COHESITY

LIVRE BLANC

Améliorez votre cyber-résilience avec un digital jump bag™

Comment restaurer rapidement une capacité de réponse minimale viable et renforcer la réponse aux incidents

TABLE DES MATIÈRES

Préface

James Blake
Vice-président en charge de
la stratégie de cyber-résilience

Cela fait plus de 30 ans que je suis en première ligne lorsqu'il faut répondre aux cyberattaques destructrices et au vol de données. J'ai de l'expérience dans la gestion des réponses aux incidents, notamment aux attaques de type wiper provenant d'États-nations, et ai été responsable de la gestion des cyber-risques pour la plus grande banque au monde.

Au cours de cette période, j'ai appris l'importance d'avoir un « jump bag ». À l'origine, ce terme désignait un conteneur physique contenant le matériel et les logiciels essentiels nécessaires pour intervenir sur un site physique victime d'une attaque. Ce sac d'intervention contenait tout le nécessaire pour enquêter rapidement sur l'incident, recueillir des preuves et atténuer les menaces. Outre le matériel et les logiciels, il contenait des éléments tels que des copies papier de la liste des principales personnes à contacter en interne et en externe, le plan de gestion de crise, les procédures à suivre selon le type d'incident auquel j'étais susceptible de répondre, ainsi qu'un téléphone portable. L'idée était d'être prêt à répondre immédiatement : lorsqu'on est sous la pression d'un incident, courir partout à la recherche de ce dont on a besoin fait perdre un temps précieux et peut conduire à oublier quelque chose d'essentiel. Le sac d'intervention contenait des outils, des détails sur les processus et un moyen de communication.

Aujourd'hui, nous vivons dans un monde d'acquisition à distance, de systèmes EDR (Endpoint Detection and Response)/XDR (eXtended Detection & Response), de machines virtuelles (VM) et d'instances cloud. Les jump bags peuvent toujours être des conteneurs physiques que nous emportons sur place. Cependant, il est désormais plus utile de préparer un digital jump bag™. Ce référentiel protégé et fiable permet d'accéder rapidement non seulement aux outils nécessaires à l'acquisition et à l'analyse à distance, mais également à toutes les autres ressources numériques requises pour garantir une réponse et une restauration réussies en cas d'incident.

Synthèse

Le digital jump bag™ constitue la base d'une salle blanche, cet environnement sécurisé et isolé dans lequel l'équipe chargée de la sécurité opérationnelle peut mener les investigations nécessaires pour comprendre comment une attaque s'est produite. Une salle blanche sert également à prendre des mesures correctives avant de restaurer afin d'éliminer la menace et d'éviter qu'elle ne se reproduise. Le contenu d'un digital jump bag dépend de la maturité, de la structure, des processus et des outils de l'entreprise.

Un digital jump bag est conçu pour permettre à une entreprise de restaurer rapidement une capacité de réponse minimale viable (MVRC, Minimum Viable Response Capability), un ensemble rationalisé d'outils, de documents et de processus essentiels pour répondre efficacement à une cyberattaque. La MVRC permet aux entreprises de contenir rapidement les violations, de restaurer les opérations critiques et de minimiser les temps d'arrêt en cas de cyber incident.

La **solution de salle blanche de Cohesity** prend en charge cette approche moderne pour aider les entreprises à lutter contre les cyberattaques destructrices. Elle offre la flexibilité nécessaire pour s'adapter à différents besoins et permet d'améliorer en permanence la capacité de cyber-résilience opérationnelle au fil du temps.

Dans ce livre blanc, vous découvrirez ce que les entreprises devraient envisager d'inclure dans leur digital jump bag afin de mettre en place une stratégie de réponse aux incidents plus robuste et plus agile.

Problèmes de cyber-résilience fréquemment ignorés

Les cyberattaques destructrices contournent souvent les outils de sécurité utilisés par l'entreprise victime. De nombreuses plateformes RaaS (Ransomware-as-a-Service) courantes, responsables de la grande majorité des attaques par ransomware que nous observons aujourd'hui, intègrent des capacités de contournement des solutions EDR/XDR. De par leur nature, les solutions EDR/XDR sont installées sur des terminaux qui, lorsqu'ils ne sont pas contournés, offrent une excellente visibilité sur les processus, les connexions réseau et les systèmes de fichiers.

Les bonnes pratiques en matière de réponse aux incidents, notamment le plan de réponse aux incidents en six étapes du SANS Institute, le guide de gestion des incidents de sécurité informatique NIST SP800-61, le cadre RE&CT et MITRE D3FEND, préconisent toutes de contenir la propagation d'un incident en isolant les réseaux et les hôtes infectés. Dans le domaine du contrôle des terminaux, cela signifie, dans le meilleur des cas, que l'entreprise ne dispose que des informations déjà collectées pour enquêter sur l'incident.

Cependant, face à un adversaire qui s'adapte en permanence, nous ne savons pas toujours quelles informations collecter pour anticiper une attaque. Nous pouvons être aveuglés par le fait que notre capacité d'enquête et de réponse est désormais inaccessible. De même, il devient impossible de récupérer des preuves à distance sur les volumes d'un hôte affecté si nous avons coupé la connectivité.

