COHESITY

LIVRE BLANC

# Comment formuler une stratégie de réponse aux cyberattaques destructrices efficace « en temps de guerre »

Restaurez rapidement et en toute sécurité après une attaque par ransomware ou d'autres cybermenaces grâce à Cohesity

# TABLE DES MATIÈRES

# Synthèse

L'équipe chargée des opérations informatiques (ITOps) doit adopter une autre approche que celle utilisée dans les scénarios traditionnels de continuité de l'activité et de reprise après sinistre pour lutter contre les cyberattaques destructrices, notamment les ransomwares et les attaques de type wiper. Les équipes opérationnelles chargées de la cybersécurité doivent relever plusieurs défis pour garantir le bon déroulement des enquêtes et la mise en œuvre des corrections appropriées. Il ne suffit pas de restaurer les produits et services le plus rapidement possible. Les entreprises doivent également s'assurer que la restauration est effectuée de manière sécurisée pour éviter tout temps d'arrêt supplémentaire dû à une réinfection ou à une nouvelle attaque.

Ce livre blanc documente les bonnes pratiques à mettre en œuvre pour faire face aux cyberattaques destructrices et montre comment Cohesity peut aider votre entreprise à atteindre ces résultats opérationnels.

# Analyse de la situation : pourquoi votre entreprise fonctionne différemment en « temps de paix » et en « temps de guerre »

On entend par « temps de paix » les périodes pendant lesquelles les opérations quotidiennes de votre entreprise se déroulent normalement. Les alertes émises par les outils de sécurité sont généralement envoyées aux consoles de votre centre des opérations de sécurité (SOC) ou de votre fournisseur de services de sécurité gérés. Ces alertes sont triées et classées par ordre de priorité, les faux positifs sont éliminés, et des preuves supplémentaires sont recueillies pour identifier tout signe d'intrusion dans l'infrastructure de votre entreprise. Lorsque les analystes du SOC sont convaincus qu'un acteur malveillant attaque l'entreprise, ils déclarent un incident et poursuivent leur enquête. L'entreprise passe alors en mode « temps de guerre ».

Au cours de l'enquête, si les analystes découvrent que la confidentialité, l'intégrité ou la disponibilité des systèmes et des données de l'entreprise ont été compromises, ils signalent la violation et poursuivent leur processus de réponse aux incidents.

Le temps de séjour d'un acteur malveillant est le temps qu'il passe au sein d'une entreprise avant d'être découvert. Il peut être détecté grâce aux alertes des outils de sécurité. Cependant, les entreprises se rendent souvent comptent qu'elles subissent une attaque seulement lorsqu'elles ne peuvent plus accéder à leurs systèmes. Ce temps de séjour peut varier considérablement. Il peut aller de quatre à cinq jours pour les attaques utilisant un ransomware à la demande (RaaS, Ransomware as a Service) à plusieurs centaines de jours pour les attaques par ransomware pilotées par des individus, voire plusieurs années dans le cas d'attaques menées par des États-nations.

Voici quelques exemples illustrant comment la confidentialité, l'intégrité ou la disponibilité peuvent être compromises :

- **Confidentialité** : Les données de l'entreprise ont été divulguées à des tiers non autorisés. Il peut s'agir de données exfiltrées par des gangs de ransomware à des fins criminelles ou par des États-nations qui espionnent l'entreprise avant de lancer une attaque de type wiper.
- **Intégrité** : Au cours des multiples étapes d'une cyberattaque destructrice, les cybercriminels vont modifier les fichiers de configuration, les registres, les systèmes de gestion des identités et même, dans certains cas, les microprogrammes, afin de persister au sein des entreprises victimes. Tous ces changements affectent l'intégrité des systèmes.
- **Disponibilité** : Une cyberattaque destructrice vise à rendre l'infrastructure informatique de l'entreprise (qui lui est nécessaire pour fournir ses produits et services à ses clients) indisponible. Pour ce faire, les cybercriminels chiffrent les données et/ou les systèmes, comme dans le cas des attaques par ransomware, ou les suppriment, comme lors des attaques de type wiper.

Il est important de comprendre que tous les incidents ne dégénèrent pas. Le SOC détecte constamment des incidents et y répond dès qu'ils apparaissent pour éviter qu'ils ne se transforment en violations. Certaines violations sont contenues en interne et peuvent être gérées à l'aide de manuels standards de réponse aux incidents.

Cependant, certains incidents (en particulier les attaques par ransomware et de type wiper) peuvent avoir un impact considérable. Ils peuvent désactiver les systèmes utilisés pour fournir les produits et services aux clients ainsi que les systèmes informatiques internes nécessaires pour gérer l'incident. Il peut s'agir des systèmes utilisés pour accéder physiquement aux installations, communiquer avec les régulateurs et les parties ou personnes concernées, ou assurer la coordination avec les assureurs, les forces de l'ordre et la presse. L'entreprise peut alors déclarer une **cybercrise** et mettre en place un flux de travail différent pour pouvoir gérer l'incident.

L'entreprise peut reprendre son activité comme en « temps de paix » lorsque les équipes sécurité et informatique ont traité l'incident, la violation ou la crise, restauré les systèmes dans un état fiable et atténué les menaces de récurrence.

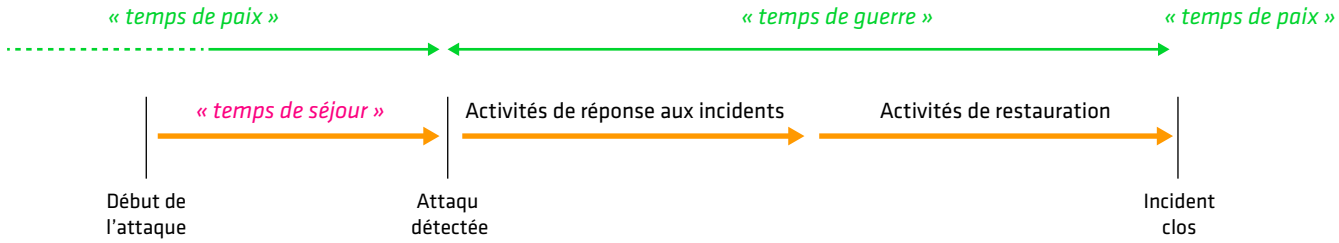



*Illustration 1. Les phases de « temps de guerre » et de « temps de paix » lors d'une cyberattaque destructrice.*

# Pourquoi les cyberattaques destructrices diffèrent de la continuité de l'activité

Les causes profondes des pannes informatiques étaient peu nombreuses avant l'avènement des cyberattaques destructrices : inondation, incendie, défaillance matérielle ou logicielle, erreur de configuration ou coupure de courant. Ces incidents ne nécessitaient qu'un minimum d'enquête, et la réponse standard était simplement de restaurer le dernier snapshot de sauvegarde.

Les ransomwares, en revanche, sont beaucoup plus complexes. Contrairement aux virus ou aux vers traditionnels, ce ne sont pas des fichiers binaires uniques que vous pouvez analyser. Les acteurs malveillants attaquent via une chaîne de 14 étapes, puisant parmi des centaines de techniques pour atteindre leurs objectifs à chaque étape. Ils innovent constamment, rendant les configurations de contrôle de sécurité obsolètes d'un jour à l'autre.

La situation géopolitique mondiale actuelle aggrave encore la menace et augmente le risque que des États-nations lancent des attaques de type wiper. Les capacités opérationnelles, les moyens financiers et la motivation sans précédent de ces auteurs de menaces obligent les entreprises à se doter d'une cyber-résilience supérieure à celle requise pour faire face aux gangs criminels spécialisés dans les ransomwares.

