GESTION DES INCIDENTS DE SÉCURITÉ DE L'INFORMATION

Savadogo Yassia
ARCEP/CIRT-BF
savadogo.yassia[at]arcep.bf

AGENDA

- Introduction
- Définition d'un incident de sécurité de l'information
- Schéma de classification des incidents de sécurité
- Identification des parties prenantes
- Gestion des incidents de sécurité
- Conclusion

INTRODUCTION

- Les incidents de sécurité des systèmes d'information sont de plus en plus nombreux et multiformes
- Dans le but de mutualiser les actions pour leur résolution, un CIRT a été mis en place au Burkina Faso
- La gestion des incidents de sécurité doit être une activité organisée avec des étapes définies

DÉFINITION D'UN INCIDENT DE SÉCURITÉ

INCIDENT

Définition générale

- Evènement causant des dommages ou susceptible de le faire à des personnes ou à des organisations

INCIDENT INFORMATIQUE

Définition utilisée en Systèmes d'information

- **Selon COBIT**

  Tout évènement ne faisant pas partie du fonctionnement normal d'un service et qui cause, ou peut causer, une interruption ou une réduction de la qualité de ce service

- **Selon ITIL**

  Tout évènement ne faisant pas partie du fonctionnement standard d'un service et qui cause, ou peut causer, une interruption ou une diminution de la qualité de ce service

INCIDENT DE SÉCURITÉ DE L' INFORMATION

- **Selon l'ISO 27000 (Sécurité de l'information)**

  Un ou plusieurs évènements intéressant la sécurité de l'information, indésirable(s) ou inattendu(s) présentant une probabilité forte de compromettre les opérations liées à l'activité de l'organisme et de menacer la sécurité de l'information **[ISO/IEC TR 18044:2004]**

INCIDENT DE SÉCURITÉ DU SYSTÈME D'INFORMATION

- **Incident SSI**

  Tout évènement potentiel ou avéré, indésirable et/ou inattendu, impactant ou présentant une probabilité forte d'impacter la sécurité de l'information dans ses critères de Disponibilité, d'Intégrité, de Confidentialité et/ou de Preuve

SCHÉMA DE CLASSIFICATION DES INCIDENTS DE SÉCURITÉ

SCHÉMA DE CLASSIFICATION ADOPTÉ PAR LES CIRTS

Classes d'incidents	Types d'incidents	Description/Exemples
Contenu Abusif	Spam	pourriel ou polluriel est une communication électronique non sollicitée, en premier lieu via le courrier électronique. Il s'agit en général d'envois en grande quantité effectués à des fins publicitaires.
	Harcèlement	Discrédits, ou discrimination contre une personne d'un point de vue cyber
	Enfant/Sexe/Violence/…	Pornographie infantile, glorification de la violence

SCHÉMA DE CLASSIFICATION ADOPTÉ PAR LES CIRTS

Classes d'incidents	Types d'incidents	Description/Exemples
Code malicieux	Virus	Logiciel intentionnellement introduit dans un système pour un but nocif. L'interaction d'un utilisateur est normalement nécessaire pour activer ce code.
	Ver	
	Cheval de Troie	
	Spyware	
	Dialler	
Collecte d'informations	Scanning	Attaques qui consistent à envoyer des requêtes à un système pour découvrir ses failles. Ceci inclut également tout type de processus de test pour collecter des informations sur les hôtes, les services et les comptes. Exemple : fingerd, requête DNS, ICMP, SMTP (EXPN, RCPT,…)
	Sniffing	Observer et enregistrer le trafic réseau (Ecoute)
	Ingénierie sociale	Collecte d'informations sur un être humain sans utiliser de moyens techniques (ex : mensonges, menaces,…)

SCHÉMA DE CLASSIFICATION ADOPTÉ PAR LES CIRTS

Classes d'incidents	**Types d'incidents**	**Description/Exemples**
Tentatives d'intrusion	Exploiter des Vulnérabilités connues	Une tentative pour compromettre un système ou interrompre tout service en exploitant les vulnérabilités avec des identifiants standardisés comme un nom CVE (ex : Buffer overflow, Portes dérobées, cross side scripting ,etc).
	Tentatives de connexion	Tentatives de connexion multiples (vol ou crack de mots de passe, force brute).
	Signature d'une nouvelle attaque	Une tentative pour exploiter une vulnérabilité inconnue.
Intrusions	Compromission d'un compte privilégié	Une compromission réussie d'un système ou d'une application (service). Ceci peut être causé à distance par une nouvelle vulnérabilité ou une vulnérabilité inconnue, mais aussi par un accès local non-authorisé.
	Compromission d'un compte non privilégié	
	Compromission d'une application	