Outre les outils de sécurité, de nombreux autres systèmes sont impliqués dans les phases d'enquête, d'atténuation et de restauration de la réponse aux incidents. Ceux-ci peuvent être impactés par des cyberattaques destructrices, notamment des ransomwares et des attaques de type wiper, mais leur importance est souvent négligée dans les analyses d'impact sur l'activité. J'ai travaillé sur des incidents au cours desquels les intervenants ne pouvaient pénétrer dans les bâtiments car les contrôles d'accès physiques avaient été compromis. De nombreuses entreprises n'ont pas pu communiquer avec la presse, les autorités réglementaires, les forces de l'ordre, les cyber-assureurs ou les personnes concernées par les données compromises, car leurs serveurs VoIP et de messagerie avaient été touchés. De nombreux exercices théoriques organisés par les entreprises simulant une attaque par ransomware ne prennent pas suffisamment en compte les répercussions des techniques ciblées de leurs adversaires. Après tout, les auteurs des attaques veulent s'assurer que les entreprises auront du mal à répondre aux incidents et à restaurer leur activité.

Les plateformes RaaS étant capables d'intégrer les exploits des vulnérabilités récemment corrigées en seulement cinq jours, nous devons les identifier dans les systèmes et les corriger avant de remettre les systèmes en production. Sinon, le même adversaire, ou un autre affilié utilisant la même plateforme RaaS, reviendra à la charge.

Nous devons également identifier le vecteur d'accès initial qui nous indique le premier système touché, appelé « patient zéro », puis suivre le déroulement de l'incident. Il est nécessaire de comprendre comment l'adversaire maintient sa persistance, escalade les privilèges et trouve d'autres artefacts de l'attaque pour s'assurer que la restauration est sécurisée. Les équipes d'intervention doivent également comprendre la nature des données susceptibles d'avoir été compromises pour se conformer aux obligations réglementaires de notification.

L'analyse des systèmes chiffrés ne suffit pas. En règle générale, les groupes de ransomware déploient leurs outils de chiffrement à la toute fin de leur cycle d'attaque, dans les dernières minutes ou heures d'une attaque qui peut s'être déroulée pendant plusieurs jours, voire plusieurs

semaines, sur notre infrastructure. Le chiffrement, qui est très bruyant, peut déclencher des contrôles de sécurité et être détecté par les utilisateurs. Mais à ce moment là, il est trop tard. Cet impératif de rapidité explique en partie pourquoi les outils de chiffrement ne garantissent souvent pas l'intégrité des données. Les victimes qui paient une rançon pour obtenir les clés de déchiffrement subissent ainsi d'importantes pertes de données. Limiter le périmètre aux systèmes chiffrés, sans chercher à savoir comment l'adversaire a pu s'introduire et s'installer sur votre réseau, c'est courir à la catastrophe.

Les entreprises qui adoptent cette approche devront souvent restaurer leurs systèmes des dizaines de fois, mais seront malgré tout réinfectées encore et encore. Ce cercle vicieux peut être brisé en menant une enquête approfondie sur l'incident et en utilisant les informations recueillies pour corriger les menaces.

Demandez-vous simplement comment se serait déroulé votre dernier exercice de simulation si vous n'aviez pas de téléphone ni d'e-mail, si vous n'aviez pas pu accéder à vos locaux et si vous n'aviez pas eu accès aux systèmes de gestion des identités et des accès au début de l'événement.

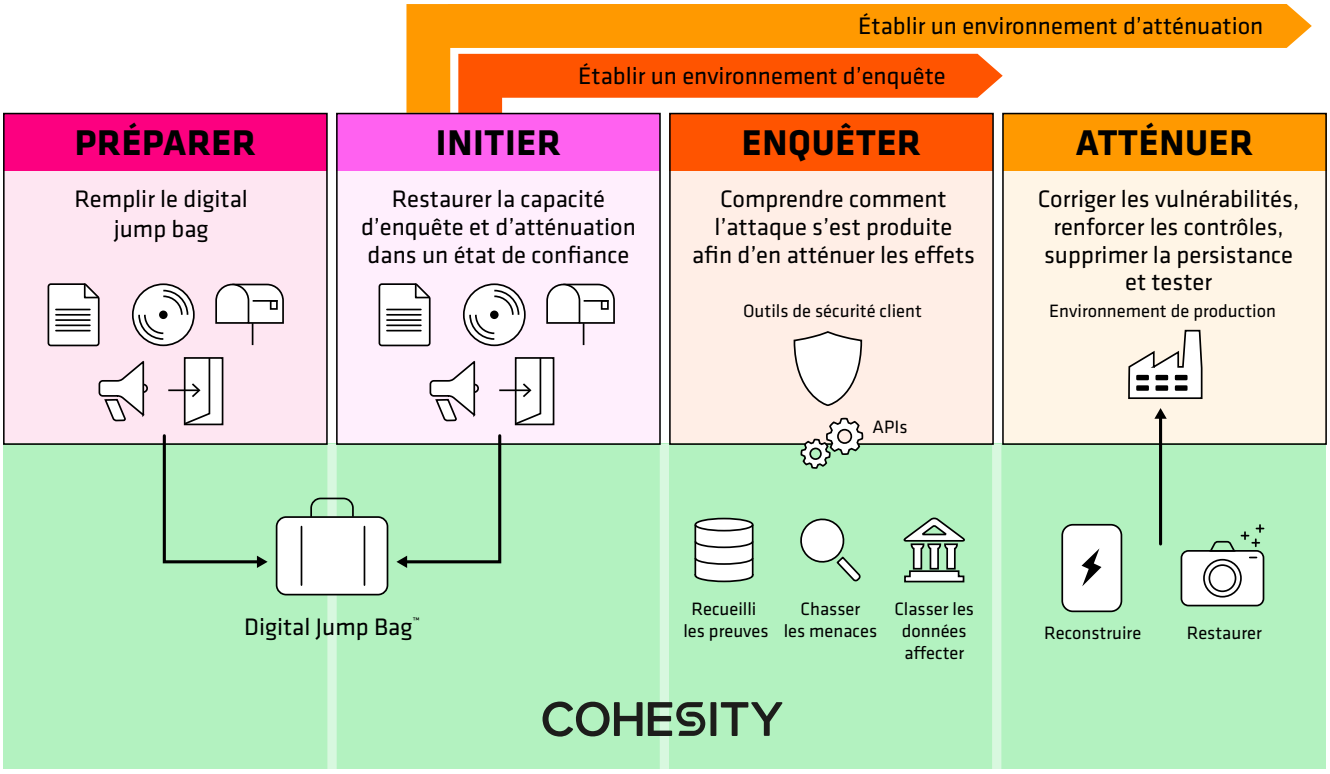
Comment le digital jump bag s'intègre dans la solution de salle blanche de Cohesity

