COHESITY

LIVRE BLANC

Comment développer votre résilience face aux ransomwares

TABLE DES MATIÈRES

La cyber-résilience par rapport à la résilience des données

La plupart des entreprises ont une stratégie de résilience des données qui se se compose d'une continuité de l'activité et d'une reprise après sinistre, mais la technologie et les processus conçus pour cette résilience des **données** n'entraînent pas toujours une véritable **cyber**-résilience à l'ère des ransomwares.

Pour créer une entreprise cyber-résiliente, il faut de la communication, de la collaboration, des outils de sécurité, des systèmes d'authentification, des plateformes de sauvegarde et une foule d'autres systèmes pour :

- Enquêter sur la manière dont l'attaque s'est produite
- Communiquer avec les personnes concernées, les autorités de régulation et les forces de l'ordre
- Atténuer la menace d'une nouvelle attaque
- Restaurer la production

Les cyberattaques destructrices, ou attaques de type wiper, bouleversent le schéma traditionnel de détection-réponse-restauration. Elles rendent ce processus plus itératif, car il est souvent nécessaire de restaurer les capacités de réponse et de communication avant même de pouvoir lancer les investigations. Dans ces situations, la plateforme de sauvegarde et de restauration devient un élément crucial, car elle sert de source de référence pour les analyses de preuves menées par les équipes de réponse aux incidents.

Les entreprise qui souhaitent devenir cyber-résilientes et faire face aux cyberattaques modernes doivent se concentrer sur deux domaines essentiels pour réussir :

1. La capacité de restaurer doit être hors de portée des cybercriminels
2. La planification de la réponse doit prévoir de restaurer rapidement non seulement les systèmes de production, mais aussi les plateformes de sécurité, d'authentification et de communication nécessaires pour répondre à l'incident de manière efficace et efficiente

La nature itérative du processus de restauration–réponse–restauration dans les attaques par ransomware ou de type wiper exige une collaboration étroite entre l'équipe chargée de la sécurité (SecOps) et celle chargée des opérations informatiques (ITOps) afin de minimiser l'impact de ces attaques.

Créer un programme de cyber-résilience

Dans les scénarios traditionnels de continuité de l'activité et de reprise après sinistre, notamment les inondations, les incendies ou les catastrophes naturelles, la cause profonde de l'événement peut être déterminée rapidement. Dans le cas d'une attaque par ransomware, le cybercriminel s'efforce d'empêcher toute restauration afin que la victime n'ait d'autre choix que de payer une rançon.

Ces cybercriminels s'adaptent en permanence aux défenses de leur cible. Il est donc indispensable d'avoir un programme d'investigation et de réponse normatif pour identifier la nature de l'attaque et déterminer la stratégie de restauration adéquate. L'enquête permet également aux entreprises d'identifier les vulnérabilités qui ont permis à l'attaque de réussir, et de renforcer leurs défenses pour prévenir de futurs incidents. Cela contraste avec une catastrophe traditionnelle, où la réponse peut être quasi instantanée.

Être résilient face à une cyberattaque, ou y survivre, demande bien plus qu'un simple plan d'utilisation de la technologie. Les équipes informatiques et de sécurité doivent comprendre qui sont les cybercriminels et quels types d'attaques ils lancent. Ce type de renseignement leur permet de mettre en place des défenses ciblées, et ainsi d'avoir de meilleures chances de bloquer les attaques ou de les détecter plus tôt. Des cadres comme MITRE ATT&CK permettent aux entreprises de quantifier les menaces et de communiquer les mesures correctives de manière standardisée.

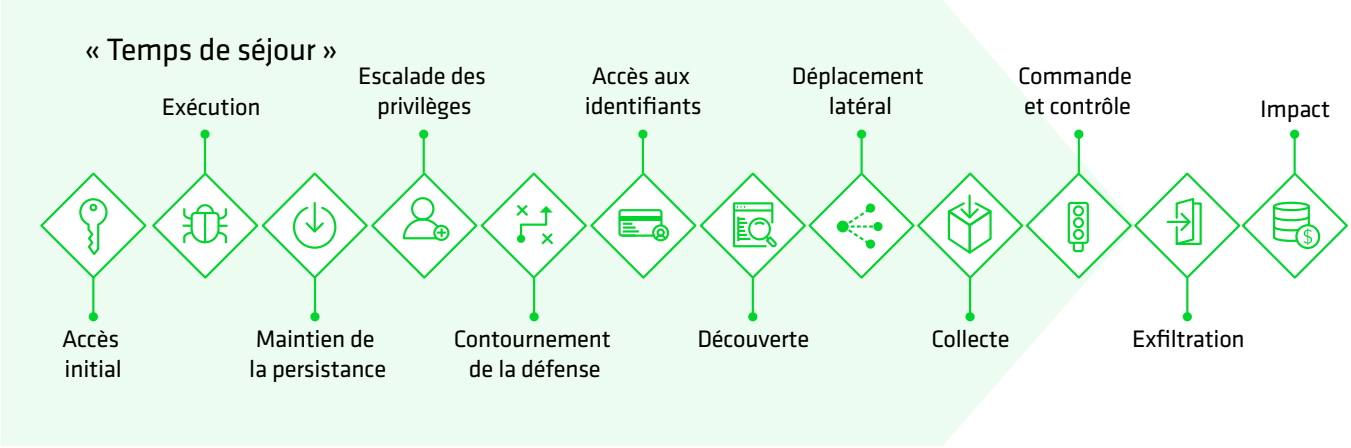
Par exemple, le schéma ci-dessous montre ce que les cybercriminels peuvent faire lorsqu'ils séjournent dans un environnement avant d'activer leur ransomware. Ils peuvent mener des actions pour réussir à déployer le ransomware, ou pour maintenir une présence persistante sur le réseau afin de pouvoir lancer de futures attaques. Le « temps de séjour », peut varier de quelques jours à plusieurs mois. Savoir comment un cybercriminel opère dans l'environnement permet aux équipes de sécurité de rechercher de manière proactive les indicateurs d'une attaque.

> Le temps de séjour correspond à la durée pendant laquelle un acteur malveillant a accès à un système compromis avant que l'attaque ne soit détectée. Plus un cybercriminel arrive à séjourner longtemps sur un système, plus il a de chances de causer des dommages ou de voler des informations sensibles.

