5 ÉTAPES ESSENTIELLES

POUR AMÉLIORER LA CYBER-RÉSILIENCE DE VOTRE ENTREPRISE

COHESITY

RÉSILIENCE TOTALE

INTRODUCTION

L'augmentation du nombre d'attaques par ransomware et leurs conséquences de plus en plus graves révèlent une vérité gênante : investir massivement dans la prévention ne suffit pas à contrer les menaces d'aujourd'hui.

Qu'on le veuille ou non, les cyberattaques ne sont pas près de disparaître. Et elles changeront en permanence, que ce soit en termes de fréquence, de gravité ou d'ampleur.

Voilà pour les mauvaises nouvelles.

Et maintenant, la bonne nouvelle. Il existe un playbook éprouvé pour améliorer la cyber-résilience, et des entreprises comme la vôtre l'utilisent pour repenser leur approche et obtenir de meilleurs résultats.

Dans ce livre électronique, nous présentons ce guide opérationnel comme une progression en cinq étapes vers la cyber-résilience. Si vous menez des actions concrètes à chacune de ces cinq étapes, vous vous alignerez sur les bonnes pratiques en matière de réponse aux cyber incidents et de restauration en cas de cyberattaque. Vous en tirerez également des avantages substantiels en termes de sécurité, d'économies et de diminution des risques.

LE CONTEXTE

Malgré une plus grande sensibilisation aux cybermenaces, notamment aux ransomwares, les cyberattaques continuent de causer d'énormes dommages en termes d'exploitation, de finances et de réputation. En réalité, elles représentent la principale menace pour les entreprises à l'échelle mondiale.

L'impact financier est considérable :

540 000 €
de perte par heure d'indisponibilité[1]

Plus d'1 Md€
de rançons versées chaque année suite à des attaques de ransomware[2]

Le rapport de Sophos sur l'état des ransomwares en 2024[3] présente des statistiques tout aussi préoccupantes :

Parmi les 59 % d'entreprises interrogées qui ont été victimes d'un ransomware l'année dernière, **94 % ont déclaré que les pirates avaient ciblé leurs sauvegardes,**, et **57 % de ces tentatives de compromission des sauvegardes ont abouti.**

De plus :

- **70 % des attaques ont entraîné le chiffrement des données.**
- **La rançon demandée s'élevait en moyenne à 2 M€.**
- **34 % des entreprises ont mis plus d'un mois à restaurer leurs systèmes.**

Il est temps de mettre en place de nouvelles stratégies, capacités et solutions plus efficaces.

[1] Splunk, Les coûts cachés des temps d'arrêt : Le problème à 400 Md € auquel sont confrontées les entreprises du Global 2000 (en anglais) : https://www.splunk.com/en_us/pdfs/gated/ebooks/the-hidden-costs-of-downtime.pdf

[2] Chainalysis, Les paiements liés aux ransomwares ont dépassé 1 Md € en 2023, atteignant un niveau record après une baisse en 2022, 07/02/24 (en anglais) : https://www.chainalysis.com/blog/ransomware-2024/

[3] Sophos, L'état des ransomwares en 2024 (en anglais) : https://www.sophos.com/en-us/content/state-of-ransomware

LA CYBER-RÉSILIENCE PEUT S'AVÉRER PARTICULIÈREMENT DIFFICILE POUR DEUX RAISONS :

1. Une cyber-restauration n'est pas une reprise après sinistre.

Même si votre entreprise dispose de solides processus de reprise après sinistre, vous ne pouvez pas compter dessus pour restaurer vos système en cas de cyberattaque.

En cas de sinistre, que ce soit un incendie, une inondation, une panne de courant ou même une erreur de configuration, vous pouvez rapidement effectuer une analyse des causes racines pour comprendre ce qui s'est passé. Lors d'une cyberattaque, il peut se produire des centaines de choses qui nécessiteront une enquête approfondie et des corrections. De plus, votre adversaire s'efforce activement de compromettre vos efforts de restauration et vous presse de payer une rançon.

