Pourquoi la résilience est essentielle en 2026

Cybersecurity
Progress. Protected.

Comment aborder la cyber-résilience

Les organisations privilégient de plus en plus la résilience et la reprise après incident plutôt que l'objectif traditionnel de prévention des atteintes à la sécurité des données. Plutôt que de partir du principe que les incidents peuvent être totalement évités, les acteurs majeurs mettent en place des systèmes capables de résister aux défaillances, maintenir les activités sous pression et se rétablir rapidement après des événements perturbateurs. Cela implique une compréhension plus étendue de la cybersécurité, considérée comme une gestion plutôt qu'une élimination des risques, et un renforcement de la mentalité selon laquelle il faut partir du principe qu'une brèche est inévitable.

Selon Gartner®, « d'ici 2028, la moitié des RSSI rebaptiseront officiellement leur programme de cybersécurité en programme de cyber-résilience ».

Gartner : Prédictions pour 2026 : Les programmes de cybersécurité deviennent des programmes de cyber-résilience, Arthur Sivanathan, Charlie Winckless, Will Candrick. [1er décembre 2025] ID : G00841555.

En réalité, la résilience n'est pas synonyme de perfection. C'est cette constance face à la pression qui consiste à en faire suffisamment, chaque jour, pour que, lorsque la situation devient critique, vous ne paniquiez pas et sachiez exactement quoi faire. La fragilité apparaît lorsque les rôles, les responsabilités et les priorités ne sont pas clairement définis, que les infrastructures sont rigides et enchevêtrées, que les équipes croulent sous les alertes et les angles morts, que les contrôles d'identité sont insuffisants, ou encore que le modèle Zero Trust n'existe que sur papier et non en pratique.

Une organisation résiliente se distingue des autres et crée une valeur ajoutée. Elle a conscience des scénarios plausibles, et sait qui fait quoi, quand et comment, qu'il s'agisse des technologies, des processus ou des personnes.

Paysage des menaces : pourquoi la résilience est essentielle en 2026

Commençons par la vitesse. Les malwares s'appuyant sur l'IA et les chaînes d'attaques autonomes font désormais passer les délais d'intrusion de plusieurs jours à quelques heures, voire quelques minutes. Les attaques s'adaptent en temps réel, enchaînant les exploitations de vulnérabilités sans intervention humaine.

En novembre 2025, Anthropic a annoncé avoir identifié et déjoué l'une des toutes premières campagnes de cyberespionnage utilisant un agent d'IA pour autonomiser ses opérations. Pour les entreprises, cela laisse présager un avenir où les attaques pourront prendre de l'ampleur et s'adapter à une vitesse fulgurante, et où une résilience proactive et des défenses alimentées par l'IA seront indispensables.

Vient ensuite le problème de la complexité. Les infrastructures hybrides (cloud, sur site, SaaS) introduisent une complexité adaptative qui nécessite des contrôles intégrés capables d'évoluer au gré des changements d'environnement. Chaque nouvelle intégration ouvre une nouvelle porte d'entrée, et les attaquants en ont pleinement conscience. Les lacunes de sécurité dans les modules open source, les environnements de développement et les packages commerciaux présents dans les chaînes d'approvisionnement montrent à quel point la confiance aveugle reste un risque.

Les erreurs de configuration dans le cloud restent l'une des vulnérabilités les plus exploitées dans les environnements hybrides. Les espaces de stockage non sécurisés, les rôles trop permissifs et les API mal maîtrisées constituent des points d'entrée discrets pour les pirates. Une gestion continue de la posture de sécurité et des contrôles automatisés de conformité sont indispensables pour combler ces lacunes.

60 %

de toutes les atteintes à la sécurité

résultent de l'élément humain.