Considérez chaque action du schéma comme une étape de l'attaque. Il peut être surprenant de constater que 10 des 12 étapes sont exécutées avant même que la charge utile ne soit activée. Dans le cas d'une attaque par ransomware, les systèmes sont déjà entièrement compromis avant que le chiffrement ou l'exfiltration des données ne commence. Ce point d'ancrage sur le réseau permet aux cybercriminels de saboter les efforts de restauration et de lancer de nouvelles attaques pour extorquer plusieurs rançons. Ce type de ransomware, appelé « double-bubble » ou « double-tap », est de plus en utilisé par les cybercriminels pour générer des revenus réguliers.

Pour la victime, une seule attaque peut être dévastatrice, car elle peut l'empêcher de fournir ses biens et ses services. Mais être victime de plusieurs attaques augmente le risque de pertes secondaires, notamment :

- Une atteinte à la réputation
- Des litiges avec les personnes concernées et les partenaires
- Des amendes réglementaires pour ne pas avoir protégé correctement les informations des personnes concernées



Pour compliquer davantage la situation, plus un cybercriminel séjourne longtemps sur le réseau, plus il y a de chances que des artefacts de l'attaque soient stockés dans les sauvegardes. Si ces artefacts sont restaurés sans avoir été identifiés et supprimés, l'attaque peut recommencer. Ce type de scénario se produit souvent lorsque les entreprises qui ont été victimes d'une attaque par ransomware ne s'assurent pas de restaurer des données saines.

Les entreprises sont tenues de suivre les processus de DFIR (Digital Forensics & Incident Response) pour s'assurer de restaurer des données saines dans les centres des opérations de sécurité (SOC). Historiquement, ces processus de DFIR s'appuient sur :

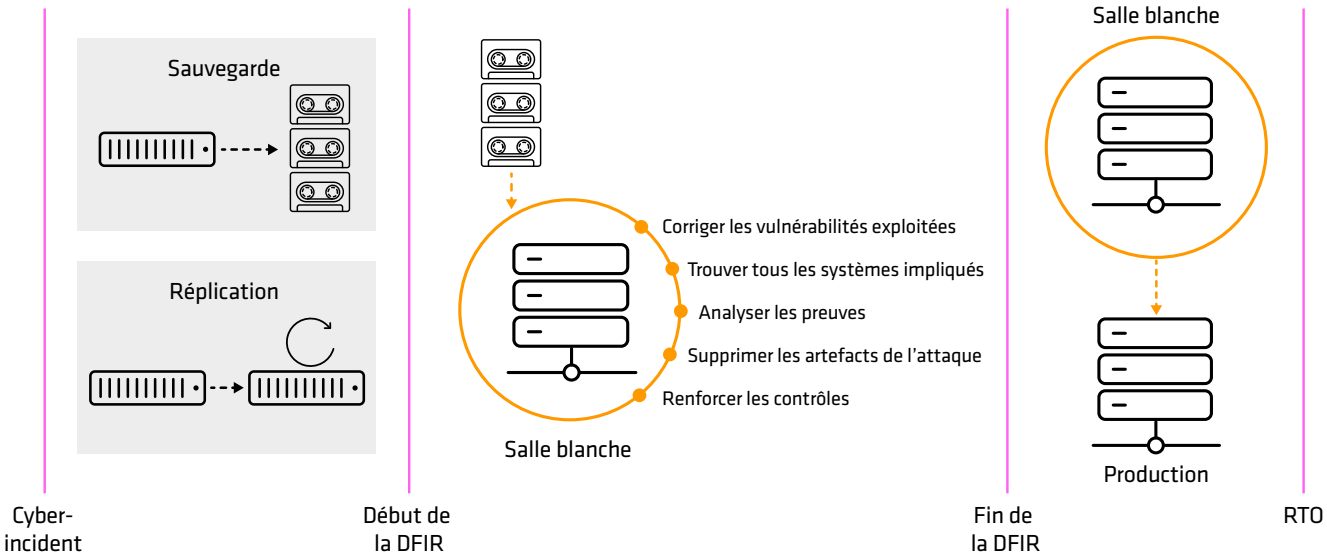
- La création d'une image des preuves d'un hôte compromis
- L'application de processus et d'outils d'investigation pour reconstituer la chronologie de l'incident
- La recherche et l'analyse des artefacts binaires utilisés lors de l'attaque
- La découverte des méthodes d'escalade des privilèges et de persistance utilisées
- La recherche d'autres systèmes compromis afin d'élargir le périmètre de l'incident
- La recherche des vulnérabilités à corriger avant de remettre une plateforme en production
- La recherche des raisons pour lesquelles les mesures de prévention et de détection n'ont pas permis d'arrêter ou de détecter l'attaque

Ces tâches sont généralement effectuées dans un environnement de restauration isolé (IRE, Isolated Recovery Environment), également appelé « salle blanche ».

Bien entendu, créer l'image des preuves d'un système qui a été effacé ou chiffré ne fournira pas de preuves significatives. Les équipes de réponse aux incidents s'appuient donc de plus en plus sur des référentiels de sauvegarde pour mener leur enquête. Utiliser les données de sauvegarde leur permet de voir les changements au fil du temps et de suivre le cycle de vie de l'attaque.

Cohesity fournit une plateforme immuable et adaptée aux exigences de preuves pour lancer le processus de DFIR. Les enquêteurs ont accès à des snapshots historiques du système de fichiers qui peuvent être rapidement instanciés et orchestrés via une API. Cela leur fournit le contexte des systèmes impactés, et leur permet d'avoir des informations sur le système de fichiers pendant toute la durée de l'incident. C'est comme si l'analyste disposait d'un super-pouvoir lui permettant de voyager dans le temps. Les analystes peuvent comparer les systèmes de fichiers au fil du temps afin d'identifier les savoir-faire des cybercriminels (par exemple, modifier des fichiers de configuration pour maintenir une présence persistante, remplacer des fichiers binaires et des bibliothèques légitimes par des copies malveillantes, ou identifier d'autres artefacts malveillants utilisés lors de l'attaque).

L'objectif de délai de restauration (RTO) correspond à la durée maximale acceptable pour restaurer un réseau ou une application, et retrouver l'accès aux données après une interruption imprévue.



Inclure l'infrastructure de sauvegarde dans le processus de DFIR permet de mener à bien les enquêtes avant de remettre les données en production. Le problème : cela peut avoir un impact négatif sur l'objectif de délai de restauration (RTO) fixé par l'entreprise. Après tout, la plupart des RTO n'ont pas été calculés pour tenir compte des enquêtes requises pendant une cyberattaque.

