Une organisation peut traiter analyser les fichiers avec un référentiel fiable comme un chantier distinct. Elle commence par reconstruire les composants plutôt que corriger au hasard, enchaîne avec comparer le noyau et les extensions à des sources de référence, puis décide de isoler les fichiers récemment modifiés pour examen selon les accès encore disponibles. Les observations portant sur du code obfusqué, des fichiers placés dans des répertoires inhabituels ou des modifications sans justification servent à confirmer ou écarter les hypothèses. À l'inverse, éditer directement un fichier suspect sans garder de copie fragilise l'analyse, d'autant que une suppression approximative peut casser le site sans retirer les mécanismes de persistance. L'étape est avancée lorsque l'équipe obtient un ensemble de fichiers dont chaque différence importante est expliquée, remplacée ou supprimée et sait nommer les incertitudes restantes. Une prochaine revue est nommée sans ambiguïté.

Sur le plan opérationnel, limiter les effets sans effacer les traces ne consiste pas à confondre confinement et nettoyage définitif. L'objectif est de empêcher l'incident de s'étendre tout en conservant les éléments nécessaires à la compréhension, avec une progression qui sépare observation et correction. Commencez par restreindre les accès non indispensables, poursuivez avec mettre en pause les changements éditoriaux et techniques, puis utilisez préserver une copie de travail avant toute suppression si le contexte le permet. Rapprochez des connexions persistantes, des tâches automatiques inattendues ou des modifications qui réapparaissent des changements connus, car une remise en ligne trop rapide peut relancer la même chaîne de compromission. Le résultat recherché reste un environnement plus stable, dans lequel les vérifications et les corrections deviennent traçables. Le prochain contrôle reste clairement attribué.

Quand cette étape peut-elle être considérée comme maîtrisée ?

Sur le plan opérationnel, définir des critères d'acceptation concrets ne consiste pas à déclarer l'incident clos dès que le site s'affiche. L'objectif *intervention désinfection* est de vérifier que le site fonctionne, que les accès sont maîtrisés et que les symptômes ne réapparaissent pas, avec une progression adaptée au niveau d'incertitude. Commencez par tester les parcours publics et administratifs, poursuivez avec contrôler les comptes, fichiers et tâches automatiques, puis utilisez faire relire les changements par une autre personne lorsque c'est possible si le contexte le permet. Rapprochez des erreurs persistantes, des redirections résiduelles ou des modifications qui reviennent des changements connus, car une validation limitée à l'affichage de la page d'accueil donne une confiance trompeuse. Le résultat recherché reste une décision de remise en service basée sur des critères observables et consignés. Le prochain contrôle reste clairement attribué.

Quand cette étape peut-elle être considérée comme maîtrisée ?

Sur le plan opérationnel, vérifier qui peut encore agir sur wordpress ne consiste pas à changer un seul mot de passe en laissant les autres accès intacts. L'objectif est de identifier les comptes, clés, sessions et accès techniques capables de modifier l'installation, avec une progression lisible pour chaque intervenant. Commencez par revoir les administrateurs et les comptes d'hébergement, poursuivez avec révoquer les sessions devenues douteuses, puis utilisez renouveler les secrets depuis un poste considéré comme sain si le contexte le permet. Rapprochez des utilisateurs inconnus, des rôles modifiés, des connexions inhabituelles ou des clés partagées des changements connus, car un nettoyage de fichiers reste fragile si un accès compromis demeure actif. Le résultat recherché reste une chaîne d'accès réduite, attribuable et mieux contrôlée avant la remise en service. Le prochain contrôle reste clairement attribué.

Quand cette étape peut-elle être considérée comme maîtrisée ?

