas pratiques – mon vécu en tant que membre de l’équipe de réponse

MSP

Restauration opérationnelle

Durcissement des systèmes

Consultant externe

Récolte d’évidences

Durcissement des systèmes

Spécialiste OpSec

Analyse préliminaire

Confinement

Récolte d’évidences

Synthèse & Conseils clés

Ce ne sont pas les incidents qui définissent votre organisation, mais la façon dont vous y répondez.

Résumé en 3 actions concrètes :

- ✔ Clarifier les rôles et responsabilités
- ✔ Développer et tester un playbook
- ✔ Organiser un exercice de simulation

- ❖ Un programme IRP efficace repose sur l'équilibre entre stratégie et opérationnel
- ❖ La préparation en amont conditionne la qualité de la réponse
- ❖ La rapidité de détection et de coordination est cruciale pour limiter les impacts
- ❖ Chaque incident est une opportunité d'apprentissage
- ❖ La résilience se construit par l'amélioration continue et l'engagement de toute l'organisation

Questions & Réponses

Documentation disponible avec le code QR