COHESITY

LIVRE BLANC

Renforcer la cyber-résilience dans un monde en proie à des cyberattaques destructrices

Évaluez votre entreprise à l'aide du modèle de maturité de la résilience aux cyberattaques destructives de Cohesity.

TABLE DES MATIÈRES

Synthèse

Les données sont vitales pour les entreprises commerciales et les organisations à but non lucratif. Elles sont essentielles aux processus et aux flux de travail de l'entreprise, qui sont aujourd'hui tellement dépendants de l'informatique que le retour à des processus manuels (de type « papier et stylo ») perturberait considérablement sa capacité à fournir ses produits ou services.

Ces perturbations relevaient jusqu'à présent de la continuité de l'activité et de la reprise après sinistre, et résultaient d'un petit nombre de scénarios bien définis, notamment une inondation, un incendie, une panne d'électricité, une mauvaise configuration ou une défaillance d'équipement. Aujourd'hui, elles sont généralement dues à des cyberattaques destructrices.

Dans ce livre blanc, nous verrons pourquoi les approches traditionnelles utilisées par les équipes chargées des opérations informatiques (ITOps) pour gérer les scénarios de continuité de l'activité et de reprise après sinistre ne sont plus adaptées à cette nouvelle menace. Nous verrons également pourquoi les processus de réponse aux incidents historiquement utilisés par les équipes chargées de la sécurité opérationnelle (SecOps) pour faire face aux cyberattaques non destructrices sont aujourd'hui insuffisants.

Enfin, nous proposerons des mesures pragmatiques pour que les entreprises puissent renforcer leur résilience face aux cyberattaques destructrices grâce au modèle de maturité de la résilience aux cyberattaques destructives de Cohesity. Grâce à ce modèle, les entreprises peuvent évaluer le niveau actuel de maturité de leur résilience et élaborer une feuille de route pour l'améliorer au fil du temps.

La nouvelle menace et l'échec des approches traditionnelles

Si les origines des ransomwares remontent au « cheval de Troie AIDS » lancé en 1989, ces attaques ne sont devenues facilement monnayables qu'avec l'apparition des crypto-monnaies, une vingtaine d'années plus tard, entraînant la déferlante d'attaques que nous connaissons aujourd'hui.

En 2012, un autre type d'attaque destructrice est apparu avec la découverte de Flame et Shamoon, des logiciels malveillants de type wiper. Ceux-ci ont ciblé et détruit les données liées aux intérêts des compagnies pétrolières iraniennes et saoudiennes, respectivement. Contrairement aux attaques par ransomware, que les criminels utilisent à des fins financières, ces attaques de type wiper sont l'œuvre d'États-nations ou de leurs partisans pour nuire aux intérêts ou à l'économie d'un autre État. Dans le contexte géopolitique actuel, le monde a récemment connu une augmentation significative des attaques de type wiper.

Depuis les origines de la discipline de la sécurité de l'information jusqu'à la montée en puissance d'attaques par ransomware destructrices, les entreprises ont surtout été confrontées au vol de données. Contrairement à une fraude ou au vol d'un bien matériel, l'entreprise qui se fait voler des données en possède toujours une copie et peut les utiliser pour continuer à fournir ses produits et services à ses clients. Les conséquences de ces attaques sont des pertes secondaires, à savoir une atteinte à sa réputation, des litiges potentiels avec ses partenaires ou les personnes victimes du vol de données, ou encore des amendes réglementaires.

Aujourd'hui, à l'ère des cyberattaques destructrices, notamment des attaques par ransomware et de type wiper, une perte primaire vient s'ajouter à ces pertes secondaires : l'entreprise devient incapable de fournir ses produits et ses services. Bien qu'une grande partie des pertes secondaires soient irrécupérables (leur cause étant antérieure à l'incident du fait de l'absence de contrôles appropriés pour prévenir l'incident), chaque seconde consacrée aux activités de réponse et de restauration augmente les pertes primaires de l'entreprise. Avec les attaques sur la confidentialité des données d'une entreprise, nous pouvions tolérer des processus de réponse

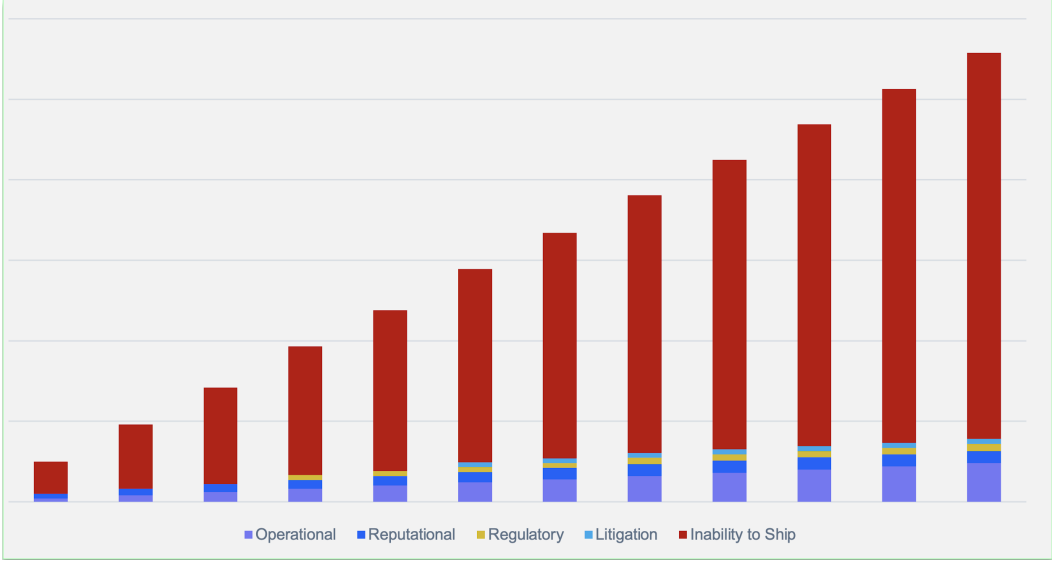

Illustration 1 : *Effets indicatifs du temps sur différents types de pertes*

et de restauration inefficaces et inefficients. Nous n'avons plus ce privilège avec les attaques contre l'intégrité ou la disponibilité des données essentielles à l'entreprise.