Schéma de classification adopté par les CIRTs

Classes d'incidents	Types d'incidents	Description/Exemples
Disponibilité	DoS	Dans ce type d'attaque, un système est bombardé avec une grande quantité de paquets que les processus deviennent lents ou que le système crache. Exemple d'un Dos distant : SYS-a, PING-flooding ou des bombes E-mails (DDOS : TFN, Trinity, etc). Toutefois, la disponibilité peut aussi être affectée par des actions locales (ex : destruction, interruption d'alimentation électrique, etc).
	DDoS	
	Sabotage	
Sécurité de l'information	Accès non autorisé aux informations	En plus d'un abus local des données et des systèmes, la sécurité de l'information peut être mise en mal par un compte ou une application compromise. Aussi, les attaques qui interceptent et accèdent aux informations pendant leur transmission sont possibles (écoute, usurpation, ou hijacking).
	Modification non autorisée aux informations	

SCHÉMA DE CLASSIFICATION ADOPTÉ PAR LES CIRTS

Classes d'incidents	Types d'incidents	Description/Exemples
Fraud	Usage non autorisé des ressources	L'utilisation des ressources à des buts non autorisés, incluant des activités à but lucratif (ex. l'usage d'email pour participer dans des transactions illégales.
	Droit d'auteur (Copyright)	Vendre ou installer des copies de logiciels commerciaux illégalement ou d'autres matériels sous droit d'auteur (Warez).
	Mascarade	Type d'attaques dans lequel, une entité assume illégitimement l'identité d'un autre dans le but de bénéficier de lui.
Autres	Tout incident qui ne fait pas partie des catégories citées ci-dessus.	Si le nombre d'incidents dans cette catégorie croit, ceci indique que le schéma de classification doit être révisé.

IDENTIFICATION DES PARTIES PRENANTES

INDENTIFICATION DES PARTIES PRENANTES

- Pour mieux gérer les incidents, un CIRT doit identifier ses parties prenantes
- Les parties prenantes sont les entités dont les incidents sont traités par le CIRT
- On peut identifier une partie prenante par:
  - ✓ Les plages d'adresses IPv4 et IPv6
  - ✓ Le(s) numéro(s) de Système Autonome (AS)
  - ✓ Les nom(s) de domaine
  - ✓ Simple description