# Investiguer et corriger un logiciel malveillant traditionnel par rapport à un ransomware

Les logiciels malveillants traditionnels, notamment les virus et les vers, sont détectés en analysant les systèmes à la recherche de fichiers binaires malveillants. Une fois identifiés, les équipes de sécurité peuvent simplement les mettre en quarantaine ou les supprimer. Les attaques par ransomware ou de type wiper, en revanche, impliquent une chaîne d'événements qui permettent aux cybercriminels d'accéder à votre infrastructure dans les jours qui suivent l'annonce d'une nouvelle vulnérabilité. Ces attaques peuvent exploiter votre infrastructure informatique pour permettre aux cybercriminels de s'implanter dans votre environnement (attaque de type « **live off the land** », ou LOLT), de profiter de comptes autorisés, de modifier des configurations pour élever des privilèges ou maintenir leur persistance, de préparer des données sensibles en vue de les exfiltrer, et d'utiliser des scripts et des macros natifs intégrés à vos systèmes d'exploitation et applications. Et tout cela en contournant les contrôles qui vous permettent de détecter ces attaques, d'y répondre et de restaurer vos systèmes. Contrairement aux logiciels malveillants traditionnels, il n'y a pas de fichier binaire unique à rechercher et à supprimer.

À la suite d'une attaque par ransomware ou de type wiper, il faut enquêter sur les circonstances de l'incident pour pouvoir restaurer de manière sécurisée. Les entreprises doivent corriger les menaces et les vulnérabilités détectées pour éviter toute réinfection et tout temps d'arrêt supplémentaire. C'est l'essence même de tout cadre de réponse aux incidents de cybersécurité conforme aux bonnes pratiques.

Les entreprises doivent corriger trois éléments critiques pour s'assurer de pouvoir résister à une attaque similaire à l'avenir et empêcher que les systèmes restaurés ne soient à nouveau infectés par l'attaque actuelle :

1. **Surface d'attaque** : Les vecteurs d'accès initiaux des ransomwares les plus courants sont, par ordre de prévalence : les vulnérabilités des infrastructures connectées à Internet, la réutilisation d'identifiants d'accès légitimes et les techniques d'ingénierie sociale, notamment les e-mails de phishing. Vous devez comprendre comment le « patient zéro » (le point d'entrée initial ou la première victime identifiée) a été compromis, puis corriger la menace sur les systèmes restaurés. Cela peut impliquer de corriger les systèmes vulnérables, de les placer derrière une protection, par exemple un pare-feu d'application Web (WAF), et de supprimer l'e-mail de phishing ayant permis l'accès initial de la boîte de réception d'un utilisateur.
2. **Techniques de contournement ou lacunes dans les contrôles de sécurité** : Prévenir ou détecter rapidement les incidents de sécurité (avant qu'ils n'aient un impact sur la confidentialité, l'intégrité ou la disponibilité) engendre des coûts opérationnels, mais permet d'éviter une perte de revenus, une atteinte à la réputation, d'éventuelles amendes réglementaires coûteuses et de potentiels litiges avec les partenaires commerciaux ou les personnes dont les données ont été affectées.

Les gangs de ransomware intègrent des techniques de contournement dans leurs plateformes RaaS afin de déjouer les contrôles de sécurité courants, notamment les outils EDR (Endpoint Detection and Response) et XDR (Extended Detection and Response). Ils ont également l'avantage d'agir en premier, avant que les renseignements sur les cybermenaces ne soient mis à jour et diffusés pour inclure leurs techniques d'attaque.

Avant de relancer la production, vous devez comprendre pourquoi les contrôles de sécurité existants n'ont pas réussi à bloquer ou à détecter l'attaque avant qu'elle n'interrompe les services informatiques. Vous devez ensuite vous assurer que les outils de sécurité sont restaurés dans un état fiable et que leurs règles sont mises à jour afin de prévenir ou de détecter rapidement toute attaque future.

3. **Mécanismes de persistance** : Lors d'une attaque typique de ransomware ou de type wiper, les cybercriminels laissent souvent derrière eux des dizaines d'artefacts. Ceux-ci leur permettent de s'implanter et de continuer à accéder aux systèmes qui seraient restaurés sans avoir été correctement nettoyés. Les entreprises passent souvent des jours à restaurer des systèmes qui seront réinfectés en quelques minutes et remis hors service à cause d'un mécanisme de persistance qu'elles auront négligé. Les cyberattaques destructrices se déroulent en plusieurs étapes. Il faut donc généralement combiner la recherche de menaces et l'analyse de preuves pour établir une chronologie de l'attaque et identifier tous les artefacts à traiter.

# Le malentendu autour des indicateurs de compromission (IOC)

Le concept d'indicateurs de compromission (IOC) est essentiel pour obtenir des renseignements tactiques sur les cybermenaces. Avant de parler des mesures que les entreprises doivent entreprendre en temps de guerre pour faire face à une cyberattaque destructrice, il est important de définir ce qu'est un IOC.

Les IOC fournissent des indices suggérant qu'un système ***pourrait*** avoir été compromis. Les IOC indiquent où commencer à rechercher des comportements malveillants, mais ils ne sont souvent que des indicateurs, et non une fin en soi. Pour restaurer de manière sécurisée, les entreprises doivent dresser un tableau de l'attaque et l'analyser afin de mettre en œuvre les mesures d'atténuation appropriées décrites dans la section précédente. Par exemple, un fichier de configuration modifié qui réexécute un code spécifique au redémarrage est un IOC, au même titre qu'une DLL malveillante qui porte le même nom qu'une DLL légitime et a été déposée dans un répertoire. Manipuler la variable PATH pour que cette DLL malveillante s'exécute avant la DLL légitime est également un IOC. Ces IOC nous indiquent qu'un événement est en cours, mais ils ne brossent pas un tableau complet de l'attaque.

Les entreprises doivent impérativement rechercher les IOC pour pouvoir répondre aux incidents de cybersécurité, mais elles doivent également les appliquer dans le bon contexte. Se fier uniquement aux IOC peut entraîner des actions inappropriées. De plus, restaurer prématurément à partir de sauvegardes sans mener d'enquête approfondie peut entraîner une réinfection ou causer d'autres problèmes de disponibilité.

Mettre aveuglément des fichiers en quarantaine ou restaurer les versions précédentes d'un fichier à partir d'un snapshot de sauvegarde contenant l'IOC ne résout pas la cause profonde. Vous ne savez toujours pas comment les cybercriminels ont réussi à s'introduire pour effectuer ces modifications, donc ils peuvent continuer à attaquer vos systèmes. De plus, rétablir des configurations plus anciennes et incompatibles pourrait entraîner des problèmes de disponibilité. Ceci est particulièrement vrai si, par exemple, les fichiers binaires ont été corrigés et remplacés par des versions plus récentes depuis le début de l'attaque.

De même, l'absence d'IOC dans un snapshot de sauvegarde ne garantit pas qu'il soit « propre ». Les IOC servent simplement à signaler des activités malveillantes. Les supprimer laisse la « destination » intacte. Restaurer automatiquement des snapshots plus anciens peut empêcher l'équipe de réponse aux incidents de détecter l'attaque sous-jacente.

