DELL Technologies

Renforcez votre cybersécurité et la maturité de votre approche Zero-Trust.

Comblez les lacunes en matière de ressources et de connaissances pour renforcer vos défenses contre les cyberattaques.

Les menaces actuelles en constante évolution, en particulier à cause de l'essor de l'IA générative, créent de nouveaux défis inattendus, même pour les spécialistes de la cybersécurité les plus chevronnés. Découvrez comment un partenariat avec des professionnels de la sécurité expérimentés peut vous aider à éviter les cyberattaques et à conserver des pratiques de sécurité fiables.

Les cybermenaces agissent comme des insectes pendant un pique-nique

Vous aurez beau vous débarrasser d'eux, ils seront vite remplacés par d'autres.

Dans un monde de plus en plus interconnecté où les organisations s'appuient fortement sur des infrastructures numériques et où les données représentent des marchandises d'une importance considérable, il est préférable de partir du principe que votre environnement IT a déjà été compromis suite à une attaque sophistiquée.

La bonne nouvelle, c'est qu'il existe des partenaires chevronnés qui se concentrent sur le point de convergence entre la technologie et la cybersécurité.

Dell Technologies propose des solutions innovantes et une expertise précieuse, dont vous ne disposez peut-être pas en interne, afin de vous accompagner au mieux dans un monde où les menaces évoluent constamment.

- Sécurité matérielle et logicielle
- Informations sur les risques émergents
- Compréhension des techniques d'attaque avancées
- AIOps pour répondre aux menaces en constante évolution
- Nouvelles stratégies de sécurité et pratiques d'excellence

Mettez en place des couches de défense qui améliorent en permanence les pratiques de sécurité et adoptez une approche Zero-Trust.

Dell Technologies est un partenaire de cybersécurité qui fournit des services professionnels et des solutions matérielles et logicielles complets, ainsi qu'un solide écosystème de partenaires qui limite les risques d'attaque, identifie et réduit les failles de sécurité et vous aide à restaurer rapidement vos opérations métier.

Réduction de la surface d'attaque →

Détection et réponse face aux cybermenaces →

Restauration rapide après une attaque →

Périphérie **Datacenter** **Multicloud**

Services professionnels

Écosystème de partenaires commerciaux/technologiques **Chaîne logistique sécurisée**

DELL Technologies

Réduction de la surface d'attaque

Consolidez vos défenses et limitez les capacités de ciblage en réduisant les points d'entrée que privilégient les cybercriminels.

Renforcez votre posture de sécurité en identifiant et limitant les failles de sécurité et les points faibles susceptibles de compromettre les applications, les systèmes ou les réseaux de différents domaines, y compris la périphérie, le datacenter et le Cloud.

IDENTIFIEZ les failles de sécurité

- Failles de sécurité logicielles
- Erreurs de configuration
- Faibles mécanismes d'authentification
- Systèmes non corrigés
- Privilèges utilisateur excessifs
- Ports réseau ouverts
- Sécurité physique insuffisante

IMPLÉMENTEZ des mesures préventives

- Collaborez avec des fournisseurs sécurisés
- Appliquez une segmentation réseau complète
- Isolez les données stratégiques
- Mettez en place des contrôles d'accès stricts
- Mettez à jour et appliquez des correctifs aux systèmes et applications
- Identifiez et résolvez les failles de sécurité à l'aide de l'IA, d'évaluations régulières et de tests

Adoptez une approche Zero-Trust

La mise en place d'une architecture Zero-Trust signifie que votre organisation ne fait pas automatiquement confiance à tout ce qui se trouve à l'intérieur comme à l'extérieur de son périmètre. Ainsi, toute tentative de connexion à vos systèmes est vérifiée avant d'en accorder l'accès. Il s'agit d'un modèle établi et recommandé par le département de la Défense des États-Unis qui intègre **7 piliers interdépendants** qui consolident systématiquement la maturité.

1. Confiance dans les utilisateurs
2. Confiance dans les appareils
3. Confiance dans les données
4. Applications et charges applicatives
5. Réseaux et environnements
6. Visibilité et analytique
7. Automatisation et orchestration

DELL Technologies

Réduction de la surface d'attaque

Identifiez les points faibles qui nuisent à vos systèmes avant qu'ils ne posent problème.

La cybersécurité n'est pas une tâche ponctuelle, mais un processus continu. Avec l'aide d'un partenaire de services de sécurité, les audits réguliers, les tests d'intrusion et les évaluations des failles de sécurité peuvent vous aider à identifier et à colmater les brèches afin de limiter les risques.