Toute la solution de salle blanche de Cohesity repose sur le digital jump bag. Il prend en charge les étapes critiques de la réponse aux incidents et de la restauration pour permettre aux entreprises de restaurer des données saines en production, comme le montre l'illustration ci-dessous.

Voyons ce qui se passe à chacune de ces étapes.

Préparer

Lors de cette étape, nous définissons le contenu du digital jump bag, notamment les configurations réseau ou hyperviseur qui prennent en charge les couches de systèmes interdépendants à restaurer dans l'environnement d'atténuation. Consultez la section « Que pourrait contenir votre digital jump bag ? » pour obtenir des suggestions qui vous permettront de passer aux étapes suivantes.



Initier

Lors de cette étape, nous restaurons la MVRC. Les outils nécessaires à la communication, à la collaboration et à l'investigation des incidents sont restaurés dans un état fiable à partir du digital jump bag dans l'environnement isolé de la salle blanche. Le digital jump bag établit également les environnements d'enquête et d'atténuation.

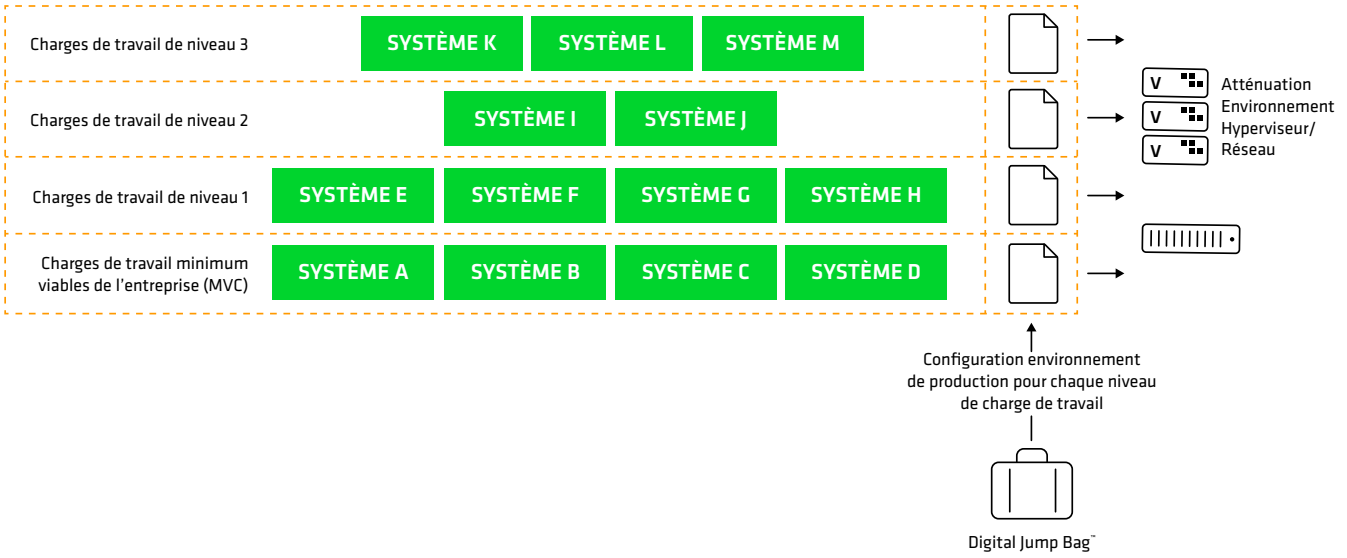
Enquêter

L'équipe chargée des opérations de sécurité (SecOps) utilise les outils de sécurité restaurés dans un état fiable dans la salle blanche isolée, et s'appuie sur les capacités natives de Cohesity en matière de classification des données, de recherche de menaces et d'analyse de preuves du système de fichiers pour comprendre la chronologie de l'incident de bout en bout. Comme les outils de sécurité sont restaurés dans un état fiable dans la salle blanche et que les capacités de sécurité de Cohesity ne sont pas soumises aux techniques de contournement de la défense utilisées contre les contrôles des terminaux, les problèmes de contournement et d'isolation dus au confinement sont résolus. Les fournisseurs partenaires de l'alliance pour la sécurité des données de Cohesity proposent un ensemble complet d'outils de sécurité qui sont indispensables dans mes centres d'opérations de sécurité et préconfigurés pour fonctionner avec les solutions Cohesity.

Atténuer

L'équipe des opérations informatiques (ITOps) utilise les informations recueillies par l'équipe SecOps soit pour restaurer puis nettoyer les systèmes, soit pour les reconstruire et les remettre dans un état fiable. Contrairement à la phase d'enquête, la phase d'atténuation implique la restauration complète des systèmes interdépendants.