Pour détecter des IOC, il faut également collecter, analyser et diffuser des renseignements sur les cybermenaces. Ceux-ci sont cependant souvent en retard par rapport aux tactiques en constante évolution des cybercriminels. Cela signifie qu'il y a un délai entre le moment où l'acteur malveillant modifie son comportement et celui où nos outils de sécurité détectent les nouvelles techniques d'attaque. Cela explique pourquoi certaines des plus grandes entreprises au monde sont toujours victimes de ransomware bien qu'elles disposent de budgets importants en matière de cybersécurité et que leurs équipes utilisent certainement les outils de cybersécurité les plus récents et les plus performants du marché. Le cybercriminel modifie son comportement avant que les outils de cybersécurité existants ne détectent ce changement, et peut ainsi s'introduire dans l'entreprise sans être détecté. Une fois à l'intérieur, sa capacité à contourner les défenses rend les contrôles de sécurité des terminaux inefficaces. Le temps que le fournisseur de l'outil de sécurité prenne conscience du nouveau comportement de l'acteur malveillant et que les renseignements sur les menaces pertinents soient intégrés à son outil, il est trop tard. L'outil a été contourné et ne se déclenchera pas.

Pour atténuer ces difficultés, envisagez d'adopter en temps de paix une activité comme la recherche proactive et périodique de menaces en utilisant une solution telle que **Cohesity DataHawk**. La solution fonctionne indépendamment des contrôles de sécurité traditionnels et ne peut être contournée. DataHawk vous permet de détecter les attaques qui pourraient avoir échappé aux sources de renseignements sur les cybermenaces.

# Gagner la guerre : enquête, atténuation des menaces et restauration sécurisée

La meilleure approche consiste à renforcer la résilience et la préparation en disposant des solutions technologiques adéquates pour améliorer l'efficacité des personnes chargées d'intervenir en cas d'incident. Il est également important de définir des processus clairs et un modèle opérationnel afin que chacun sache exactement quoi faire. Utilisez l'automatisation et l'orchestration dès que possible. De plus, le personnel doit être correctement formé et participer à des exercices réalistes afin de savoir répondre, et pas seulement réagir, lorsque le pire se produit.

La cyber-résilience n'est pas un produit que l'on peut acheter. C'est une propriété émergente qui se manifeste lorsque votre entreprise est préparée à faire ce qu'il faut lorsqu'un cyber-incident se produit. Pour rendre votre entreprise cyber-résiliente, vous devez collaborer avec un fournisseur qui a une vision réaliste des défis auxquels les entreprises sont confrontées après une cyberattaque destructrice, et qui vous offre la technologie adéquate ainsi que l'assistance nécessaire pour élaborer une stratégie robuste de réponse aux incidents.

**Répondre aux incidents de cybersécurité est une activité complexe. Pour réussir, il faut reconnaître cette complexité, et non l'ignorer. Prétendre le contraire ne fera que nuire à l'entreprise au pire moment possible : lors d'un incident.**

# Bonnes pratiques en matière de cybersécurité, de recherche de preuves numériques et de réponse aux incidents

Il existe quatre cadres largement adoptés pour la recherche de preuves numériques et la réponse aux incidents :

1. Guide de gestion des incidents de sécurité informatique NIST SP800-61
2. Plan de réponse aux incidents en six étapes du SANS Institute
3. Cadre RE&CT (« React »)
4. MITRE D3FEND (« Data-Driven Defense »)

Dans ce livre blanc, nous nous concentrerons sur le modèle du SANS Institute. Cela dit, tous les cadres se rejoignent largement quant aux étapes à suivre pour se préparer à une cyberattaque et y répondre :

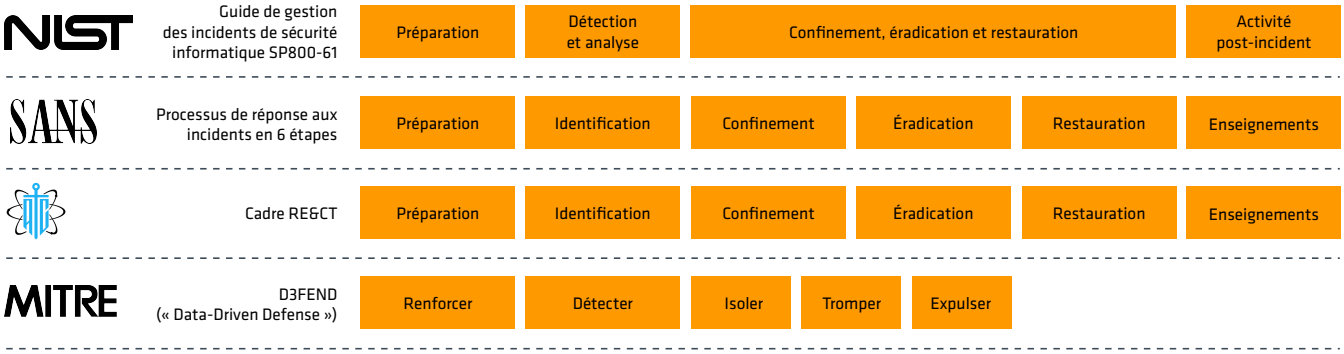



*Illustration 2. Bonnes pratiques en matière de cybersécurité, de recherche de preuves numériques et de réponse aux incidents.*

# Mettre en œuvre les bonnes pratiques opérationnelles avec Cohesity

En situation de guerre, tous les cadres de réponse aux incidents de cybersécurité basés sur les bonnes pratiques incluent les étapes suivantes : confinement, enquête, atténuation des menaces et, enfin, restauration. Les entreprises qui négligent les étapes de confinement, d'enquête et d'atténuation pour passer directement à la restauration laissent en place les vulnérabilités qui ont permis l'attaque.

Les failles dans les défenses qui n'ont pas détecté ou empêché l'attaque restent ouvertes, et souvent, les mécanismes de persistance et autres artefacts de l'attaque sont réactivés. Cela entraîne fréquemment une réinfection ou une nouvelle attaque, et par conséquent des temps d'arrêt prolongés. Il n'est pas rare que les entreprises qui adoptent une approche centrée sur la restauration pour répondre aux attaques par ransomware doivent restaurer leurs données plus d'une douzaine de fois.

## Identification

L'identification se fait en deux étapes :

1. **Prendre conscience qu'un incident potentiel est en cours** : Cela peut être le rapport d'un utilisateur ou d'un tiers à trier pour que sa validité et son périmètre soient confirmés, ou une alerte provenant d'un contrôle technique.
2. **Comprendre comment l'attaque s'est produite** : Cela garantit que la menace est correctement éliminée, que les vulnérabilités exploitées sont supprimées et que les contrôles sont renforcés. Les systèmes peuvent ainsi être restaurés dans un état sécurisé et résilient.

Examinons chaque étape plus en détail.

### Prise de conscience initiale

Techniquement, la prise de conscience initiale est une activité menée en temps de paix. En effet, l'entreprise ne peut pas déclarer être en guerre tant qu'elle n'a pas détecté qu'une attaque est en cours. Il est donc important de discuter des mécanismes de détection des attaques telles que les attaques par ransomware pour comprendre comment cela peut affecter le flux de travail de réponse aux incidents.

Les plateformes RaaS ont banalisé le contournement des outils de sécurité populaires tels que l'EDR et le XDR, les rendant incapables de détecter les attaques. Dans le cadre MITRE ATT&CK, la taxonomie la plus populaire pour décrire la manière dont les cyberattaques sont menées, la tactique d'évasion de la défense compte près de deux fois plus de techniques que la tactique classée juste après parmi les 13 existantes. Ces mécanismes utilisés par les auteurs d'attaques par ransomware ne peuvent pas échapper à la détection d'anomalies de **Cohesity DataProtect** et aux capacités de recherche de menaces de DataHawk.

Les alertes, notamment celles générées par la **détection d'anomalies basée sur l'IA** de DataProtect, affichent un haut niveau de **fiabilité**, ce qui garantit qu'il ne s'agit pas de faux positifs. Elles sont également très **précises**, c'est-à-dire que l'analyste SOC reçoit dans l'alerte des informations détaillées sur ce qui se passe. Cela accélère le processus de triage et d'investigation, et réduit ainsi le temps nécessaire pour restaurer les systèmes en production de manière sécurisée.

