LIVRE BLANC

Bonnes pratiques en matière de cybersécurité et de cyber-résilience

Un document de l'alliance pour la sécurité des données

Table des matières

Synthèse

Imaginez que votre entreprise ou votre organisme public soit une Formule 1. Vous passez des heures chaque jour à vous préparer à concourir dans la plus haute catégorie de courses internationales, mais aucun circuit n'est le même. La concurrence varie. Les pilotes sont humains. Les conditions météorologiques fluctuent. Votre réussite dépend toutefois avant tout d'une chose : la présence d'une équipe technique exceptionnelle au stand.

Il en va de même pour la cyber-résilience. Disposer d'une cyberdéfense technique intégrée, qui combine une sécurité des données et une gestion des données exceptionnelles, à l'instar d'une équipe de Formule 1, permet à votre entreprise de rester sur la bonne voie et de terminer en beauté.

En novembre 2022, plus d'une douzaine de poids lourds de l'industrie de la sécurité ont formé l'**alliance pour la sécurité des données** afin de donner aux entreprises et aux gouvernements davantage de moyens de remporter la course contre les cyberattaques. Sa mission est claire : sécuriser et protéger les données. L'Alliance y parvient en associant la sécurité des données et la gestion des données à la cybersécurité afin d'améliorer la cyber-résilience. Elle fournit pour cela des architectures et des intégrations techniques essentielles, propose des bonnes pratiques et offre un leadership éclairé autour d'un objectif commun.

Ce livre blanc de l'Alliance pour la sécurité des données explique comment les hauts dirigeants peuvent répondre aux principales priorités de l'entreprise, notamment réduire les risques et renforcer la conformité, en investissant de manière plus judicieuse dans la cyber-résilience. Ce document fait référence à la nouvelle discipline d'ingénierie de la cyber-résilience du NIST, et présente les bonnes pratiques adaptées à la vision et aux technologies collectives de l'alliance pour la sécurité des données. Il explique comment les entreprises membres font évoluer les idées et les stratégies de lutte contre les menaces du niveau de l'entreprise individuelle à celui du secteur (conformément au cadre de la cybersécurité du NIST), notamment en ce qui concerne l'identification, la protection, la détection, la réponse et la récupération.

Les enjeux de la cyber-résilience

Dans le monde numérique actuel, consommateurs et employés attendent des entreprises, quel que soit leur type ou leur taille, qu'elles fonctionnent sans interruption. C'est même ce qu'exigent certaines obligations contractuelles, notamment les accords de niveau de service. Les incidents (qu'ils soient planifiés ou non) peuvent toutefois entraîner des temps d'arrêt. C'est là que la cyber-résilience prend toute son importance.

> « Convertir les données en valeur de manière sécurisée et éthique est l'impératif économique de la prochaine décennie. Celui qui contrôle le cycle de vie de ses données maîtrisera davantage son avenir. Les données ayant de plus en plus de valeur, elles deviendront une cible privilégiée de l'espionnage industriel et des cyberattaques d'état. »[1]
>
> – **Dr. Jan-Peter Ohrtmann,** Partenaire, PwC

L'objectif de la cyber-résilience est de garantir la continuité des opérations et de l'activité face à la prolifération des menaces. La cybersécurité (les pratiques incontournables en matière de cyber-hygiène, notamment installer régulièrement des correctifs, détecter les menaces et découvrir les vulnérabilités) est un élément fondamental de la cyber-résilience, mais elle ne suffit pas. La cyber-résilience va bien au-delà de la reprise après sinistre. Les entreprises doivent en effet également anticiper les perturbations, y résister, récupérer et s'adapter rapidement, en quelques minutes ou quelques heures, et non en quelques jours ou quelques semaines.

[1] PwC. « Les grandes tendances de la confidentialité en 2030 : une feuille de route pour les PDG » (en anglais), Dr. Jan-Peter Ohrtmann, 21 Jan 2021.

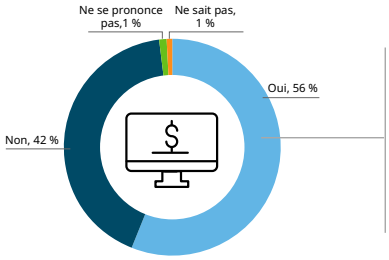
Stéphanie Balaouras, VP et directrice de groupe chez Forrester, écrivait en mai 2020 : « Les entreprises résilientes ont une stratégie et un cadre pour identifier et atténuer les risques, une planification et un état de préparation rigoureux de la continuité des activités, des capacités flexibles de réponse aux crises et aux incidents, ainsi que des systèmes d'entreprise conçus pour offrir redondance et la fiabilité ». [2] Quelques années et des centaines de milliers d'attaques par ransomware plus tard, les entreprises ont elles aussi désormais besoin de stratégies et de cadres cyber-résilients.

