Cybersécurité – réponse aux incidents

AUTEUR : DELAUTRE BENJAMIN

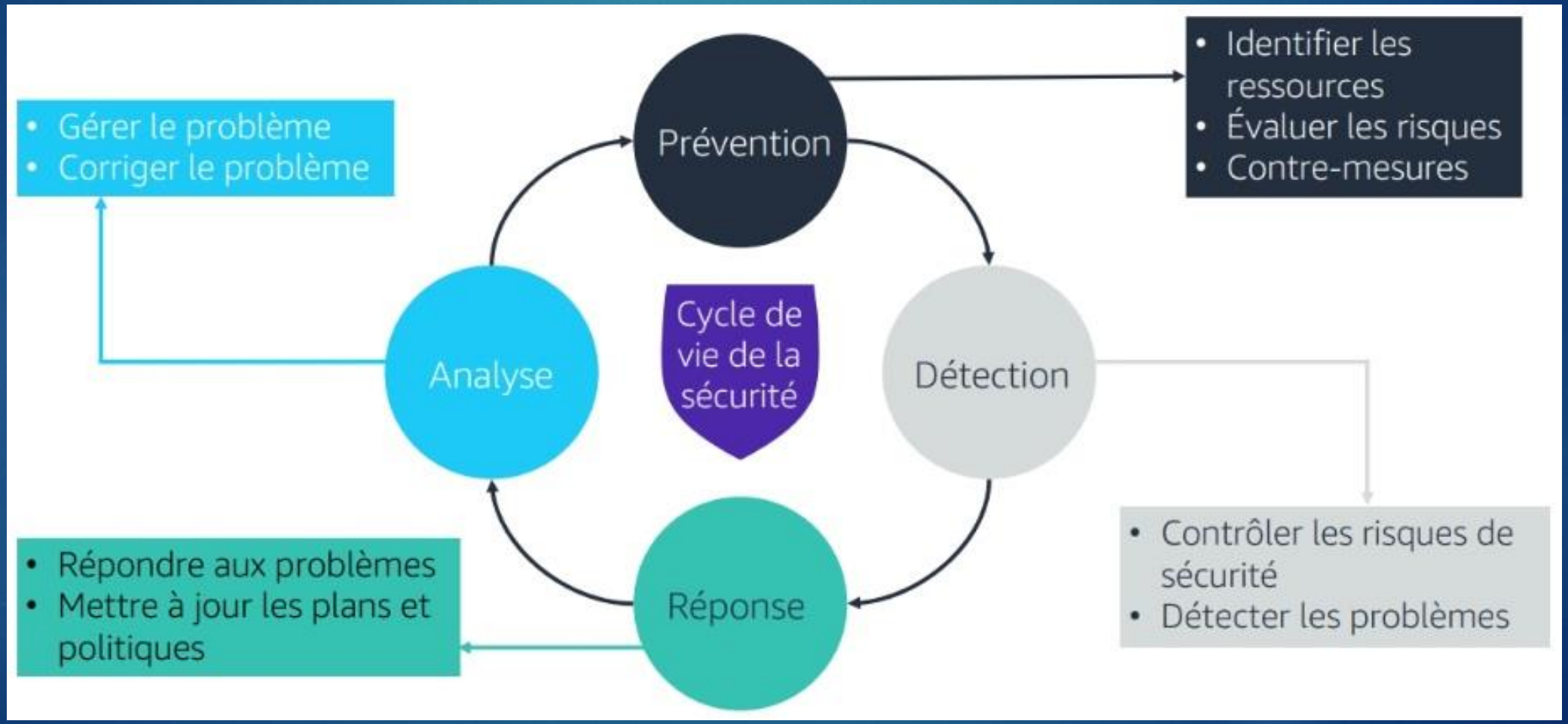
Qu’est-ce que la cybersécurité ?