Si, lors du triage, il apparaît que les systèmes nécessaires pour répondre aux incidents ont été affectés, ou que le chiffrement ou la suppression de systèmes dans l'entreprise dépasse un certain seuil prédéfini, l'entreprise peut déclarer une **cybercrise**. Un flux de travail prédéfini en cas de cybercrise permet à une entreprise de mettre en place différentes escalades, et d'établir à l'avance l'autorité qu'auront les personnes chargées de répondre aux incidents pour mener certaines actions dépassant le cadre de leurs fonctions habituelles en cas de cyber-violation.

Il peut s'avérer que les systèmes nécessaires à la réponse aux incidents soient affectés, indisponibles ou pas fiables. Cette situation peut engendrer les problèmes suivants :

- Les listes de contact des parties prenantes chargées de répondre aux incidents (dirigeants, régulateurs, fournisseurs de cyber-assurance, sociétés de réponse aux incidents sous contrat, partenaires de la chaîne logistique et presse) peuvent être indisponibles.
- Les flux de travail de réponse aux incidents peuvent être indisponibles.
- Les contrats de votre police de cyber-assurance et les intervenants chargés de répondre aux incidents peuvent ne pas être disponibles.

- Les serveurs de gestion et les configurations des systèmes de contrôle d'accès physique ou des contrôles environnementaux des bâtiments peuvent être hors service.
- Les systèmes de communication nécessaires pour contacter les parties prenantes, notamment les e-mails ou la VoIP, peuvent être indisponibles ou ne pas être fiables.
- Les configurations ou les microprogrammes des routeurs et des commutateurs peuvent ne pas être fiables, auquel cas les connexions Internet des applications logicielles à la demande ou les communications peuvent être surveillées ou perturbées.
- Les outils de sécurité peuvent avoir été contournés ou rendus inutilisables.

Il est compréhensible que la plupart des entreprises privilégient la restauration des applications les plus critiques, c'est-à-dire celles qui sont indispensables pour reprendre la fourniture de leurs produits et services (également appelées « Minimum Viable Company », ou MVC). Cependant, les entreprises victimes d'une cyberattaque destructrice se rendent compte qu'un sous-ensemble de comptes, d'applications et d'infrastructures est également nécessaire pour gérer efficacement l'incident. Ces systèmes garantissent que l'entreprise peut restaurer ses systèmes de production critiques dans un **état sécurisé** tout en respectant ses obligations réglementaires.

Cohesity définit ce sous-ensemble d'infrastructures et de ressources indispensables pour gérer les efforts de réponse et de restauration comme la capacité de réponse minimale viable (MVRC). Supposons que certains composants de la MVRC ne soient plus fiables ou plus disponibles. Dans ce cas, les entreprises doivent pouvoir rendre ces ressources disponibles rapidement et reconstituer un ensemble d'outils fiables pour gérer les actions de réponse. La **solution de salle blanche de Cohesity** permet aux entreprises de restaurer rapidement leur MVRC dans un état fiable et de rendre les ressources nécessaires à la gestion de l'incident disponibles en quelques minutes.

## Comprendre comment l'attaque s'est produite

Une fois que le triage initial est terminé et qu'il est certain qu'une cyberattaque destructrice est en cours, l'analyste déclare un incident et poursuit son enquête de manière plus approfondie. En règle générale, les gangs de ransomware déploient leurs chiffreurs sur les serveurs et les terminaux en dernier lieu, car c'est l'étape la plus bruyante de l'attaque, celle qui risque le plus de déclencher des contrôles de détection et d'avoir des impacts visibles pour les utilisateurs finaux.

Enquêter et corriger uniquement les systèmes chiffrés ne permettra probablement pas de découvrir la cause profonde de l'attaque. L'enquête doit s'étendre au-delà de ces systèmes. Les systèmes non chiffrés sont souvent plus intéressants pour l'enquêteur, car ils sont susceptibles de contenir des mécanismes de persistance que les cybercriminels pourraient utiliser pour revenir après toute tentative de restauration.

Avant d'examiner plus en détail ce niveau d'identification avancé, il est important de comprendre comment le confinement, un autre aspect des processus de réponse aux incidents basés sur les bonnes pratiques, peut nous empêcher de mener cette tâche à bien.

# Confinement

Les cadres de réponse aux incidents exigent tous la mise en place d'un confinement, car celui-ci empêche l'attaque de se propager et interrompt toute activité de commande et de contrôle ou d'exfiltration de données. Cependant, le confinement présente également certains défis pour les équipes chargées de la sécurité opérationnelle (SecOps) :

- **L'imagerie à distance ne fonctionne pas dans un environnement isolé**. La plupart des entreprises n'acquièrent plus physiquement le contenu des disques durs mais privilégient l'imagerie des preuves à distance. Cependant, isoler un hôte infecté (ou le réseau de l'hôte) peut soudainement empêcher l'entreprise d'accomplir cette tâche. **DataProtect** fournit une interface utilisateur et une API qui permettent à la personne chargée de répondre aux incidents d'effectuer une analyse des preuves au niveau des fichiers, non seulement sur le dernier snapshot, mais sur toute une série de snapshots sur l'ensemble de la période de rétention définie par l'entreprise. Cela permet aux analystes des preuves numériques de voyager dans le temps à la recherche des fichiers binaires et autres artefacts que le cybercriminel aurait supprimés, et d'identifier rapidement les modifications malveillantes apportées aux configurations et autres fichiers. Contrairement aux solutions de sécurité des terminaux et aux SIEM qui conservent généralement les journaux sur une courte période, Cohesity permet aux personnes chargées de répondre aux incidents d'examiner les événements et le contenu des journaux sur toute la période pendant laquelle les sauvegardes du système sont conservées, le tout étant fourni par une plateforme immuable afin de garantir une chaîne de contrôle solide. Mieux encore, ces capacités sont fournies sans connexion réseau. Elles ne peuvent donc pas être espionnées ni perturbées, car DataProtect utilise une copie hors ligne du système de fichiers pour cette tâche.

- **Les solutions de terminaux sont isolées, et il devient impossible d'envoyer des requêtes ou de recevoir des réponses.** Bien que l'architecture des différentes solutions pour terminaux, notamment les EDR et les XDR, puisse varier, presque toutes disposent d'un serveur de gestion central qui reçoit les données télémétriques des clients des terminaux. Si le confinement coupe la connexion entre le serveur de gestion et les terminaux, les analystes n'ont plus que les informations précédemment envoyées au serveur de gestion. Ils ne peuvent plus travailler en mode « question-réponse » pour approfondir en temps réel ce qui se passe sur les terminaux.
- Le confinement implique également de créer des environnements isolés dans lesquels il est possible de mettre en œuvre des techniques de réponse aux incidents et de restauration. La solution de salle blanche de Cohesity offre une approche flexible pour créer de tels environnements. Elle permet aux entreprises de s'aligner sur les bonnes pratiques en matière de réponse aux incidents et d'adopter un modèle de responsabilité partagée approprié entre l'équipe chargée de la sécurité opérationnelle (SecOps) et celle chargée des opérations informatiques (ITOps). Cette approche permet aux entreprises d'éviter les temps d'arrêt prolongés et de prévenir toute réinfection une fois la restauration terminée.
- La solution de salle blanche de Cohesity :
- Permet de restaurer rapidement la MVRC ou l'infrastructure affectée ou contournée, ce qui est indispensable pour enquêter sur l'incident et le corriger.
- Établit un environnement d'enquête isolé qui permet aux équipes SecOps d'utiliser les capacités de sécurité natives de la **plateforme Cohesity Data Cloud** en plus de leurs outils de sécurité pour comprendre l'attaque de bout en bout, planifier les corrections appropriées, et ainsi prévenir de futures attaques.
- Crée un environnement d'atténuation isolé dans lequel les résultats de l'enquête de l'équipe SecOps servent à déterminer quelles corrections apporter. Il peut s'agir de reconstruire rapidement des systèmes à partir d'images d'installation et de configurations éprouvées, de restaurer des systèmes et de corriger leurs vulnérabilités, de renforcer les contrôles afin qu'ils ne puissent pas être contournés, et de réussir à prévenir ou à détecter de futures attaques similaires. Enfin, il est possible de tester la fonctionnalité et les performances des systèmes avant de les restaurer dans les systèmes de production.