Les développements récents dans le domaine des ransomwares à la demande (RaaS) ne vont faire qu'empirer les choses pour les personnes chargées de protéger l'entreprise. Par le passé, nous avons globalement été confrontés à quelques dizaines d'opérateurs de ransomware qui géraient leur propre infrastructure et lançaient les attaques. Le nombre d'attaques était limité, car les opérateurs de ransomware devaient réunir les compétences techniques nécessaires pour faire fonctionner leur infrastructure.

Nombre de ces opérateurs ont trouvé plus rentable de mettre leurs plateformes et boîtes à outils de ransomware à la disposition d'« affiliés » n'ayant pas besoin de compétences techniques, mais seulement de ressources humaines pour mener l'attaque. En échange, les affiliés conservent généralement 80 % des rançons collectées, et l'opérateur de la plateforme empoche les 20 % restants. Grâce au RaaS, les opérateurs de plateformes peuvent également se consacrer davantage à la création d'outils d'attaque innovants pour leur plateforme afin de se différencier des autres fournisseurs. En conséquence, le phishing, qui était le principal vecteur d'attaque, a été remplacé par d'autres techniques plus efficaces, notamment l'exploitation des vulnérabilités des infrastructures connectées à Internet. Ces attaques peuvent se produire en l'espace de quelques jours, bien avant que les entreprises ne puissent appliquer des correctifs pour fermer la surface d'attaque. Autre tendance croissante : la réutilisation d'identifiants volés lors d'attaques précédentes.

Bien que nous soyons confrontés à un problème croissant d'attaques de plus en plus graves, la plupart des dépenses en matière de cybersécurité sont traditionnellement consacrées à la protection et à la détection car les attaques contre la confidentialité sont depuis toujours au centre des préoccupations. Et bien que ces dépenses soient essentielles pour empêcher l'entreprise de crouler sous les tentatives d'intrusion presque quotidiennes, elles ne suffisent pas pour faire face au volume et à la sophistication des cyberattaques destructrices d'aujourd'hui. Un simple coup d'œil aux actualités qui ont fait la une de la presse ces 12 derniers mois montre que les ransomwares ont considérablement perturbé les opérations de nombreuses entreprises dont les budgets de cybersécurité se chiffrent en dizaines de millions. Il ne suffit donc pas d'investir dans la protection et la détection. Nous ne cessons de renforcer nos défenses, mais nos adversaires créent de meilleurs outils ou utilisent l'ingénierie sociale pour les franchir.

Presque tous les cadres de cybersécurité les plus récents, notamment le **NIST Cybersecurity Framework 2.0** et les réglementations comme la **directive 2.0 de l'UE sur la sécurité des réseaux et de l'information (NIS2)** ou la **loi de l'UE sur la résilience opérationnelle numérique (DORA)**, visent à renforcer la résilience : il ne s'agit là pas seulement de la capacité des entreprises à prévenir et à détecter une cyberattaque, mais aussi à résister en répondant et en restaurant leurs systèmes, deux fonctions dans lesquelles elles n'ont traditionnellement pas suffisamment investi.

L'entreprise moyenne compte plus de 130 outils de cybersécurité différents, dont la grande majorité n'a pas été suffisamment intégrée et opérationnalisée pour éviter qu'elle ne soit victime d'une cyberattaque. Tout nouvel investissement dans la prévention et la détection ne diminuera probablement qu'une fraction du cyberrisque. En revanche, cela créera davantage de frictions avec les utilisateurs, l'entreprise deviendra moins agile, les équipes informatiques seront moins sensibilisées aux alertes, les coûts de licence augmenteront et l'infrastructure de sécurité sera encore plus lourde à gérer. À l'inverse, investir dans la réponse et la restauration permet d'obtenir la cyber-résilience nécessaire pour se conformer aux cadres et aux réglementations les plus récents et pour faire face aux cybermenaces modernes.

Les 5 obstacles à la cyber-résilience

Les méthodes traditionnelles de continuité de l'activité et de restauration après sinistre ne sont pas adaptées aux cyberattaques

Dans de nombreuses entreprises, la fonction de réponse appartient aux équipes supervisées par le responsable de la sécurité des systèmes d'information (RSSI), et la fonction de restauration aux équipes supervisées par le directeur des systèmes d'information (DSI). C'est principalement cette répartition qui empêche l'entreprise de passer de la cybersécurité à la cyber-résilience. Ces deux fonctions ont développé ces capacités de manière largement indépendante l'une de l'autre, car elles devaient à l'origine répondre à d'autres menaces : en effet, historiquement, les RSSI s'occupaient des vols de données, tandis que les DSI s'occupaient de la reprise après sinistre et de la continuité de l'activité. Les stratégies de continuité de l'activité et de reprise après sinistre s'articulaient autour d'un nombre limité de scénarios de menace faciles à comprendre, notamment les inondations, les incendies, les tremblements de terre, les coupures de courant, les défaillances d'équipement ou les erreurs de configuration.

Si les entreprises dotées d'énormes budgets de cybersécurité et de programmes de continuité de l'activité/reprise après sinistre bien établis font la une des journaux lorsqu'elles sont victimes d'un ransomware, c'est parce que ces deux aspects n'ont pas été adaptés pour résister aux cyberattaques destructrices. Cela entraîne des coûts considérables et des perturbations importantes pour les clients.

Les plans de continuité de l'activité et de reprise après sinistre du DSI sont conçus pour répondre à un petit nombre de causes profondes bien définies. L'automatisation et l'orchestration peuvent jouer un rôle important dans la restauration, et c'est le dernier snapshot d'un système qui est généralement utilisé pour cette opération.

En revanche, dans le cas d'une cyberattaque destructrice, l'adversaire cible activement les sauvegardes pour les rendre indisponibles afin d'augmenter les chances de réussite de l'attaque. Ces adversaires peuvent utiliser n'importe quelle combinaison parmi les quelques centaines de techniques ATT&CK de MITRE, de manière itérative et dans n'importe quel ordre, pour pénétrer dans l'entreprise en exploitant ses vulnérabilités. Une fois à l'intérieur, ils escaladent les privilèges, maintiennent leur persistance même en cas de restauration à partir d'une sauvegarde, se déplacent latéralement dans l'entreprise, volent des données et finissent par les supprimer ou les chiffrer.