Source : *Rapport de Verizon sur les atteintes à la sécurité des données en 2025*

N'oublions pas l'aspect humain. L'hameçonnage reste le principal vecteur d'attaque, désormais amplifié par l'IA générative qui produit de faux emails hautement réalistes. L'IA favorise la multiplication des attaques ciblant les identités à un tel point que le rapport 2025 de Verizon sur les atteintes à la sécurité des données confirme que le facteur humain est à l'origine de 60 % de toutes les atteintes. À elles seules, les tactiques de compromission des emails d'entreprise (BEC) par l'IA ont entraîné des pertes financières record. Le rapport IC3 du FBI pour 2024 fait état de 2,77 milliards de dollars de pertes annuelles.

Ces tendances illustrent bien les enjeux financiers : selon le rapport d'IBM sur le coût des atteintes à la sécurité des données en 2025, le coût moyen d'une atteinte s'élève à 4,44 millions de dollars, tandis que les entreprises qui ont recours à l'IA pour assurer leur sécurité économisent près de 1,9 million de dollars par atteinte. Plutôt qu'une simple statistique, c'est un argument en faveur de la rapidité et de l'automatisation.

Enfin, de nouvelles réglementations ajoutent à la complexité : NIS2 et la loi sur la résilience opérationnelle numérique (DORA). Entrée en vigueur en janvier 2025, la directive DORA impose aux entités financières des exigences uniformes en matière de gestion du cyber-risque, de tests de résilience opérationnelle et de contrôle des tiers.

1,9
million de dollars

d'économie par incident lorsque les entreprises ont recours à l'IA pour leur sécurité.

Source : *Rapport de Verizon sur les atteintes à la sécurité des données en 2025*

Actuellement en cours de transposition dans les États membres, la directive NIS2 élargit son champ d'application, impose la responsabilité des dirigeants et harmonise les obligations de notification des incidents dans les secteurs critiques. Qu'elles soient américaines ou européennes, le message des réglementations est le même : la résilience n'est plus une option, ni une préoccupation propre à un secteur donné, ni même une question purement technique : il s'agit désormais d'une obligation réglementaire pour les entreprises.

En résumé, la cyber-résilience en 2026 rime avec simplicité, visibilité, réactivité et conformité.

Cycle de vie de la résilience : 6 étapes, 3 dimensions

La cyber-résilience n'est pas une simple mesure de contrôle ni un produit miracle. Vous pouvez la considérer comme un cycle, un rythme auquel votre organisation apprend à s'adapter. Ce cycle de vie se compose de six étapes, chacune d'entre elles touchant à trois dimensions : la technologie, les processus et les personnes. Ensemble, elles constituent le pilier de la continuité lorsqu'un imprévu survient.

Toutes les organisations ne partent pas du même point. Certaines disposeront déjà de moyens avancés en matière de détection, d'orchestration et de veille. D'autres ne s'appuieront peut-être que sur un petit nombre de mesures de sécurité fondamentales, telles que la protection des endpoints et les pare-feux.

Le cycle de vie de la résilience n'est pas un modèle de maturité linéaire que toutes les organisations doivent mettre en œuvre dans son intégralité pour être considérées comme résilientes. Il s'agit plutôt d'un ensemble d'objectifs qui peuvent être abordés de manière progressive, en fonction de la maturité de l'organisation, de sa propension au risque et des ressources disponibles.

ANTICIPATION — Prenez conscience de vos risques avant qu'ils ne vous rattrapent

Pour anticiper, il faut d'abord comprendre votre surface d'attaque et les menaces les plus susceptibles de la cibler.

Des technologies telles que la cartographie des surfaces externes, la Threat Intelligence et la surveillance des risques liés aux identités offrent une visibilité précoce, tandis que des processus tels que l'évaluation des risques métiers et les exercices de simulation réalistes préparent les équipes à faire face à des scénarios plausibles.

Enfin, les dirigeants ont besoin d'informations claires, de seuils de risque et de critères de décision pour pouvoir agir rapidement. Lorsque les attaquants exploitent des vulnérabilités à une vitesse fulgurante et que l'hameçonnage par l'IA se développe rapidement, l'anticipation offre l'avantage en termes de temps nécessaire à la résilience.