IDENTIFICATION DES PARTIES PRENANTES

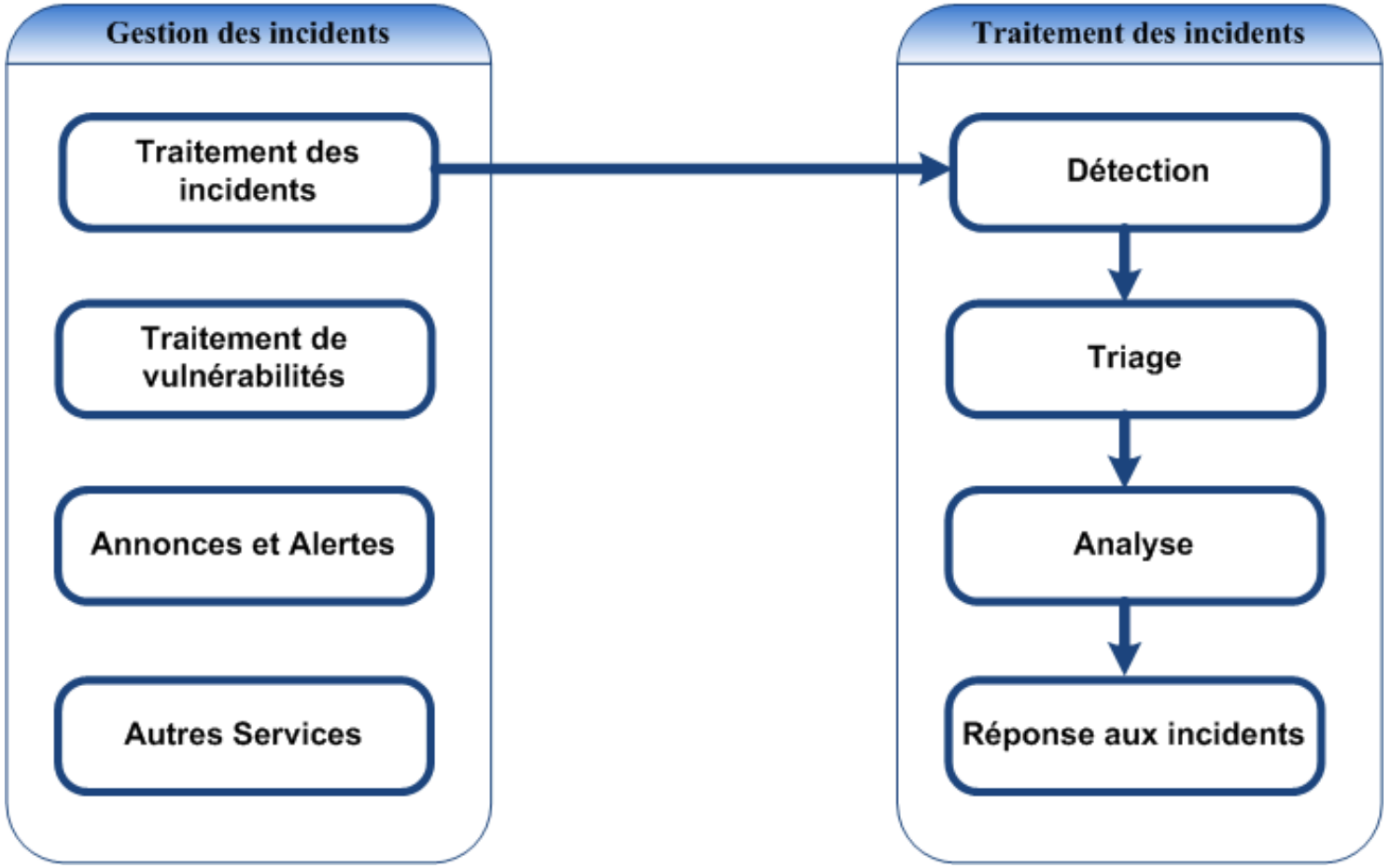
Types d'identifications des parties prenantes recommandés

Type d'identification Institutions	Plage d'adresses IP	Numéro AS	Noms de domaine	Simple description
Gouvernementale				
Financière				
Recherche et Enseignement				
FAI				
Intégrateur/ Constructeur				
Industrie				