Les entreprises qui paient le plus lourd tribut à une cyberattaque destructrice sont celles dont l'adversaire a rendu les sauvegardes inutilisables, ou qui ont restauré les systèmes attaqués sans prendre les mesures correctives appropriées pour éliminer les menaces et les vulnérabilités, si bien que ces mêmes systèmes sont réinfectés en l'espace de quelques secondes ou de quelques minutes.

L'enquête ne renseigne pas sur l'atténuation

Lorsqu'elle restaure un environnement après une cyberattaque destructrice, l'équipe chargée des opérations informatiques (ITOps) dépend de l'équipe chargée de la sécurité opérationnelle (SecOps) pour comprendre comment éviter d'être réinfectée et de subir une nouvelle attaque. L'enquête de l'équipe SecOps permet de découvrir :

- Quelles vulnérabilités ont été exploitées par l'adversaire, afin que l'équipe ITOps puisse les corriger avant que les systèmes ne soient remis en production.
- Quels comptes malveillants et fournisseurs d'authentification il faut supprimer des systèmes.
- Quels e-mails traînent dans les boîtes de réception des utilisateurs en attendant d'être réutilisés.
- Quels mécanismes de persistance résident dans les fichiers de configuration modifiés et doivent être supprimés
- Si l'adversaire a remplacé des binaires ou des bibliothèques par des binaires ou des bibliothèques malveillants.

- Si des registres ou des forêts de domaines ont été modifiés.
- Quels contrôles n'ont pas permis d'arrêter ou de détecter l'attaque, afin qu'ils puissent être renforcés pour éviter que cela se reproduise.
- Tout artefact de l'attaque qu'il faudra supprimer du système restauré.

De plus, les attaques de type LotL (« Living off the Land ») étant de plus en plus répandues, les outils utilisés pour administrer l'environnement sont utilisés contre lui. Quel est l'impact de l'indisponibilité de PowerShell ou de SSH sur la restauration ?

Lorsqu'il agit de manière isolée, le DSI peut promettre un objectif de délai de restauration (RTO) qui dépend simplement de la vitesse du disque, du réseau et du logiciel de restauration, sans tenir compte du temps que prendront les étapes de confinement, d'enquête et d'éradication de la phase de réponse. Ce n'est que lorsqu'un incident se produit qu'une entreprise comprend qu'elle doit soit ajouter un délai de réponse imprévu, soit s'en passer et entreprendre de multiples itérations de restauration qui allongeront le RTO. Sinon, elle sera réinfectée presque immédiatement. Le DSI et le RSSI doivent travailler ensemble pour définir avec le conseil d'administration et les cadres supérieurs des attentes réalistes en termes de RTO, qui permettent à la fois de répondre et de restaurer.

Les contrôles de sécurité peuvent faire défaut

Le RSSI peut avoir construit une grande partie de ses capacités autour des scénarios de vol de données. L'entreprise peut avoir supposé que des fonctions essentielles de l'informatique, de la sécurité et même du bâtiment seraient disponibles en cas d'attaque, alors que ce n'est pas le cas. Il est par exemple déjà arrivé que les systèmes de contrôle d'accès aux portes soient effacés, empêchant l'accès physique aux bâtiments et aux salles nécessaires pour commencer à répondre. Les systèmes de voix sur IP et d'e-mail ont également été touchés, empêchant l'entreprise de communiquer avec les assureurs, les partenaires commerciaux, les autorités de régulation, les forces de l'ordre et la presse. (La presse a dû contacter les employés de l'entreprise via LinkedIn pour savoir ce qui se passait. Ils ont découvert que ces derniers n'étaient au courant de rien, car personne ne pouvait communiquer avec eux. Cela a entraîné des articles négatifs dans la presse).

L'équipe ITOps collabore avec les unités commerciales pour définir les priorités en matière de continuité de l'activité et de reprise après sinistre, et se concentre souvent d'abord sur les applications métier essentielles, sans tenir compte de la sécurité. Mais il est essentiel de restaurer une capacité de réponse minimale viable fiable afin que les équipes ITOps et SecOps puissent collaborer avec leurs interlocuteurs internes et externes pour gérer l'incident.

Les contrôles de sécurité peuvent ne pas fonctionner après une cyberattaque destructrice

Dans presque tous les cadres de réponse aux cyber-incidents, que ce soit le **plan de réponse aux incidents en six étapes du SANS Institute** ou le **guide de gestion des incidents de sécurité informatique NIST SP800-61r2**, la phase de confinement est essentielle pour empêcher que les attaques de type ransomware et wiper ne se propagent. Le problème, c'est que nous devons aujourd'hui accéder au terminal pour enquêter, éradiquer et restaurer. La création d'imagerie de preuves à distance et les contrôles de sécurité de terminaux tels que l'**EDR (End-Point Detection & Response)** et l'**XDR (eXtended Detection & Response)** font partie de l'arsenal de sécurité d'aujourd'hui.

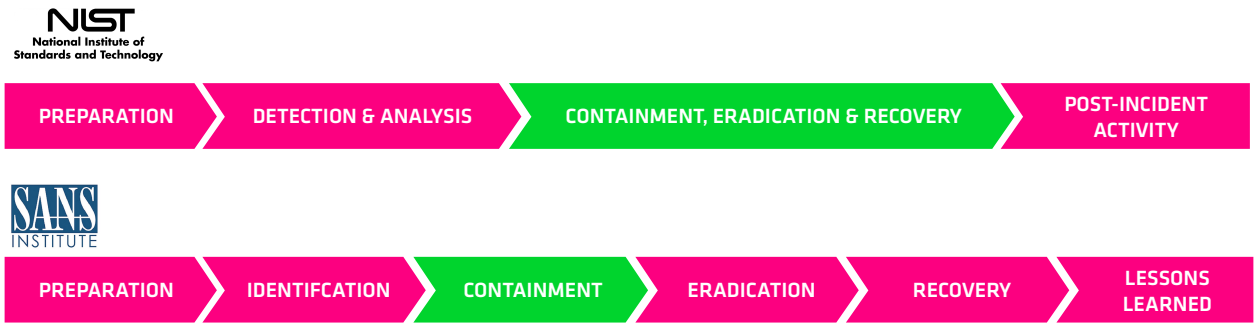

Illustration 2 : *Le confinement fait partie des bonnes pratiques en matière de réponse aux incidents, mais il peut entraver l'utilisation des outils de sécurité*

Les contrôles de sécurité ne sont pas toujours fiables

Le cadre MITRE ATT&CK (la norme de facto pour analyser le comportement de l'acteur malveillant lors d'une cyberattaque) est composé de 14 tactiques qui décrivent les étapes de bout en bout suivies par un attaquant. La tactique « contournement de la défense » décrit comment un acteur malveillant peut contourner les contrôles de sécurité. ***Notez que cette tactique particulière comporte 42 techniques, plus que toutes les autres***. Ne pas protéger vos sauvegardes et vous fier entièrement à des contrôles de sécurité basés sur la détection et installés sur un terminal peut compromettre votre sécurité. Votre entreprise risque en effet de ne pas détecter les attaques par ransomware et de type wiper en cours et de ne pas être capable de restaurer ses données.