RÉSISTANCE — Limitez les risques de compromission

La résistance consiste avant tout à fermer les voies faciles que les adversaires cherchent à emprunter.

La technologie met en œuvre les principes Zero Trust, couvrant aussi bien l'authentification résistante à l'hameçonnage que les politiques d'accès granulaires dans les environnements cloud et sur site, avec prise en charge de la gestion de la posture de sécurité dans le cloud (CSPM) pour maintenir des niveaux de sécurité de référence, et une gestion plus rigoureuse des identités des personnes et des machines.

Des normes de configuration, des exigences en matière de correctifs, des contrôles des accès privilégiés et une attention croissante portée à la sécurité des solutions SaaS viennent renforcer cette approche. Les personnes restent un élément essentiel, car

l'expertise en sécurité intégrée et des formations adaptatives en fonction des rôles veillent à ce que des pratiques sécurisées soient systématiquement mises en œuvre dans l'ensemble de l'entreprise.

EXPOSITION — Révélez les risques cachés

La visibilité permet une détection précoce des menaces qui échappent aux couches de prévention. Qu'elles soient fournies via des fonctionnalités de XDR ou des services de détection managés, les plateformes de détection doivent offrir une robuste télémétrie au niveau des identités et des endpoints, optimisée pour détecter les signes avant-coureurs des ransomwares, tels que le vol d'identifiants et les mouvements latéraux.

L'intégration de la plateforme de protection des applications cloud (CNAPP) et de CSPM renforce la visibilité sur les API, les privilèges et les charges de travail multicloud, tandis que la surveillance de la chaîne d'approvisionnement logicielle réduit les risques liés aux dépendances.

Ces moyens technologiques ne sont efficaces que s'ils s'appuient sur des processus qui adaptent les détections à des référentiels tels que MITRE ATT&CK pour garantir la fluidité des flux de travail des SOC et réduire la lassitude liée aux alertes. Des analystes qualifiés transforment les données télémétriques en informations utiles et contribuent à enrichir les connaissances en vue de scénarios futurs.

RÉACTIVITÉ — Automatisez les 15 premières minutes et préparez les intervenants

Lorsqu'un incident survient, c'est la rapidité de la réponse qui détermine si les perturbations peuvent être maîtrisées. La technologie permet une réponse immédiate grâce à des guides SOAR ou des services de MDR qui isolent les ressources compromises, renforcent les exigences d'authentification et vérifient l'intégrité des sauvegardes avant même une réponse des intervenants humains.

Pour les organisations ne disposant pas de SOC en interne ni de capacités d'automatisation, ces mêmes résultats peuvent être obtenus grâce à des services de détection et de réponse managées (MDR) qui offrent une surveillance continue, des enquêtes menées par des experts et des procédures de confinement prédéfinies adaptées aux scénarios d'attaque courants.

Les processus doivent être conçus en fonction du rythme des attaques actuelles, avec des circuits de communication prédéfinis, des procédures de remontée et des arbres décisionnels pour les communications réglementaires ou juridiques. Les personnes jouent un rôle déterminant : des responsabilités clairement définies, des exercices réguliers et une hiérarchie bien établie permettent aux équipes d'agir en toute confiance lorsque chaque seconde compte.

RESTAURATION — Rétablissement rapide et complet

Les organisations résilientes partent du principe qu'elles seront confrontées à un incident potentiellement catastrophique. La véritable question est de savoir si les systèmes peuvent continuer de fonctionner, si les rôles et les responsabilités sont clairement définis en situation de crise, et si les procédures de reprise sont connues et ont fait l'objet de tests. C'est tout aussi important que la technologie sous-jacente.