2. Même les entreprises et les experts les plus avertis peuvent sous-estimer la gravité d'une attaque par ransomware.

Vous pouvez supposer que des systèmes fiables vous aideront à remettre vos systèmes en ligne, ou compter sur des données et des preuves pour comprendre ce qui s'est passé.

Mais lors d'une cyberattaque, les systèmes sur lesquels vous comptez pour enquêter sur l'incident peuvent être hors service, avoir été contournés ou compromis.

Lorsque les données fiables sont mélangées à des données erronées, le processus de restauration est plus long et plus difficile.

Voilà pourquoi de nombreuses entreprises intelligentes ont encore du mal à assurer une restauration rapide, propre et fiable.

5 ÉTAPES ESSENTIELLES POUR AMÉLIORER LA CYBER-RÉSILIENCE

Suivez chaque étape de ce plan pratique pour progresser.

ÉTAPE UN

PROTÉGEZ TOUTES VOS DONNÉES. GRÂCE À UNE GOUVERNANCE GLOBALE.

Cela peut sembler simple, mais de nombreuses entreprises ne franchissent toujours pas cette première étape cruciale, probablement en raison de la prolifération des données.

La croissance organique des données a conduit à leur fragmentation et à la création de silos, ce qui a considérablement élargi la surface d'attaque et rendu les entreprises plus vulnérables que jamais. En parallèle, la gestion et la sécurisation des données à grande échelle pèsent de plus en plus sur l'efficacité opérationnelle.

Cette combinaison (plus de données à plus d'endroits, et moins de capacité pour les gérer efficacement) a créé les conditions idéales pour que les pirates puissent faire des ravages.

AVANTAGES NOTABLES DE L'ÉTAPE UN

- **Sécurité renforcée**
- **Risque réduit**
- **Conformité et gouvernance améliorées**
- **Coûts réduits et ROI amélioré**
- **Efficacité informatique accrue**

ACTIONS CLÉS POUR METTRE EN ŒUVRE L'ÉTAPE UN

1. **Adoptez une plateforme de données moderne qui prend en charge plus de 1 000 sources de données, notamment :**

- Machines virtuelles (VM)
- Applications SaaS
- Bases de données
- environnements NAS (données non structurées)

2. **Assurez-vous que votre plateforme fonctionne dans les environnements en local, dans le cloud et en mode SaaS.**
Vos données étant dispersées, votre plateforme doit disposer de modèles de déploiement flexibles, unifiés par une interface utilisateur (UI) commune et des API.

3. **Simplifiez vos opérations grâce à une UI intuitive.**
Si votre UI est conviviale, même une petite équipe peut gérer efficacement un parc informatique gigantesque. Nos clients bénéficient d'une efficacité opérationnelle supérieure grâce à une UI unique et à un ensemble d'API permettant d'automatiser les flux de travail sur notre plateforme.

4. **Bénéficiez d'une puissante compression du stockage.**
Optez pour une plateforme offrant une forte compression des données. Vous réaliserez ainsi des économies substantielles lorsque vous travaillerez l'échelle du pétaoctet. Le système de fichiers unique que nous proposons est la norme dans le secteur. Une compression de stockage très performante permet de réduire le coût total de possession (TCO).

ÉTAPE DEUX

ASSUREZ-VOUS QUE VOS DONNÉES SONT TOUJOURS RESTAURABLES.

Les attaquants ciblent les sauvegardes. Ils savent que vous serez beaucoup plus enclin à payer une rançon s'ils parviennent à compromettre cette dernière ligne de défense, car votre entreprise n'aura alors pas d'autre recours.

Et s'il est tentant de supposer qu'une plateforme de données moderne garantit d'emblée des sauvegardes restaurables, ce n'est pas tout à fait vrai.

Vous devez prendre plusieurs mesures pour que les attaquants aient plus de difficultés à accéder à vos systèmes, et pour que votre entreprise puisse restaurer des sauvegardes saines s'ils y parviennent.