En résumé, de nombreuses entreprises prévoient que l'équipe du DSI utilise les processus et les technologies classiques de continuité de l'activité et de reprise après sinistre pour répondre à une cyberattaque destructrice, si la sauvegarde elle-même n'a pas été prise pour cible. L'équipe du DSI ne peut pas restaurer tant que l'équipe du RSSI n'a pas enquêté sur l'incident et établi les mesures correctives nécessaires ou défini le risque de réinfection. Dans le même temps, l'équipe du RSSI peut avoir négligé l'impact d'une telle attaque sur sa capacité à remplir ses fonctions de réponse, et peut être tributaire de l'équipe du DSI pour restaurer sa capacité de réponse.

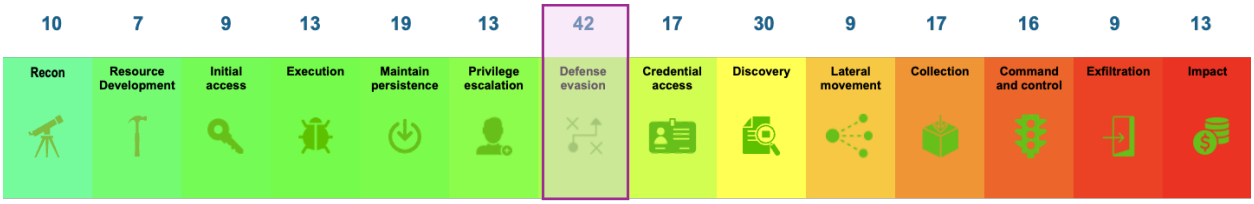

Illustration 3 : *Le contournement de la défense compte le plus grand nombre de techniques ATTaCK parmi les 14 tactiques.*

Passer de la cybersécurité à la cyber-résilience

Presque toutes les entreprises de réponse aux incidents retenues qui traitent quotidiennement ce type d'incidents savent qu'il est essentiel de mettre en place des environnements de réponse et de restauration isolés pour minimiser le RTO réalisable en cas de cyberattaque destructrice. Ces entreprises doivent collaborer avec leurs clients dans la phase de chaos qui suit l'incident pour mettre en place ces environnements, mais c'est grâce à eux que les systèmes peuvent être rétablis tout en minimisant les chances de réussite d'une nouvelle attaque.

Certains fournisseurs de gestion des données habitués à répondre aux scénarios traditionnels de continuité de l'activité et de reprise après sinistre proposent des environnements isolés dédiés aux seuls besoins de restauration de l'équipe ITOps, oubliant ainsi la relation intrinsèque entre la réponse et la restauration qui est nécessaire pour assurer la cyber-résilience.

La remise en service des systèmes peut prendre beaucoup de retard si l'on ne s'attaque pas aux causes profondes de l'incident, car il faut restaurer après chaque nouvelle attaque. L'entreprise subit alors des interruptions de service bien plus longues que ce qu'elle considérait comme tolérable lorsqu'elle établissait ses plans de restauration, car chacune de ces tentatives de restauration prend le RTO qu'elle s'était engagée à respecter.

Cohesity estime que les besoins de réponse de l'équipe SecOps sont aussi importants que les besoins de restauration de l'équipe ITOps pour réduire l'impact. Les approches qui consistent à s'empresser de restaurer les systèmes sans comprendre la nature de l'attaque ne suppriment pas la surface d'attaque ou les artefacts de l'attaque. Les attaques en cours réinfecteront les systèmes restaurés en quelques minutes. Les gangs spécialisés dans les attaques par ransomware recourent de plus en plus aux attaques de type « double tap », c'est-à-dire qu'ils reviennent attaquer les entreprises qu'ils ont déjà frappées et qui ont refusé de payer la rançon. Ces attaquants exploiteront les mêmes vulnérabilités que la première fois si elles n'ont pas été corrigées.

Cohesity a conçu une plateforme unique dotée de capacités dont les deux équipes peuvent se servir pour améliorer l'efficacité et l'efficience de la fonction de réponse et de restauration.

Bienvenue en salle blanche

Il existe de nombreuses définitions d'une salle blanche. Pour Cohesity, c'est un environnement isolé dans lequel l'équipe SecOps peut mener les enquêtes nécessaires pour comprendre comment une attaque s'est produite. Établir une chronologie de l'incident lui permet de rédiger un manifeste des mesures correctives à prendre lors de la phase de restauration pour éradiquer la menace et éviter qu'elle ne se reproduise.

La salle blanche appartient généralement à l'équipe SecOps. À ce stade de l'enquête, les systèmes ne sont pas restaurés. Ils sont analysés de manière isolée, de sorte que les interdépendances n'ont guère d'importance. Grâce à l'isolation, seuls des outils de sécurité éprouvés sont utilisés pour éviter le contournement de la défense (évoquée précédemment), l'adversaire ne peut pas observer ou perturber les actions de réponse, et les machines qui ont déjà été restaurées ne risquent pas d'être réinfectées par des systèmes dans la salle blanche.

La salle blanche fait partie (et dépend) d'une capacité de réponse minimale viable que Cohesity peut mettre en place en quelques minutes. Bâtir une infrastructure fiable et reconnue permet de soutenir la collaboration, la communication et les autres flux de travail du processus de réponse et de restauration. L'entreprise peut déjouer les nombreuses techniques de contournement des cybercriminels en restaurant les outils de l'équipe ITOps dans un état éprouvé utilisé dans un environnement isolé.