Utiliser les sauvegardes pour créer un environnement de salle blanche réduira le temps d'arrêt global et garantira que les données restaurées sont saines. Il ne sera donc plus nécessaire de répéter le processus en cas de réinfection. Les entreprises peuvent ainsi respecter leurs RTO et éviter les temps d'arrêt continus.

La cyber-résilience, de la planification à l'exécution

Soyez prêt

Mettez en place une équipe interfonctionnelle avec toutes les parties prenantes et chargez-la de la résilience face aux ransomwares.

Les incidents liés aux ransomwares diffèrent des autres cyberattaques. Ils ont un impact sur l'ensemble de l'entreprise et sur sa capacité à fournir des produits et des services à ses clients. Chaque seconde passée à répondre et restaurer est une perte directe. Le personnel ne peut ni communiquer, ni travailler. La presse sera impatiente de publier des reportages sur l'incident. Et les clients seront frustrés. Il est essentiel de s'assurer que tous les membres d'une entreprise connaissent leur rôle en cas de cyberattaque.

Cela inclut de déterminer :

- Comment la communication s'effectuera si les méthodes primaires, notamment les e-mails, ne fonctionnent pas.
- Qui sera en charge de chaque fonction et étape de la réponse
- Quel processus suivre si un membre de l'équipe n'est pas disponible, et qui sera le contact secondaire.

Les employés qui ne sont pas directement impliqués dans la réponse et la restauration doivent également savoir ce que l'on attend d'eux. Pourquoi ? Parce qu'en l'absence d'informations fiables, les rumeurs et les conjectures peuvent entraver la réponse et ralentir la restauration.

Effectuez une simulation réaliste d'attaque par ransomware avec toutes les parties prenantes.

L'une des meilleures façons de fédérer votre entreprise est d'organiser une simulation réaliste d'attaque par ransomware axée sur ses spécificités. Vous obtiendrez des informations sur certaines des menaces et des défis auxquels vous serez probablement confronté lorsque vous devrez répondre à une véritable attaque par ransomware.

Tenez compte de tous les impacts dans le calcul du risque de ransomware. Les impacts sont les suivants :

- Impact primaire :
  - L'incapacité de l'entreprise à fournir ses produits et services.
- Impacts secondaires :
  - Les coûts opérationnels liés à l'enquête et à la réponse aux incidents, notamment les services professionnels et les éventuels paiements au groupe de ransomware.
  - L'atteinte à la réputation de l'entreprise
  - Les amendes réglementaires liées à l'incident de ransomware ou au paiement effectué à des entités sanctionnées
  - La perte de capital intellectuel
  - Les litiges avec les partenaires ou les clients liés aux violations de données.

Intégrez le risque lié aux ransomwares dans la gestion des risques de l'entreprise.

Bien que cela semble évident, de nombreuses entreprises ne considèrent pas l'impact des ransomwares comme un risque opérationnel important. Intégrer le risque lié au ransomware dans la gestion des risques de l'entreprise permet d'établir des niveaux de gouvernance appropriés pour soutenir correctement les stratégies de cybersécurité, et de maintenir des niveaux de gestion des risques adaptés.

Créez une stratégie de ransomware à l'échelle de l'entreprise. Celle-ci doit vous permettre de :

- **Définir des critères clairs permettant de déterminer si un incident doit être considéré comme une attaque par ransomware ou pas.** Les flux de travail permettant de répondre aux ransomwares et de restaurer sont différents de ceux utilisés pour les logiciels malveillants traditionnels et l'exfiltration de données. Il faut définir clairement les critères permettant à un analyste SOC de déclarer un

incident afin qu'il puisse engager les actions appropriées en matière d'enquête, de confinement et d'éradication. Sans cette clarté, une attaque par ransomware peut se propager au sein d'une entreprise pendant que le SOC cherche à obtenir l'autorisation de prendre ces mesures.

- **Définir votre stratégie de cyber-sauvegarde.** La stratégie de sauvegarde pour les scénarios de cyber-résilience peut différer de la stratégie de résilience des données pour les événements traditionnels de reprise après sinistre et de continuité de l'activité. Elle dépend de la structure et de la maturité de la capacité de réponse et de restauration.
  - Données de sauvegarde uniquement : démarrez les serveurs nécessaires pour enquêter sur l'incident, reconstruisez l'infrastructure à partir de zéro, puis restaurez les données. Cette stratégie doit définir comment les images de référence (golden master) utilisées pour restaurer sont conservées, notamment la recherche des vulnérabilités et des mauvaises configurations.
  - Infrastructure de sauvegarde : restaurez l'ensemble de l'infrastructure, puis nettoyez-la en restaurant différentes parties à différents points en fonction de la réponse à l'incident.
- **Définir les catégories de résilience opérationnelle.** Basez ces catégories sur votre bilan d'impact sur l'activité en matière de résilience des données existant, et incluez la possibilité de mettre en place nos outils de réponse dans une salle blanche et vos stratégies de sauvegarde en matière de cyber-résilience.
  - **Incluez la capacité à restaurer les communications et l'infrastructure de sécurité nécessaires pour répondre à l'incident et restaurer l'activité.** Tenez compte des éléments suivants :
    - Contrôle d'accès physique
    - Services de nom de domaine
    - Communications vocales
    - E-mail
    - Plateformes de collaboration utilisées pour coordonner la réponse
    - Gestion de cas
    - Outils d'analyse de preuves et de réponse aux incidents
    - Recherche et gestion des vulnérabilités
    - Gestion des identités et des accès
- **Définir dans quelles conditions l'entreprise envisagerait de payer la rançon.**
  - Comment l'entreprise pourrait-elle sécuriser les fonds nécessaires au paiement de la rançon ?
  - La police d'assurance de l'entreprise comprend-elle le paiement d'une rançon ?
  - L'assureur considère-t-il les actions des acteurs partisans du ransomware comme des combattants ?
  - L'assureur couvre-t-il les paiements aux entités sanctionnées ?
  - Quelle est l'approche de l'entreprise en matière de négociation avec un opérateur de ransomware ?
  - Quelles sont les implications en termes de réputation, de réglementation et de criminalité (par exemple, si le groupe payé est sanctionné) ?
  - Comment votre entreprise obtiendrait-elle la cryptomonnaie nécessaire pour payer la rançon ? Tenez compte du temps nécessaire pour vérifier l'identité du client conformément à la procédure KYC (Know Your Customer).
- **Assurez-vous que votre stratégie relative aux ransomwares est régulièrement mise à jour :** cela permettra de mieux refléter la nature changeante des attaques par ransomware.

