Exercice : Simulation de Gestion d'Incident

KOUASSI GLOHNDY

Rapport de Simulation – Gestion d'Incident IT

Vous travaillez dans le département IT d'une entreprise et vous recevez un rapport indiquant qu'un service critique est hors ligne. Suivez le processus de gestion des incidents pour enregistrer, catégoriser, prioriser et attribuer cet incident.

- ✓ Rédigez un rapport détaillé des étapes que vous suivez, y compris le diagnostic initial, les actions de résolution tentées et la communication avec les parties prenantes concernées.
- ➢ Décrivez également comment vous surveillerez et communiquerez sur l'avancement jusqu'à la résolution de l'incident.

1. Contexte

Le département IT reçoit une alerte indiquant que le service de messagerie interne (critique pour les communications internes et externes) est hors ligne.
Cet incident a un impact direct sur les opérations de l'entreprise (impossibilité de communiquer avec les clients et partenaires).

---

2. Enregistrement de l'incident

- Numéro d'incident : INC-2025-0908-001
- Date/heure de détection : 08/09/2025 – 09h15
- Source : Rapport automatique du système de monitoring + signalement par utilisateurs via le service desk
- Description : Service de messagerie interne inaccessible pour tous les utilisateurs.

---

3. Catégorisation

- Catégorie : Applications → Communication → Messagerie
- Sous-catégorie : Indisponibilité totale du service
-

---

4. Priorisation

- Impact : Élevé (toute l’entreprise est affectée, communication bloquée)
- Urgence : Élevée (nécessité de rétablir rapidement le service pour limiter les pertes)
- Priorité attribuée : P1 – Critique

---

5. Attribution

- Incident assigné à : Équipe Infrastructure & Réseaux (responsable du serveur de messagerie).
- Responsable désigné : Chef d’équipe Infrastructure

---

6. Diagnostic initial

- Vérification de l’état du serveur de messagerie : service non démarré
- Analyse des journaux système : erreur de surcharge disque détectée
- Vérification réseau : OK
- Vérification authentification Active Directory : OK

---

7. Actions de résolution tentées

- Libération d’espace disque (suppression fichiers temporaires et journaux anciens).
- Redémarrage du service de messagerie.
- Test de connexion utilisateur : échec initial, puis succès partiel.
- Application d’un patch de maintenance recommandé par l’éditeur.
- Redémarrage complet du serveur.

---

8. Communication avec les parties prenantes

- 09h20 : Notification envoyée aux utilisateurs – incident identifié, investigation en cours.
- 09h40 : Mise à jour envoyée – cause identifiée (surcharge disque), action corrective en cours.
- 10h00 : Mise à jour envoyée – service partiellement restauré, tests en cours.
- 10h20 : Notification finale – incident résolu, service totalement opérationnel.

---

9. Suivi et clôture

- Surveillance post-résolution : suivi renforcé du serveur pendant 24h via monitoring.
- Ticket d’incident mis à jour avec les détails techniques et actions correctives.
- Clôture officielle du ticket après validation par les utilisateurs clés.

---

10. Amélioration continue (Post-mortem)

- Mise en place d’une alerte automatique sur l’espace disque pour éviter récidive.
- Planification d’une politique de purge automatique des logs.
- Documentation mise à jour dans la base de connaissances.