NéoRecovery

néowoft

En cas de cyberattaque, savez-vous ce qui est à risque et comment réagir pour limiter l'impact sur votre activité ?

Avec **NéoRecovery**, identifiez, contenez et redémarrez rapidement grâce à un accompagnement d'experts, structuré et opérationnel.

80 % des entreprises victimes de cyberattaque n'ont pas de plan de réponse adapté*

Réagissez vite, reprenez le contrôle :
Méthodologie | Expertise | Rebond

- **Un cadre clair, une action rapide :** Nous intervenons sans délai pour contenir l'incident et limiter son impact, avec une méthodologie éprouvée qui évite les erreurs coûteuses.
- **Une équipe engagée, sur le terrain :** Nos équipes d'experts formés à la réponse à incident sont présentes dans toute la France, assurant une intervention rapide et adaptée à votre contexte.
- **Une analyse complète et transparente :** Nous identifions précisément l'origine, l'impact et les vulnérabilités exploitées, pour vous fournir une vision claire et des recommandations pragmatiques.
- **Une reprise rapide et maîtrisée :** Nous vous accompagnons pour relancer vos activités rapidement, tout en renforçant durablement votre sécurité pour prévenir les futurs incidents.

De l'attaque à la reconstruction, une méthodologie en 4 temps.

- **Diagnostic**
  Identifier la cause, les systèmes compromis et la méthode d'attaque.
- **Confinement**
  Isoler les systèmes touchés, bloquer les flux malveillants et préserver les preuves.
- **Reconstruction**
  Restaurer des environnements sains, appliquer les correctifs et sécuriser les accès.
- **Analyse post-incident**
  Produire un rapport, mesurer l'impact et définir des actions préventives.

*Sources : IBM X-Force Threat Intelligence Index 2024

NéoRecovery

Notre intervention s’appuie sur une analyse rigoureuse, pour comprendre l’incident, sécuriser votre environnement et vous donner les moyens d’agir.

Des livrables complets, pensés pour enclencher les bonnes décisions :

- **Compréhension de l’attaque** : faille exploitée, vecteur d’entrée, malware identifié.
- **Actions menées et à prévoir :** mesures prises et recommandations pour vous sécuriser.
- **Éléments de preuve :** preuves techniques de l’incident, utiles pour analyse ou poursuites.
- **Plan de remédiation :** feuille de route priorisée pour corriger, renforcer et prévenir.

Un rapport clair, opérationnel et exploitable, pour réagir vite et renforcer durablement votre posture de sécurité.

La cyberattaque peut frapper à tout moment. Être prêt, c’est savoir réagir vite et efficacement.

- Saurez-vous agir vite pour éviter l’arrêt total ?
- Avez-vous les experts et outils pour identifier la menace ?
- Avez-vous déjà une équipe prête à intervenir en urgence ?
- Vos process sont-ils prêts à gérer la crise sans faille ?