Les clients réutilisent souvent leurs environnements de développement comme environnement d'atténuation pendant la durée de la restauration suite à un incident. Les systèmes interdépendants sont intégrés dans l'environnement d'atténuation avec des configurations réseau identiques à celles des environnements de production. Les configurations réseau ou hyperviseur de chaque couche de systèmes interdépendants sont stockées dans le digital jump bag. Ceci est illustré ci-dessous.



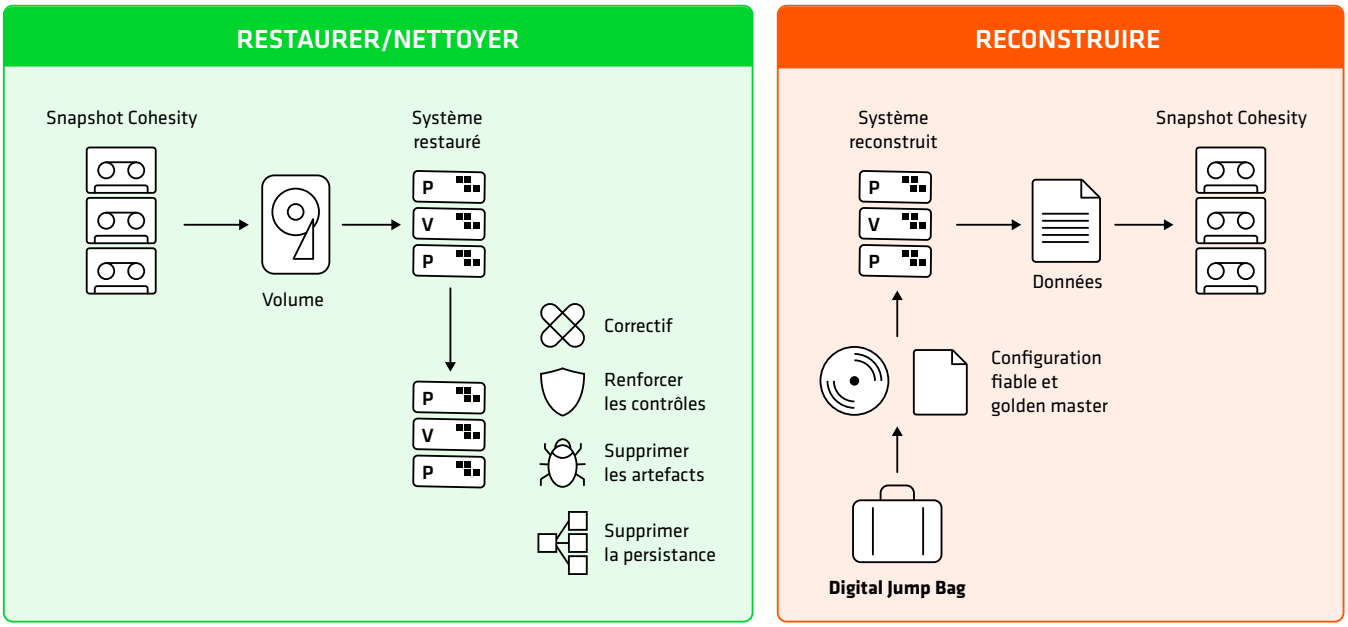
Alignement de la salle blanche de Cohesity sur les bonnes pratiques en matière de réponse aux incidents.

Avec la solution de salle blanche de Cohesity, la stratégie consistant à « restaurer et nettoyer » ou à « reconstruire dans un état fiable » peut être appliquée globalement ou choisie au cas par cas lors d'un incident, en fonction du niveau d'effort de correction requis et du risque de menaces résiduel. Examinons brièvement chacune de ces options :

- **Restaurer et nettoyer** : Les systèmes sont restaurés à partir de leur snapshot, et les étapes d'atténuation définies par l'équipe SecOps lors de la phase d'enquête sont mises en œuvre. Les données n'étant généralement pas utilisées pour transporter des charges utiles malveillantes, leur restauration peut souvent s'effectuer parallèlement à la reconstruction du système, ce qui réduit encore davantage les délais de restauration.
- **Reconstruire les systèmes dans un état fiable** : Le digital jump bag contiendra des configurations éprouvées, des scripts d'installation et des images d'installation de référence (« golden master »). Une fois les systèmes reconstruits, les données seront restaurées à partir des snapshots.

La section « **Utiliser le jump bag pour établir la capacité de réponse minimale viable** » détaille la comparaison de chaque approche.

Une entreprise qui dispose d'un environnement répondant aux besoins d'investigation de l'équipe SecOps et d'un environnement permettant à l'équipe ITOps d'utiliser des mesures d'atténuation pour garantir une restauration sécurisée est capable de mettre en place un modèle de responsabilité partagée efficace et approprié en matière de cyber-résilience. Cette approche permet d'optimiser la vitesse de la restauration sécurisée en garantissant que les ressources ITOps et SecOps peuvent être pleinement utilisées.