Des technologies telles que les sauvegardes inaltérables, les procédures de restauration testées, les options de basculement vers le cloud et les contrôles d'intégrité garantissent que les systèmes reprennent leur fonctionnement sans réintroduire de risques. Des processus permettent d'aligner les objectifs de RTO et de RPO sur l'impact métier, définir

des plans de basculement des fournisseurs et formaliser des exercices de reprise en cas d'attaque par ransomware, de compromission des services SaaS et d'indisponibilité des partenaires.

Les équipes mènent à bien les efforts de rétablissement en assurant la coordination des services juridiques, financiers, de communication et des rôles en contact avec la clientèle, apportant ainsi clarté et stabilité à un moment où la confiance est plus que jamais essentielle.

CONTINUITÉ — Apprenez et adaptez-vous

L'adaptation permet à la résilience de s'améliorer plutôt que de stagner. La technologie facilite cette démarche grâce à l'analyse post-incident, la consolidation des plateformes et la suppression des outils redondants, afin de minimiser les lenteurs opérationnelles.

Des processus permettent de traduire les enseignements tirés en mises à jour des politiques, en hiérarchisation des actions et en améliorations de la gouvernance, avec une attribution claire des responsabilités. La dimension humaine reste essentielle : pour être performantes sur le long terme, les équipes ont besoin d'un climat de sécurité psychologique et d'une charge de travail raisonnable.

Un rapport d'étude de Forrester sur la toxicité au sein des équipes de sécurité indique que « les équipes de sécurité engagées, collaboratives, en bonne santé et bénéficiant d'un environnement psychologiquement sûr sont moins confrontées à des incidents de sécurité ». Forrester rappelle également que « les équipes qui ne bénéficient pas de cette sécurité psychologique signalent davantage d'atteintes à la sécurité, notamment 3,5 fois plus d'incidents internes que la moyenne mondiale ».

Obstacles concrets (et conseils pour les surmonter)

Les organisations sont confrontées à plusieurs obstacles tenaces qui peuvent faire échouer même les meilleures intentions. Regardons de plus près quelques-uns de ces obstacles et découvrons comment les aborder.

Le premier problème est celui du budget, car la plupart des entreprises doivent jongler avec des infrastructures de plus en plus étendues. « D'après une enquête menée par Gartner auprès de 162 grandes entreprises entre août et octobre 2024, les organisations utilisent en moyenne 45 outils de cybersécurité[1]. »

Chaque console supplémentaire engendre un enchevêtrement d'outils interdépendants qui augmentent les coûts et créent des angles morts, rendant ainsi la consolidation indispensable. Concentrez-vous sur l'essentiel, qu'il s'agisse par exemple des contrôles d'identité, de la gestion des risques ou des moyens de sauvegarde et de restauration, et maîtrisez ces aspects avant de vous tourner vers des outils spécialisés.

« 58 % des RSSI citent les contraintes budgétaires comme l'un des principaux obstacles à leurs efforts de cyber-résilience. À ce titre, le renforcement de la cyber-résilience passe davantage par une réaffectation des ressources que par de nouveaux investissements. »

Gartner : *Cyber-résilience au niveau de la direction : 3 messages que les RSSI doivent faire passer, Christopher Mixter, Leigh McMullen, Christine Lee. [4 décembre 2025] ID : G00838385.*

Vient ensuite la surabondance des alertes qui submerge les équipes des SOC, les obligeant à se concentrer sur des faux positifs tandis que les menaces réelles passent inaperçues. Comme nous l'avons déjà évoqué, la solution ne réside pas dans un plus grand nombre d'alertes, mais dans des alertes plus pertinentes. Adaptez vos détections aux usurpations d'identité, aux anomalies liées aux solutions SaaS et aux chaînes de ransomwares connues, et appuyez-vous sur une IA régulée pour réduire les faux positifs.

Le facteur humain reste cependant une inconnue, car les collaborateurs cliquent sur des liens, réutilisent leurs mots de passe et ont souvent une mauvaise compréhension des menaces potentielles. La solution réside dans une formation concise et basée sur des scénarios, qui donne l'impression d'être concrète et non théorique. L'IA générative peut optimiser ces programmes grâce à des simulations adaptatives et des incitations personnalisées.