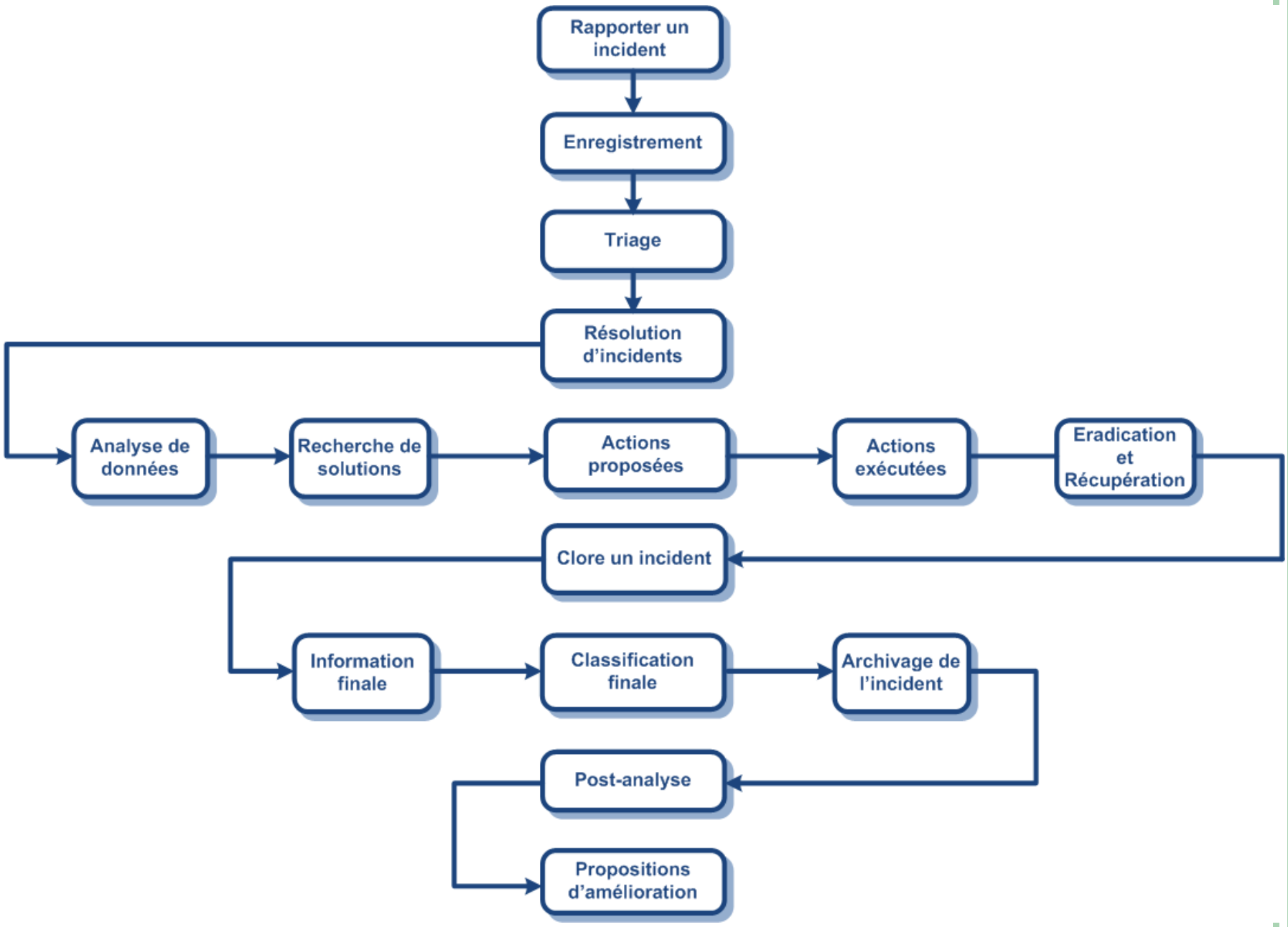
GESTION DES INCIDENTS DE SÉCURITÉ

GESTION DES INCIDENTS

Processus de gestion et de traitement des incidents



WORKFLOW DE TRAITEMENT D'INCIDENTS



PROCESSUS DE TRAITEMENT D'INCIDENTS

1. **Rapporter un incident**

   - **Communication avec le CIRT**

     - ✓ Pour des communications ne contenant pas des informations sensibles, le CIRT utilisera des courriels non chiffrés
     - ✓ Pour les communications sécurisées, les courriels chiffrés avec PGP ou le téléphone seront utilisés

PROCESSUS DE TRAITEMENT D'INCIDENTS

1. Rapporter un incident

Å Tâches de la partie prenante

- ✓ La partie prenante doit fournir des informations de contact
  - Nom et organisation
  - E-mail
  - Numéro de téléphone
- ✓ L'adresse IP et le type d'incident (spam, scanning, Dos, etc.) doivent être précisés
- ✓ Si l'incident concerne le scanning, joindre une partie des logs montrant le problème

PROCESSUS DE TRAITEMENT D'INCIDENTS

1. Rapporter un incident

Å Tâches de la partie prenante

- ✓ Si l'incident concerne un spam ou un malware, joindre une copie entière de l'entête du courriel considéré comme spam et malware
- ✓ Si l'incident concernant l'hameçonnage (phishing), joindre l'URL

PROCESSUS DE TRAITEMENT D'INCIDENTS

1. **Rapporter un incident**

- Le CIRT reçoit un incident rapporté par une de ses parties prenantes
- Via :
  - Courriel (e-mail) : incidents[at]cirt.bf
  - Formulaire web : http://www.cirt.bf/index.php/signaler-un-incident/
  - Téléphone : 50375360
  - Fax : 50375364

PROCESSUS DE TRAITEMENT D'INCIDENTS

1. Rapporter un incident

Formulaire web

Nom (obligatoire)

Organisation(obligatoire)

Numéro de téléphone(obligatoire)

Email (obligatoire)

Sujet — Contenu abusif

Catégorie — Spam

Remarque

A G V S 4 U

Identifier les lettres

Envoyer

PROCESSUS DE TRAITEMENT D'INCIDENTS

1. **Enregistrement**

   - Un incident rapporté est automatiquement enregistré dans le système de traitement des incidents

2. **Triage**

   - Dans le processus de traitement des incidents, la phase de triage consiste en étapes:
     - ✓ Vérification
     - ✓ Classification initiale
     - ✓ Assignation

PROCESSUS DE TRAITEMENT D'INCIDENTS

2. Triage

2.1. Vérification d'un incident

- L'incident rapporté est-il un vrai?
- L'incident a-t-il été rapporté par une des parties prenantes?