Les cybermenaces, en particulier les ransomwares, sont toujours plus fréquentes et plus sophistiquées. Les entreprises du monde entier doivent donc promouvoir une nouvelle coopération entre des équipes et des solutions de sécurité et de gestion des données habituellement en silos, afin d'optimiser la cyber-résilience dans des environnements, fonctionnant 24h/24, 7j/7 et 365j/an, tout en répondant aux besoins de continuité de l'activité. Les entreprises ne pourront résister aux cyberattaques, aux catastrophes naturelles et aux pannes de système, et s'en remettre, qu'en intégrant des technologies et des processus.

Dans ce contexte, la protection des données devient de plus en plus une priorité pour les entreprises et les gouvernements. La fidélité des clients, la réputation des marques et la sécurité nationale dépendent d'une protection exceptionnelle des données. Les dirigeants stratégiques attendent donc de leurs homologues techniques (directeurs des systèmes informatiques [DSI] et responsables de la sécurité de l'information [RSSI]) qu'ils mettent en place le personnel, les stratégies et les solutions nécessaires pour atteindre les objectifs de cyber-résilience de l'entreprise. Il est difficile de gérer des solutions de sécurité autonomes souvent en silos, centrées sur les menaces et complexes, alors que les menaces de ransomware évoluent. La sécurité et la gestion des données ont également manqué de cohérence et d'uniformité pour détecter, prévenir et empêcher les cybercriminels d'extorquer des sommes importantes.

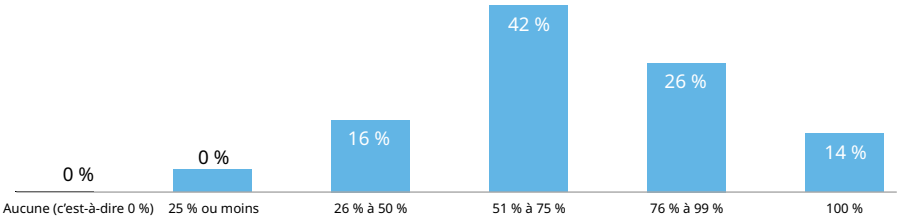
Enterprise Strategy Group (ESG) indique que plus de la moitié des entreprises victimes d'une attaque par ransomware réussie admettent avoir payé une rançon pour pouvoir à nouveau accéder à leurs données, applications ou systèmes[3]. En outre, selon Palo Alto Networks, le montant moyen des rançons a augmenté de 71 % au cours des cinq premiers mois de l'année 2022, approchant le montant record d'un million d'euros[4]. Pourtant, même les entreprises qui paient la rançon ne sont pas certaines de récupérer leurs données. Seulement 1 entreprise sur 7, soit 14 % des entreprises interrogées dans le cadre du rapport ESG, ont indiqué avoir récupéré l'intégralité de leurs données après avoir payé.[5]

Les entreprises ont-elles payé des rançons à la suite d'attaques réussies ?



« **Plus de la moitié** des entreprises victimes d'une attaque par ransomware réussie admettent à un moment donné avoir payé une rançon pour récupérer l'accès à leurs données, applications ou systèmes. »

Pourcentage de données récupérées après paiement de la rançon.



[2] Forrester. « La résilience des entreprises n'est plus une option » (en anglais), Stephanie Balaouras, 12 mai 2020.
[3] Enterprise Strategy Group. « Le long chemin à parcourir pour se préparer aux ransomwares » (en anglais), mars 2022.
[4] Palo Alto Networks. « Rapport 2022 sur les menaces liées aux ransomwares de l'unité 42 » (en anglais), 7 juin 2022.
[5] Enterprise Strategy Group. « Le long chemin à parcourir pour se préparer aux ransomwares » (en anglais), mars 2022.

Les responsables techniques peuvent travailler plus intelligemment avec les budgets existants (et ne pas avoir à demander de nouveaux budgets de sécurité) pour faire face à la prolifération des ransomwares. Ils doivent pour cela s'associer à des entreprises de premier plan axées sur les données. Ensemble, ils peuvent s'attaquer à la protection contre les ransomwares et à la récupération par le biais de contrôles et de processus axés sur l'ingénierie de la cyber-résilience. Le NIST définit l'ingénierie de la résilience comme une discipline émergente qui s'utilise avec l'ingénierie de la sécurité des systèmes pour développer des systèmes sécurisés résistants et fiables.

Les données sont au cœur de l'activité numérique des entreprises et des administrations, mais elles doivent être davantage prises en compte dans les stratégies de sécurité. L'alliance pour la sécurité des données place les données au centre afin d'unifier la sécurité et les stratégies de gestion et ainsi d'améliorer les résultats.