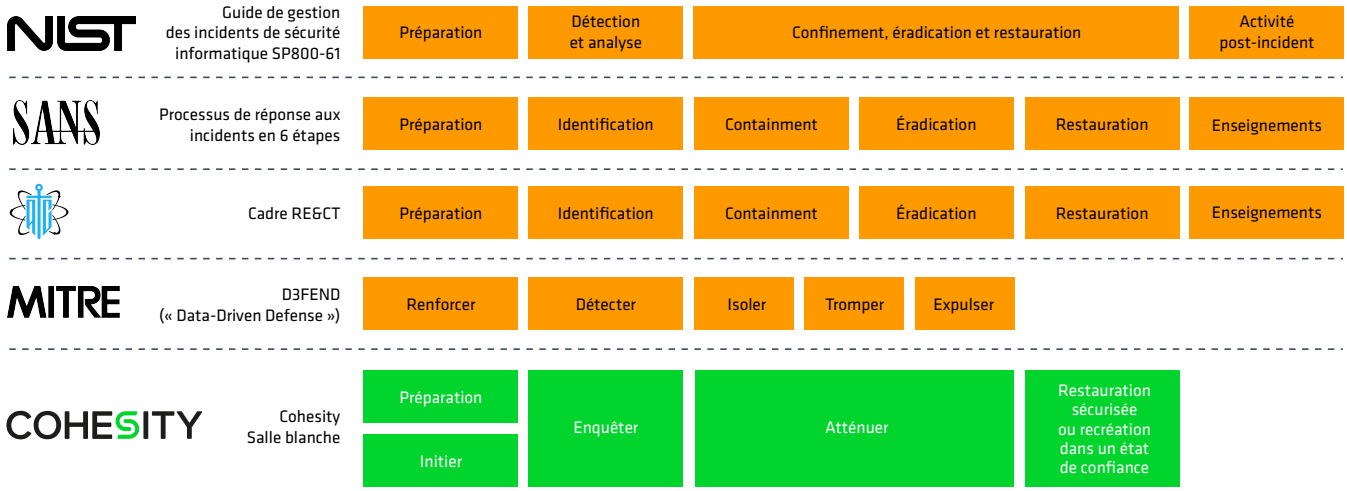
La salle blanche de Cohesity offre aux clients la possibilité de restaurer et de nettoyer leurs charges de travail ou de les reconstruire rapidement dans un état fiable.

Une fois les systèmes reconstruits ou restaurés, il est possible de réaliser des tests fonctionnels et de performance sur cette couche de charges de travail. Un snapshot est pris, puis l'ensemble de la charge de travail interdépendante est restauré dans l'environnement de production, avec la certitude que l'incident a été entièrement analysé, que les menaces ont été atténuées et que les performances et fonctionnalités ont été restaurées.

Ces cas de test peuvent être stockés dans le digital jump bag pour chaque niveau de restauration des charges de travail interdépendantes. Si un élément a été omis lors de l'enquête et de l'atténuation, il n'est pas nécessaire de revenir au point de départ. En effet, le snapshot pris à la fin de la phase d'atténuation peut servir de base pour poursuivre l'enquête et l'atténuation.

Comment la salle blanche de Cohesity s'aligne sur les bonnes pratiques en matière de réponse aux incidents

Le digital jump bag de Cohesity et la capacité de réponse minimale viable s'alignent sur les bonnes pratiques en matière de réponse aux cyber incidents décrites dans le plan de réponse aux incidents en six étapes du SANS Institute, le guide de gestion des incidents de sécurité informatique NIST SP800-61, le cadre RE&CT et MITRE D3FEND Grâce à cette approche, les entreprises qui appliquent déjà ces méthodologies peuvent facilement intégrer la solution de salle blanche de Cohesity à leur flux de travail existant. Les clients qui souhaitent améliorer leur maturité en matière de réponse aux incidents et de restauration peuvent adopter la solution de salle blanche de Cohesity pour mettre en œuvre ces bonnes pratiques.



Alignement de la salle blanche de Cohesity sur les bonnes pratiques en matière de réponse aux incidents

Réunir la sécurité et les opérations informatiques pour assurer la résilience

La cyber-résilience est un sport d'équipe : elle ne peut être assurée uniquement par l'équipe ITOps ou par l'équipe SecOps. Les deux doivent avoir des processus intégrés et des outils complémentaires. De même, aucun fournisseur ne peut à lui seul garantir la cyber-résilience. La solution de salle blanche de Cohesity est conçue pour permettre à l'équipe SecOps d'exploiter et de contrôler l'environnement d'enquête, tandis que l'équipe ITOps possède et utilise l'environnement d'atténuation. Cette répartition des environnements et ce transfert de tâches entre les équipes permettent de garantir un modèle de responsabilité partagée clair, minimisant ainsi le risque d'oublier certaines activités. Il est possible de rétablir de manière itérative des snapshots précédemment atténués à l'étape d'enquête si certains aspects de l'attaque ont été omis lors de l'enquête et de l'atténuation initiales, sans avoir à recommencer depuis le début. Cela réduit considérablement la durée de l'enquête et de la restauration finale.

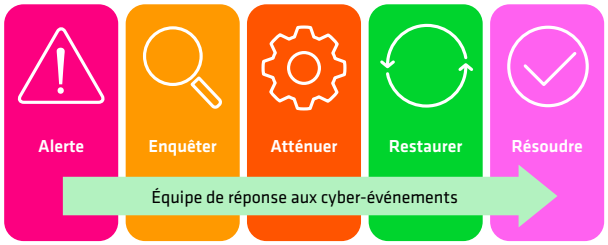
Dès que l'équipe SecOps a fini d'examiner une charge de travail dans l'environnement d'enquête, elle peut la transférer à l'équipe ITOps et à l'environnement d'atténuation pour qu'elle soit reconstruite, restaurée et nettoyée. Cela permet d'utiliser les ressources des équipes de façon optimale.

Réagir plus rapidement, restaurer plus intelligemment : l'équipe CERT (Cyber Event Response Team) de Cohesity

De nombreuses entreprises n'ont pas l'expertise ou les ressources nécessaires pour répondre efficacement aux cyber incidents.