2.2 . Classification initiale d'un incident

- L'incident doit être classé selon le schéma de classification ci-dessous
- Beaucoup d'informations sont nécessaires à cette étape

PROCESSUS DE TRAITEMENT D'INCIDENTS

2. Triage

2.3. Comment prioriser les actions entre les parties prenantes

- Pour différencier les niveaux de services
- Le CIRT repartira les parties prenantes en différentes catégories en fonction des priorités
- Un autre facteur à prendre en compte dans la priorisation est la sévérité de l'incident à traiter

PROCESSUS DE TRAITEMENT D'INCIDENTS

2. Triage

2.3. Comment prioriser les actions entre les parties prenantes?

Exemple

- Pour un CIRT qui en fonction de sa mission, doit protéger l'administration publique et a en plus un contrat avec des institutions financières pour la fourniture de services de traitement d'incidents.
- Dans ce cas , on doit diviser les incidents potentiels en trois groupes en fonction de leur sévérité.

PROCESSUS DE TRAITEMENT D'INCIDENTS

2. Triage

2.3. Comment prioriser les actions entre les parties prenantes?

Groupe	Sévérité	Exemple d'incidents	Temps de réponse
Rouge	Elevé	Å Disponibilité Å Code Malicieux Å Intrusions	3heures
Orange	Moyen	Å Tentatives d'intrusion Å Sécurité de l'information Å Fraude	24heures
Jaune	Faible	Å Contenu abusif Å Collecte d'informations	3jours

PROCESSUS DE TRAITEMENT D'INCIDENTS

2. Triage

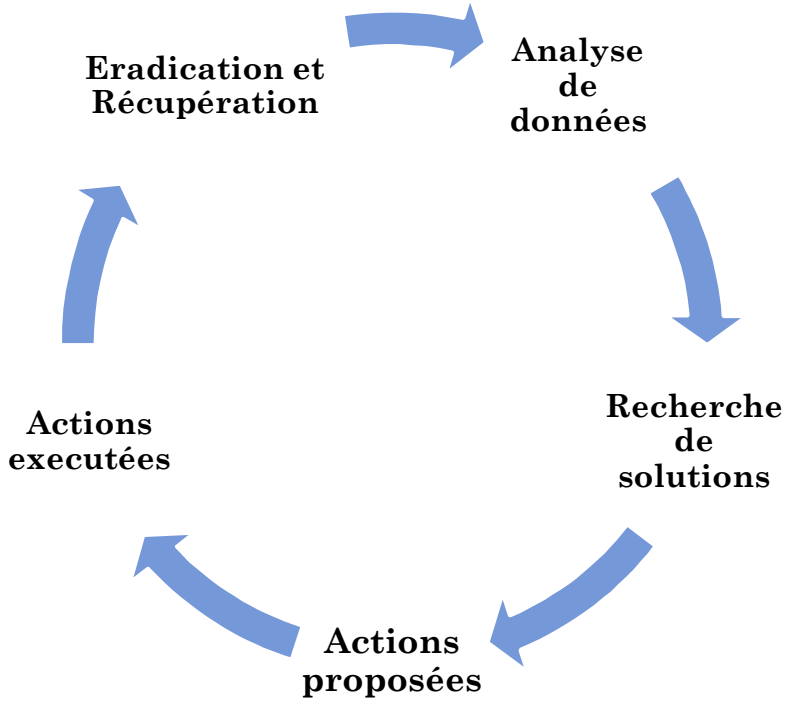
2.4. Assigner un incident

- Un incident est assigné au responsable du traitement d'incident
- Cette personne peut être celle qui est la première à prendre l'incident à partir de la boite de réception des incidents
- Une personne peut être spécialiste du traitement d'un incident donné (spam, malware)
- Un incident peut être assigné à une personne en fonction de sa disponibilité

PROCESSUS DE TRAITEMENT D'INCIDENTS

3. Résolution d'incidents

- La phase la plus longue pour la résolution de l'incident
- S'effectue selon le cycle suivant