Sur le plan opérationnel, surveiller la période qui suit la reprise ne consiste pas à accumuler des alertes sans définir qui les traite. L'objectif est de observer les changements, accès et comportements qui pourraient signaler une persistance ou une nouvelle anomalie, avec une progression lisible pour chaque intervenant. Commencez par suivre les modifications de fichiers, poursuivez avec revoir les connexions et erreurs significatives, puis utilisez planifier des contrôles espacés selon le risque si le contexte le permet. Rapprochez le retour d'un compte inconnu, d'une redirection ou d'un fichier déjà supprimé des changements connus, car abandonner le suivi dès la remise en ligne retarde la détection d'une réinfection. Le résultat recherché reste une reprise surveillée avec des seuils d'escalade et un responsable clairement identifié. Pour approfondir ce contrôle sans casser la logique de reprise, la ressource [[ANCRE]] peut servir de repère, à condition de l'adapter au périmètre réellement observé. Le prochain contrôle reste clairement attribué.

1. Préserver une copie de travail avant toute suppression sans modifier plusieurs variables au même moment.
2. Tester les parcours publics et administratifs, puis consigner le résultat avant de poursuivre.
3. Suivre les modifications de fichiers, puis consigner le résultat avant de poursuivre.
4. Documenter ce qui serait perdu ou réintroduit sans modifier plusieurs variables au même moment.
5. Contrôler les données utilisées par les extensions sensibles sans modifier plusieurs variables au même moment.

Quand cette étape peut-elle être considérée comme maîtrisée ?

Sur le plan opérationnel, vérifier la qualité des copies disponibles ne consiste pas à prendre la sauvegarde la plus récente comme choix automatique. L'objectif est de déterminer si une copie est complète, datée dans le bon ordre et suffisamment saine pour servir de point de reprise, avec une progression adaptée au niveau d'incertitude. Commencez par inventorier les copies de fichiers et de base de données, poursuivez avec contrôler leur cohérence dans un environnement séparé, puis utilisez documenter ce qui serait perdu ou réintroduit si le contexte le permet. Rapprochez des sauvegardes partielles, non testées, trop anciennes ou déjà porteuses d'éléments suspects des changements connus, car restaurer sans contrôle peut remettre en place la cause de l'incident ou supprimer des données légitimes. Le résultat recherché reste une décision de reprise fondée sur la qualité réelle des copies plutôt que sur leur simple existence. Le prochain contrôle reste clairement attribué.

Comment garder une mémoire exploitable de l'incident, des hypothèses, des actions et des contrôles ?

Une organisation peut traiter rendre la reprise compréhensible après coup comme un chantier distinct. Elle commence par garder les résultats de validation et les points restant ouverts, enchaîne avec noter l'état avant changement, puis décide de associer chaque action à son motif selon la continuité à préserver. Les observations portant sur des interventions impossibles à attribuer, des fichiers modifiés sans explication ou des décisions reprises plusieurs fois servent à confirmer ou écarter les hypothèses. À l'inverse, consigner uniquement la solution finale fragilise l'analyse, d'autant que sans trace, une équipe répète les vérifications et perd la logique de la reprise. L'étape est avancée lorsque l'équipe obtient un dossier synthétique qui facilite le suivi, la prévention et le passage de relais et sait nommer les incertitudes restantes. Une prochaine revue est nommée sans ambiguïté.

Quelle décision prendre pour la suite ?

Sur le plan opérationnel, vérifier la base de données par zones utiles ne consiste pas à lancer des remplacements globaux sans sauvegarde ni périmètre. L'objectif est de repérer les comptes, contenus, options et tâches stockées qui peuvent conserver une modification malveillante, avec une progression qui sépare observation et correction. Commencez par examiner les utilisateurs et leurs rôles, poursuivez avec rechercher les contenus ou options récemment altérés, puis utilisez contrôler les données utilisées par les extensions sensibles si le contexte le permet. Rapprochez des comptes ajoutés, des scripts dans les contenus, des options inconnues ou des valeurs qui reviennent après nettoyage des changements connus, car ignorer la base de données laisse parfois une source de réinfection invisible dans les fichiers. Le résultat recherché reste des données vérifiées avec prudence, en conservant les relations nécessaires au fonctionnement du site. Le prochain contrôle reste clairement attribué.