- Définition :

« La sécurité informatique, ou cybersécurité, consiste à protéger les ordinateurs, les réseaux, les programmes et les données contre tout accès, modification ou destruction involontaire ou malveillant. La cybersécurité consiste également à **garantir que les fonctions** professionnelles **et les tâches** personnelles **peuvent toujours être exécutées avec un minimum d’interférences à un taux de réponse ou de débit raisonnable.** »

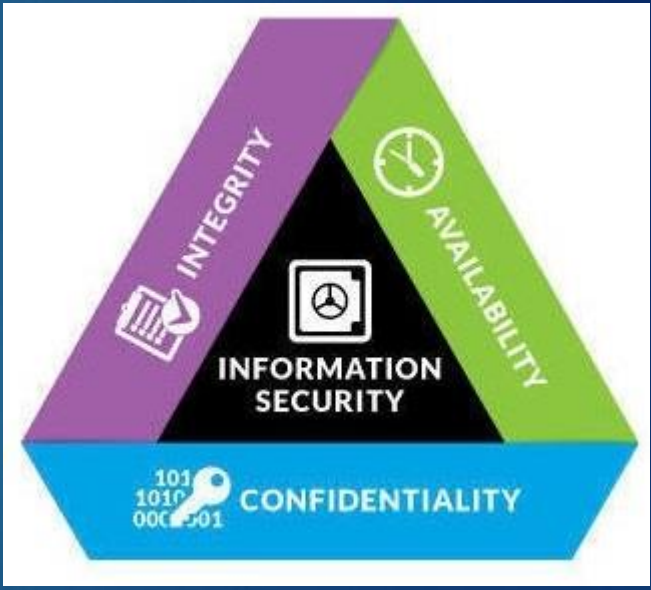
- 4 étapes fondamentales doivent être respectées pour assurer son cycle de vie.

Concept : cycle de vie de la sécurité



Concept : Sécurité des informations

- Quand on évalue la sécurité des informations, on doit penser **CIA** !
  - **Confidentiality** : les données privées sont-elles protégées pour empêcher tout accès non autorisé ?
  - **Integrity** : des mesures sont-elles en place pour s'assurer que les données n'ont pas été altérées, qu'elles sont correctes et authentiques ?
  - **Availability** : les utilisateurs autorisés peuvent-ils accéder aux données quand ils en ont besoin ?



Événements, alertes et incidents

- **Événement :** tout peut être un événement. Comme un login réussi, un émail, un changement de GPO (stratégie de groupe)
- **Alerte :** la notification d'une événement qui demande potentiellement une action.
- **incident (avec un petit i) :** un événement qui a violé la triade CIA mais **n'a pas causé d'impact sur le business**. Possiblement un utilisateur isolé
- **Incident (avec un grand I):** un événement qui a violé la triade CIA et **a eu un impact business**. Cela affecte toute l'organisation.

6 étapes de la réponse aux incidents

- Un **plan de réponse aux incidents est un document contenant un ensemble de instructions pour une entreprise lors d'un incident de cybersécurité**. Ces instructions suivent un ensemble spécifique d'étapes, mais le contenu réel va être spécifique à cette entreprise.

- Le document est conçu pour être un guide pour une entreprise depuis le tout début avant même que l'incident ne se produise, jusqu'à la dernière phase de découverte comment l'incident s'est produit et comment l'empêcher à l'avenir.

IMP, BCP, DRP ?

- Un **IMP** (*Incident Management Plan*) se concentre sur la protection des données sensibles **pendant un événement** et définit la portée des actions à entreprendre lors de l'incident, y compris les rôles et responsabilités spécifiques de l'équipe d'intervention en cas d'incident.

- **BCP** (*Business Conitnuity Plan*) et **DRP** (*Disaster Recovery Plan*) ont des objectifs plus larges :
  - **BCP** : Il garantit que votre entreprise pourra continuer à fonctionner en cas de perturbation importante. Il décrira d'abord les fonctions de votre entreprise et indiquera les systèmes qui doivent rester intacts pour que les entreprises fonctionnent. Ensuite, un BCP doit présenter un plan sur la manière dont ces systèmes seront entretenus pendant une perturbation.
  - **DRP** : un DRP se concentre sur la définition des objectifs de rétablissement (RTO et RPO) et les mesures à prendre pour ramener l'organisation à un état opérationnel après qu'un incident se soit produit

6 étapes de la réponse aux incidents

- NIST, SANS,… plusieurs modèles de réponse aux incidents. Quel que soit le nombre d'étapes, en vérité, il **repose tous sur le même principe**. Pour cette présentation, on partira sur le modèle du SANS.