Cohesity fournit également un certain nombre de capacités natives pour répondre aux besoins de l'équipe SecOps en salle blanche. Grâce aux capacités de recherche de menaces de **Cohesity DataHawk**, les personnes chargées de répondre aux incidents disposent d'un flux organisé de plus de 170 000 indicateurs de compromission (IoC) utilisés par les opérateurs de ransomware dans le cadre MITRE ATT&CK. Les entreprises peuvent ainsi comprendre les techniques que leurs adversaires utilisent tout au long du cycle de vie de l'attaque.

Il est possible d'ajouter à ce flux organisé les propres renseignements sur les menaces du client ou ceux fournis par une tierce partie. Les artefacts que l'équipe SecOps du client trouve sur les systèmes lors de la phase d'analyse de preuves peuvent être réinjectés dans Cohesity pour repérer d'autres systèmes impactés. Ces systèmes peuvent alors être inclus dans le champ de l'enquête.

Comme la recherche de menaces avec Cohesity ne dépend pas d'un agent de terminal, elle n'est pas sensible aux techniques de contournement de la défense utilisées contre les systèmes XDR et EDR. Elle est aussi totalement passive et ne peut donc pas être détectée ou perturbée par l'adversaire. Comme la recherche de menaces avec Cohesity est alimentée par la sauvegarde, elle continuera à fonctionner même si l'entreprise a isolé ses hôtes et ses réseaux pour les confiner. En outre, dans de nombreuses entreprises, les sauvegardes sont conservées plus longtemps que les journaux des solutions de sécurité. Les entreprises peuvent ainsi détecter les activités des États-nations qui mènent des attaques de type « low and slow », notamment des attaques de type wiper prépositionnées avec des temps d'arrêt prolongés.

Dans le cas d'une analyse de preuves numérique traditionnelle, les enquêteurs devaient s'appuyer sur une seule image de preuve prise après l'événement, et formuler des hypothèses pour expliquer comment un système s'était retrouvé dans un état final particulier. Avec **Cohesity DataProtect** les enquêteurs chargés d'analyser les preuves peuvent désormais parcourir librement l'ensemble de la chronologie de l'incident et charger des images de l'état d'un système de fichiers en quelques secondes. Les enquêteurs d'aujourd'hui peuvent utiliser leurs outils pour comparer les systèmes de fichiers afin d'identifier

rapidement les écarts de configuration et repérer les mécanismes de persistance ainsi que les comptes malveillants. Ils peuvent également extraire des binaires pour les faire exploser dans des bacs à sable, et ainsi produire davantage d'IoC qui pourront alimenter la capacité de recherche de menaces de DataHawk.

Si de nombreuses entreprises maîtrisent les implications réglementaires des données stockées dans leurs magasins de données structurées (notamment les bases de données), la plupart d'entre elles possèdent une multitude de données non structurées qui contiennent des données réglementées et d'autres données sensibles. Il est notoirement difficile de comprendre ces données, car elles peuvent être disséminées dans toute l'entreprise et, en cas de cyberattaque destructrice, elles seront probablement chiffrées ou supprimées. La capacité de classification des données de Cohesity DataHawk utilise des détections avancées basées sur l'intelligence artificielle (IA) /le machine learning (ML) pour localiser et classer ces données réglementées directement à partir des sauvegardes. Cela permet de se conformer plus facilement aux exigences réglementaires, qui imposent d'informer le régulateur et les personnes concernées de toute compromission de données confidentielles.

Cohesity a créé l'**alliance pour la sécurité des données** afin d'intégrer le contexte des données d'une entreprise aux outils de l'équipe SecOps. À l'ère du cloud, des conteneurs et des hyperviseurs (où l'infrastructure peut être instanciée en quelques secondes), ce sont les données qui sont difficiles à remplacer. Ce sont également les données qui sont soumises à des règles de conformité, et que le cybercriminel cherche à voler, à chiffrer ou à effacer. Cohesity a noué des relations avec des fournisseurs de sécurité de premier plan, notamment Palo Alto Networks, Cisco, CrowdStrike, ServiceNow, Tenable, Qualys, BigID, Okta, Securonix, CyberArk et Zscaler, ainsi qu'avec des entreprises spécialisées dans la fourniture de services professionnels liés à la sécurité, comme Mandiant et TCS. Elle révolutionne la manière dont le contexte des données peut transformer la réponse et la restauration informatiques, et permet aux entreprises d'exploiter pleinement leurs investissements existants en matière de cybersécurité.

L'importance des tests

Une salle de test est un environnement de restauration qui appartient généralement à l'équipe ITOps, et dans lequel les systèmes sont soit rapidement reconstruits à partir de sources connues fiables, soit restaurés et nettoyés. C'est là que sont prises les mesures d'atténuation des menaces définies par l'équipe SecOps. C'est également là que les interdépendances entre les différents hôtes sont rétablies. La capacité fonctionnelle restaurée est ensuite testée pour s'assurer que les mesures de restauration et d'atténuation n'ont pas réintroduit de problèmes dans la production. Les systèmes ayant fait l'objet de mesures d'atténuation sont ensuite sauvegardés une dernière fois. Cela permet de disposer d'une base de référence au cas où un problème surviendrait, afin d'éviter d'avoir à reprendre les actions de réponse du début.

Cohesity SmartFiles permet de stocker des supports d'installation éprouvés sur un support immuable, afin de s'assurer que les cybercriminels ne puissent pas y accéder. Celui-ci peut ensuite rapidement être montés sur des systèmes Windows et Linux, afin que les outils informatiques d'orchestration ou de script puissent reconstruire les systèmes. Cohesity DataProtect permet de sauvegarder et de cloner des copies de référence (« golden master ») des systèmes pour pouvoir restaurer les configurations et les données à partir de snapshots de l'ensemble de la chronologie, conformément aux conclusions de l'enquête menée par l'équipe SecOps.

- Take proactive measures to reduce the impact of an attack so businesses have trusted resources available when they need them.
- [a] Increase your incident response readiness with a hardened platform, adherence to the 3-2-1 backup rule, and clear communication protocols.

- Destructive cyber attacks target an organization's ability to respond and recover.
- Endpoint security controls can't always be trusted post incident.