Soyez proactif

- **Étudiez les opérateurs de ransomwares ainsi que leurs outils, leurs techniques et leurs procédures** (TTP, Tools, Techniques, and Procedures).
  - Obtenez des informations gouvernementales, commerciales ou open-source sur les gangs de ransomware, leurs campagnes et leurs techniques.
  - Privilégiez la collecte et l'analyse de renseignements sur les opérateurs de ransomware et les auteurs d'attaques de type wiper qui ciblent votre marché vertical ou votre zone géographique.
  - Faites correspondre les techniques qu'ils utilisent au cadre MITRE ATT&CK.
  - Planifiez des tests de phishing réguliers, et intégrez les dernières techniques utilisées par les groupes de ransomware.

  - Assurez-vous que les vulnérabilités exploitées par les opérateurs de ransomware sont corrigés en priorité dans votre programme de gestion des vulnérabilités.
  - Analysez comment les opérateurs de ransomware exploitent les relations entre les tiers et les fournisseurs de services gérés pour cibler des entreprises comme la vôtre. Tenez-en compte dans vos évaluations et contrôles des risques liés aux tiers.
- **Consignez et conservez les coordonnées.** Incluez tous les membres et membres suppléants de votre équipe de réponse, le personnel clé et les principales parties prenantes, de préférence via un canal de communication hors bande qui ne serait pas affecté par un incident lié à un ransomware.
- **Créez des canaux de signalement.** Incluez des tiers, notamment les clients, les entreprises homologues et les partenaires de la chaîne d'approvisionnement, pour signaler les incidents liés à un ransomware.
- **Mettez en place un canal pour permettre aux utilisateurs en interne de signaler tout comportement susceptible de s'apparenter à une attaque par ransomware.** Notez :
  - Le nom et le rôle de la personne qui effectue le signalement
  - Quand cela s'est produit
  - Ce qu'ils ont remarqué
  - Pourquoi ils ont pensé qu'il s'agissait d'un ransomware
  - Ce qu'ils faisaient au moment des faits
  - Où ils se trouvaient physiquement et à quels réseaux ils étaient connectés
  - Quel compte ils utilisaient
  - Quel(s) système(s) ils utilisaient (système d'exploitation, nom d'hôte, adresse IP)
  - Le compte auquel ils étaient connectés
  - Les personnes qu'ils ont contactées et ce qu'ils leur ont dit
  - Les éléments auxquels ils accèdent généralement dans le cadre de leurs fonctions
- **Créez un canal de signalement pour permettre aux forces de l'ordre et aux agences de cybersécurité de vous signaler les incidents liés à des ransomwares ou de type wiper impliquant votre entreprise.**
- **Constituez une équipe de réponse aux cybercrises.** Celle-ci doit comprendre :
  - Des dirigeants de l'entreprise
  - Des membres de l'équipe informatique (notamment la restauration et la gestion des vulnérabilités)
  - Des membres de l'équipe des technologies opérationnelles (le cas échéant)
  - Des membres de l'équipe chargée de la sécurité opérationnelle (notamment le responsable de la réponse aux incidents, un membre de l'équipe d'analyse des preuves et, si l'entreprise en dispose, un membre de l'équipe de rétro-ingénierie des logiciels malveillants, de la recherche de menaces et des renseignements sur les menaces)
  - Un conseiller juridique
  - Un membre de l'équipe des relations publiques
  - Un membre de l'équipe des ressources humaines
- **Si nécessaire, faites appel aux services d'une entreprise spécialisée dans la réponse aux incidents.**
  - Obtenez une autorisation préalable pour faire appel à l'entreprise chargée de répondre aux incidents.
  - Si vous faites appel à un assureur pour la réponse aux incidents, sachez qu'il peut également, en plus de traiter l'incident lié au ransomware proprement dit, chercher des preuves de non-conformité afin de vérifier les attestations fournies lors de la souscription de la police.
- **Rédigez des modèles de communiqués de crise et d'annonces de violation.** Avoir rédigé l'essentiel d'une déclaration vous permettra de répondre rapidement et d'éviter les spéculations, même si vous devez ajouter des détails par la suite.
  - Nommez un porte-parole et un suppléant qui soient tous deux formés aux relations presse et sachent décrire comment l'entreprise a répondu à la violation.
  - Préparez un canal de communication (qui ne sera pas affecté par un incident) pour les briefings et les interviews avec les médias.
- **Tissez à l'avance des relations avec les forces de l'ordre et les équipes CERT (Computer Emergency Response Team) nationales.**
- **Faites évaluer par un conseiller juridique tout accord conclu avec les forces de l'ordre.**
- **Faites évaluer par un conseiller juridique les plans de réponse proposés, les déclarations envisagées et les risques de responsabilité civile, réglementaire et pénale.**