Nous avons amélioré notre solution de sécurité des données de classe mondiale avec un service dédié, l'équipe CERT (Cyber Event Response Team), pour minimiser l'impact.

L'équipe CERT de Cohesity est composée d'experts spécialisés dans la restauration rapide en cas de cyberattaque. Elle s'assure que vos données sont restaurées et que votre entreprise reprend ses activités après un temps d'arrêt minime.



L'équipe CERT de Cohesity est disponible pour tous les clients dans le cadre de leur abonnement.

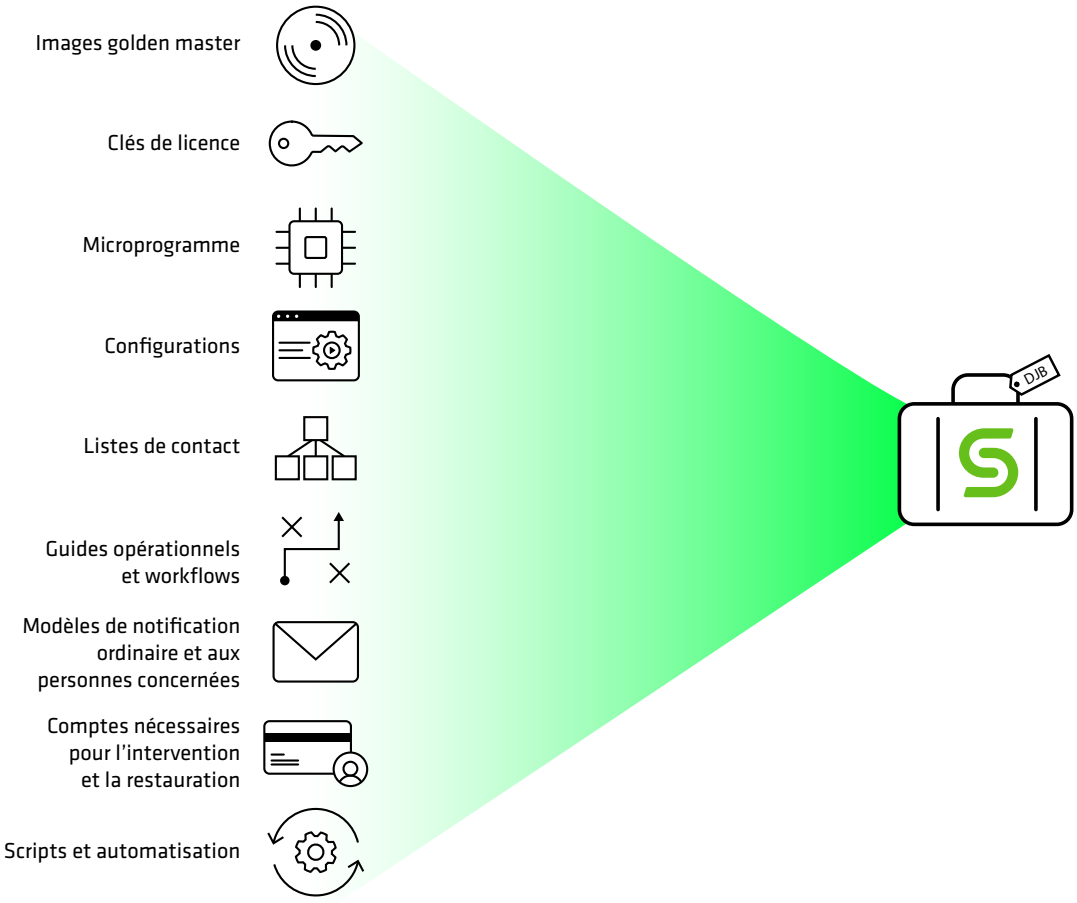
Que pourrait contenir votre digital jump bag ?

Le contenu de votre digital jump bag dépend de vos processus de tri, d'enquête et d'atténuation, ainsi que des outils que vous utilisez pour les mettre en œuvre.

Nos clients incluent généralement les éléments suivants dans leurs digital jump bags :

Documentation

- Une liste de contacts comprenant les parties prenantes internes et les entités externes, notamment les forces de l'ordre, les centres de partage et d'analyse d'informations, les compagnies d'assurance, les intervenants en cas d'incident et les régulateurs.
- Diagrammes de réseau.
- Éventuellement une sauvegarde ou une copie (« dump ») de la base de données de gestion de la configuration de l'entreprise.
- Une copie du runbook/flux de travail de réponse aux incidents.
- Contrats et documents stratégiques relatifs aux services de réponse aux incidents retenus et aux cyber-assureurs.
- Manuels d'utilisation des applications et des outils.