Les lacunes du modèle Zero Trust sont un autre aspect qui mérite votre attention. Beaucoup considèrent qu'il s'agit d'un produit que l'on peut acheter, mais en réalité, le modèle Zero Trust est opérationnel. IBM le décrit comme une stratégie de sécurité destinée aux environnements hybrides modernes, s'appuyant sur des outils tels que la segmentation, les contrôles des identités et des accès ainsi que la visibilité, qui constituent le modèle lui-même.

[1] Communiqué de presse de Gartner, « Gartner identifie les principales tendances de cybersécurité pour 2025 », 3 mars 2025.

Mise en œuvre d'une organisation résiliente

Que faut-il conserver en interne ou externaliser ? Commencez par évaluer votre maturité avec lucidité. Comparez vos capacités actuelles aux six étapes de la résilience. Si vous ne disposez pas du personnel nécessaire pour assurer une surveillance 24/7, ne faites pas semblant d'en avoir : confiez la détection et la réponse à des spécialistes qui sont experts en la matière.

En revanche, si la gestion des identités et l'application des correctifs constituent vos points faibles, conservez ces tâches en interne. Ce sont des aspects « culturels », en quelque sorte, ce qui signifie qu'ils renvoient à des pratiques et des comportements profondément ancrés dans les méthodes de travail de votre organisation, et qu'ils dépendent des habitudes, des valeurs et des décisions quotidiennes des personnes plutôt que de la technologie.

À conserver en interne :

- **Hygiène des identités et des accès :** Authentification multifacteur, gestion des accès privilégiés, stratégies sans mot de passe : tous ces éléments sont étroitement liés à la culture d'entreprise et aux opérations quotidiennes.
- **Gestion des configurations et des correctifs :** Elle est essentielle pour réduire la surface d'attaque et nécessite également une coordination étroite avec les équipes internes, ce qui justifie de garder cette activité en interne.
- **Exercices de sauvegarde et de rétablissement :** Leur prise en charge garantit la confiance et l'alignement sur les priorités métiers.

Possibilité d'externalisation :

- **Détection et réponse managées (MDR) :** La surveillance continue et la recherche active des menaces exigent souvent des moyens et une expertise qui dépassent les capacités de la plupart des équipes internes.
- **Threat Intelligence et assistance à la remédiation :** Les prestataires externes bénéficient d'une meilleure visibilité et disposent de moyens de remédiation plus rapides.
- **Renforts pour la réponse aux incidents :** En cas de graves atteintes à la sécurité, les équipes externes apportent des compétences spécialisées et une réponse rapide.

Cette distinction tient essentiellement à la culture, l'échelle et la confiance. La gestion des identités et l'application des correctifs reposent sur des comportements et des processus internes, ce qui rend leur externalisation difficile. La surveillance continue et la Threat Intelligence, en revanche, tirent parti de l'envergure des prestataires et de leur visibilité à l'échelle mondiale. La sauvegarde et la restauration sont des processus trop sensibles pour être entièrement délégués. Elles nécessitent un contrôle direct afin de garantir leur adéquation avec les priorités métiers.

Cette répartition reflète également ce que révèlent les données : l'intensification des menaces et la complexité croissante de la chaîne d'approvisionnement exigent une surveillance continue, associée à des mesures de sécurité rigoureuses. Comme le note Gartner[2], cette « expansion rapide des menaces oblige sans cesse les équipes chargées de la cybersécurité et de la chaîne d'approvisionnement à s'adapter, tandis que l'utilisation croissante de l'IA générative chez les partenaires commerciaux accroît le risque d'atteinte à la sécurité des données et de fuites de propriété intellectuelle ». Cela souligne la nécessité de maintenir une vigilance et des pratiques rigoureuses de cyber-hygiène.