> « Les cyber-menaces constantes et de plus en plus sophistiquées d'aujourd'hui nécessitent une approche concertée. Un seul fournisseur ne peut pas résoudre tous les problèmes de cybersécurité, il faut que toutes les parties prenantes s'associent pour lutter contre les acteurs malveillants. »
>
> – **Sanjay Poonen,** PDG et Président, Cohesity

Les attaques par ransomware se multiplient

Les ransomwares devraient causer plus de 30 milliards d'euros de dommages dans le monde cette année. Une entreprise devrait être attaquée toutes les 2 secondes d'ici 2031, contre une toutes les 11 secondes en 2022.[6] Pourquoi devient-il chaque année plus difficile de contenir et d'arrêter cette menace croissante ? Les entreprises qui cherchent à développer leur cyber-résilience sont confrontées à de nombreux défis. Vous en trouverez plusieurs ci-après.

Les défis humains

Les êtres humains ne sont pas parfaits. Les attaques par ransomware les plus répandues se produisent par le biais d'e-mails d'hameçonnage et d'identifiants volés (ces derniers représentant 40 % des attaques par ransomware).[7]

- Les entreprises manquent de temps et de ressources pour éduquer et former correctement les employés et les partenaires à la sensibilisation à la sécurité afin de contrer les attaques (par ex. l'hameçonnage).
- Les rôles de l'informatique et de la sécurité sont en silos. Presque un tiers (31 %) des membres d'équipes SecOps récemment interrogés pensent que la collaboration avec le service informatique n'est pas solide, 9 % d'entre eux la qualifiant de « faible ».[8]

Les défis d'organisation et de processus

Même si les ransomwares provoquent des temps d'arrêt de plus en plus courts, les études signalent qu'il y a toujours entre 11 et 21 jours de latence. La faute en incombe principalement à des flux de travail de sécurité et à des processus de partage de l'information mal conçus pour contrer ces menaces. Par exemple :

- Appliquer des correctifs sur les applications et les systèmes vulnérables est chronophage et coûteux.
- Les systèmes existants susceptibles de contribuer à la protection des données, notamment la sauvegarde, requièrent des spécialistes informatiques.
- Les surfaces d'attaque sont plus vastes, si bien que les données sont plus difficiles à protéger.
- Il existe de nombreux runbooks de reprise après sinistre, mais la plupart d'entre eux ne prennent pas en compte la complexité de la réponse aux ransomwares et de la récupération suite à une attaque.

[6] Cybersecurity Ventures. « Une attaque par ransomware se produira toutes les 2 secondes d'ici 2031 » (en anglais). 3 janvier 2023.
[7] Verizon. « Rapport d'enquête sur les violations de données », 2022.
[8] Censuswide pour l'enquête Cohesity, juin 2022.

Les défis technologiques

Selon IDC, la Global DataSphere devrait plus que doubler entre 2022 et 2026, les entreprises étant les principales responsables de la croissance des données.[9] De nombreux environnements technologiques, notamment ceux qui possèdent une mosaïque de produits performants et de plateformes de sécurité et d'infrastructure disparates, n'ont pas été conçus pour traiter des données en local, dans le cloud et à la périphérie à une telle échelle. Face à l'explosion des données (tellement de types différents, dans tellement d'endroits différents), ces environnements plient sous la pression des ransomwares.

- Les solutions existantes ne sont pas bien intégrées, ce qui entraîne une complexité persistante.
- Les environnements cloud et hybrides introduisent de nouveaux défis en matière de protection contre les ransomwares et de récupération en cas d'attaque.
- Face à l'incertitude économique, la question se pose de savoir s'il faut augmenter les investissements liés à la sécurité ou optimiser ce qui existe déjà.
- La plupart des technologies ne sont pas capables d'exploiter l'efficacité et l'évolutivité que permettent l'intelligence artificielle et le machine learning (IA/ML).

Une action concertée

Signe que les ransomwares ne diminuent pas et doivent être pris au sérieux, le NIST (National Institute of Standards and Technology) américain a récemment mis à jour sa publication intitulée « Développer des systèmes cyber-résilients : une approche d'ingénierie de la sécurité des systèmes » (en anglais) et a mis l'accent sur l'ingénierie de la cyber-résilience. Cette nouvelle discipline spécialisée de l'ingénierie des systèmes, qui s'utilise conjointement à l'ingénierie de la sécurité des systèmes, permet de développer des systèmes sécurisés, résistants et fiables.

L'ingénierie de la cyber-résilience vise à construire, concevoir, développer, mettre en œuvre, maintenir et préserver la fiabilité des systèmes. Ils peuvent alors anticiper, résister, récupérer et s'adapter à des conditions défavorables, à des tensions, à des attaques, ou à des compromissions qui utilisent ou sont déclenchées par des cyber-ressources. Du point de vue de la gestion des risques, la cyber-résilience vise à réduire le risque pour la mission, l'activité, l'organisation, l'entreprise ou le secteur de dépendre des cyber-ressources.