Ressources pour la phase d'initiation : collaboration et communication

- Vous devrez probablement communiquer avec les parties prenantes internes et les tierces parties externes, notamment les forces de l'ordre, les centres de partage et d'analyse de l'information, les compagnies d'assurance, les intervenants en cas d'incident, les régulateurs, la presse et les personnes concernées. À cette fin, votre digital jump bag pourrait contenir les éléments suivants :
  - Un microprogramme et une configuration de routeur et de commutateur réputés fiables pour permettre une connectivité sécurisée. L'entreprise peut également conserver un équipement de secours fiable.
  - Un logiciel et une configuration de pare-feu pour limiter les entrées et les sorties aux seules ressources nécessaires pour la réponse et la restauration (notamment l'accès à Cohesity Helios).
  - Le support d'installation du système d'exploitation de base et les clés de licence utilisés comme base pour reconstruire d'autres systèmes, notamment ceux des environnements d'enquête et d'atténuation.
  - Des scripts d'automatisation et d'orchestration, par exemple des fichiers Answerfiles Windows pour installer sans assistance, des playbooks Ansible, ou l'outil d'Infrastructure-as-Code (IAC) Terraform.
  - Le logiciel et la configuration du serveur de gestion de la voix sur IP (VoIP). Il est important de comprendre qu'il ne s'agit pas de l'ensemble de l'environnement de production VoIP. Cela ne comprend que les lignes relatives aux activités de réponse et de restauration. La configuration VoIP de production sera remise en ligne après enquête, lorsque toutes les menaces détectées auront été atténuées.
  - Le logiciel et la configuration du serveur de messagerie. Comme le serveur VoIP, il ne s'agit pas d'une capacité de production. Il permet simplement aux ressources impliquées dans les activités de réponse et de restauration de communiquer entre elles.
  - D'autres outils de collaboration utilisés par l'entreprise, notamment les systèmes de gestion des tickets, de réunion ou équivalent, peuvent être inclus dans le jump bag.
  - Des modèles pour notifier le régulateur et les personnes concernées

Ressources pour l'environnement de la phase d'enquête

L'équipe chargée de la sécurité opérationnelle est généralement propriétaire de l'environnement utilisé au cours de la phase d'enquête. Son objectif est de comprendre la chronologie de l'attaque de bout en bout afin que l'entreprise puisse prendre des décisions éclairées pour restaurer sa capacité de production tout en se protégeant contre toute réinfection ou nouvelle attaque. Les systèmes sont examinés en interne en combinant les capacités natives de Cohesity en matière de sécurité opérationnelle (classification des données, recherche de menaces, analyse de preuves sur le système de fichiers) et d'autres outils de sécurité pris en charge par Cohesity. La recherche de menaces avec Cohesity n'est pas affectée par le confinement de l'incident. Ce processus est passif, donc invisible pour l'adversaire, et n'est pas soumis aux techniques de contournement courantes des solutions de sécurité des terminaux. Dans l'environnement de la phase d'enquête, les systèmes sont généralement étudiés de manière isolée.

- Supports d'installation et configurations pour les logiciels de sécurité. Cela permet de réinstaller les outils dans un état fiable dans l'environnement isolé de la salle blanche, et ainsi de garantir que les activités liées aux outils et aux réponses ne sont pas contournées ou interrompues.
- Les outils de sécurité peuvent être réinstallés dans un état fiable dans la salle blanche. Ces outils dépendent fortement des préférences de votre équipe de réponse aux incidents de sécurité, mais on retrouve généralement :
  - Des outils EDR (Endpoint Detection and Response) et XDR (Extended Detection and Response) comme Palo Alto Networks, Cisco XDR ou CrowdStrike

- Des outils de capture et d'analyse des preuves, notamment Dissect, Flare, Redline, Sleuth Kit, Autopsy, CyLR ou Unix-like Artifacts Collector (UAC)
- Des indicateurs de compromission et des outils de partage des preuves tels que Cortex, Kuiper ou MISP
- Des analyseurs de journaux d'événements comme Event Log Explorer, Event Log Observer, Hayabusa, LogonTracer ou Windows Event Log Analyzer (WELA)
- Des scanners de vulnérabilités tels que Qualys, Rapid7 neXpose, Tenable Nessus ou OpenVAS
- Un logiciel de capture et d'analyse de paquets, par exemple Wireshark
- Des analyseurs Netflow/SFlow
- Des outils de capture et d'analyse de la mémoire comme Volatility, Memoryze, Orochi, Rekall ou WindowsSCOPE.
- Des bacs à sable, des outils de rétro-ingénierie et d'analyse des logiciels malveillants, notamment Cuckoo, CAPA, CAPE, Ghidra, Joe Sandbox, Mastiff, Radare 2 ou Valkyrie Comodo.
- Des outils d'analyse de l'historique du navigateur web comme Internet History Forensics
- La plupart des outils mentionnés ci-dessus sont disponibles dans des distributions de logiciels de sécurité tels que Kali Linux ou SIFT Workstation du SANS Institute. Vous pouvez les stocker dans le digital jump bag plutôt que d'installer chaque outil individuellement.

Ressources pour l'environnement de la phase d'atténuation

L'équipe chargée des opérations informatiques est généralement propriétaire de l'environnement d'atténuation. Dans l'environnement d'atténuation, les systèmes d'exploitation et les applications sont soit reconstruits à partir de supports d'installation et de configurations fiables contenus dans le digital jump bag, soit restaurés à partir de snapshots de sauvegarde et nettoyés à l'aide des informations obtenues par l'équipe de sécurité opérationnelle lors de la phase d'enquête. Des mesures correctives sont prises pour atténuer les menaces, à savoir corriger les vulnérabilités, appliquer les contrôles ou règles manquants afin de prévenir ou de détecter de futures attaques similaires. De plus, tout mécanisme de persistance, compte malveillant ou autre artefact d'attaque est supprimé. Dans l'environnement d'atténuation, les systèmes interdépendants nécessaires pour fournir un produit ou des services sont regroupés et reconstruits ou atténués, jusqu'à ce que les performances et les fonctionnalités puissent enfin être testées en restaurant les données à partir d'un snapshot de sauvegarde. Un snapshot est pris à ce moment-là et les systèmes sont restaurés dans l'environnement de production.

- Si l'entreprise préfère « reconstruire » plutôt que « restaurer et nettoyer », le digital jump bag contiendra les supports d'installation et les configurations nécessaires pour la pile d'applications.
- La configuration réseau ou hyperviseur requise pour la charge de travail interdépendante actuelle. Cela permet à l'environnement d'atténuation de reproduire l'environnement de production dans lequel la charge de travail sera plus tard restaurée.
- Des cas de test pour les charges de travail.