Comment ESET contribue à la cyber-résilience en tant que catalyseur technologique

La cyber-résilience ne peut être assurée par un seul prestataire ou un ensemble de mesures de contrôle. Le rôle d'ESET est axé sur la sécurité en milieu professionnel : les endpoints, les appareils des utilisateurs, ainsi que les capacités de télémétrie et de réponse associées.

Cela ne remplace pas la gestion des identités, la gouvernance des solutions SaaS, la prévention des pertes de données ni la planification de la reprise des processus métiers, qui restent des éléments essentiels d'une stratégie de résilience complète.

Si vous en avez assez de faire du bricolage avec des solutions individuelles, la première étape consiste à opter pour une solution clé en main : déployez-la rapidement, gérez-la facilement et améliorez la visibilité sur les endpoints, les identités et les données, afin que vos contrôles fondamentaux soient fiables et fonctionnent en toute transparence. ESET peut vous apporter son soutien technique dans les quatre domaines suivants :

[2] Communiqué de presse de Gartner, « Gartner estime que la cybersécurité de la chaîne d'approvisionnement se situe au sommet d'une courbe d'attentes exagérées », 29 septembre 2025.

1. Anticipation

ESET Threat Intelligence (ETI) fournit des rapports sur des menaces soigneusement sélectionnées et des flux d'informations en temps réel afin d'informer les décideurs, d'affiner les évaluations des risques organisationnels et d'améliorer la préparation. Cela comprend :

- Des analyses détaillées des APT et des profils des acteurs, des exploitations de vulnérabilités zero-day, des botnets, des TTP et des IoC.
- Des flux de données aux formats STIX/TAXII et accès via API s'intégrant aux plateformes de SIEM et de SOAR pour un enrichissement automatisé.
- Des rapports rédigés par des experts, accompagnés de résumés mensuels et de briefings privés sur les groupes APT, pour une prévision stratégique des menaces, et une réponse rapide et éclairée.

2. Résistance et exposition

L'architecture de protection d'ESET se charge d'empêcher les intrusions et de renforcer l'efficacité de la détection :

- ESET Endpoint Security utilise une défense multicouche pour bloquer différentes menaces telles que les ransomwares, les attaques sans fichier et les APT, en combinant l'analyse des comportements en temps réel, la Cloud Intelligence, la recherche des menaces et la sécurité mobile au sein d'une console ESET PROTECT.
- ESET Inspect, un composant de la plateforme ESET PROTECT permettant la mise en œuvre de la technologie de XDR, combine des fonctionnalités d'EDR au niveau des endpoints et une télémétrie étendue afin de mettre en évidence les anomalies, automatiser la création d'incidents, régler précisément les règles de détection et alimenter les workflows d'investigation et de réponse en aval.
- Depuis mars 2026, ESET a étendu son architecture de protection au-delà des endpoints avec le lancement de Cloud Workload Protection (CWP). La solution sécurise les charges de travail dans le cloud et les configurations du périmètre, tout en générant des données de télémétrie qui renforcent à la fois la détection et la gestion des risques dans les environnements hybrides.
- Des contrôles des politiques et des configurations strictes sont appliqués via la plateforme ESET PROTECT, notamment les paramètres de l'agent de gestion, les politiques de pare-feu et d'accès réseau, ainsi que les contrôles de visibilité, configurables à l'aide de modèles de politiques centralisées.
- Le chiffrement complet des disques (FDE), fourni par ESET Full Disk Encryption et géré de manière centralisée via la plateforme ESET PROTECT, réduit l'impact de la perte ou du vol d'un endpoint en protégeant les données au repos et en facilitant la maîtrise des incidents ainsi que la conformité réglementaire.