Cela peut rassurer les entreprises, car la pénurie de talents a un impact sur la collaboration entre les équipes informatiques et de sécurité. Dans un rapport récent, 77 % des décideurs informatiques et 78 % des professionnels SecOps ont reconnu que cela avait un impact.[10] Ce même rapport souligne que le manque de coordination entre les équipes informatique et SecOps conduit les personnes interrogées à penser que leur entreprise est plus exposée aux cybermenaces. Toutes les personnes interrogées craignent particulièrement :

- Les pertes de données (42 %)
- les interruptions de l'activité (42 %)
- La perte de clients (40 %)
- L'accusation et le blâme de l'équipe en cas d'erreur (35 %)
- Le paiement d'une rançon (32 %)
- Le licenciement de talents des deux équipes (IT et SecOps) (30 %).

[9] IDC. « Prévisions mondiales d'IDC pour la Global DataSphere, 2022–2026 » (en anglais), mai 2022.
[10] Censuswide pour l'enquête Cohesity, juin 2022.

L'approche du cadre de résilience du NIST en matière de cybersécurité comprend notamment un ensemble de lignes directrices, de normes et de bonnes pratiques conçues pour permettre aux entreprises de gérer et de réduire les risques liés à la cybersécurité. Le cadre fournit un langage commun et une approche systématique de gestion des risques de cybersécurité dans différents secteurs et industries. Il s'appuie sur cinq fonctions essentielles : identifier, protéger, détecter, répondre et récupérer. Ces fonctions permettent aux entreprises de comprendre leurs risques en matière de cybersécurité, de protéger leurs ressources, de détecter les incidents de cybersécurité, d'y répondre et de s'en remettre rapidement.

Au niveau le plus élevé, un cadre de cyber-résilience comprend deux concepts essentiels : résister à une attaque et récupérer suite à une attaque.

Approche moderne : centrez votre stratégie de sécurité sur les données

En Formule 1, la voiture est au cœur des préoccupations. Comment optimiser sa vitesse ? Comment optimiser sa performance ? Comment faire tout cela en toute sécurité ? Dans les entreprises et les administrations, les données représentent la Formule 1. Elles sont au cœur de l'activité numérique des entreprises et des administrations. Et pourtant, de nombreuses stratégies de sécurité et de gestion ne placent pas les données au premier plan. Elles se concentrent trop sur l'infrastructure et les systèmes, notamment dans les clouds.

La mission de l'alliance pour la sécurité des données est centrée sur les données, et vise plus particulièrement à unifier la gestion et la sécurité des données derrière la cyber-résilience. L'objectif est de proposer des intégrations et des architectures techniques innovantes, une collaboration solide en matière de données et de sécurité, des bonnes pratiques et un leadership éclairé sur les données.

Cette vision est à la fois différente et complémentaire de celle de la CSA (Cloud Security Alliance). Cette dernière a en effet pour mission de définir et de faire connaître les bonnes pratiques pour garantir un environnement sécurisé pour le cloud computing. Les entreprises ont du mal à sécuriser et à suivre les données sensibles dans le cloud. Selon le rapport de recherche de la CSA sur l'état de la sécurité des données dans le cloud (en anglais), seulement 4 % des entreprises estiment que toutes leurs données cloud sont suffisamment sécurisées, plus d'un quart d'entre elles ne suivent pas leurs données réglementées, près d'un tiers ne suivent pas leurs données confidentielles ou internes, et 45 % ne suivent pas leurs données non classifiées.

Grâce aux intégrations et aux bonnes pratiques de l'Alliance pour la sécurité des données, les entreprises pourront tisser un ensemble cohérent de processus et de contrôles afin de minimiser l'impact des cyberincidents. Cela renforcera également la confiance organisationnelle dans les données stockées en tout lieu, dans des environnements informatiques publics, privés et hybrides.

> « Pour devenir cyber-résilient, il faut commencer par maîtriser les fondamentaux, notamment en ce qui concerne les données. Il est essentiel de savoir où se trouvent vos données sensibles, quelle est leur nature, qui y a accès et quels sont les risques associés. Notre communauté de la sécurité doit placer ses données au cœur de sa stratégie de sécurité. »
>
> – **Tyler Young,** RSSI, BigID

En plaçant les données au centre de sa stratégie de cybersécurité, votre entreprise peut :

- Réduire les risques
- Stimuler l'agilité
- Améliorer la résilience

Vous pouvez bénéficier de ces avantages en anticipant les menaces tout au long des différentes phases du cycle d'un ransomware :

Six bonnes pratiques en matière de cyber-résilience

Si vous vous concentrez sur vos données et que vous faites appel à des partenaires de premier plan dans le domaine de la sécurité et de la gestion des données, votre entreprise peut avoir les bases de la cyber-résilience dont elle a besoin pour faire face à toutes les éventualités. Vous trouverez ci-dessous six bonnes pratiques pour construire votre environnement cyber-résilient. (Elles complètent les bonnes pratiques du NIST en matière de cyber-résilience, qui comprennent un éventail d'actions, notamment : élaborer et mettre en œuvre des politiques et des procédures, tester et mettre à jour régulièrement les plans de réponse aux incidents, et établir des partenariats avec d'autres entreprises afin de partager des renseignements sur les menaces).