AVANTAGES NOTABLES DE L'ÉTAPE DEUX

- ☑ **Restauration plus rapide et sécurisée**
- ☑ **Protection renforcée contre les attaques**
- ☑ **Préparation à l'audit**
- ☑ **Alignement avec le Zero Trust**

ACTIONS CLÉS POUR METTRE EN ŒUVRE L'ÉTAPE DEUX

1. **Renforcez votre plateforme en configurant des fonctionnalités puissantes telles que :**

- L'authentification multifacteur (MFA)
- L'immuabilité (afin que les données ne puissent être ni modifiées ni supprimées)
- Les contrôles d'accès basé sur les rôles (RBAC)
- La séparation des tâches (répartition des tâches critiques entre différentes personnes)

2. **Mettez en place une isolation des données**

En protégeant une copie de vos données les plus importantes par air-gap et en respectant la **règle de sauvegarde 3-2-1-1** (trois copies des données, deux supports différents, une hors site et une immuable), vous disposerez toujours d'une copie de vos données en cas d'urgence.

Chez Cohesity, nous fournissons également un système avancé de gestion des clés afin que nos clients puissent toujours accéder à leurs données en cas d'attaque.

Cet accès garantit que les sauvegardes sont toujours restaurables.

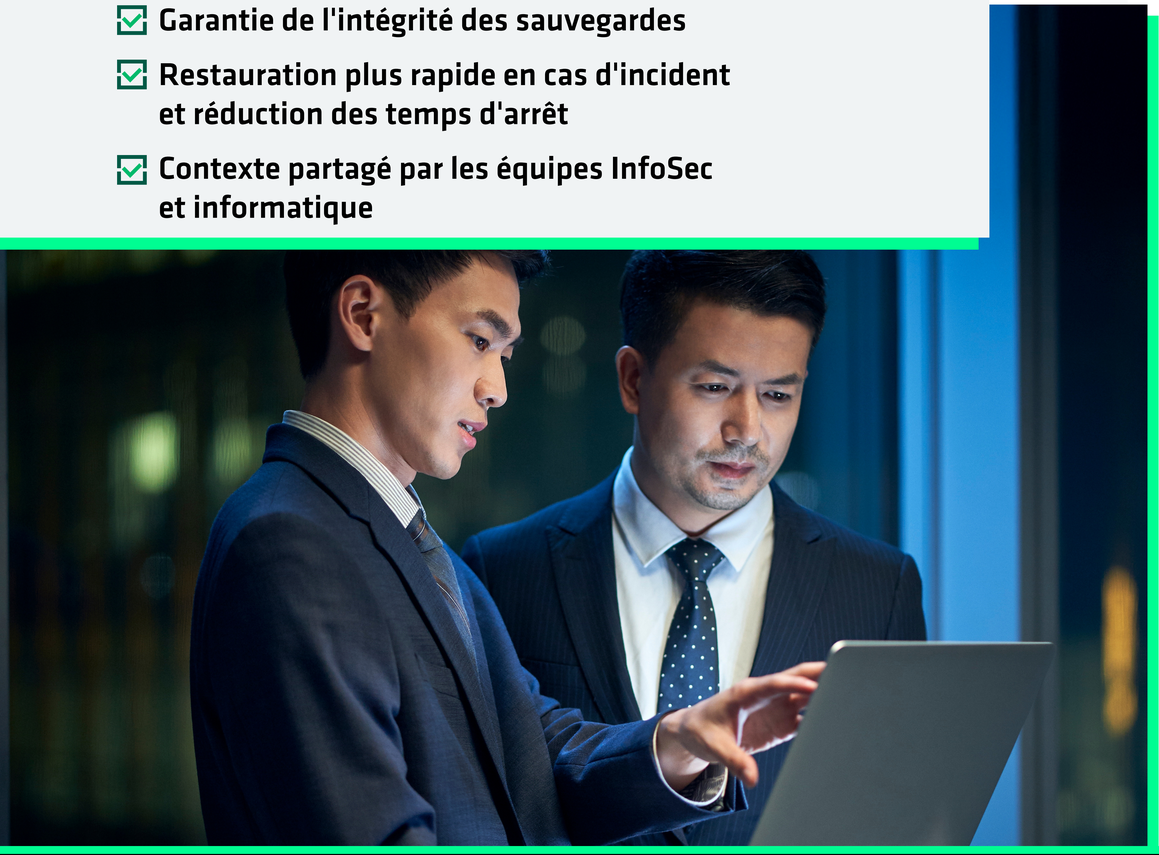
ÉTAPE TROIS

DÉTECTEZ ET ENQUÊTEZ SUR LES MENACES.