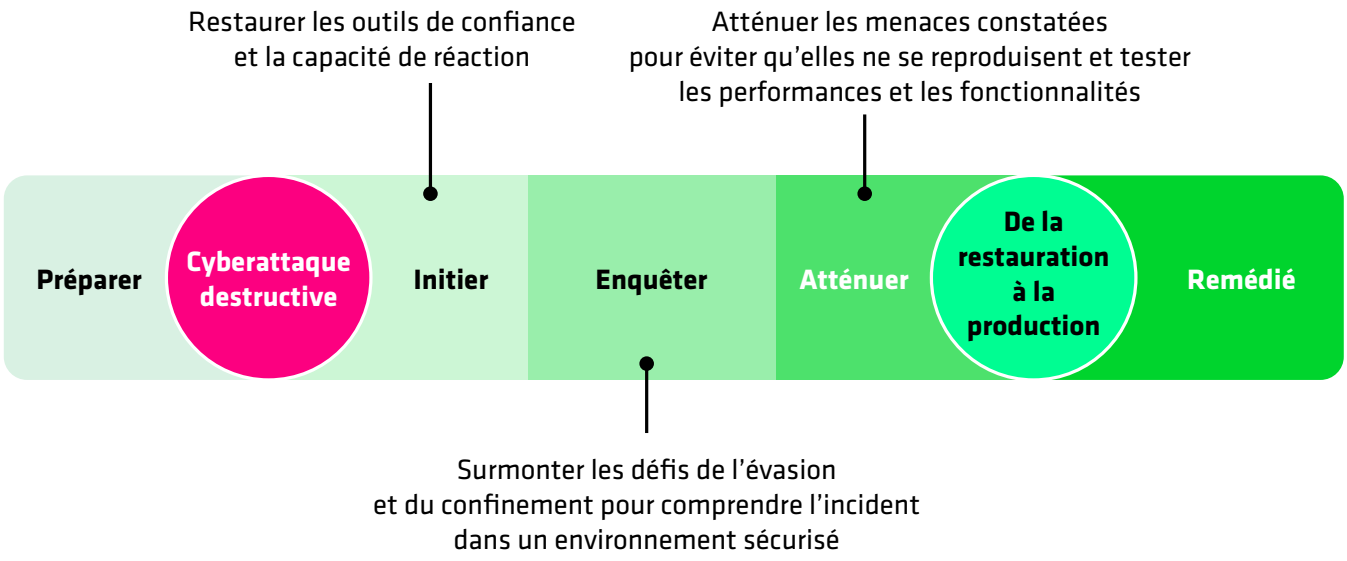



*Illustration 3. Les quatre étapes de la solution de salle blanche de Cohesity qui permettent aux clients de corriger les cyberattaques.*

# Repenser l'identification : comment la solution de salle blanche de Cohesity peut vous aider

L'entreprise a suivi les bonnes pratiques en matière d'analyse des preuves numériques et de réponse aux incidents et a maintenant isolé les réseaux et les hôtes infectés. À ce stade, l'infrastructure affectée qui est nécessaire pour enquêter sur l'incident et le corriger est remise dans un état fiable : vous pouvez faire confiance à votre connexion Internet et utiliser vos services informatiques, métier et de sécurité dans le cloud. En outre, votre capacité de communication avec les parties prenantes est rétablie. Plus important encore, vos équipes SecOps et ITOps ont désormais toutes les ressources et la documentation requises pour prendre en charge la réponse aux incidents et la restauration.

Nous allons maintenant voir comment Cohesity permet d'approfondir l'enquête lorsque les ressources sur lesquelles vous enquêtez ont été isolées par le confinement.

## Découvrir les vulnérabilités exploitées lors de l'attaque

Les gangs de ransomware et les États-nations qui se préparent à lancer des attaques de type wiper obtiennent généralement un premier accès en exploitant les vulnérabilités des ressources connectées à Internet. Il est même arrivé que des cybercriminels obtiennent un accès initial grâce à des vulnérabilités, installent des mécanismes de persistance leur permettant de rester sur les systèmes, puis des correctifs afin d'empêcher d'autres pirates d'y accéder.

Comment les entreprises peuvent-elles déterminer quelles vulnérabilités existaient au moment d'une attaque ? Cette tâche s'avère encore plus difficile si l'adversaire a effacé le système ou si des mesures de confinement empêchent d'accéder au système pour faire une analyse des vulnérabilités.

La solution **Cohesity CyberScan** permet aux entreprises d'analyser les snapshots de sauvegarde à la recherche de vulnérabilités en utilisant leur licence Tenable Vulnerability Management. Cela permet aux équipes de sécurité d'identifier les vulnérabilités pendant une attaque même si un système est inaccessible parce qu'il est confiné, qu'il a été effacé ou corrigé par un cybercriminel après une intrusion.

## Analyser les preuves sur le système de fichiers

L'analyse des preuves sur un système de fichiers est une discipline fondamentale de la réponse aux incidents. De nombreuses entreprises utilisent des outils d'acquisition à distance pour l'imagerie des preuves. Cependant, une fois les mesures de confinement en place, les systèmes qui nécessitent une imagerie des preuves ne sont souvent plus accessibles.

DataProtect permet aux analystes d'accéder non pas à un seul snapshot du volume des systèmes de fichiers, mais à toute une série chronologique de snapshots. Cela permet aux enquêteurs de revenir sur la chronologie d'un incident et de consulter l'ensemble de la période de rétention des sauvegardes. Il est possible de monter rapidement une série chronologique de volumes et de la comparer pour identifier les deltas malveillants. Les objets de fichiers peuvent être extraits pour mener des opérations de rétro-

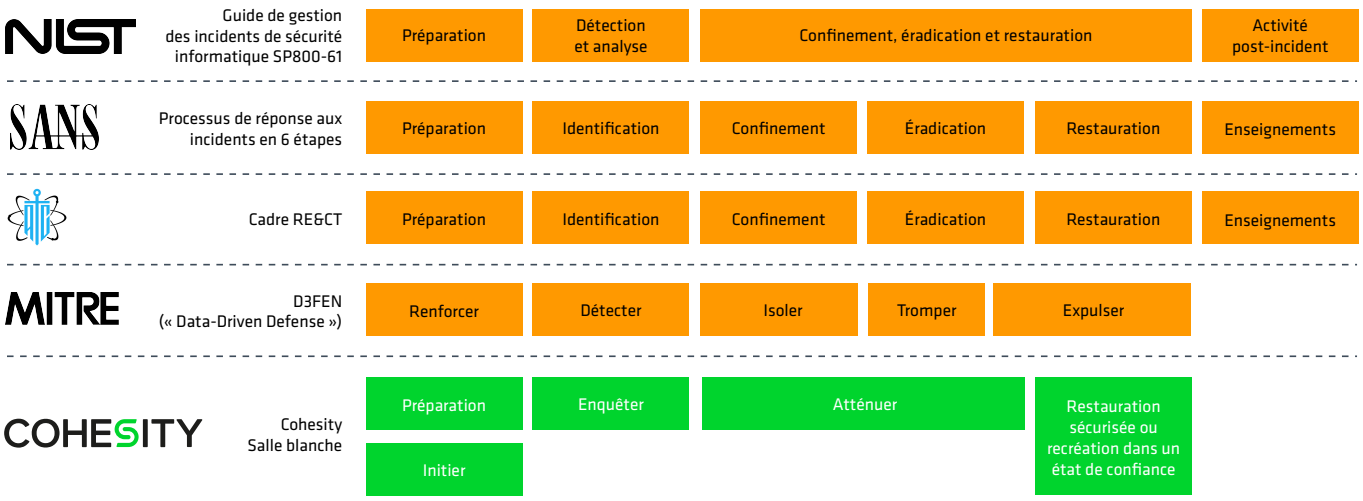



*Illustration 4. Alignement de la salle blanche de Cohesity sur les bonnes pratiques en matière de réponse aux incidents*

ingénierie, pour exploser dans des bacs à sable, ou pour les envoyer vers des services dans le cloud afin qu'ils soient analysés.