1. Rester vigilant : surveillez en permanence votre posture de sécurité

Le manque de budget et de ressources empêche les entreprises de suivre l'évolution constante du paysage des menaces. Elles sont contraintes d'effectuer des tâches chronophages, notamment exporter manuellement leurs données vers plusieurs feuilles de calcul, et doivent en permanence traquer les menaces au lieu d'anticiper les attaques ou les compromissions potentielles. Cela entraîne une prise de décision non ciblée et une planification stratégique inadéquate à tous les niveaux de l'entreprise. Le NIST conseille aux équipes d'élaborer et de mettre en œuvre des stratégies et des procédures relatives à la cybersécurité. Les équipes de cybersécurité ont pourtant besoin de nouvelles approches pour aborder et gérer de manière proactive les cyber-risques actuels et émergents. Elles doivent mieux comprendre où prioriser leurs efforts, comment mesurer objectivement les progrès au fil du temps et quand communiquer efficacement les résultats aux parties prenantes afin d'atténuer les attaques et

de réduire considérablement le nombre d'incidents nécessitant une réponse rapide.

Pour prévenir les cyberattaques, il faut non seulement mettre en œuvre la formation et la sensibilisation des employés à la cybersécurité recommandées par le NIST, mais aussi mettre en place des contrôles d'accès et des systèmes de surveillance. Cela suppose également d'avoir une visibilité totale des ressources et des expositions, un contexte détaillé des menaces de sécurité potentielles et des métriques claires permettant de mesurer objectivement le cyber-risque. Les entreprises capables d'anticiper les cyberattaques et de communiquer ces risques pour faciliter la prise de décision pourront mieux se défendre contre les menaces émergentes.

Les données représentent un défi particulier, car elles sont la ressource la plus dynamique de toutes. Les données sensibles augmentent et prolifèrent rapidement, et les entreprises doivent savoir où elles se trouvent, quelle est leur classification, comment on y accède, etc., pour comprendre les risques qu'elles encourent et comment les protéger.

Les plans de cyber-résilience les plus performants commencent par une évaluation. Les équipes doivent évaluer les forces, les faiblesses, les opportunités et les menaces informatiques, mais aussi identifier les solutions nécessaires pour mettre en place des défenses de cybersécurité et répondre efficacement aux cyberattaques. (Voir la liste de contrôle à la fin du document pour plus de détails). En combinant une expérience des menaces de premier plan avec une expertise dans les solutions de sécurité et de gestion des données intelligentes qui fonctionnent sur site et dans le cloud, les entreprises peuvent développer des programmes de préparation à la cybersécurité plus efficaces.

2. Ne jamais faire confiance, toujours vérifier : une architecture basée sur les principes du Zero Trust

Le modèle de sécurité traditionnel, centré sur l'idée de faire confiance mais de contrôler, n'est plus valable dans les environnements actuels des entreprises et des administrations, car les périmètres n'existent plus. Les bonnes pratiques de l'entreprise numérique exigent une architecture basée sur les principes du Zero Trust (notamment ne jamais faire confiance et toujours vérifier, ainsi que le principe du moindre privilège) pour que vous sachiez qui accède à quelles informations et à quel moment.

Toute compromission d'informations sensibles nuit à la réputation et à l'avantage des entreprises, ainsi qu'à l'agilité et à la conscience situationnelle des pouvoirs publics. C'est pourquoi il est désormais essentiel de protéger chaque identité (humaine ou machine) sur le plus grand nombre d'appareils et d'environnements. Une identité numérique est l'ensemble des informations relatives à une personne, une entreprise ou un appareil électronique qui existe en ligne. La transformation numérique d'un grand nombre d'entreprises a entraîné l'apparition d'une multitude d'identités ayant un accès sans précédent aux données. Le nombre d'identités bénéficiant d'un accès et d'un contrôle privilégiés sur plusieurs appareils dépasse aujourd'hui largement le nombre d'utilisateurs. Votre équipe en charge de la sécurité doit donc mieux protéger une surface d'attaque plus large. En outre, gérer la sécurité de l'identité de votre patrimoine de données à l'aide de plusieurs outils existants génère de la complexité et crée des failles que les pirates peuvent exploiter. Associer des contrôles d'accès basés sur les rôles complets à des stratégies de type « ne jamais faire confiance, toujours vérifier » permet de mieux protéger votre entreprise contre les ransomwares et les menaces internes.