Utiliser le jump bag pour établir la capacité de réponse minimale viable

Lorsqu'un client utilise le digital jump bag pour mettre en place les systèmes dans la MVRC, il a deux possibilités : restaurer un système préassemblé, ou le reconstruire à partir de sources fiables.

- **Maintenir la capacité de réponse minimale viable :** Construisez les systèmes nécessaires à la MVRC, sauvegardez-les au niveau du volume, puis stockez ces sauvegardes dans le digital jump bag. Restaurez les snapshots pour établir la capacité de réponse minimale viable si vous suspectez qu'un incident de cybersécurité affecte les systèmes nécessaires à la réponse et à la restauration ou que les outils de sécurité sont contournés.
- **Reconstruire à partir des ressources du digital jump bag** : Ici, les configurations fiables et les images de référence (« golden master ») des systèmes requis pour la MVRC sont conservées dans le digital jump bag. Déployez le digital jump bag si un incident de cybersécurité ayant un impact sur les systèmes nécessaires à la réponse et à la restauration se produit, ou si vous suspectez que les outils de sécurité sont contournés. Ces systèmes sont reconstruits à l'aide de scripts ou d'outils d'orchestration.

Chaque stratégie présente des avantages et des inconvénients, qui sont présentés dans le tableau ci-dessous :

Maintenir une capacité de réponse minimale viable, la sauvegarder et restaurer le snapshot après un incident.	
Avantages :	**Inconvénients :**
Accès rapide aux systèmes fonctionnels lors de la réponse	Les correctifs et les mises à jour nécessitent davantage d'étapes (reconstruction, mise à jour/correction, sauvegarde), et donc des ressources permanentes. Ces étapes peuvent entraîner des erreurs susceptibles d'affecter la réponse et la restauration. Supposons qu'une entreprise n'ait pas été en mesure de sécuriser ses systèmes informatiques et ait été touchée par l'incident. Qu'est-ce qui garantit que les systèmes de capacité de réponse minimale viable construits et sauvegardés n'auront pas les mêmes problèmes ?
Possibilité de restaurer uniquement les composants requis	Occupe beaucoup plus d'espace dans le digital jump bag, ce qui entraîne des coûts de licence
	Une mise à jour ou un correctif peut être nécessaire pendant la réponse, ce qui peut entraîner des retards
	Peut introduire des dépendances au niveau de l'infrastructure
Pré-requis :	
Réussir le test de construction de la MVRC à partir du digital jump bag	
Faire une sauvegarde de la MVRC, activer la conservation légale à des fins juridiques, la répliquer et l'archiver hors site	

Reconstruire la capacité de réponse minimale viable à partir de sources fiables après un incident	
Avantages :	**Inconvénients :**
Les sources sont relativement faciles à maintenir. En effet, lorsqu'une nouvelle version d'un système d'exploitation, d'une application ou d'une configuration est disponible, elle est simplement exportée vers le jump bag.	La reconstruction de l'infrastructure prend du temps
Très portable grâce à la réplication et à l'archivage	
S'adapte plus facilement aux changements de matériel et de plateforme	
L'empreinte de sauvegarde dans le digital jump bag est considérablement réduite (une image Windows Server 2025 occupe environ 3,6 Go et peut être partagée entre différents systèmes, alors que chaque serveur de la capacité de réponse minimale viable qui utilise cette image nécessiterait environ 35 Go).	
Pré-requis :	
Établir un processus pour remplir et mettre à jour le digital jump bag	
S'entraîner à utiliser le contenu dans différents scénarios	
Conserver le matériel nécessaire à portée de main, ou définir un processus permettant d'effacer de manière sécurisée le matériel existant	

Conclusion

Face à des cyberattaques de plus en plus sophistiquées et destructrices, les entreprises doivent abandonner leurs solutions de restauration réactive et adopter un modèle de résilience stratégique. Cela implique d'intégrer un digital jump bag complet à leur stratégie de réponse aux incidents afin d'être mieux armées pour répondre rapidement aux cyberattaques. Un digital jump bag bien préparé rend la MVRC possible et sert de base à une salle blanche. Il fournit aux équipes de sécurité les outils, les processus et la documentation essentiels pour enquêter sur les incidents, contenir les menaces et restaurer les opérations avec un minimum de perturbations.

La solution de salle blanche de Cohesity offre un environnement fiable qui accélère la réponse aux incidents et prend en charge les enquêtes tout en minimisant le risque d'attaques secondaires.

La conception modulaire de Cohesity permet de créer rapidement un environnement isolé. Cela facilite le processus de réponse et de restauration, et permet aux équipes de collaborer pour atténuer plus rapidement les menaces.

À propos de Cohesity

Cohesity est le leader de la sécurité des données alimentée par l'IA. Plus de 12 000 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 San Jose, en Californie, et des bureaux dans le monde entier. Pour en savoir plus, suivez Cohesity sur **LinkedIn**, **X** et **Facebook**.

Découvrez comment Cohesity peut accélérer votre transition vers une sécurité des données moderne sur **www.cohesity.com/fr/**.

Lectures recommandées

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

- Renforcer la cyber-résilience dans un monde en proie à des cyberattaques destructrices
- Topologies modernes de sécurité et de gestion des données : un guide pour les responsables informatiques
- 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)

En savoir plus sur Cohesity

COHESITY

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

2000056-002-FR 4-2025