3. Réponse et restauration

ESET intègre des fonctionnalités de coordination de la réponse aux incidents, de télémétrie d'investigation et de contrôles facilitant la restauration :

- ESET Inspect joue un rôle direct dans la réponse aux incidents en générant des rapports d'incident détaillés, en établissant des corrélations entre les données télémétriques des endpoints et en facilitant les processus d'investigation qui permettent de définir les mesures de confinement et de remédiation sur l'ensemble de la plateforme ESET PROTECT.
- Des intégrations via API permettent à ESET PROTECT de transmettre automatiquement les détections et les incidents à des solutions de SIEM/SOAR (par ex. Microsoft Sentinel, BlockAPT) via des connecteurs automatisés pour mettre en œuvre des scénarios d'orchestration, de confinement et d'intervention.
- L'API de gestion des incidents d'ESET prend en charge la détection des incidents, leur regroupement, la gestion des règles et des exclusions, la mise à jour de l'état et les commentaires des analystes pour la mise en œuvre de flux de réponse structurés au sein d'outils externes d'orchestration et de gestion des cas.
- Pour les scénarios de rétablissement, la fonctionnalité Ransomware Remediation de la plateforme ESET PROTECT crée automatiquement des sauvegardes sécurisées des fichiers dès la détection d'une activité suspecte et les restaure lorsqu'un ransomware est détecté, pour aider les organisations à récupérer les données affectées et réduire les temps d'arrêt après la maîtrise de l'incident.

4. Continuité

La visibilité opérationnelle, les mesures et les boucles de feedback sont essentielles :

- ESET PROTECT offre un système de reporting complet qui vous permet de générer des rapports prédéfinis ou personnalisés (PDF/CSV) et de programmer leur envoi automatique aux parties prenantes, y compris des rapports spécifiques de LiveGrid® et du MDR.
- Les intégrations prennent en charge des tableaux de bord pour la direction en automatisant la transmission des indicateurs de menaces vers les systèmes de SIEM et les outils de reporting métiers. Le module LiveGuard intègre des modèles de rapports permettant de suivre l'activité des fichiers suspects.
- Le service de MDR offre aux clients un reporting structuré sur les réponses et les résultats via les rapports ESET PROTECT, adaptés aux dirigeants et aux équipes opérationnelles.

Le message est très simple : évitez les infrastructures trop complexes. ESET se charge de tous les aspects techniques pour que vous puissiez vous concentrer sur les processus et les collaborateurs, et assurer la continuité de vos activités.

Feuille de route

Cette feuille de route présente un parcours type, et non une recette universelle. Le parcours concret, ainsi que le rythme auquel les organisations le suivent, dépendent de leur niveau de maturité actuel, leurs priorités métiers, leur exposition réglementaire, leurs contraintes budgétaires et leurs décisions relatives à l'externalisation ou à la prise en charge en interne.

COURT TERME
0 À 90 JOURS

1 RENFORCEMENT DES CONTRÔLES D'IDENTITÉ

Mettez en place une authentification multifacteur (MFA) résistante à l'hameçonnage afin de réduire le risque de prise de contrôle, examinez les comptes privilégiés et les comptes des machines, et recherchez régulièrement tout identifiant exposé.

2 VÉRIFICATION DE LA DISPONIBILITÉ DES SAUVEGARDES ET DE LA RESTAURATION

Réalisez un exercice de restauration après une attaque de ransomware et vérifiez l'inaltérabilité des sauvegardes ainsi que les délais de restauration afin d'assurer la résilience.

3 AUDIT DES RISQUES EXTERNES

Gartner souligne que la gestion des risques est fondamentale, car elle « accorde la priorité aux menaces les plus importantes pour votre activité ». Pour mettre cela en pratique, dressez l'inventaire des actifs, des identités SaaS et des intégrations tierces accessibles via Internet, puis corrigez les erreurs de configuration à haut risque.

MOYEN TERME
3 à 9 MOIS

4 MISE EN ŒUVRE DU MODÈLE ZERO TRUST

Zero Trust est un concept de sécurité qui nécessite une approche holistique. Commencez par procéder à une micro-segmentation des systèmes stratégiques, en mettant en place des contrôles continus de l'état des appareils et en appliquant des contrôles d'accès au niveau des sessions.