Dans l'analyse des preuves numériques traditionnelle, les personnes chargées de répondre aux incidents collectent généralement une seule image du système après l'attaque, émettent une hypothèse sur la manière dont le système s'est retrouvé dans cet état, puis remontent le temps pour rassembler des preuves permettant de confirmer ou d'infirmer cette théorie. En revanche, avec DataProtect, ces intervenants peuvent voir les modifications apportées au système de fichiers sur une période beaucoup plus longue, même si les efforts de confinement ont isolé l'hôte infecté.

## Recherche de menaces

Les personnes chargées de répondre aux incidents doivent généralement aussi rechercher les IOC. Cette recherche se pratique en temps de guerre et peut être classée en deux catégories :

**Recherche d'IOC fournis par un tiers**. Celui-ci peut être un fournisseur de renseignements sur les cybermenaces, une agence gouvernementale, ou des entreprises similaires. Les clients de Cohesity qui utilisent DataHawk peuvent bénéficier du flux fréquemment mis à jour de plus de 117 000 IOC utilisés par les auteurs de ransomware et les États-nations. La capacité d'analyse des menaces de DataHawk prend également en charge les flux de renseignements sur les menaces commerciaux de CrowdStrike pour lesquels l'entreprise possède une licence, et peut utiliser tout IOC fourni au format YARA par d'autres tiers.

**Analyse des IOC découverts par votre entreprise**. Les personnes chargées de répondre aux incidents qui trouvent des artefacts au cours d'une enquête voudront vérifier si ces IOC existent dans toute l'infrastructure de l'entreprise. À partir de là, elles détermineront s'il faut inclure d'autres systèmes dans le périmètre de la réponse aux incidents.

Pour ce faire, on crée généralement des règles YARA qui décrivent l'artefact trouvé de manière à ce qu'il puisse être détecté sans générer de faux positifs inutiles. Avec Cohesity, vous pouvez effectuer une analyse des preuves (comme indiqué dans la section précédente), extraire des artefacts du système de fichiers, et les faire exploser dans des bacs à sables comme Cuckoo qui, grâce à un plug-in, peut générer automatiquement des règles YARA pour tous les IOC liés à ce fichier. La capacité de recherche de DataHawk ne dépend pas des agents des terminaux. Elle continue de fonctionner même si l'entreprise a isolé ses systèmes pour les confiner. Elle n'est pas vulnérable aux techniques courantes de contournement de la défense qui empêchent les solutions de sécurité des terminaux de détecter efficacement les menaces.

Des capacités telles que Cohesity Global Search permettent aux personnes chargées de répondre aux incidents de rechercher rapidement des fichiers dans toute l'infrastructure sauvegardée. Cela peut les aider à orienter

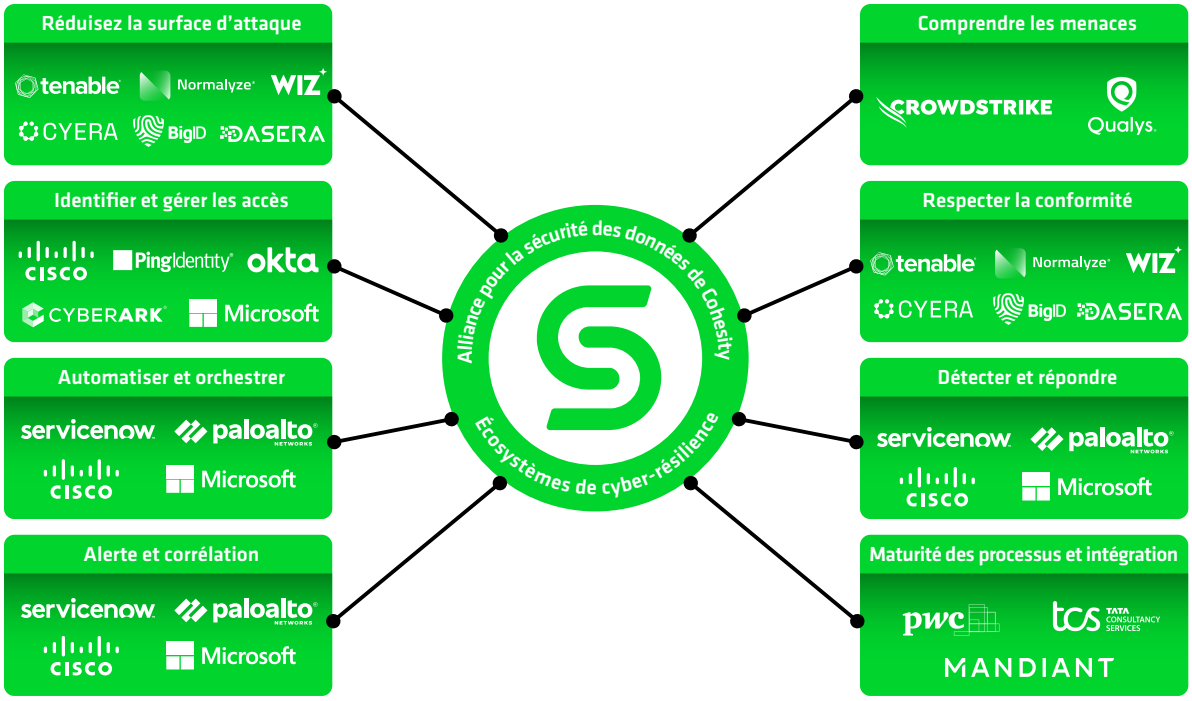



*Illustration 5. Alliance pour la sécurité des données de Cohesity : Un écosystème pour la cyber-résilience.*

leurs efforts d'investigation lorsqu'ils recherchent un artefact ou un fichier particulier.

## Satisfaire aux exigences réglementaires

De nombreuses réglementations récemment mises à jour (notamment HIPAA, DORA et NIS 2) imposent non seulement des processus solides de réponse aux incidents, mais exigent également des entreprises qu'elles informent les régulateurs et les personnes concernées en cas de violation de la cybersécurité. Pour identifier une violation, il faut comprendre sa nature, évaluer son impact et veiller à ce que les personnes concernées soient informées en temps opportun.

Si l'incident a affecté la communication, Cohesity permet de restaurer cette capacité dans le cadre de la MVRC. Les modèles de communication peuvent être conservés dans le **Digital Jump Bag**™, l'élément fondamental sur lequel repose toute salle blanche. De plus, DataHawk peut **analyser les sauvegardes pour identifier les données sensibles et réglementées** afin de permettre aux entreprises de respecter leurs obligations réglementaires. Cela s'avère particulièrement utile après une cyberattaque destructrice, lorsque des magasins de données critiques sont chiffrés ou effacés.