Cette étape combine les puissantes capacités d'analyse et de recherche de menaces.

AVANTAGES NOTABLES DE L'ÉTAPE TROIS

- **Détection précoce et atténuation des menaces**
- **Garantie de l'intégrité des sauvegardes**
- **Restauration plus rapide en cas d'incident et réduction des temps d'arrêt**
- **Contexte partagé par les équipes InfoSec et informatique**



ACTIONS CLÉS POUR METTRE EN ŒUVRE L'ÉTAPE TROIS

1. Soyez proactif et recherchez régulièrement les menaces dans vos sauvegardes. Considérez cette **analyse proactive des menaces** comme une règle d'hygiène à respecter en permanence. Cela vous aidera à :

- Éliminer tout changement le plus rapidement possible
- Identifier les logiciels malveillants ou autres vulnérabilités

2. Utilisez les capacités de **recherche de menaces** pour identifier des menaces spécifiques. Nos flux de menaces sélectionnés et nos intégrations avec les fournisseurs de l'écosystème de sécurité de notre alliance pour la sécurité des données, notamment CrowdStrike, Palo Alto Networks, Cisco et bien d'autres, vous permettent de bénéficier à la fois de leur expertise collective et des données que nous pouvons apporter à ces systèmes.

Vos équipes de sécurité de l'information (InfoSec) et informatique disposeront également des mêmes informations.

Nous aidons nos clients à restaurer leurs systèmes en cas de cyberattaque depuis de nombreuses années, et sommes convaincus que votre plateforme de données doit impérativement intégrer des capacités natives de détection et de recherche des menaces.

Pourquoi ? Parce que d'autres systèmes de sécurité peuvent être désactivés ou hors ligne lorsque vous êtes victime d'une attaque.

ÉTAPE QUATRE

PRATIQUEZ LA RÉSILIENCE DE L'APPLICATION.

Vous êtes déjà bien préparé si vous avez suivi les étapes 1 à 3 ci-dessus. Votre plateforme est opérationnelle, renforcée et vous avez étendu votre déploiement avec une solution d'isolation des données.

Vous avez également acquis une bonne expérience pour effectuer des analyses et des recherches de menaces régulières. Bravo !

À l'étape quatre, vous passez à la vitesse supérieure en vous entraînant à répondre et à restaurer vos systèmes pour l'infrastructure, les données et les applications. En effet, mieux vaut éviter de tester ces processus pour la première fois pendant une attaque réelle, lorsque vos systèmes sont hors service et que vous êtes sous pression.

Vous pensez peut-être : « Tout remettre en ligne est un processus chronophage. Comment puis-je effectuer des tests réguliers tout en continuant à faire mon travail quotidien ? »

AVANTAGES NOTABLES DE L'ÉTAPE QUATRE

- ☑ **Restauration plus rapide et plus sûre**
- ☑ **Meilleur RTO**
- ☑ **Moins de risque de réinfection**
- ☑ **Perturbations et risques financiers réduits**

C'est là que l'orchestration entre en jeu.

L'orchestration vous permet d'automatiser les flux de travail de réponse et de restauration, et de commencer à « répéter » la remise en ligne de vos systèmes en cas d'attaque. Ces répétitions vous aideront à améliorer vos capacités de réponse et de restauration, et l'orchestration vous permettra d'affiner ces pratiques tout en réduisant les efforts manuels.

Un exemple clé de l'automatisation à l'œuvre : notre solution de salle blanche vous permet de créer un environnement séparé dans lequel vous pouvez effectuer une analyse des preuves et examiner en détail les données infectées, comprendre ce qui s'est passé, puis éliminer l'artefact de l'attaque pour pouvoir restaurer vos systèmes en toute sécurité. Cette approche offre un mélange unique de rapidité, d'automatisation et de puissantes capacités d'analyse des preuves qui permettent aux personnes chargées de répondre aux incidents de collaborer avec les équipes informatiques. Résultat : une réponse aux cyber incidents et une restauration plus rapides.