  - 1. Préparation
  - 2. Identification
  - 3. Confinement
  - 4. Eradication
  - 5. Récupération
  - 6. Retour sur expérience

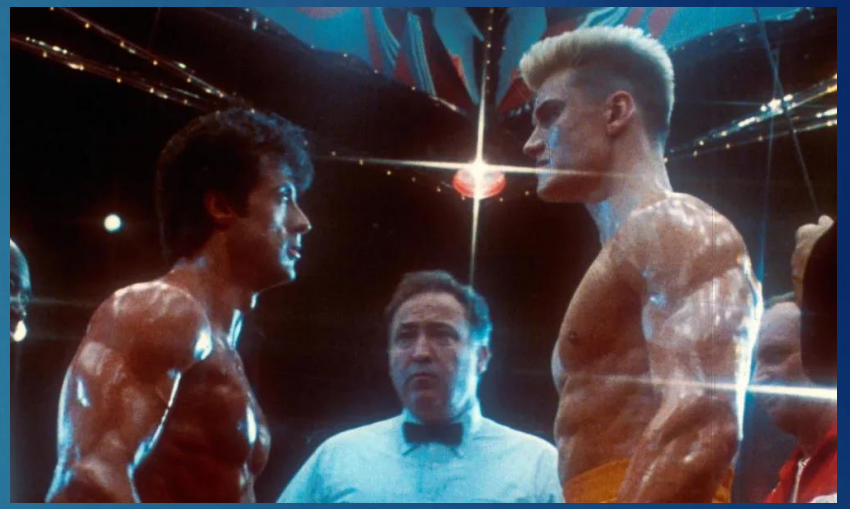
1. Préparation

- Avoir un plan ! Se demander quoi faire pendant un incident est le pire des moments
- Avoir les employés formés et des protocoles en place. Ce n'est pas un jeu. Il faut être réellement capable de lancer le processus.
- Identifier les compétences et les outils requis
- Si on n'a pas les ressources en interne, savoir qui contacter

Rocky se prépare pour les incidents

2. Identification

- Peu de certitude sur qu'est RELLEMENT l'incident. C'est pour ça qu'on a la phase d'identification.
- Pouvoir identifier les anomalies (avoir une baseline avec un IDS, par exemple) ou tout changements inconnus
- Savoir **faire la distinction entre un incident et un événement** qui produit une alerte
- Les alertes préoccupantes concernent : process inhabituels, de nouveaux comptes avec privilèges, des fichiers inhabituels, des tâches planifiés,…
- Durant l'investigation, **attention à ne pas altérer les preuves** (les fichiers logs, par exemple)



Il identifie la menace : ce n'est pas David Bowie mais un russe de 2m avec 200kg de muscles.

3. Confinement

- Se concentre sur le court-terme : **la priorité est d'arrêter les dégâts** et d'éviter qu'il y en ait davantage.
  - Assigner un incident responder
  - Pouvoir déterminer le niveau d'importance de l'incident et pouvoir le catégoriser
  - Notifier le managerment
  - Isoler les éléments du réseau (offline vs. Isolation VLAN)

- Si on isole l'attaquant dans une VLAN, on continue le monitoring. Il faut alors être discret pour ne pas alerter l'intrus

Il le confine dans un ring.

4. Éradication

- Démarrer la solution à long terme pour la phase de récupération
  - Supprimer, resconstruire et restaurer les systèmes affectés
  - Trouve l'origine du problème et la réparer
  - Ajouter des filtres à l'IDS, appliquer des patchs et supprimer le malware
  - Rescanner pour voir si on ne trouve pas d'autres traces de l'intrus.

- /!\ Ne pas se précipiter pour restaurer les données, effacer les éléments malveillants ou de savoir l'étendue réelle des dégâts. Il faut aussi collecter de quoi apprendre de l'incident qui s'est produit.

Rocky propose un crochet du gauche pour éradiquer la menace.

5. Récupération

- Réintroduction des systèmes affectés dans le réseau. Ces éléments sont surveillés pour s'assurer qu'il n'y a pas de réinfection.

- Si nécessaire, Les vulnérabilités sont patchés, les comptes compromis sont changés ou remplacés par des méthodes d'accès plus sécurisées

Retour à la normale. Il ne reçoit plus de coups.

6. Retour sur expérience

- Fait immédiatement après la phase de récupération
- Finalisation de la documentation et des rapports
- Trouver des moyens pour prévenir ce genre d'incidents à l'avenir
- Ne pas blâmer les personnes impliquées
- Le rapport sera une explication de qui, quoi, ou, pourquoi et comment
- La documentation sera bénéfique pour entrainer des futurs membres de l'équipe.

« Je connais ses techniques, il ne pourra plus m'avoir. »

Merci pour votre attention !