## Intégration des outils de la sécurité opérationnelle

La cyber-résilience est un sport d'équipe : aucun fournisseur ne peut à lui seul enquêter sur un incident et y apporter toutes les corrections nécessaires. C'est pourquoi Cohesity a créé l'**alliance pour la sécurité des données**. Cet écosystème collaboratif permet de mettre la puissance des données et des données dans le temps au service d'outils et de services de sécurité plus larges grâce à des intégrations visant à assurer une gouvernance, une investigation et une restauration communes.

## Automatisation et orchestration

Cohesity prend en charge l'intégration des API afin qu'une plateforme SOAR (Security Orchestration and Automated Response) puissent piloter ces tâches d'investigation et rendre les analystes encore plus efficaces.

# Éradication et restauration

Nous avons fusionné les étapes d'éradication et de restauration en une seule étape d'atténuation car, chez Cohesity, nous estimons qu'aucune entreprise ne devrait chercher à restaurer son activité après une cyberattaque destructrice sans prendre les mesures nécessaires pour empêcher l'attaquant de réinfecter ses systèmes ou de mener une nouvelle attaque similaire.

La solution de salle blanche de Cohesity permet de rapidement restaurer des volumes. Il est ainsi possible de restaurer l'intégralité d'un système de fichiers avant d'appliquer les mesures d'atténuation nécessaires pour éliminer les menaces. Cela garantit de pouvoir restaurer le système de manière sécurisée et facilite la reconstruction rapide des systèmes à partir d'images logicielles fiables et de configurations éprouvées. Chaque approche a ses avantages et ses inconvénients :

| **Approche basée sur la restauration et le nettoyage** | |
|---|---|
| **Avantages :** | **Inconvénients :** |
| Il est plus simple de gérer un incident avant qu'il ne se produise. | Les enquêtes doivent être plus approfondies. |
| | Il faut généralement plus de temps pour corriger que pour reconstruire les systèmes. |
| **Approche basée sur la reconstruction** | |
| **Avantages :** | **Inconvénients :** |
| Possibilité de restaurer les données, de reconstruire les systèmes et d'enquêter sur les incidents en parallèle, ce qui permet de restaurer très rapidement les systèmes dans un état sécurisé. | L'enquête n'a généralement pas besoin d'être aussi poussée, car les systèmes sont dans un état fiable. |
| La correction est plus rapide, car il suffit généralement de valider la sécurité des configurations, de renforcer les contrôles et d'appliquer des correctifs sur les systèmes vulnérables. | Créer des scripts de réinstallation nécessite des compétences particulières. |
| | Les supports d'installation, les clés de licence, les fichiers de configuration et les scripts doivent être conservés dans le digital jump bag. |

Certains clients de Cohesity choisissent de prendre en charge à la fois les sauvegardes et les reconstructions au niveau du volume. Cela leur permet de choisir la méthode de restauration sécurisée la plus appropriée pour chaque hôte compromis, en fonction du niveau d'effort requis pour nettoyer ce système et du degré de certitude que le nettoyage ne laissera aucun artefact de l'attaque.

Les clients transforment souvent leur environnement de développement pour l'utiliser comme environnement d'atténuation de la salle blanche de Cohesity. Cette approche permet de mettre à plat les serveurs de production tout en poursuivant les activités d'atténuation dans l'environnement isolé de la salle blanche. L'environnement d'atténuation est configuré pour imiter la structure de l'environnement de production à l'aide des configurations stockées dans le digital jump bag.

Les systèmes peuvent être testés une fois que les menaces découvertes pendant la phase d'investigation ont été atténuées grâce à la restauration et au nettoyage ou à la reconstruction dans un état fiable. Il peut s'agir de tests fonctionnels et/ou de tests de performance destinés à vérifier que la correction, l'application de correctifs et le renforcement des contrôles n'ont pas affecté la capacité du système à fonctionner.

Pour finir, un snapshot de ces systèmes est pris, et ce pour deux raisons :

1. Si un artefact d'attaque vous échappe, vous n'avez pas besoin de recommencer depuis le début. Le snapshot pris après la correction servira de nouvelle base de référence pour l'investigation et les corrections supplémentaires, et sera transmis à l'étape d'enquête.
2. L'environnement d'atténuation ayant été configuré pour ressembler à l'environnement de production, ce snapshot peut simplement être « transféré » sur le réseau de production.

# Enseignements

Toute entreprise souhaitant renforcer sa cyber-résilience doit suivre une stratégie d'amélioration continue. Il est essentiel de comprendre ce qui a fonctionné, ce qui n'a pas fonctionné et ce qui pourrait être amélioré pour garantir que l'entreprise ne subisse pas de temps d'arrêt prolongés et puisse gérer les incidents futurs de manière plus efficace et efficiente. Comme le dit l'adage, « aucun plan ne survit au contact de l'ennemi ». Il est important de simuler des attaques réelles pour tester la restauration technique, améliorer les processus, identifier les possibilités d'automatisation et développer la mémoire musculaire de vos analystes et des personnes chargées de répondre aux incidents.

L'un des principaux avantages de la solution de salle blanche de Cohesity est qu'elle permet aux entreprises de simuler un incident complet de bout en bout sans affecter les systèmes de production. DataProtect permet de cloner des systèmes de production. Ceux-ci peuvent ensuite être attaqués par une équipe interne ou une société externe spécialisée dans les tests de pénétration afin de simuler une attaque par ransomware ou de type wiper de bout en bout. Il est possible d'effectuer l'intégralité du flux de travail de réponse et de restauration immédiatement après avoir pris le snapshot de référence des systèmes corrigés. Les entreprises disposent ainsi d'un scénario réaliste qui leur permet de s'assurer que les personnes, les compétences, les processus et les technologies d'assistance adéquats sont en place pour minimiser l'impact d'une cyberattaque destructrice le jour où elles en seront victimes.