À cette étape, vous travaillerez également avec l'équipe CERT de Cohesity (Cyber Event Response Team), qui est chargée de répondre aux cyber-événements. Ces experts vous aideront à répondre aux incidents et à les traiter, qu'il s'agisse de ransomwares sophistiqués, de violations de données ou d'attaques ciblées. Vous ne serez jamais seul.

ACTIONS CLÉS POUR METTRE EN ŒUVRE L'ÉTAPE QUATRE

1. Entraînez-vous grâce à l'orchestration et aux répétitions

- Automatisez vos processus de réponse et de restauration
- Organisez des exercices pour affiner vos plans d'intervention, notamment en ce qui concerne la séquence de récupération de l'infrastructure, des données et des applications

2. Utilisez une salle blanche

- Créez un environnement séparé et sécurisé pour l'analyse des preuves
- Identifiez et éliminez les menaces avant de restaurer l'infrastructure, les sources de données et les applications

3. Bénéficiez de l'assistance d'experts

- Contactez l'équipe CERT de Cohesity si vous êtes victime d'une attaque

ÉTAPE CINQ

OPTIMISEZ VOTRE POSTURE DE SÉCURITÉ DES DONNÉES.

Non seulement les gangs de ransomware sont de plus en plus actifs, mais vous avez également plus de données à gérer que jamais auparavant (en local, en mode SaaS, dans le cloud, à la périphérie). Tout le monde se demande toujours : « Que contient ce compartiment S3 non sécurisé que personne ne connaît ni ne surveille ? »

Outre les compartiments S3 non sécurisés, les risques cachés peuvent également inclure des bases de données orphelines, des identifiants exposés, etc.

Des mesures proactives telles que la gestion de la posture de sécurité des données (DSPM, data security posture management) et la classification des données peuvent contribuer à réduire ces risques.

AVANTAGES NOTABLES DE L'ÉTAPE CINQ

- ☑ **Visibilité et classification des données améliorées**
- ☑ **Identification et atténuation proactives des risques**

ACTIONS CLÉS POUR METTRE EN ŒUVRE L'ÉTAPE CINQ

1. Trouvez où se trouvent vos données

- Analysez votre environnement, identifiez l'emplacement de vos données et évaluez leur niveau de protection. DSPM vous offre toute une gamme d'outils pour accomplir cette tâche.
- Comprenez le contenu de votre patrimoine de sauvegarde et assurez-vous qu'il est correctement protégé grâce à nos intégrations complètes avec certains des meilleurs fournisseurs du secteur, notamment Cyera et BigID.

2. Évaluez les conséquences possibles d'une violation ou ce qui a pu se produire en cas d'exfiltration de données

- Bénéficiez de la couverture dont vous avez besoin et réduisez vos risques grâce à la classification des données intégrée à nos produits.
- Répondez rapidement en cas d'incident lorsque les avocats demandent : Quelles données ont été affectées ? Quel est leur degré de sensibilité ? Quel est le risque pour nous ? Combien de clients ont été touchés ? Quels types d'enregistrements ont été affectés ?

CONCLUSION

Vous comprenez désormais les cinq étapes essentielles pour améliorer la cyber-résilience de votre entreprise, et disposez des informations pratiques nécessaires pour mettre en œuvre ces étapes dans votre environnement.

Chez Cohesity, nous sommes idéalement positionnés pour vous accompagner tout au long de cette évolution afin que vous puissiez bénéficier de la cyber-résilience la plus solide possible.

Pour en savoir plus sur la façon de restaurer rapidement et en toute sécurité après une attaque par ransomware, nous vous recommandons de lire :

« COMMENT ÉLABORER UNE RÉPONSE MILITAIRE ADAPTÉE AUX CYBERATTAQUES DESTRUCTRICES »

COHESITY

RÉSILIENCE TOTALE