Pratiques de chaîne logistique sécurisées

La sécurité doit être garantie plus tôt que vous ne le pensez. Mettez en place des fondations solides à l'aide d'appareils et d'une infrastructure conçus, fabriqués et livrés avec une chaîne logistique sécurisée, un cycle de vie du développement sécurisé et une modélisation rigoureuse des menaces.

Sécurité intégrée

Travaillez avec des appareils et une infrastructure équipés d'une sécurité matérielle intégrée conçue pour détecter et contrer les attaques avant qu'elles ne fassent des dégâts.

Correctifs et mises à jour réguliers

Remédiez aux failles de sécurité identifiées et limitez le risque qu'elles soient exploitées en maintenant les applications, les firmware et les systèmes d'exploitation à jour grâce aux derniers correctifs de sécurité.

Moindre privilège

Restreignez les droits d'accès aux comptes d'utilisateur et système en accordant le niveau minimal nécessaire à l'exécution des tâches. Cette approche limite les dommages potentiels qu'un attaquant pourrait causer en cas d'accès non autorisé.

Segmentation réseau

Isolez les ressources essentielles pour limiter l'accès réseau au moyen d'une segmentation réseau moderne pour les données, les groupes opérationnels et les applications métier stratégiques. Cette approche permet de contenir une attaque en empêchant tout mouvement latéral.

Sécurité des applications

Mettez en œuvre des pratiques de codage sécurisées, effectuez des tests de sécurité et des analyses de code réguliers, utilisez les pare-feu d'applications Web (WAF) pour vous aider à vous protéger contre les attaques courantes au niveau des applications et réduire la surface d'attaque des applications Web.

Partenariats et services professionnels

Collaborez avec des prestataires de services de cybersécurité et créez des partenariats avec des partenaires commerciaux et technologiques pour bénéficier d'une expertise et de solutions qui pourraient ne pas être disponibles en interne.

Sensibilisation et formation des utilisateurs

Formez les collaborateurs et les utilisateurs à la reconnaissance et au signalement des potentielles menaces de sécurité, des tentatives de phishing et des tactiques d'ingénierie sociale afin de limiter les risques d'exploitation de failles de sécurité humaines.

DELL Technologies

Détection et réponse face aux cybermenaces

Les pratiques de sécurité à l'ancienne sont comme l'accès à Internet par ligne commutée, trop lentes et inefficaces dans notre actuel environnement exigeant.

Pour contrer les cybermenaces sophistiquées, vous avez besoin de meilleures astuces de sécurité, telles que l'IA et le ML intégrés dans des applications, ainsi que des méthodologies qui identifient et réagissent aux éléments connus et inconnus.

Mettez en place de puissants systèmes de détection et de prévention d'intrusion

Tirez parti de l'IA et du ML pour détecter les anomalies

Établissez une surveillance en temps réel du trafic réseau et du comportement des utilisateurs

Améliorez la résilience en collaborant avec des fournisseurs de services professionnels chevronnés pour acquérir une expertise spécialisée.

En tant que partenaire technologique expérimenté, Dell Technologies peut vous aider à mettre en place des protocoles proactifs de réponse aux incidents et de récupération, en identifiant les rôles et les responsabilités, et en garantissant une communication et une coordination fluides entre les parties prenantes.

Améliorez votre capacité à détecter et à réagir proactivement aux cybermenaces en adoptant les méthodes avancées suivantes :

- Intelligence sur les menaces
- Réponse aux incidents
- Gestion des événements et des informations de sécurité
- Protection des points de terminaison
- Analytique comportementale

Facilitez une restauration rapide et efficace et limitez la perte de données avec :

- Une stratégie de collaboration et un plan de réponse bien définis face aux incidents
- Des sauvegardes régulières des données et des systèmes stratégiques
- Des solutions de stockage hors site sécurisées et le chiffrement des données

DELL Technologies

Détection et réponse face aux cybermenaces

Restez vigilant et agissez rapidement.

La détection et la réponse face aux cybermenaces impliquent de rester vigilant et d'anticiper les scénarios les plus défavorables. Établissez un plan de réponse et de restauration continuellement mis à jour et mis en pratique afin que l'ensemble de votre organisation sache comment limiter les effets d'une attaque. Il s'agit d'un processus continu et itératif qui nécessite une combinaison de technologies, de personnel qualifié, de processus bien définis et de collaboration entre équipes.