Réduisez la surface d'attaque

- **Installez les correctifs en priorité sur les systèmes présentant des vulnérabilités souvent exploitées par les groupes de ransomware.** Identifiez les vulnérabilités de vos ressources critiques et corrigez-les.
- **Renforcez les systèmes.** Donnez la priorité aux systèmes critiques et aux vecteurs d'attaque utilisés par les gangs de ransomware qui ont été identifiés grâce à vos renseignements sur les menaces. Configurez correctement les ports et les protocoles sur les appareils et désactivez ceux qui ne sont pas utilisés à des fins professionnelles. Les opérateurs de ransomware utilisent des outils légitimes dans les attaques de type LotL (« Living off the Land »). Restreindre l'accès à ces outils réduit donc le risque d'attaque.
- **Veillez à respecter les bonnes pratiques relatives à l'utilisation du protocole RDP (Remote Desktop Protocol) et d'autres services de bureau à distance.** Les services d'accès à distance constituent un vecteur d'accès initial privilégié pour les opérateurs de ransomware. Appliquez le verrouillage de comptes après un nombre spécifié de tentatives, l'authentification multifacteur (MFA), et la journalisation de toutes les tentatives de connexion à un bureau à distance. Assurez-vous qu'une raison professionnelle valable justifie d'accéder à distance aux services de bureau à distance. Auditez votre réseau pour détecter toute utilisation non autorisée des services de bureau à distance.
- **Désactivez ou bloquez les protocoles de partage de fichiers.** Cela inclut le protocole SMB (Server Message Block) sortant et la suppression ou la désactivation des versions obsolètes des protocoles de partage de fichiers. Les auteurs de menaces utilisent les protocoles de partage de fichiers pour propager des logiciels malveillants dans les entreprises.
- **Assurez-vous que les identifiants et les droits d'accès sur tous les systèmes sont gérés selon le principe du moindre privilège et limitez le nombre de comptes à privilèges.**
- **Empêchez l'utilisation des comptes à privilèges pour les activités quotidiennes.**
- **Mettez en œuvre la segmentation du réseau.** La segmentation du réseau reste l'un des moyens les plus efficaces pour limiter la propagation des ransomwares et augmenter les chances de détecter les déplacements latéraux.
- **Utilisez des configurations de base et un contrôle des modifications de la mise en œuvre.** Utiliser des configurations de base et la connaissance des modifications permettent de comparer les images de sauvegarde à des images réputées fiables lors des enquêtes.
- **Identifiez les référentiels de données mal sécurisés au sein de votre entreprise.** La classification des données de Cohesity DataHawk analyse les sauvegardes afin d'identifier les données sensibles sans affecter les systèmes de production. Cette vue complète de l'emplacement des données sensibles permet aux entreprises d'évaluer leurs risques.

Protégez vos sauvegardes

- **Assurez-vous que les systèmes de sauvegarde sont suffisamment protégés par air-gap.** Cela devrait empêcher les cybercriminels de les supprimer ou de les corrompre. Cohesity FortKnox améliore la cyber-résilience en stockant une copie immuable des données dans un coffre-fort dans le cloud géré par Cohesity via un air-gap virtuel.
- **Assurez-vous que les systèmes de sauvegarde utilisent des magasins de données immuables qui empêchent les cybercriminels de les corrompre ou de les supprimer.** Le Cohesity Data Cloud, par exemple, repose sur une plateforme de stockage immuable dotée d'une capacité DataLock qui empêche même les utilisateurs disposant de privilèges élevés de supprimer les sauvegardes.
- **Utilisez l'authentification multifacteur sur les comptes administrateur de sauvegarde.** Mettez en œuvre plusieurs options au cas où votre serveur primaire de gestion des identités et des accès serait affecté par un ransomware. Cohesity prend en charge les approches multifacteur SSO et TOTP.
- **Utilisez le contrôle d'accès basé sur les rôles (RBAC) pour attribuer le moindre privilège.** Les utilisateurs de votre système de sauvegarde ne doivent disposer que des privilèges minimaux requis pour accomplir les tâches liées à leur rôle. Cohesity dispose d'un RBAC granulaire pour prendre en charge le moindre privilège.
- **Assurez-vous que les systèmes de sauvegarde disposent d'une séparation des tâches pour empêcher un compte administrateur compromis d'effectuer des modifications malveillantes.** La capacité Quorum de Cohesity permet aux entreprises de définir plusieurs niveaux d'autorisation pour les tâches liées à la sauvegarde et à la restauration.
- **Adoptez une stratégie de sauvegarde 3-2-1.** Conservez trois copies de vos données sur deux supports différents, dont au moins une copie hors site.

- **Testez régulièrement vos sauvegardes.** Les tests de sauvegarde doivent être réguliers et automatisés. Communiquez les résultats des tests afin que les équipes concernées puissent prendre les mesures correctives nécessaires le cas échéant. Cohesity DataProtect prend en charge les tests automatisés.
- **Collectez et communiquez les métriques relatives à la couverture des sauvegardes terminées/échouées/testées des systèmes critiques.**
- **Veillez à ce que l'infrastructure de sauvegarde ait une capacité suffisante pour suivre la croissance.**
- **Assurez-vous que le système de sauvegarde peut prendre en charge les fonctions de cybersécurité nécessaires pour répondre à un incident lié à un ransomware.** Lors d'un incident, l'équipe de sécurité ne peut pas créer d'image de preuves du système touché, car celui-ci est chiffré. Elle doit donc s'appuyer sur le système de sauvegarde pour enquêter sur l'incident. Cohesity a intégré des capacités de réponse (notamment la classification des données, les flux de renseignements sur les menaces et la recherche de menaces) à sa plateforme de gestion des données. Elle propose également des solutions préintégrées avec des fournisseurs de sécurité de premier plan comme Splunk, Cisco, Palo Alto, Tenable, Qualys, Crowdstrike et ServiceNow par l'intermédiaire de l'alliance pour la sécurité des données.
- **Créez et maintenez des images de référence (« golden masters ») des systèmes critiques pour pouvoir les reconstruire plus rapidement suite à un incident.** Maintenez des modèles d'image comprenant un système d'exploitation préconfiguré et les logiciels associés qui peuvent être rapidement déployés pour reconstruire un système en salle blanche.

Renforcez votre protection contre les ransomwares

- **Identifiez les lacunes de vos mesures actuelles de prévention et de détection contre les techniques ATT&CK utilisées par les groupes de ransomware.** Faites-le en permanence pour maximiser vos chances de prévention ou de détection à mesure que les cybercriminels adaptent leur comportement.
  - Plusieurs indicateurs de compromission (IOC) typiques peuvent être utilisés dans les phases de prévention, de détection et de réponse :
    - Des transactions de fichiers anormales (écarts dans le volume de chiffrement et de suppression)
    - Des heures de démarrage suspectes des services et des applications
    - La présence de services et d'applications inconnus et inattendus
    - La présence d'un accès à distance non autorisé/logiciel VPN
    - Une baisse des performances du système (augmentation de l'utilisation du CPU/de la RAM)
    - Performances de l'instrumentation de sécurité de l'hôte dégradées/désactivées
    - Agents de sécurité désactivés
    - Des connexions inconnues/inattendues au nom de domaine et à l'adresse IP
    - Des anomalies de protocole
    - Des hachages de fichiers réputés malveillants
    - Des modifications suspectes des fichiers de configuration
    - Un trafic entrant et sortant ou une source/destination anormal
    - Des processus et texte suspects dans les vidages de mémoire
    - Des comptes suspects parmi les utilisateurs connectés (historiques et actuels)
    - Des partages réseau et partages réseau montés suspects
    - Des comptes utilisateurs suspects
    - Des certificats installés suspects
    - Des entrées suspectes dans les caches ARP et DNS
    - Des anomalies dans la date/l'heure sur les systèmes, dans les fichiers journaux ou sur les serveurs NTP
    - Des entrées ou baux suspects dans les journaux DHCP
    - Des chaînes d'agent utilisateur anormales
    - Des balises et mises à jour d'application non standard
    - Des binaires à l'intérieur de la capture complète de paquet
- **Testez le contenu de prévention et de détection.** Testez toutes les règles créées relatives aux IOC des ransomwares.