Les données sont désormais partout. Votre entreprise doit donc trouver un moyen d'unifier intégralement la gestion et la sécurité des données (des terminaux aux charges de travail dans le cloud, de la sauvegarde à la production, de l'identité aux données) pour stopper les acteurs malveillants. Une approche de la prévention des attaques axée sur les données (complémentaire à la recommandation du NIST de mettre en œuvre le chiffrement et d'autres contrôles de sécurité pour protéger les données) nécessite d'avoir une visibilité et un contrôle sur l'ensemble de vos données. Avoir une visibilité complète vous permet de minimiser le risque lié aux données sur l'ensemble de vos systèmes cloud et locaux en matière de sécurité des données, de confidentialité, de conformité et de gouvernance.

3. Connaître ses données : développez l'intelligence

Le NIST recommande de tester et de mettre à jour régulièrement les plans de réponse aux incidents et de réaliser régulièrement des évaluations de vulnérabilité et des tests de pénétration. Cette démarche est essentielle, car le fait de détecter rapidement les logiciels malveillants vous permet de refuser en toute confiance de payer une rançon. Au-delà de ces conseils pour les systèmes de production, vous pouvez découvrir les risques de cybersécurité et les angles morts de votre environnement de production en lançant des analyses automatisées à la demande des données de production et des snapshots de sauvegarde pour détecter les vulnérabilités connues. Ces analyses permettent également d'évaluer facilement votre posture face au risque et de répondre aux exigences strictes de sécurité et de conformité sans impacter votre environnement de production.

Analysez les snapshots de production et de sauvegarde afin d'évaluer leur santé et leur capacité de récupération. Vérifiez les sauvegardes pour être sûr qu'aucune vulnérabilité connue n'est réinjectée dans l'environnement de production lors des restaurations. Toutes ces opérations vous permettent de développer l'intelligence et d'obtenir une vue globale de tous les risques de cybersécurité dans votre environnement de production. Vous pourrez ainsi y remédier avant qu'un acteur malveillant ne les exploite.

La classification des données alimentée par l'intelligence artificielle et le machine learning (IA/ML) améliore également les capacités de protection contre les ransomwares, de détection des menaces et de réponse aux incidents. Vous conservez ainsi une longueur d'avance sur les cybercriminels. Vous pouvez découvrir en permanence des données sensibles et réglementées, notamment les données à caractère personnel (DCP), les informations de santé protégées et les données PCI, et réduire les faux positifs grâce à une classification des données basée sur le ML. Cette intelligence des données permet de renseigner la posture de sécurité, de maintenir à jour les contrôles de sécurité dépendants, notamment la prévention des pertes de données (DLP), et d'aider les équipes d'intervention à comprendre l'impact d'une attaque par ransomware ou d'un cyber-incident.

4. Stimuler la collaboration : faites de la cyber-résilience un sport d'équipe

La résilience exige de la préparation, de la réactivité, de la ténacité et de l'adaptabilité. Dans le monde connecté moderne, les responsables de la sécurité doivent exploiter une architecture et des processus qui englobent des environnements en local, dans le cloud et à la demande (SaaS), tout en mettant en œuvre des processus de sécurité axés sur la continuité de l'activité. Les programmes SecOps doivent s'appuyer sur des solutions et des processus qui permettent de prévenir les actions hostiles lorsque c'est possible, mais aussi de les détecter et d'y répondre lorsqu'il n'est pas possible de les prévenir.

Pour faire preuve de résilience, il faut arrêter les attaquants avant qu'ils n'atteignent leurs objectifs dans un environnement cible. Les entreprises doivent comprendre parfaitement le paysage des menaces et les vecteurs d'attaque pour prendre en charge leurs efforts de résilience. Pour ce faire, elles doivent connaître en détail les renseignements sur les menaces et les surfaces d'attaque, à condition que ces informations soient spécifiques à l'entreprise et non pas généralisées. Enfin, le programme de sécurité doit impérativement déboucher sur des processus qui soutiennent la résilience de l'entreprise. Il est essentiel de planifier la réponse aux incidents et d'établir des partenariats pour assurer la viabilité de l'entreprise et de votre programme de sécurité.

Le NIST recommande d'établir des partenariats et des collaborations avec d'autres entreprises pour partager les renseignements sur les menaces et les bonnes pratiques. Votre entreprise a de meilleures chances de protéger vos données contre les attaques par ransomware si vous repensez et adaptez vos processus pour vous appuyer sur une collaboration IT/SecOps. Vos chefs d'entreprise seront également plus sereins.

