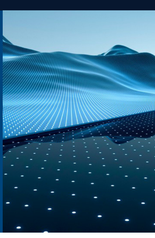
# 10 recommandations en matière de cybersécurité

**La technologie progresse à un rythme si rapide, et à mesure que nous adoptons de nouveaux outils et systèmes qui améliorent nos capacités, nous créons simultanément de nouvelles opportunités pour les cyberattaquants qui cherchent à exploiter les failles de sécurité. Dans ce paysage, il est crucial de mettre en œuvre des mesures de cybersécurité robustes pour vous protéger contre ces menaces émergentes, en veillant à ce que l'innovation puisse se poursuivre dans un environnement sécurisé. Afin que les organisations s'adaptent aux nouveaux risques, les experts en cybersécurité de Dell Technologies recommandent 10 actions fondamentales pour faire progresser leur maturité en matière de cybersécurité.**

## 1 Comprendre le paysage des menaces et des risques.



Les partenaires expérimentés en cybersécurité peuvent fournir une expertise et des ressources précieuses pour vous aider à naviguer dans le paysage des menaces en constante évolution.

- Menez des évaluations approfondies des failles de sécurité et des tests d'intrusion pour identifier les potentiels points faibles qui doivent être traités et identifier les lacunes que vous pourriez rencontrer dans votre stratégie.
- Bénéficiez de compétences et de connaissances spécialisées qui ne sont peut-être pas disponibles en interne, telles que des informations sur les risques émergents, des techniques d'attaque avancées et les dernières stratégies et pratiques d'excellence en matière de sécurité.
- Définissez des droits d'accès justifiés pour établir le cadre de sécurité approprié pour la mise en œuvre des contrôles et de la gouvernance de vos activités.

## 2 Élaborer une stratégie de cybersécurité complète.

La cyberrésilience nécessite un effort coordonné impliquant les équipes IT, les professionnels de la cybersécurité, la direction et, parfois, des experts externes.

- Favorisez la sensibilisation de l'ensemble de l'entreprise : la sécurité relève de la responsabilité de chacun.
- Utilisez l'automatisation dans la mesure du possible.
- Vous devez disposer d'un plan IRR bien rodé qui informe toutes les bonnes personnes lorsqu'une cyberattaque se produit.

## 3 Travailler avec des fournisseurs disposant d'une chaîne logistique sécurisée.

La sécurité doit être garantie plus tôt que vous ne pourriez le penser. Établissez une base fiable en collaborant avec des fournisseurs qui privilégient la sécurité dès la conception et pendant la fabrication et la livraison des appareils et de l'infrastructure. Les fournisseurs qui offrent une chaîne logistique sécurisée, un cycle de vie de développement sécurisé et une modélisation rigoureuse des menaces peuvent vous aider à garder une longueur d'avance sur les cyberattaquants.

- Garantissez la confidentialité, l'intégrité et la disponibilité des informations qui décrivent ou traversent la chaîne logistique IT, ainsi que des informations sur les parties impliquées dans la chaîne logistique IT.
- Assurez-vous que les produits ou services IT de la chaîne logistique sont authentiques et inchangés, et qu'ils répondent aux spécifications de l'acquéreur, sans fonctionnalités supplémentaires indésirables.
- Réduisez les failles de sécurité susceptibles de limiter la fonction prévue d'un composant, d'entraîner un échec de composant ou de fournir des opportunités d'exploitation.

## 4 Adopter les principes Zero-Trust.

Zero-Trust est un concept de sécurité centré sur l'idée qu'une organisation ne doit pas faire aveuglément confiance à tout ce qui se trouve à l'intérieur ou à l'extérieur de son périmètre. Au contraire, elle doit vérifier tout élément qui tente de se connecter à ses systèmes avant de lui en accorder l'accès.

- Oubliez le modèle de sécurité basé sur le périmètre et adoptez les principes Zero-Trust.
- Appliquez le principe du moindre privilège, pour que les comptes utilisateur et système ne disposent que des droits d'accès minimaux requis pour leurs tâches. Cette approche réduit la surface d'attaque et l'impact potentiel des accès non autorisés par des cyberattaquants.
- Intégrez des solutions telles que la micro-segmentation, la gestion des identités et des accès (IAM), l'authentification multifacteur (MFA) et l'analytique de la sécurité, entre autres.

## 5 Réduire la surface d'attaque.

La surface d'attaque représente des failles de sécurité potentielles et des points d'entrée qui peuvent être exploités par des acteurs malveillants. Pour améliorer leur posture de sécurité, les organisations doivent minimiser la surface d'attaque, limiter les risques et renforcer les cyberdéfenses globales contre les menaces nouvelles et émergentes.

- Formez les collaborateurs et les utilisateurs à la reconnaissance et au signalement des potentielles menaces de sécurité, des tentatives d'hameçonnage et des tactiques d'ingénierie sociale afin de limiter les risques d'exploitation avérée de failles de sécurité humaines.
- Mettez en œuvre des mesures préventives, telles que la segmentation complète du réseau, l'isolement des données stratégiques, l'application de contrôles d'accès stricts, ainsi que la mise à jour et l'application de correctifs réguliers sur les systèmes et les applications.
- Assurez-vous que les systèmes, les réseaux et les appareils sont correctement configurés et utilisez les meilleures pratiques en matière de sécurité, telles que la désactivation des services inutiles, l'utilisation de mots de passe forts et l'application de contrôles d'accès.