- **Mettez en œuvre la détection des anomalies du système de fichiers des terminaux qui correspondent aux attaques par ransomware et de type wiper, notamment le chiffrement ou la suppression de fichiers.** Cohesity utilise le machine learning (ML) pour identifier ces modèles.
- **Mettez en œuvre des filtres de passerelle de messagerie pour bloquer les e-mails contenant des indicateurs malveillants connus.**
- **Mettez en place un mécanisme permettant de supprimer les e-mails identifiés comme contenant du contenu lié à un ransomware de la boîte de réception des utilisateurs.**
- **Mettez en œuvre la politique et la vérification du protocole DMARC (Domain-based Message Authentication Reporting and Conformance).** Vous serez moins susceptible de recevoir des e-mails usurpés ou modifiés provenant de domaines valides.
- **Désactivez les macros pour les fichiers Microsoft Office transmis par e-mail, sauf si elles sont nécessaires pour des raisons professionnelles.**
- **Utilisez des applications qui permettent de répertorier/d'établir une liste blanche des ressources critiques pour vous assurer que seuls les logiciels autorisés peuvent s'exécuter.** Utilisez les stratégies de restriction logicielle de Microsoft ou AppLocker sur les plateformes Windows. Utilisez les listes d'autorisation du répertoire plutôt que d'essayer de répertorier toutes les applications possibles. Une restriction par défaut visant à limiter l'exécution de nombreux vecteurs d'attaque par ransomware permet aux applications de s'exécuter à partir des répertoires PROGRAMFILES, PROGRAMFILES(X86) et SYSTEM32, mais cela n'empêche pas les attaques de type LotL (« living off the land »). Interdisez tous les autres emplacements, sauf si une exception est accordée pour une application spécifique.
- **Comprenez les pratiques de gestion des risques et de cyber-hygiène de la chaîne d'approvisionnement, les partenaires tiers et les fournisseurs de services gérés.** De nombreuses attaques par ransomware sont facilitées par des tiers.
  - Comprenez le rôle de l'entreprise et du partenaire dans la gestion et les contrôles des cyberrisques. Veiller à ce que les rôles et les responsabilités soient clairement définis et mesurés, et à ce que des mécanismes d'action de correction soient inclus dans les accords contractuels.
- **Utilisez l'authentification multifacteur pour autant de services que possible, en particulier pour l'accès à distance et les comptes à privilèges.**
- **Mettez en œuvre une segmentation logique ou physique du réseau afin de séparer les unités commerciales ou les catégories de ressources informatiques, ainsi que tous les environnements de technologie opérationnelle.** rmettra de limiter la propagation des ransomwares en cas d'att
- **Réduisez les possibilités d'utiliser le PowerShell dans les attaques de type LotL.**
  - Limitez l'utilisation de PowerShell à des utilisateurs spécifiques au cas par cas
  - Mettez à jour PowerShell vers la version 5.0 ou ultérieure, et désinstallez toutes les versions antérieures de PowerShell
  - Assurez-vous que la journalisation du module, du bloc de script et de la transcription est activée.
  - Veillez à ce que le journal des événements Windows « PowerShell » et le journal « PowerShell Operational » aient une période de rétention d'au moins 180 jours sur les systèmes où PowerShell est activé
- **Analysez le trafic historique du réseau pour détecter les modèles de trafic est-ouest et nord-sud anormaux.** Utilisez les métadonnées du trafic réseau (NetFlow/sFlow) ou, si possible, la capture complète de paquet ou un système de détection/prévention des intrusions sur le réseau.
- **Sécurisez les contrôleurs de domaine.**
  - **Assurez-vous qu'aucun logiciel supplémentaire n'est installé sur les contrôleurs de domaine, à l'exception des agents de gestion des données et de sécurité.** L'accès aux contrôleurs de domaine doit être limité au groupe des administrateurs. Tous les utilisateurs de ce groupe doivent utiliser un compte restreint distinct pour leurs activités quotidiennes.
  - **Configurez le pare-feu hôte sur les contrôleurs de domaine pour empêcher l'accès à Internet.**
  - **Activez Kerberos pour l'authentification et l'audit NTLM pour vous assurer que seules les réponses NTLM v2 sont envoyées sur le réseau, si possible.**
  - **Vérifiez LSASS.EXE pour comprendre quelles applications seraient affectées si les protections d'authentification de sécurité locale étaient activées.** Cela empêchera l'injection de code d'acquérir des identifiants et activera ces protections si l'impact est acceptable.
  - **Assurez-vous que la signature SMB est requise entre les hôtes et les contrôleurs de domaine.** Cela empêche l'utilisation d'attaques par rejeu sur le réseau.

Renforcez votre système de détection des ransomwares

- **Recherchez de manière proactive dans les données historiques pour trouver des compromis.** Utilisez les nouveaux renseignements sur les menaces et IOC liés aux groupes de ransomware pour lesquels il n'existe aucune règle de prévention ou de détection. Cohesity intègre un flux de renseignements sur les menaces qui fournit plus de 110 000 IOC utilisés par les groupes de ransomware et permet de les rechercher dans les sauvegardes. Rechercher passivement dans les sauvegardes plutôt que dans les systèmes actifs empêche les cybercriminels de détecter l'activité. Cela évite ainsi qu'ils utilisent les techniques de contournement de la défense dont ils se servent sur les solutions des terminaux. De plus, les périodes de rétention des sauvegardes sont généralement plus longues que celles des solutions de sécurité, ce qui permet d'étendre l'horizon de détection.
- **Mettez en œuvre un mécanisme pour détecter les changements inhabituels dans l'utilisation du processeur et du disque.** Ces métriques sont généralement collectées par les plateformes ITOps, mais elles peuvent également être transmises à l'équipe de sécurité afin d'améliorer la détection.
- **Identifiez les protocoles réseau inhabituels.** Ceux-ci incluent notamment I2P ou TOR, qui sont connus pour être utilisés par les groupes de ransomware.
- **Identifiez les connexions réseau qui utilisent des ports ou des destinations connus pour servir aux activités de commande et de contrôle en cas d'attaque par ransomware ou de type wiper.**