Découvrez des produits de sécurité fiables qui fonctionnent parfaitement ensemble pour contrer les ransomwares, et investissez en toute confiance. Il s'agit notamment de solutions SIEM (security information and event management) et SOAR (security orchestration, automation and response) qui permettent d'accélérer le délai de découverte, l'enquête et la correction des attaques par ransomware. L'équipe SecOps peut enrichir ces flux de travail intégrés, préétablis et extensibles pour automatiser la réponse aux incidents et unifier les opérations entre les équipes sécurité, informatique et réseau. Assurez-vous

en outre de pouvoir réaliser des intégrations préétablies à l'aide d'un kit de développement logiciel (SDK) sécurisé et d'API de gestion personnalisables qui vous offrent la flexibilité nécessaire pour exploiter votre environnement comme vous le souhaitez.

5. Consolider et simplifier : exploitez une plateforme moderne de gestion et de sécurité des données

L'évolutivité et la compatibilité sont des éléments supplémentaires pour lutter contre les attaques par ransomware. La cyber-résilience nécessite de la collaboration. Il est donc important d'exploiter une plateforme de sécurité et de gestion des données extensible et moderne, dotée d'une architecture riche en API et API-first, qui fonctionne sur plusieurs sites et couvre la plage de sources de données la plus large possible. Consolider plusieurs fonctions de gestion des données sur une plateforme unique vous permet de simplifier vos opérations. Au lieu de faire des copies des données et de les déplacer, vous avez également une solution qui vous permet de réutiliser les données sur place en leur apportant des applications à valeur ajoutée pour les tâches quotidiennes et plus complexes (par exemple l'analyse de virus, le masquage de données, l'analyse des journaux d'audit de fichiers et la classification des données). De plus, une seule plateforme extensible vous permet de réduire l'empreinte de vos données et la surface d'attaque disponible pour les ransomwares.

6. Gagner en rapidité et en confiance : intégrez l'infrastructure de sauvegarde à l'infrastructure et aux opérations de sécurité

Les complexités liées à la sécurité et à la gestion des données ne peuvent être résolues seules, en particuliert en cas de violation. Rétablir la disponibilité opérationnelle le plus rapidement possible (dans les objectifs de délai de récupération et de de point de récupération [RTO/RPO]) nécessite une approche intégrée dans laquelle la sauvegarde n'est pas en silo, mais fait partie intégrante de l'infrastructure et des opérations de sécurité.

Les entreprises qui investissent dans la sécurité et la gestion des données bénéficieront de solutions étroitement intégrées qui couvrent tout le spectre des cadres de sécurité. L'un des plus populaires est le cycle de réponse aux incidents, ou PICERL, de l'Institut SANS :

- **Preperation (Préparation)** – Évaluations, plans, formation, gestion des identités, etc.
- **Identification (Identification)** – Suivi de la sensibilisation, détection précoce etc.
- **Containment (Maîtrise)** – Notification, sauvegardes, preuves, etc.
- **Eradication (Éradication)** – Restaurations, analyse de cause racine, suppression du programme malveillant etc.
- **Recovery (Récupération)** – Analyse des vulnérabilités, reprise des opérations, base de référence, etc.
- **Lessons Learned (Enseignements tirés)** – Création de rapports, mises à jour des procédures, etc.

Avec des intégrations soigneusement étudiées, vous et votre équipe êtes capables de contrer les attaques rapidement et en toute confiance, depuis la planification jusqu'à la récupération (et même d'utiliser l'IA/ML automatisée pour détecter les cyberattaques potentielles en alertant les équipes sur les schémas inhabituels autour de vos données). En cas de violation, vous pourrez également récupérer des données propres (à n'importe quel point dans le temps et à n'importe quel emplacement), qui ont été soumises à une analyse de vulnérabilité afin d'éviter de réinfecter le système, et ainsi réduire les temps d'arrêt.

Liste de vérification des capacités de cyber-résilience

Plusieurs fonctionnalités automatisées et complètes permettent de contrer efficacement les ransomwares, notamment :

