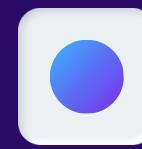




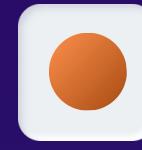
GESTION DES INCIDENTS NSA-800



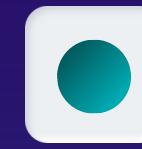
Plan



Context



Périmètre



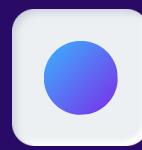
Limites/Contraintes



Methodologie



Schéma Fonctionnel



Etude de Cas



Budget



Introduction

TO THE CYBERSECURITY INCIDENT MANAGEMENT

La gestion des incidents en cybersécurité est une discipline visant à détecter, analyser, contenir et répondre aux incidents de sécurité informatique.

Elle permet aux organisations de réduire l'impact des incidents et de minimiser les dommages causés par les attaques informatiques.



Context

Context



Un client est intéressé par notre profile pour mettre en place un système de monitoring de gestion des incidents. Dans cette seconde phase du projet, il consistera à mettre en place une politique de gestion des incidents.



Périmètre

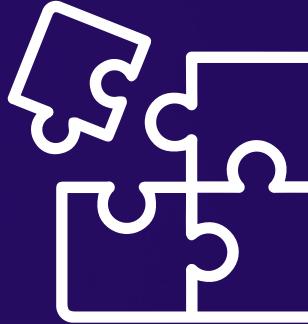
Périmètre

- Incidents des logiciels et des applications
- Incidents concernant le matériel





Limite/Contrainte



Les incidents tels que :

- Incendies,
- Vols..., ne sont pas pris en compte.