- Until you know how you were attacked and close the vulnerabilities and bolster controls you will be vulnerable to re-attack.
- Traditional security tools struggle to function when an organization has isolated systems in response to ransomware or wipers.

- Recovery without closing the vulnerabilities, adding additional preventive and defective controls and the eradication of persistence mechanisms and other attack artefacts leaves you open to re-attack.
- Mitigations and recovery may have caused functional problems.

Illustration 4 : *Chronologie de l'incident montrant la progression depuis l'attaque jusqu'à la restauration*

Réunir l'informatique et la sécurité pour assurer la cyber-résilience

Pour renforcer la cyber-résilience, il est essentiel de réunir les flux de travail, les équipes et les technologies de réponse utilisés par l'équipe SecOps avec les flux de travail, les équipes et les technologies de restauration utilisés par l'équipe ITOps. Se concentrer sur ces fonctions de manière isolée sans tenir compte du reste ne fera qu'aggraver les conséquences d'un cyber-événement.

L'approche de Cohesity, qui consiste à fournir une plateforme unique pour les deux équipes, accélère les actions de réponse de l'équipe SecOps tout en s'intégrant à leurs outils de sécurité existants. Cela permet d'améliorer l'efficacité et l'efficience tant de la réponse que de la restauration, de renforcer la résilience et de réduire les impacts.

Comment utiliser une salle blanche pour répondre à un incident

De nombreuses entreprises n'ont pas l'environnement adéquat pour enquêter rapidement sur les incidents et s'assurer qu'elles ne réinfectent pas leurs systèmes en restaurant leurs données.

Regardez notre webinaire à la demande pour découvrir comment créer une stratégie de réponse aux incidents qui renforce l'état de préparation et les capacités de réponse de votre entreprise sans introduire de risques supplémentaires.

Regardez le webinaire

Présentation du modèle de maturité de la résilience aux cyberattaques destructrices de Cohesity

Dans ce document, nous abordons plusieurs concepts éprouvés visant à améliorer la cyber-résilience. La prochaine étape logique consiste à évaluer vos capacités de résilience et à comprendre comment (et où) vous pouvez vous améliorer.

Voici donc le **modèle de maturité de la résilience aux cyberattaques destructrices de Cohesity**.

L'objectif de ce modèle de maturité est de permettre aux entreprises de développer leur résilience face aux cyberattaques destructrices telles que les attaques par ransomware et de type wiper. Le modèle définit des points de référence clairs et propose une feuille de route structurée pour aider les entreprises à mettre en place des opérations efficaces, efficientes et résilientes face aux cyberattaques.

Le modèle de Cohesity est aligné sur les cadres de réponse et de restauration les plus courants en matière de cybersécurité, notamment le plan de réponse aux incidents en six étapes du SANS Institute, le cadre RE&CT, MITRE D3FEND et le guide de gestion des incidents de sécurité informatique NIST SP800-61, afin que les entreprises puissent adopter les bonnes pratiques à l'échelle du secteur.

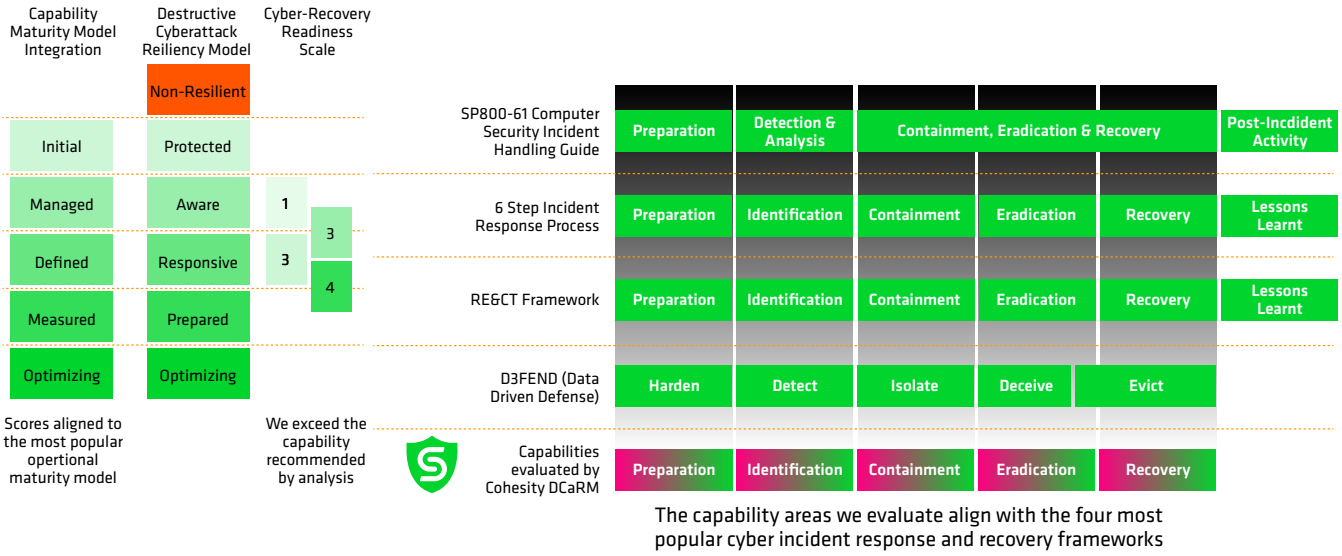

Illustration 5 : *Alignement indicatif du modèle de maturité de la résilience aux cyberattaques destructrices de Cohesity sur les cadres communs de réponse et de restauration*

Grâce à ce modèle de maturité, les entreprises peuvent évaluer leur capacité opérationnelle tout au long des cinq étapes à suivre pour devenir cyber-résilientes :

1. Se préparer à un incident
2. Identifier l'attaque et enquêter
3. Contenir la propagation de l'attaque
4. Éradiquer les menaces et réduire la surface d'attaque pour prévenir de futures attaques
5. Restaurer les systèmes dans un état sécurisé

Les niveaux de maturité du modèle sont décrits dans le tableau ci-dessous :