Surveillance continue

Les outils de sécurité tels que les systèmes de détection d'intrusion (IDS), les systèmes de prévention d'intrusion (IPS), l'analyse des journaux et l'intelligence sur les menaces permettent d'identifier les signes d'accès non autorisé, d'intrusions, d'infections de logiciels malveillants et de violations de données.

Détection des menaces

Tirez parti de l'IA et du ML pour analyser les données afin d'identifier les tendances, les anomalies et les indicateurs de compromission (IOC) susceptibles de signaler une menace. Cela comprend la reconnaissance des signatures d'attaque connues et l'identification de comportements divergents.

Alertes et notifications

Bénéficiez d'avertissements précoces pouvant conduire à une procédure d'enquête et une réponse. Les alertes et notifications à la surface permettent d'agir rapidement avec la sécurité intégrée. Les données de télémétrie doivent être collectées au-dessus du système d'exploitation pour accélérer la détection des menaces et mobiliser le personnel de sécurité ou un centre des opérations de sécurité (SOC) lorsque des menaces ou des incidents potentiels sont détectés.

Réponse aux incidents

Exécutez un plan de réponse pour enquêter et limiter les incidents de sécurité confirmés. Cela implique 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.

Investigation numérique

Effectuez une analyse détaillée des incidents afin d'en comprendre la méthodologie d'attaque, de déterminer l'étendue de la violation, d'identifier les systèmes ou données concernés et de recueillir des preuves pour trouver et résoudre les failles de sécurité.

Mesures correctives et récupération

Prenez des mesures pour corriger les failles de sécurité, appliquer des correctifs aux systèmes, éliminer les logiciels malveillants et mettre en œuvre des mesures de sécurité renforcées pour éviter la reproduction d'incidents similaires. Restaurez les systèmes et les données concernés afin de rétablir leur état normal pour terminer le processus de récupération.

DELL Technologies

Restauration après une cyberattaque

Donnez un coup d'accélération et remettez votre entreprise sur pieds en un rien de temps.

La cyberrésilience est nécessaire dans notre monde actuel axé sur les données, il s'agit d'une attente que partagent les clients et les partenaires. Pour réussir, plusieurs couches de protection sont nécessaires pour s'assurer que les données stratégiques sont protégées et isolées afin qu'elles puissent être rapidement restaurées en toute confiance après une attaque. Évaluez votre cyberrésilience ›

- Agissez pour limiter les dégâts causés par une cyberattaque
- Restauration des services et appareils compromis ou endommagés
- Analysez l'incident pour empêcher toute attaque future
- Respect des contrats de niveau de service de l'entreprise et retour à la normale des opérations

Élaborez une stratégie de cybersécurité complète afin que votre organisation puisse effectuer des restaurations efficaces.

La restauration après une cyberattaque nécessite un effort coordonné impliquant les équipes IT, les professionnels de la cybersécurité, la direction et, parfois, des experts externes. La clé de la récupération consiste à remettre rapidement les systèmes et les opérations à la normale tout en tirant des leçons de l'incident afin de limiter les interruptions de service, restaurer l'intégrité des services et des données, réduire les conséquences financières et l'impact sur la réputation, et renforcer la cybersécurité afin d'éviter toute attaque similaire à l'avenir.

- Évaluez l'impact d'une attaque sur les opérations métier
- Hiérarchisez les services stratégiques
- Déployez des systèmes de protection des données
- Communiquez au sujet de l'incident et de l'évolution du processus de récupération
- Élaborez un plan et mettez-le en pratique, sans cesse, pour en garantir la continuité

DELL Technologies

Restauration après une cyberattaque

Remettez votre organisation en selle en réactivant les systèmes, les réseaux et les données après un incident.

La mise en place d'une stratégie de cyberrésilience intègre les personnes, les processus et la technologie dans un cadre global qui protège l'ensemble de votre organisation.

Confinement des incidents

La première étape consiste à isoler et à contenir l'impact de la cyberattaque. Cela implique la déconnexion du réseau des systèmes concernés, la désactivation des comptes compromis et la mise en œuvre de mesures pour éviter toute propagation ou tout dégât supplémentaire.

Restauration des systèmes ou appareils

Une fois qu'un incident est contenu, les systèmes et réseaux affectés par ce dernier sont restaurés afin de garantir leur intégrité et leur sécurité. Cela peut impliquer la reconstruction des systèmes compromis, la réinstallation des logiciels et l'application de correctifs et de mises à jour de sécurité. L'automatisation et l'autoréparation peuvent jouer un rôle important dans la reprise des opérations.

