# Récupération après une cyberattaque

## Restaurez vos opérations plus efficacement après un incident.

## Une stratégie de sécurité de récupération complète implique de

Limiter les conséquences de l'attaque → Reconstruire les services et appareils compromis → Restaurer les opérations → Procéder à l'analyse de l'incident puis en tirer des leçons

## Les étapes pour que la cybersécurité gagne en maturité

1. **Confinement des incidents**
   Déconnectez du réseau les systèmes affectés, désactivez les comptes compromis et stoppez les dégâts.
2. **Restauration des systèmes/appareils**
   Reconstruisez les systèmes compromis, réinstallez les logiciels et appliquez des mises à jour et correctifs de sécurité.
3. **Récupération des données**
   Restaurez les données à partir de sauvegardes ou utilisez des techniques spécialisées de récupération des données pour recouvrer des fichiers perdus ou chiffrés.
4. **Investigation numérique**
   Examinez les mécanismes de l'attaque et les failles de sécurité exploitées afin d'empêcher tout incident futur.
5. **Évaluation de la réponse aux incidents**
   Suite à une récupération, évaluez-en le processus pour identifier des points à améliorer.
6. **Utilisation de l'IA/ML**
   Accélérez la récupération en identifiant rapidement les systèmes et données affectés ainsi qu'en automatisant le processus de restauration des sauvegardes.

## La cyber-récupération est un travail d'équipe.

**Services et partenariats professionnels**
Les partenaires de cybersecurité offrent une expertise et des ressources précieuses :

- Investigation numérique
- Identification des raisons de la violation
- Mesures visant à empêcher tout incident futur

Découvrez-en davantage sur l'implémentation d'une stratégie complète de cybersécurité.

*Découvrir l'e-book* →



DELL Technologies