Répondez à l'incident

- **Identifiez et regroupez les alertes similaires liées aux ressources impactées.**
- **Faites une première estimation des pertes (impact) liées à l'incident, notamment :**
  - Les nombre estimé de terminaux chiffrés/effacés
  - Les chaînes de valeur commerciales affectées par les systèmes chiffrés/effacés
  - Les obligations réglementaires relatives aux données impactées (nombre de d'enregistrements, types de données)
  - Toute preuve d'exfiltration

> Cohesity recherche automatiquement la sauvegarde des systèmes affectés pour identifier l'impact réglementaire potentiel des incidents liés aux ransomwares. Les systèmes sauvegardés peuvent également être classés à la demande, avant un incident ou en réponse à celui-ci.

- **Identifiez les environnements de test utilisés pour l'exfiltration de données.** Identifiez les systèmes sur votre réseau dont le volume de données augmente de façon inattendue, ou qui contiennent des types de données que vous ne vous attendiez pas à trouver sur cet hôte. Cohesity recherche automatiquement la sauvegarde des systèmes affectés pour identifier l'impact réglementaire potentiel des incidents liés aux ransomwares.
- **Isolez les hôtes infectés des réseaux filaires et sans fil.**
- **Si la variante du ransomware est connue et qu'elle se propage, bloquez les canaux de communication et d'infection connus (pare-feu hôte ou réseau, passerelles de messagerie, contrôle d'accès au réseau).**
- **Activez la salle blanche.** Si les outils de sécurité, les systèmes de communication, de collaboration ou de contrôle d'accès ont été affectés, instanciez rapidement les instances réputées fiables pour pouvoir lancer les activités de réponse.
- **Restaurez la dernière sauvegarde des systèmes affectés dans un environnement de salle blanche.** Elle servira d'image de preuves pour commencer votre enquête. L'état du système à d'autres points dans le temps peut permettre d'établir des tendances historiques et d'identifier les modifications apportées au système de fichiers au fil du temps.
- **Redéployez des outils de réponse/détection fiables sur les systèmes présents dans la salle blanche.** Les cybercriminels cibleront les outils des terminaux pour être sûrs de pouvoir contourner la détection. Il n'est donc pas certain qu'ils fonctionnent correctement. Les réinstaller permet de garantir leur bon fonctionnement et de s'assurer qu'ils créent correctement les rapports.

- **Si vous ne connaissez pas la variante du ransomware, identifiez-la en procédant comme suit :**
  - Collectez les messages de rançon (fenêtres contextuelles graphiques, fichiers texte ou HTML qui peuvent s'ouvrir automatiquement après le chiffrement, fichiers image, notamment les fonds d'écran des systèmes infectés qui contiennent les e-mails de contact, fichiers audio contenant des demandes de rançon).
  - Analysez les messages de rançon pour identifier le groupe et la variante du ransomware (nom du ransomware, langue utilisée, syntaxe, structure, phrases, illustrations, adresse e-mail du contact, noms d'utilisateur, type de paiement de la demande de rançon [c.-à-d. type de cryptomonnaie, cartes-cadeaux], adresse du paiement en cas de cryptomonnaie, adresse du chat d'assistance ou URL du support)
  - Analysez les fichiers chiffrés et autres artefacts créés (schéma de renommage et extension des fichiers chiffrés, types de fichiers ciblés, emplacements des fichiers ciblés, propriété des fichiers et groupe de fichiers affectés, modifications des métadonnées des fichiers, notamment les modifications en masse des dates de création/modification des fichiers, visualisation de l'entropie et du tracé des octets, icône utilisée pour les fichiers chiffrés, indicateurs de fichiers, fichier contenant le manifeste des fichiers chiffrés ou le matériel clé, autres fichiers de données)
  - Étudiez le vecteur d'infection plus en profondeur, si nécessaire
  - Extrayez les fichiers binaires suspects des systèmes de fichiers instanciés pour mener des opérations de rétro-ingénierie si la variante est inconnue
  - Vérifiez les artefacts collectés pour identifier les groupes de ransomware et les variantes sur des sites tels que :
    - Le site de recensement des ransomwares (https://goo.gl/b9R8DE)
    - CryptoSheriff (https://www.nomoreransom.org/crypto-sheriff.php)
    - ID Ransomware
- **Recherchez des preuves de persistance.** Les snapshots historiques pris par Cohesity peuvent être instanciés pour permettre aux analystes d'examiner les systèmes de fichiers et de rechercher des preuves de persistance. Citons notamment :
  - Des mécanismes de persistance de type « outside-in » tels que l'accès authentifié à des systèmes externes via des comptes malveillants, des portes dérobées sur les systèmes périphériques, et l'exploitation de vulnérabilités sur les systèmes périphériques
  - Des mécanismes de persistance de type « inside-out » tels que l'implantation de logiciels malveillants sur les systèmes internes ou diverses modifications de type LotL [notamment le déploiement de cadres de tests d'intrusion commerciale tels que Cobalt Strike, l'utilisation de PsTools, en particulier PsExec, pour installer et contrôler à distance des logiciels malveillants et collecter des informations, et l'utilisation de scripts PowerShell)
- **Capturez une image du contenu de la mémoire pour détecter les processus suspects ou les artefacts de texte.**
- **Identifiez les clés de registre modifiées.**
- **Identifiez les fichiers compressés récemment créés.**
- **Examinez les processus et les tâches planifiés.**
- **Comparez les services réseau actifs/en cours d'exécution à ceux qui devraient fonctionner.**
- **Exécutez le playbook sur la perte de données si vous avez des preuves de test ou d'exfiltration.** Cohesity DataHawk peut identifier quelles données se trouvaient sur ces systèmes au moment de l'attaque. Les personnes chargées de répondre aux incidents peuvent ainsi identifier les obligations de conformité et informer les personnes concernées et les autorités de régulation.
- **Identifiez les vulnérabilités des systèmes exploités lors de l'attaque.** Cohesity CyberScan permet aux personnes chargées de répondre aux incidents de faire tourner le scanner de vulnérabilités Tenable Nessus sur le snapshot près du point d'attaque. Vous pouvez ainsi créer un manifeste des correctifs à appliquer sur le système avant de le remettre en production, et des vulnérabilités que les cybercriminels pourraient avoir exploitées depuis le dernier scan de vulnérabilité planifié.