	Besoins	Capacités clés
Cybersécurité (résister)	Stratégie	• Services de conseil, de mise en œuvre et de sécurité gérée pour renforcer vos défenses en matière de cybersécurité et répondre efficacement aux cyberattaques.
	Gestion et sécurité des identités	• Une plateforme et des services pour l'identité du personnel et des clients • Protection de toute identité (humaine ou machine) sur un maximum d'appareils et d'environnements.
	Gestion de la visibilité et de l'exposition	• La capacité d'inventorier toutes les ressources informatiques (matériel, logiciels, applications, données). • Une plateforme pour évaluer les risques sur l'ensemble de la surface d'attaque (dans le cloud ou en local, de l'IT à l'OT et au-delà), qui vous apporte la visibilité et la connaissance nécessaires pour hiérarchiser et valider la posture de risque. • Gestion de la posture de sécurité des données (Data security posture management, DSPM) pour pouvoir mettre en place une solide pratique de découverte, de classification et d'intelligence des données (connaître l'emplacement des données, leur nature, qui y a accès, leur flux de travail et les risques)
	XDR (Extended detection and response)	• Une solution native du cloud avec des capacités XDR pour l'ensemble de l'infrastructure de sécurité, qui accélère la détection, la réaction et la récupération • Un moyen de lancer des flux de travail pour restaurer les données et les charges de travail en cas d'attaque par ransomware.
	SIEM (Security information and event management)	• Une solution de défense contre les menaces avancées dans les environnements hybrides complexes d'aujourd'hui, qui utilise les analyses les plus avancées et repose sur une architecture native du cloud évolutive et flexible.
	SOAR (Security orchestration, automation and response)	• Une automatisation et une flexibilité qui vous permettent de gérer plus rapidement les cyberattaques et les attaques par ransomware
	Renseignements sur les menaces exploitables	• Une intelligence et une expertise complètes, au service de solutions dynamiques qui vous permettent d'élaborer des programmes plus efficaces et d'avoir confiance en votre préparation aux risques de cybersécurité. • Visibilité et contrôle de toutes les données sensibles et critiques, pour comprendre et minimiser les risques liés aux données dans le cloud et en local, avec une approche axée sur les données, pour la sécurité des données, la confidentialité, la conformité et la gouvernance
	Observabilité de l'ensemble de la pile	• Une plateforme de données extensible qui offre une sécurité unifiée, une observabilité full stack et des applications personnalisées
	Zero Trust (ZT) / Protection du périmètre et des terminaux	• Un moyen de sécuriser les zones les plus critiques du risque d'entreprise (terminaux, charges de travail cloud, identité et données) pour garder une longueur d'avance sur les adversaires et stopper les violations.
	Preuves	• Des solutions de sécurité qui vous permettent de déterminer les causes racine et les signatures du ransomware pour entamer d'éventuelles poursuites avant de l'éliminer

	Besoins	Capacités clés
Cyber-résilience (récupérer)	Sauvegarde et récupération	• Protection complète contre les cyber-menaces, détection d'anomalies, basée sur ML, récupération rapide suite à une attaque par ransomware et mobilité du cloud hybride. • Immuabilité des données • Isolation des données : séparation physique et logique des données pour renforcer la sécurité • Principes du Zero Trust (notamment l'authentification multifacteur [MFA]) • Quorum : plusieurs personnes doivent autoriser les modifications administratives ou de configuration
	Analyse de la vulnérabilité et restauration	• Salle propre, remise en service, récupérations supplémentaires de données et/ou de configurations, autorisation de l'équipe d'application, opérations éventuelles dans le centre de données pour déplacer les systèmes entre les environnements, sécurité, et réseau pour garantir l'accessibilité à la nouvelle zone opérationnelle.
	Protection contre les menaces	• Détection des logiciels malveillants et des indicateurs de compromission (IOC) avec une veille et une analyse des menaces basées sur le ML pour identifier ces dernières dans les données de sauvegarde
	Intégrations de sécurité	• API, SDK et intégrations aux opérations et aux contrôles de sécurité pour accélérer la réponse aux incidents et exploiter les contrôles et processus existants

Placer vos données au cœur de votre stratégie de cyber-résilience vous permet de concevoir une architecture qui leur offre un maximum de protection et optimise leur récupération. L'alliance pour la sécurité des données encourage les décideurs informatiques et les dirigeants d'entreprise à consulter la page www.cohesity.com/fr/company/data-security-alliance/ pour en savoir plus sur la cyber-résilience.

À propos de l’alliance pour la sécurité des données

L’alliance pour la sécurité des données a pour mission de garantir la sécurité et la protection des données. Elle y parvient en associant la sécurité des données et la gestion des données à la cybersécurité afin d’améliorer la cyber-résilience. Elle fournit pour cela des architectures et des intégrations techniques essentielles, propose des bonnes pratiques et offre un leadership éclairé autour d’un objectif commun. L’alliance pour la sécurité des données combine les meilleures solutions des sociétés de cybersécurité et des services de premier plan avec l’expertise exceptionnelle de Cohesity en matière de sécurité et de gestion des données. L’Alliance pour la sécurité des données compte parmi ses membres : BigID, Cisco, Cohesity, CrowdStrike, CyberArk, Okta, Palo Alto Networks, Securonix, Splunk, Tenable, Mandiant, Qualys, Netskope, ServiceNow, Zscaler et PwC.

2000046-001-FR 5-2023