Méthodologie de gestion des incidents



Norme ITIL

Information Technology Infrastructure Library

La détection et l'enregistrement

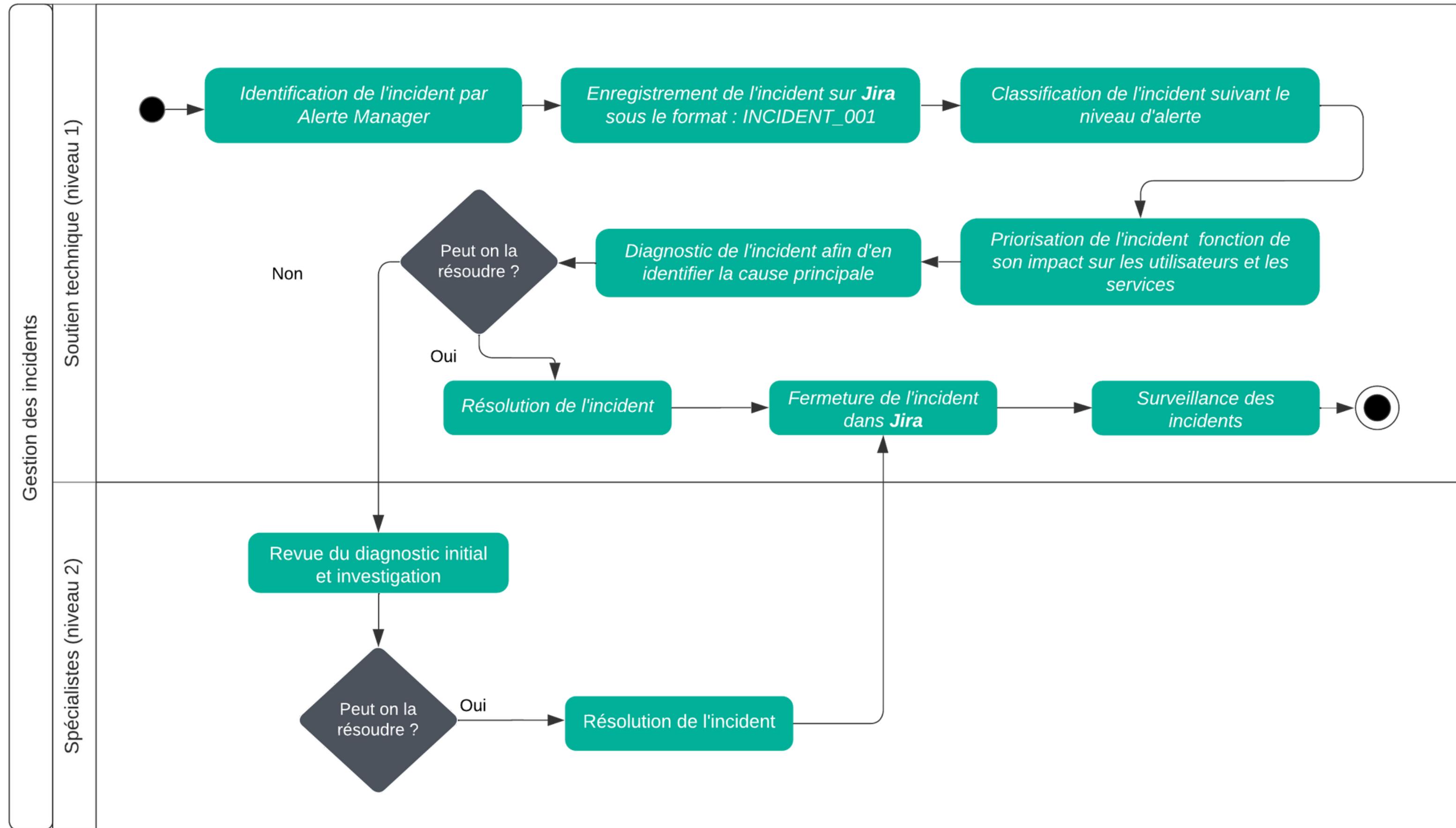
La classification et l'analyse

L'investigation et le diagnostic

La résolution et la remise en service

La fermeture de l'incident

Schéma Fonctionnel





Incident :

Database Crash

6 La résolution



L'équipe passe à la restauration de la base de données à partir d'une sauvegarde récente, la réparation de la base de données corrompue ou la mise en place d'une base de données de secours.





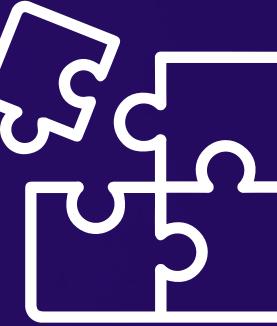
Incident :

Cessation des Services

6 La résolution

L'équipe passe à la restauration des conteneurs des divers services à partir d'une sauvegarde récente.





Incident :

Machine crash

6 La résolution



L'équipe passe à la restauration des conteneurs des divers services constitutifs de cette machine vers une nouvelle.



Budget



Coûts des opérations

| Incident | Min Coût | Max Coût | Duré/h |
|------------------------|----------|----------|--------|
| Database Crash | 50\$ | 100\$ | 1 |
| Denial Of Services | 150 | 600\$ | 1 |
| Cessation des Services | 80\$ | 300\$ | 1 |



Ceci est un budget provisoire pour les types d'incidents mentionnés en fonction de la durée de l'incidents



Budget

Coûts de formation

| Incident | Personne | Min Coût | Max Coût | Duré/h |
|-------------------------|----------|----------|----------|--------|
| Database Crash | 3 | 1000 \$ | 1500\$ | 1 |
| BackUp (Veam BackUp) | 2 | 2000 \$ | 2600\$ | 2 |
| Cessation des Services | 3 | 800\$ | 900\$ | 3 |

Ceci est un budget provisoire pour les types de formations liés sur les incidents qui peuvent survenir.





Budget

Coûts des équipements et des logiciels

| Equip/Logiciel | Min Coût | Max Coût |
|--------------------------|----------|----------|
| Systèmes de surveillance | 10\$ | 150\$ |
| VeamBacUp | 2000\$ | 2600\$ |
| Matériel de secours | 1000\$ | 3500\$ |
| Jira Software | \$1,525 | - |



Ceci est un budget provisoire pour les types d'équipements et logiciels nécessaires pour les incidents qui peuvent survenir.

Budget



| | Min Coût | Max Coût |
|--|----------|----------|
| les coûts de formation | 3800\$ | 5000\$ |
| Coûts des équipements et des logiciels | 4535\$ | 7775\$ |
| Coût des opérations | 280\$ | 1000\$ |
| Outils de communication | 2000\$ | 4000\$ |
| Total | 10,615\$ | 17,775\$ |





Merci