- **Identifiez les ressources utilisées pour faire les tests en recherchant la propriété intellectuelle, les informations financières ou les données à caractère personnel (DCP) sur les ressources non autorisées.** Les données sensibles peuvent être identifiées dans les environnements de préproduction à l'aide de la classification des données de Cohesity DataHawk.
- **Extrayez les fichiers binaires suspects des systèmes de fichiers instanciés historiques.** Analysez-les, menez des opérations de rétro-ingénierie, ou téléchargez-les sur des services tels que VirusTotal. L'instanciation des systèmes de fichiers historiques peut être orchestrée dans Cohesity par des outils SOAR (Security Orchestration & Automated Response) tels que ServiceNow Security Incident Response, Splunk Phantom et Palo Alto XSOAR.
- **Extrayez les fichiers binaires suspects des systèmes de fichiers instanciés et détruisez-les dans un bac à sable d'analyse des logiciels malveillants.**
- **Vérifiez si des systèmes similaires au sein de l'entreprise sont infectés.** Étudiez les hôtes présentant des utilisateurs et des groupes similaires. Si les systèmes ne sont pas chiffrés, comparez les instances de ces hôtes au système infecté afin d'identifier l'impact pochtentiel. Les capacités d'indexation et de recherche de Cohesity permettent d'interroger rapidement l'infrastructure de sauvegarde d'une entreprise.
- **Vérifiez les comptes locaux, les outils de gestion des identités et des accès, ainsi que les services d'annuaire pour détecter les nouveaux comptes ou la modification des autorisations/droits d'accès.**
- **Identifiez les autres systèmes qui tentent de se connecter à la commande et au contrôle du ransomware.**
- **Continuez à suivre la chaîne d'investigation à l'aide du MITRE ATT&CK afin d'identifier le patient zéro, le vecteur d'infection initial et chaque terminal infecté.**
- **Identifiez tous les contrôles de prévention ou de détection qui ont été contournés, et le mécanisme utilisé.** Ajoutez-les à votre plan d'atténuation pour renforcer les contrôles avant de restaurer la production.

Communiquez

- **Communiquez avec la presse.** Tenez la presse informée pour éviter toute spéculation préjudiciable.
- **Communiquez avec les personnes impactées.** Assurez-vous que toutes les notifications sont conformes aux obligations réglementaires et légales.
- **Communiquez avec les parties prenantes internes.** Tenez vos employés informés de la situation et de vos attentes à leur égard, car les journalistes peuvent utiliser des plateformes telles que LinkedIn pour les identifier et les contacter directement.
- **Communiquez avec les autorités de régulation pour respecter les obligations réglementaires en matière de déclaration.**
- **Informez votre compagnie d'assurance.**
- **Informez les forces de l'ordre et l'équipe CERT nationale/du secteur.**

Restaurez après l'incident

Le scénario idéal serait de détecter et supprimer l'infection, puis de restaurer les systèmes en production à l'aide d'outils tels que la restauration massive instantanée. En réalité, vous aurez probablement une combinaison de systèmes restaurés et de systèmes reconstruits à partir de zéro. Pour effectuer des restaurations complètes, vous devrez avoir accès à des « images de référence » des systèmes critiques, qui sont sécurisées et maintenues avec les derniers correctifs testés. Ces modèles peuvent être rapidement déployés pour reconstruire des systèmes qui ne peuvent être restaurés. Ils peuvent également être sécurisés à l'aide des outils disponibles dans le Cohesity Data Cloud, afin de ne pas être corrompus lors d'une cyberattaque. Vous pouvez ensuite restaurer le système d'exploitation et les applications de base, ainsi que les données associées à partir d'autres sauvegardes. Cela optimise le RTO tout en créant des sauvegardes historiques des systèmes affectés à des fins d'analyse de preuves.

Une fois les données et applications restaurées, vous devrez documenter l'incident et prendre des mesures pour éviter qu'il ne se reproduise.

Les entreprises doivent :

- Utiliser leurs connaissances sur le vecteur d'infection initial, les vulnérabilités exploitées et les mécanismes de persistance pour mettre à jour leurs plans de restauration. Cela leur permet de se protéger contre de futures attaques, et de s'assurer que chaque composant peut être ramené à un état sûr et stable
- Restaurer les systèmes restants en salle blanche, répéter les étapes ci-dessus, et mettre en quarantaine tout indicateur de compromission
- Corriger les vulnérabilités identifiées
- Réinitialiser les mots de passe de tous les systèmes et comptes affectés
- Supprimer les e-mails historiques contenant des artefacts d'exploitation des boîtes de réception supprimées
- Renforcer la surveillance ciblée des systèmes précédemment infectés

Définissez les points clés à retenir et les actions de suivi

Après avoir subi une attaque par ransomware, posez-vous les questions suivantes afin de tirer les leçons de cette expérience :

- Quels produits et services ont été affectés ?
- Quels ont été les impacts sur l'entreprise ?
- Quelles parties prenantes ont été affectées ?
- Qui étaient les auteurs de la menace ?
- Qu'est-ce qui n'a pas fonctionné dans le processus de réponse ?
- Qu'est-ce qui a bien fonctionné dans le processus de réponse ?
- Quand avons-nous détecté l'attaque ?
  - Quel a été le délai entre l'infection initiale et la détection ?
  - Pourquoi n'a-t-elle pas été détectée plus tôt ?
  - Quels contrôles n'ont pas permis de la détecter ou de la prévenir ?
- Quels contrôles ont été contournés et comment ?
- Quels ajustements faut-il apporter aux opérations commerciales pour empêcher de futurs incidents ?
- Comment éviter cela à l'avenir ?
- Avons-nous pu restaurer la production dans les RTO/RPO requis ?

Envoyez les nouveaux IOC découverts à tous les partenaires et fournisseurs autorisés.

- Mettez à jour la documentation et les playbooks.
- Communiquez le rapport d'incident final et les enseignements tirés aux parties prenantes et aux autorités de régulation.

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**.

En savoir plus sur Cohesity.com/fr/

COHESITY

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

2000048-002 FR 4-2025