5 SÉCURISATION DE LA CHAÎNE D'APPROVISIONNEMENT

Exigez des listes de composants logiciels (SBOM) de la part des fournisseurs, analysez les modules open source et commerciaux, et surveillez les fuites au niveau des développeurs. La liste des composants logiciels et l'intégrité des logiciels sont essentielles à la résilience de la chaîne d'approvisionnement.

6 RENFORCEMENT DE LA POSTURE DE SÉCURITÉ DU CLOUD

Mettez en œuvre des solutions CSPM et CNAPP afin de surveiller en permanence les configurations cloud, assurer la conformité et intégrer les résultats des workflows de détection. Cela permet de réduire les risques dans les environnements multicloud et SaaS.

LONG TERME
9 À 18 MOIS

7 MISE EN PLACE D'UNE GOUVERNANCE DE L'IA

Une gouvernance bien établie de l'IA garantit un retour sur investissement mesurable et réduit les risques. Pour y parvenir, commencez par formaliser vos politiques, identifiez et maîtrisez l'utilisation non approuvée de l'IA, et mesurez les gains d'efficacité parallèlement à la réduction des risques.

8 CONDUITE D'EXERCICES DE RÉSILIENCE À GRANDE ÉCHELLE

Organisez des exercices interfonctionnels simulant des attaques de ransomware, l'indisponibilité des fournisseurs et des scénarios d'attaques par l'IA. N'oubliez pas que ces exercices de résilience améliorent la préparation de l'organisation.

9 CONSOLIDATION DES OUTILS DE SÉCURITÉ

Réduisez le chevauchement des outils et des consoles. Investissez dans des plateformes unifiées pour les identités, les endpoints et les analyses. Comme nous l'avons vu précédemment, la consolidation des plateformes simplifie les opérations et améliore la réactivité.

Conclusion

En 2026, la cyber-résilience consiste à assurer la continuité des activités en situation de crise, et non à garantir une sécurité parfaite. Cela signifie anticiper les menaces, résister aux compromissions, répondre rapidement et rétablir les activités sans interruption. Les organisations sont confrontées à des attaques par l'IA, la complexité des environnements hybrides et des réglementations strictes.

Le renforcement de la sécurité des identités, la validation des procédures de récupération, la gestion des risques d'exposition, la mise en œuvre du modèle Zero Trust, la sécurisation des chaînes d'approvisionnement, la gouvernance de l'IA et la consolidation des outils font partie des mesures concrètes.

Si vous souhaitez simplifier vos processus, ESET peut être votre partenaire technologique de confiance avec des solutions prêtes à l'emploi, simples à utiliser et conçues pour prendre en charge les tâches les plus lourdes, afin que vous puissiez vous concentrer sur vos collaborateurs, vos processus et la continuité de vos activités.

DÉCOUVREZ LES SOLUTIONS ESET POUR ENTREPRISES

À propos d'ESET

Défense proactive. Minimisez les risques par la prévention.

Conservez une longueur d'avance sur les cybermenaces connues et émergentes **grâce à notre approche axée sur l'IA et la prévention.** Nous combinons la puissance de l'IA et l'expertise humaine pour améliorer l'efficacité et la facilité d'utilisation de la protection.

Bénéficiez d'une protection **de haut niveau** grâce à notre Threat Intelligence interne, compilée et examinée depuis plus de 30 ans, qui alimente notre vaste réseau de R&D dirigée par des chercheurs reconnus.

ESET protège votre organisation afin qu'elle puisse maximiser le potentiel de la technologie. Progress. Protected.

Prévention multicouche

IA de pointe associée à une expertise humaine

Threat intelligence de renommée mondiale

Support local et personnalisé

eset®
Cybersecurity
Progress. Protected.