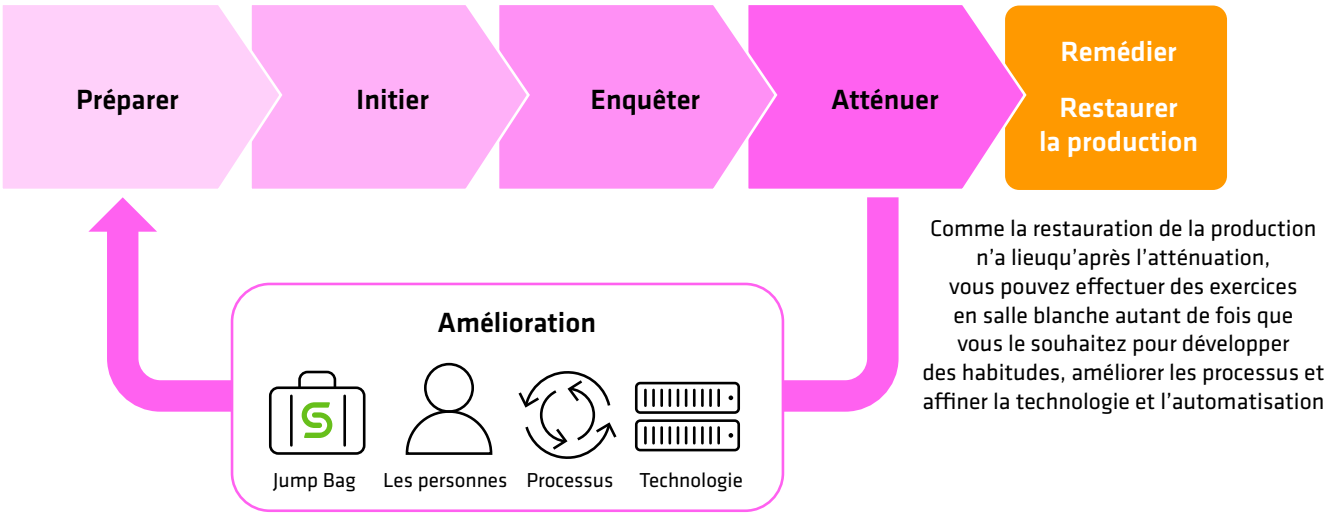
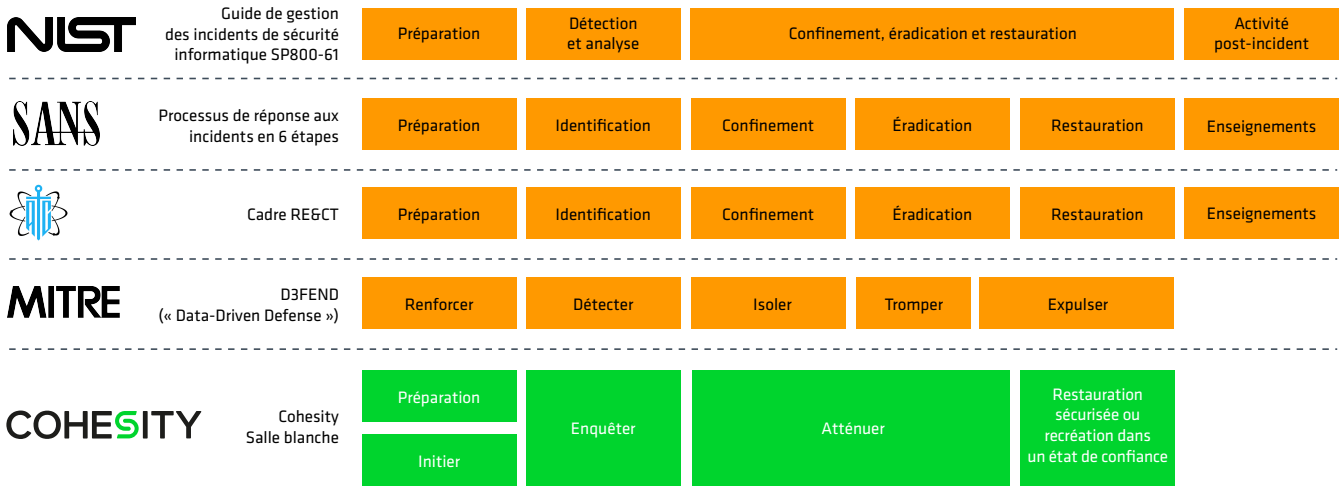



*Illustration 6. La solution de salle blanche de Cohesity permet de s'améliorer en permanence grâce à des exercices réalistes.*

# Résumé

Cohesity peut apporter une valeur ajoutée considérable en matière de restauration et rendre les étapes de l'analyse de preuves numériques et de la réponse aux incidents en temps de guerre à la fois efficaces et efficientes. Notre approche unique de la cyber-résilience réduit le temps nécessaire pour restaurer de manière sécurisée et permet aux entreprises de s'assurer qu'une attaque similaire n'entraînera pas de temps d'arrêt.



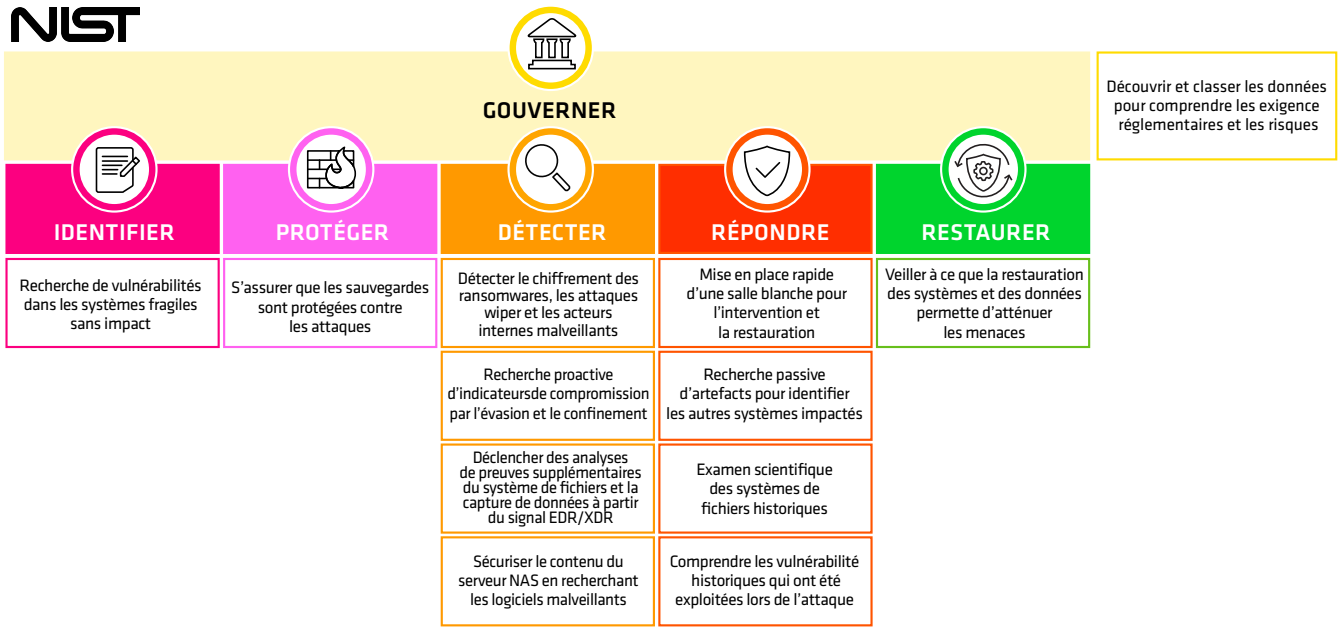




*Illustration 7. Répondre aux cyber-incidents et mettre en œuvre les bonnes pratiques du cadre de cybersécurité du NIST avec Cohesity*

# À propos de Cohesity

Cohesity est le leader de la sécurité des données alimentée par l'IA. Plus de 13 600 entreprises, dont plus de 85 des entreprises du Fortune 100 et près de 70 % des entreprises du Global 500, font confiance à Cohesity pour renforcer leur résilience et leur fournir des informations générées par l'IA générative à partir de leurs grandes quantités de données. Les solutions de l'entreprise, qui sont issues de la fusion entre Cohesity et l'activité de protection des données d'entreprise de Veritas, permettent de sécuriser et de protéger les données en local, dans le cloud et à la périphérie. Soutenue par NVIDIA, IBM, HPE, Cisco, AWS, Google Cloud et d'autres, Cohesity a son siège à Santa Clara, en Californie, et des bureaux dans le monde entier. Pour en savoir plus, suivez Cohesity sur **LinkedIn**, **X** et **Facebook**.

# Lectures recommandées

Vous trouverez ci-dessous des livres blancs, des guides et des articles de blog qui pourraient vous être utiles.

- Améliorez votre cyber-résilience avec un digital jump bag ™
- Renforcez votre cyber-résilience dans un monde en proie à des cyberattaques destructrices
- Présentation de la conception de la salle blanche de Cohesity (en anglais)
- Guide pratique sur la sécurité des données alimentée par l'IA : comment obtenir des résultats commerciaux exceptionnels
- Guide à l'usage des cadres pour une sécurité et une gestion modernes des données (en anglais)
- Topologies modernes de sécurité et de gestion des données : un guide pour les responsables informatiques

## En savoir plus sur Cohesity



COHESITY

cohesity.com/fr/
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

2000058-002-FR 4-2025