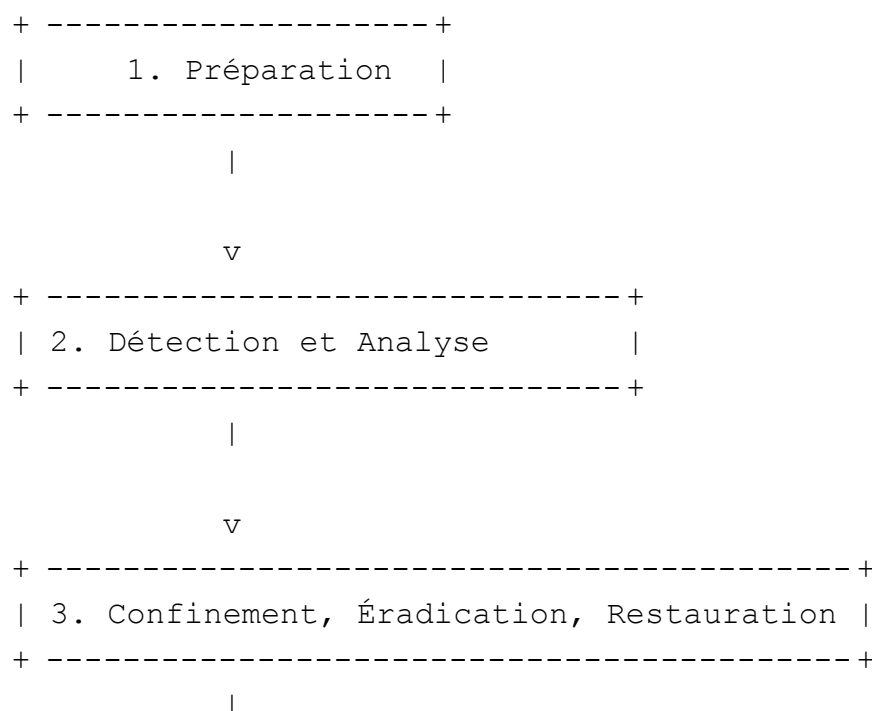


Cycle de Réponse aux Incidents (NIST 800-61)

Le cycle de réponse aux incidents, tel que défini par le NIST SP 800-61, repose sur quatre grandes phases cycliques :

1. Préparation
2. Détection et Analyse
3. Confinement, Éradication, Restauration
4. Leçons Tirées (Retour d'expérience)

Ce processus permet de réagir efficacement aux incidents de sécurité informatique tout en intégrant les enseignements pour prévenir leur récurrence.



```

      v
+ -----+
| 4. Leçons Tirées (Retour) |
+ -----+
      |

```

```

      v
+ -----+
| 1. Préparation |
+ -----+

```

Détail des Phases :

1. Préparation

Mise en place des politiques, outils, procédures, équipes (playbooks, SIEM, journaux, etc.)

2. Détection et Analyse

Identification d'un incident via SIEM, alertes, logs, utilisateurs, etc.

3. Confinement, Éradication, Restauration

Isolement de l'incident, suppression des causes, retour à l'état nominal

4. Leçons Tirées

Rapport post-mortem, amélioration continue, documentation, mise à jour des procédures