Niveau de maturité	Description
Non résilient	L'entreprise n'est pas suffisamment résiliente pour résister à une cyberattaque destructrice sans qu'il y ait d'impact significatif sur la fourniture de ses produits et services.
Récupérable	L'entreprise a mis en place des capacités de reprise après sinistre et de continuité de l'activité, mais celles-ci peuvent être attaquées par des personnes malveillantes et ne pas disposer des étapes d'investigation et de correction appropriées pour empêcher toute réinfection ou nouvelle attaque.
Renforcé	L'entreprise a protégé sa capacité à restaurer son activité après une attaque.
Sensibilisé	L'entreprise est capable de détecter les premières phases d'une cyberattaque destructrice qui ne peut être contournée et n'est pas affectée par la phase de confinement de la réponse aux incidents. Un modèle de responsabilité partagée entre les services ITOps et SecOps a également été élaboré pour traiter les incidents.
Réactif	L'entreprise est capable de restaurer les outils nécessaires pour gérer la réponse aux incidents et les communications avec les parties prenantes dans un état fiable, et dispose d'environnements isolés qui permettent d'enquêter sur les incidents, d'éradiquer les menaces et de tester les systèmes avant de restaurer la production. L'entreprise mène plusieurs actions pour améliorer en permanence sa capacité de réaction : elle organise des exercices d'attaque de bout en bout dans différentes situations, développe la mémoire musculaire des personnes chargées de répondre aux incidents afin qu'elles puissent faire face à toute situation future, optimise les processus et cherche à automatiser pour accroître l'efficacité et l'efficience. L'entreprise est capable de restaurer rapidement l'infrastructure et les ressources utilisées pour gérer et répondre à l'incident si celles-ci sont affectées par l'attaque.
Optimisé	L'entreprise se sert de mesures et de données télématiques pour optimiser en permanence ses processus, ses ressources humaines et ses technologies. La découverte et la classification proactives des données garantissent une gouvernance et une conformité réglementaire de bout en bout. Il est possible non seulement de restaurer les systèmes, mais également de reconstruire rapidement l'infrastructure dans un état fiable. L'enquête sur les incidents, la reconstruction de l'infrastructure et la restauration des données sont optimisées pour pouvoir être effectuées en parallèle.

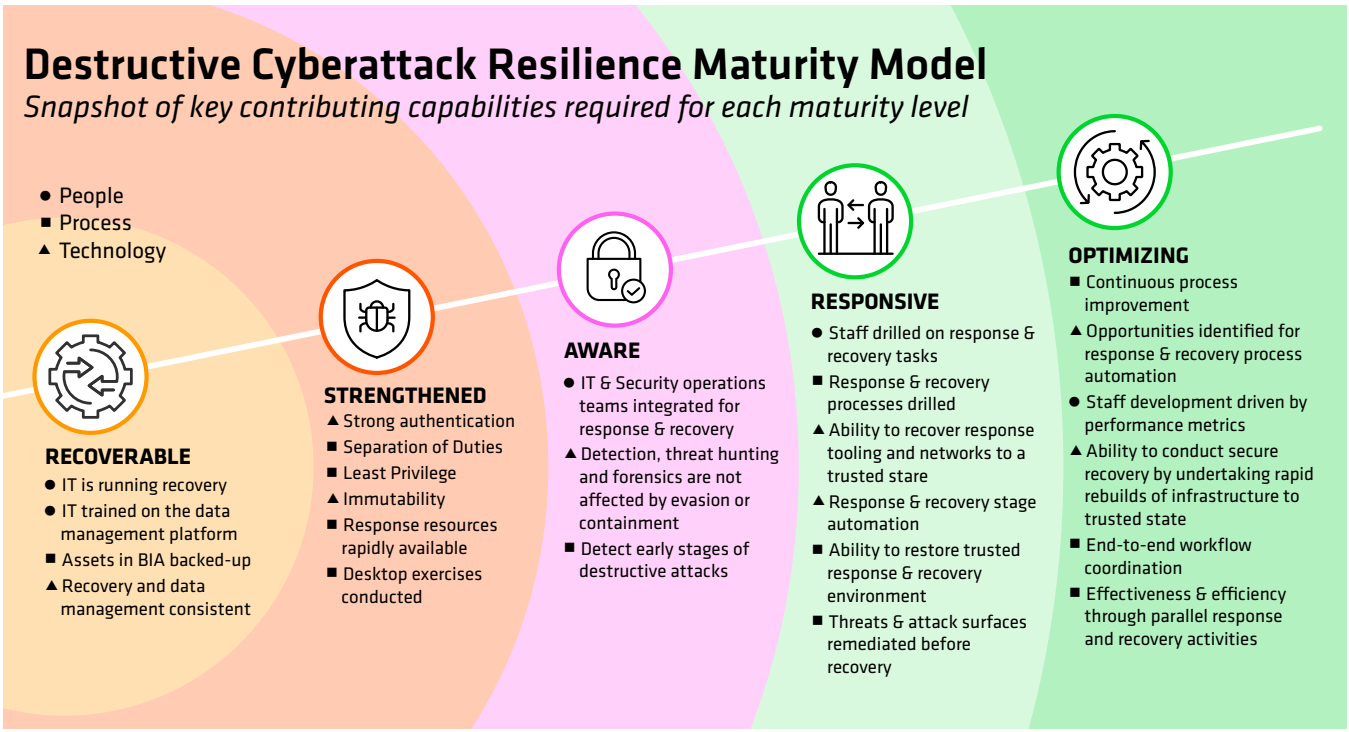

Illustration 6 : *Snapshot des principales capacités requises pour chaque niveau de maturité du modèle de maturité de la résilience aux cyberattaques destructives de Cohesity*

Le modèle de maturité de la résilience aux cyberattaques destructives de Cohesity fournit une feuille de route indépendante des fournisseurs. Cette approche permet à ses utilisateurs de s'aligner sur les cadres de réponse et de restauration basés sur les bonnes pratiques, de parvenir à un état de cyber-résilience et de développer une gouvernance, des ressources humaines et des processus appropriés. La feuille de route garantit que la technologie prend en charge et optimise les résultats opérationnels, mais ne les détermine pas.