## 6 Détecter les cybermenaces et y répondre.

Face aux menaces sophistiquées, les mesures de sécurité traditionnelles ne sont plus suffisantes. Les organisations doivent tirer parti de technologies et méthodologies avancées de détection des menaces pour identifier et répondre efficacement aux menaces connues et inconnues.

- Surveillez et analysez le trafic réseau, les journaux système et d'autres zones, ainsi que les données de sécurité, afin d'identifier les signes d'accès non autorisé, d'intrusions, d'infections par logiciels malveillants, de violations de données ou d'autres cybermenaces.
- Mettez en œuvre un plan de réponse pour enquêter rapidement et limiter les incidents de sécurité confirmés. Il s'agit notamment d'en limiter l'impact, d'identifier la cause première et de mettre en œuvre les actions nécessaires pour restaurer les systèmes et éviter davantage de dégâts.
- Utilisez des outils d'IA/ML pour détecter rapidement les cybermenaces grâce à l'analyse en temps réel des schémas ou comportements de données inhabituels. Ces technologies aident également à répondre rapidement aux menaces en évaluant leur gravité, en prédisant leurs impacts, en automatisant certaines actions défensives et en faisant évoluer les pratiques de sécurité, minimisant ainsi les dommages potentiels.

## 7 Se relever d'une cyberattaque.

Même avec des mesures proactives stratégiques en place, les organisations doivent toujours partir du principe qu'elles ont été victimes d'une faille. Elles doivent disposer de fonctionnalités résilientes et fréquemment testées pour garantir une restauration efficace après toute cyberattaque réussie.

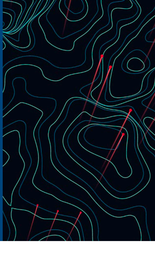
- Prenez des mesures immédiates pour limiter les dommages causés par une cyberattaque en isolant et en limitant l'impact.
- Déconnectez du réseau les systèmes concernés, désactivez les comptes compromis et mettez en œuvre des mesures pour éviter toute propagation ou tout dégât supplémentaire.
- L'utilisation de l'IA/ML peut accélérer la récupération en identifiant rapidement les systèmes et données affectés ainsi qu'en automatisant le processus de restauration des sauvegardes.

## 8 S'appuyer sur des partenaires d'expérience.

Aucun fournisseur ne dispose à lui seul de toutes les fonctionnalités nécessaires pour fournir une sécurité de bout en bout, incluant les personnes, les processus et la technologie. C'est un travail d'équipe. Par conséquent, il est essentiel de collaborer avec un réseau de partenaires expérimentés.

- Faites appel à des partenaires de cybersécurité expérimentés qui apportent une expertise et des ressources précieuses pour vous aider à naviguer dans le paysage des menaces en constante évolution.
- Bénéficiez de compétences et de connaissances spécialisées qui ne sont peut-être pas disponibles en interne, telles que des informations sur les risques émergents, des techniques d'attaque avancées et les dernières stratégies et pratiques d'excellence en matière de sécurité.
- Faites appel à l'expertise de services professionnels expérimentés et établissez des relations de collaboration avec des partenaires commerciaux de confiance pour établir une posture de sécurité complète qui vous protège efficacement contre l'évolution des cybermenaces.

## 9 Étendre la cybersécurité à la périphérie et aux environnements Cloud.



Les réseaux se sont étendus du cœur vers la périphérie et jusqu'au Cloud, et ces zones sont toutes devenues des points cruciaux de vulnérabilité. Quelle que soit la façon dont les applications sont déployées, elles doivent être sécurisées et alignées sur les politiques de l'entreprise, afin de garantir la cohérence de la gestion des utilisateurs et des applications.

- Appliquez les principes Zero-Trust aux environnements de périphérie et Cloud, en fournissant des contrôles d'accès robustes, une authentification continue, ainsi qu'une visibilité et un contrôle complets sur le trafic réseau.
- Mettez en œuvre des mesures de sécurité, telles que la segmentation du réseau, le chiffrement et la surveillance continue, à la fois au cœur du réseau et dans les environnements Cloud, pour vous protéger contre les menaces.
- Collaborez avec des services professionnels expérimentés, spécialisés dans la sécurité à la périphérie, au cœur des systèmes et dans le Cloud. Vous pourrez vous appuyer sur leur expertise pour mettre en place de mesures efficaces qui protègent intégralement votre organisation.

## 10 Gérer proactivement et augmenter la résilience de bout en bout.

La gestion de l'intelligence sur les menaces, des incidents, de la réponse et des opérations de sécurité peut améliorer les capacités d'une organisation à détecter les cybermenaces et à y répondre.

- Mettez en place des protocoles proactifs de réponse aux incidents et de récupération qui définissent clairement les rôles et les responsabilités, garantissent ainsi une communication et une coordination fluides entre les collaborateurs.
- Améliorez la visibilité de l'environnement pour permettre aux organisations de surveiller proactivement les menaces au sein de leurs réseaux et d'y répondre, tout en fournissant des alertes pour la restauration si nécessaire.
- Renforcez votre capacité à détecter proactivement les cybermenaces et à y répondre, en tirant parti de l'intelligence avancée sur les menaces, de la gestion des événements et des informations de sécurité (SIEM), des solutions de protection des points de terminaison et de l'analytique comportementale.

Ne laissez pas les risques de sécurité entraver votre innovation. Découvrez comment renforcer la maturité de votre cybersécurité et de votre approche Zero-Trust sur dell.com/SecuritySolutions

DELL Technologies