PROCESSUS DE TRAITEMENT D'INCIDENTS

3. Résolution d'incidents

3.1. Analyse de données

- Pour débuter l'analyse de données, les parties prenantes concernées seront contactées pour collecter plus d'informations sur l'incident
- Des conseils et informations initiaux seront inclus dans cette notification pour mieux orienter la résolution de l'incident

PROCESSUS DE TRAITEMENT D'INCIDENTS

3. **Résolution d'incidents**

3.2. Recherche de solutions

- Les informations collectées pendant la phase d'analyse sont utilisées dans cette phase

3.3. Actions proposées

- Une liste de tâches concrètes et pratiques sont élaborées pour chaque partie prenante. Par ex.
  - ✓ Comment stopper ou réduire une attaque en cours
  - ✓ Monitorer le trafic réseau lié à une situation (pour les FAI et FCI)
  - ✓ Assister les unités de police et de gendarmerie

PROCESSUS DE TRAITEMENT D'INCIDENTS

3. Résolution d'incidents

3.4. Actions exécutées

- Les infrastructures des parties prenantes n'étant sous le contrôle du CIRT
- Le CIRT doit s'assurer que ces parties ont exécutées les actions proposées
- C'est la phase la complexe
- Le CIRT peut contacter les parties prenantes par mail, téléphone pour s'assurer de l'exécution des actions proposées

PROCESSUS DE TRAITEMENT D'INCIDENTS

3. Résolution d'incidents

3.5. Eradication et récupération

- Toutes les actions auront pour seul but d'éradiquer les incidents
- La résolution réelle d'un problème est de restaurer un service compromis dans son état normal

PROCESSUS DE TRAITEMENT D'INCIDENTS

4. Clôture d'un incident

4.1. Information finale

- Après la résolution d'un incident, les parties concernées seront informées
- Deux questions à répondre ici
  - ✓ Qui informer?
  - ✓ Informer sur quoi?
- ○ Des indications sur les procédures de réduction des incidents seront fournies à ce niveau à chacune des parties prenantes

PROCESSUS DE TRAITEMENT D'INCIDENTS

4. Clôture d'un incident

4.2. Classification finale

- Cette étape n'est pas obligatoire
- Elle survient à un niveau où des informations supplémentaires ne sont plus nécessaires