Examinons plus en détail les niveaux de maturité :

- **Récupérable** : Une entreprise qui est à ce niveau peut avoir un niveau de maturité élevé en matière de reprise après sinistre et de continuité de l'activité. Elle a réalisé des évaluations d'impact appropriées pour identifier les services critiques et l'infrastructure qui les prend en charge, et a défini des objectifs de point de restauration (RPO) et de délai de restauration (RTO). La plateforme de gestion des données de cette entreprise ne sera pas suffisamment protégée contre les attaques d'un acteur malveillant. Elle traitera généralement un cyber incident destructeur comme un scénario traditionnel de reprise après sinistre et de continuité de l'activité, sans tenir compte des complications liées à une cyberattaque. À ce niveau, il n'y a pas de relation de travail étroite entre les équipes ITOps et SecOps pour faire face aux cyber incidents.
- **Renforcé** : À ce niveau, l'entreprise sait qu'elle sera attaquée par un adversaire et a mis en place des mesures de protection pour en atténuer l'impact. Elle a mis en œuvre des principes de sécurité comme l'accès selon le principe du moindre privilège, l'immuabilité (pour empêcher la modification ou la suppression malveillante des sauvegardes), la séparation des tâches (pour empêcher un administrateur malveillant ou compromis de faire des modifications préjudiciables) et l'isolation (pour mettre la capacité de restauration hors de portée du cybercriminel). L'isolation permet également à l'entreprise de respecter des conventions de sauvegarde sécurisée telles que le principe 3-2-1.
- **Sensibilisé** : À ce niveau, les entreprises ont adopté un modèle de responsabilité partagée bien défini entre les équipes ITOps et SecOps. Elles sont capables de rechercher des menaces et d'analyser les preuves numériques, même lorsque les acteurs malveillants

contournent les systèmes de sécurité des terminaux. L'entreprise peut en outre continuer à rechercher des menaces pendant le confinement, lorsque les hôtes et les réseaux sont isolés. Elle utilise des flux de menaces, mais ceux-ci sont souvent obsolètes et ne sont pas régulièrement mis à jour pour refléter les dernières menaces confirmées des plateformes de ransomware à la demande (RaaS) et des vulnérabilités. Les entreprises n'ont pas non plus de modèle de défense en profondeur pour détecter les premières phases d'une attaque avant que les systèmes ne soient touchés.

- **Réactif** : À ce niveau, les entreprises prennent les mesures nécessaires pour enquêter sur l'incident et corriger les menaces avant que les systèmes ne soient restaurés en production afin d'éviter toute nouvelle attaque ou réinfection par le même auteur. Des environnements d'enquête et de correction isolés sont mis en place pour répondre aux exigences de confinement. Ce niveau de maturité implique également une amélioration et une pratique continues. Ainsi, les processus, les personnes et la technologie nécessaires pour répondre à un incident et restaurer de manière sécurisée sont prêts avant qu'il ne se produise. (La première fois que vos analystes SOC, les personnes chargées de répondre aux incidents et les cadres supérieurs sont confrontés à une attaque par ransomware ou de type wiper, vous ne voulez pas que vos données soient prises en otage ou que tous les systèmes de l'entreprise soient effacés. Les exercices pratiques sont utiles, mais ils ne permettent pas de tester le flux de travail de bout en bout, les compétences et la technologie nécessaires dans un scénario réel.)

Les entreprises mettent également en place des scénarios d'attaque réalistes qui préparent tous les éléments nécessaires à la cyber-résilience. Il n'y a jamais deux incidents identiques. En variant les aspects des exercices, l'entreprise est mieux à même d'optimiser ses processus. L'entreprise recherche régulièrement des opportunités pour automatiser ses processus et développer la mémoire musculaire de ses employés.

Enfin, à ce niveau, les entreprises peuvent rapidement rétablir la confiance dans leurs réseaux et leurs outils de sécurité, et disposer en quelques minutes d'autres ressources pour lancer leurs activités de réponse. Elles ont un moyen fiable de coordonner, communiquer et enquêter sur l'attaque dans le pire des scenarios. En d'autres termes, elles sont préparées à faire face à des scénarios dans lesquels les contrôles de sécurité sont contournés, les systèmes d'accès aux portes sont hors service, et aucun système CMDB, de gestion des tickets, d'e-mail ou de voix sur IP n'est disponible pour communiquer avec les forces de l'ordre, les cyber-assureurs, la presse, les régulateurs ou les personnes concernées.

- **Optimisé** : Ce niveau représente le summum de la cyber-résilience. L'entreprise a pris des mesures proactives pour découvrir et classer les données qu'elle utilise afin de s'assurer qu'elles peuvent être restaurées, mais aussi que des mesures de gestion des risques appropriées ont été prises tout au long de leur cycle de vie. Les flux de travail sont optimisés pour s'aligner sur les réglementations et les exigences en matière de notification des personnes concernées. Cela permet d'éviter les amendes et garantit la conformité de l'entreprise avec les réglementations DORA, NIS 2, HIPAA, Prudential Regulatory Authority et Security and Exchange Commission, le cas échéant. Alors que le niveau de maturité réactif recherche des possibilités d'automatiser les flux de travail, le niveau optimisé vise la gouvernance, l'orchestration et la gestion globales de l'ensemble du processus de réponse aux incidents et de restauration, de bout en bout. Ce niveau de maturité donne aux cadres supérieurs, aux conseils d'administration et aux parties prenantes tierces l'assurance que l'entreprise est à la pointe de la cyber-résilience.

Se préparer et faire face aux cyberattaques a rendu un modèle comme celui-ci indispensable. Ces attaques représentent aujourd'hui la plus grande menace qui pèse sur l'activité des entreprises. Les experts et professionnels de la cybersécurité de Cohesity, qui possèdent des dizaines d'années d'expérience dans la réponse aux cyber incidents et la restauration, ont conçu ce modèle afin que les entreprises comme la vôtre puissent comprendre leurs capacités actuelles, évaluer leur maturité par rapport à leurs pairs dans leur secteur ou leur zone géographique, et disposer d'une feuille de route pour les améliorations futures qu'elles peuvent apporter et mesurer au fil du temps.

À propos de l'auteur

James Blake possède plus de trente ans d'expérience dans le domaine de la réponse aux cyber incidents et a mis en place des capacités de sécurité opérationnelle de bout en bout pour plus de 30 entreprises du classement Fortune / FTSE 100. Il est également intervenu après de centaines d'incidents à grande échelle, notamment de nombreuses attaques de type wiper menées par des États-nations et des dizaines d'attaques par ransomware. Il est responsable de la stratégie mondiale en matière de cyber-résilience chez Cohesity.

En savoir plus sur Cohesity.com/fr/

COHESITY

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

2000059-002 FR 4-2025