4.3. Archivage de l'incident

- Tout incident sera archivé et servir pour de futures opérations

PROCESSUS DE TRAITEMENT D'INCIDENTS

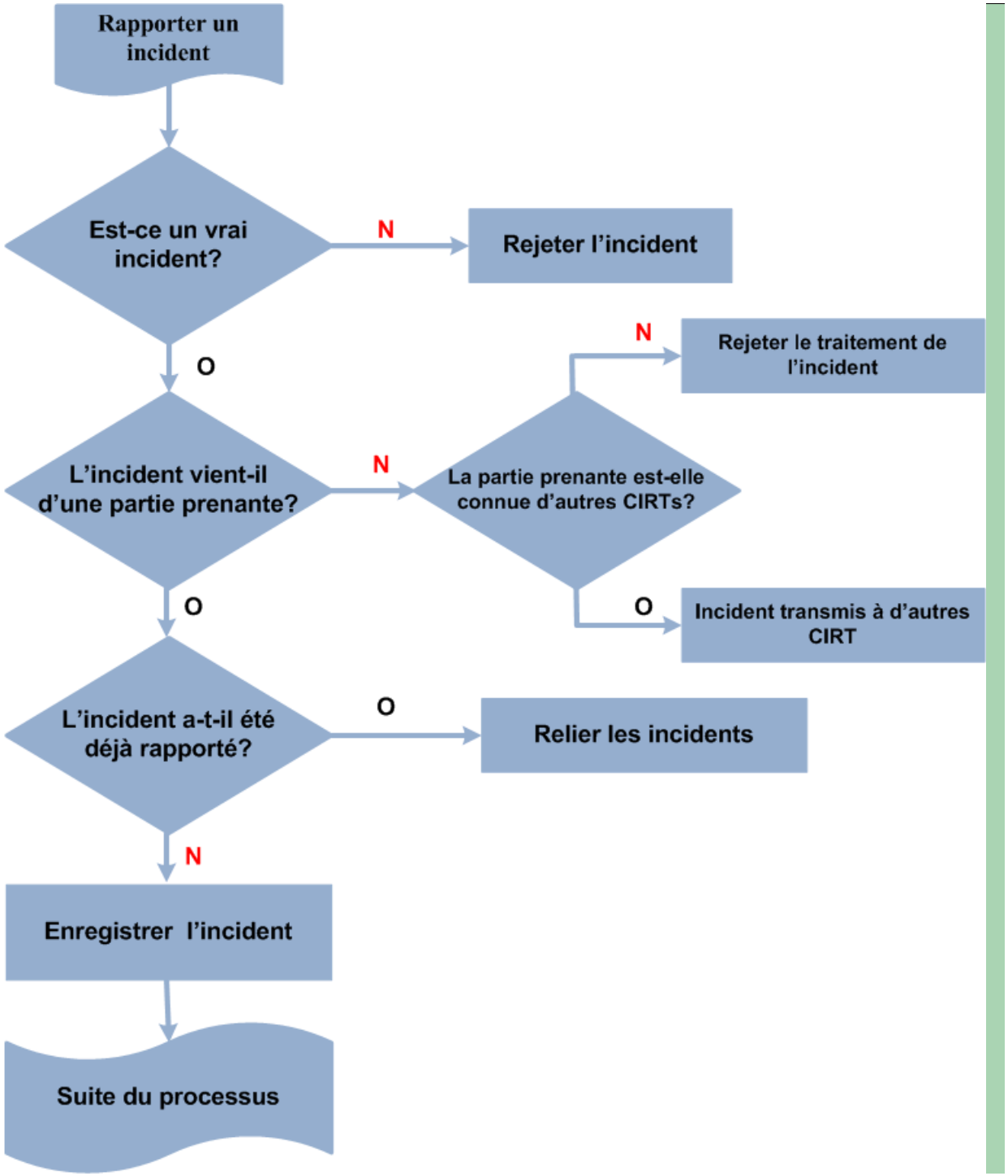
5. Post Analyse

- Très utile au CIRT dans l'optique de faire un bilan du traitement de l'incident

6. Propositions d'amélioration

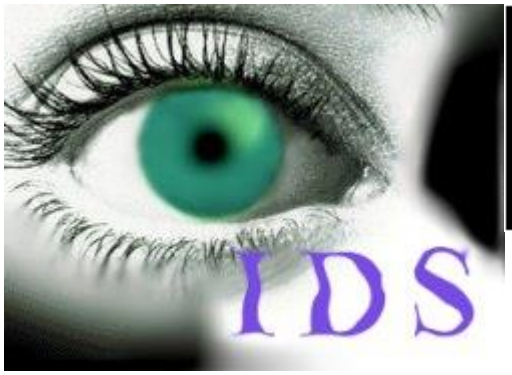
- Le traitement d'incidents est un service réactif
- Il peut être en 1ère ligne pour des actions proactives et permettre des améliorations pour une bonne culture de sécurité
- C'est l'étape où il faut faire bénéficier de l'expérience de traitement d'incidents en fournissant des conseils et des recommandations aux parties prenantes

APPROCHE DU DÉTAIL DE TRAITEMENT D'INCIDENTS



CONCLUSION

- Pour de meilleurs résultats, chaque partie prenante doit mettre en place des services proactifs à fin de mieux détecter les incidents de sécurité




```
11:22:20 <dionaea.capture> New attack from Ho Chi Minh City, Vietnam (10.81,106.64) to Aachen, Germa
11:22:21 <dionaea.capture> New attack from Taipei, Taiwan (25.04,121.53) to Aachen, Germany (50.77,6.11)
11:22:22 <dionaea.capture> New attack from Taipei, Taiwan (25.04,121.53) to Aachen, Germany (50.77,6.11)
11:22:22 <dionaea.capture> New attack from Taiwan (23.50,121.00) to Aachen, Germany (50.77,6.11) [md5: 2c
11:22:23 <dionaea.capture> New attack from Araçoiaba Da Serra, Brazil (-23.50,-47.62) to Aachen, Ger
11:22:24 <dionaea.capture> New attack from Tarnovo, Bulgaria (43.09,25.66) to Aachen, Germany (50.77,6.
11:22:25 <dionaea.capture> New attack from Stara Zagora, Bulgaria (42.43,25.64) to Aachen, Germany (5
11:22:25 <dionaea.capture> New attack from Bucharest, Romania (44.43,26.10) to Aachen, Germany (50.77,
```

Merci Beaucoup

Question???