Récupération des données

Les données qui ont pu être compromises, chiffrées ou supprimées au cours de l'attaque doivent être restaurées. Cela peut impliquer la restauration des données à partir de sauvegardes ou l'utilisation de techniques de récupération des données spécialisées pour restituer les fichiers perdus ou chiffrés.

Investigation numérique

Suite à une attaque, il est essentiel de comprendre comment la violation s'est produite, quelles failles de sécurité ont été exploitées et quelles sont les étapes à suivre pour empêcher toute attaque similaire. Les systèmes tels que la gestion des événements et des informations de sécurité (SIEM) et les fonctionnalités telles que les comparaisons BIOS hors hôte fournissent des informations utiles.

Évaluation de la réponse aux incidents

Après la récupération, il est essentiel d'évaluer le processus de réponse aux incidents et d'identifier les points à améliorer. Les enseignements tirés de l'attaque peuvent servir pour renforcer les pratiques de sécurité, mettre à jour les plans de réponse aux incidents et consolider la protection contre les incidents futurs.

Partenariats et services professionnels

Les prestataires de services de cybersécurité et les partenaires technologiques apportent une expertise et des ressources précieuses pour aider à la restauration de votre organisation. Ils peuvent vous aider avec des tâches telles que l'analyse approfondie, l'identification de l'occurrence de la violation et la recommandation de mesures pour éviter les incidents futurs.

DELL Technologies

Étendez la cybersécurité à la périphérie et aux environnements Cloud

À mesure que les réseaux s'étendent du datacenter vers la périphérie jusqu'au Cloud, les environnements sont devenus des zones propices aux failles de sécurité.

Au fil de la progression de votre stratégie de cybersécurité, votre organisation doit étendre les principes Zero-Trust à la périphérie et au Cloud pour garantir des contrôles d'accès rigoureux, une authentification continue et une visibilité et un contrôle complets du trafic réseau. À mesure que les menaces évoluent, il est judicieux de déployer des fonctionnalités d'IA en tant que première ligne de défense. En outre, aucune stratégie n'est complète si votre réseau principal et vos environnements Cloud ne disposent pas de mesures de sécurité, telles que la segmentation du réseau, le chiffrement et la surveillance continue.

Les services professionnels de cybersécurité peuvent vous aider à adopter une approche globale.

L'interconnexion de diverses solutions de sécurité peut poser des difficultés. Collaborer avec des services professionnels spécialisés dans la sécurité à la périphérie, dans le datacenter et le Cloud vous offre l'expertise nécessaire pour mettre en place des mesures efficaces qui protègent intégralement votre organisation.

Périphérie

Mettez en place plusieurs couches de sécurité à la périphérie, au sein du réseau et au sein du matériel et des logiciels.

Datacenter

Alignez votre infrastructure sur une approche Zero-Trust à l'aide de l'IA, du ML et de l'automatisation.

Multicloud

Protégez toutes les charges applicatives dans n'importe quel environnement, y compris le Cloud public, les conteneurs et les charges applicatives Cloud natives.

DELL Technologies

L'IA générative : une arme à double tranchant pour la cybersécurité

Si la nouvelle génération d'IA précipite l'arrivée de nouveaux risques, elle nous oblige également à renforcer la sécurité.

L'IA générative représente la prochaine phase de l'IA et englobe des systèmes capables de comprendre, d'apprendre, de s'adapter et de mettre en œuvre des connaissances dans le cadre de tâches variées.

D'un côté, elle promet une détection et une réponse face aux menaces, des fonctionnalités prédictives et une efficacité opérationnelle améliorées. De l'autre, elle est source de nouveaux défis qui nécessitent des stratégies de cybersécurité en constante évolution qui répondent aux risques par le biais de mesures de sécurité fiables, d'une surveillance continue, de mises à jour et de correctifs réguliers et d'une approche en constante évolution de la confidentialité et de l'éthique des données.

Sécuriser les organisations avec l'IA générative

L'IA générative est devenue un allié essentiel dans le domaine de la cybersécurité, car elle offre de nouvelles opportunités en matière de protection des organisations.

- Améliorez l'efficacité de la détection et de la réponse face aux menaces.
- Anticipez les menaces futures ou identifiez les éventuelles failles de sécurité.
- Automatisez la détection des menaces et gagnez en efficacité.
- L'analyse approfondie identifie rapidement les tendances, les anomalies et les indicateurs de compromission.
- Formation personnalisée de sensibilisation à la sécurité.
- Adaptez les opérations de sécurité avec un accès plus rapide à des informations plus importantes.

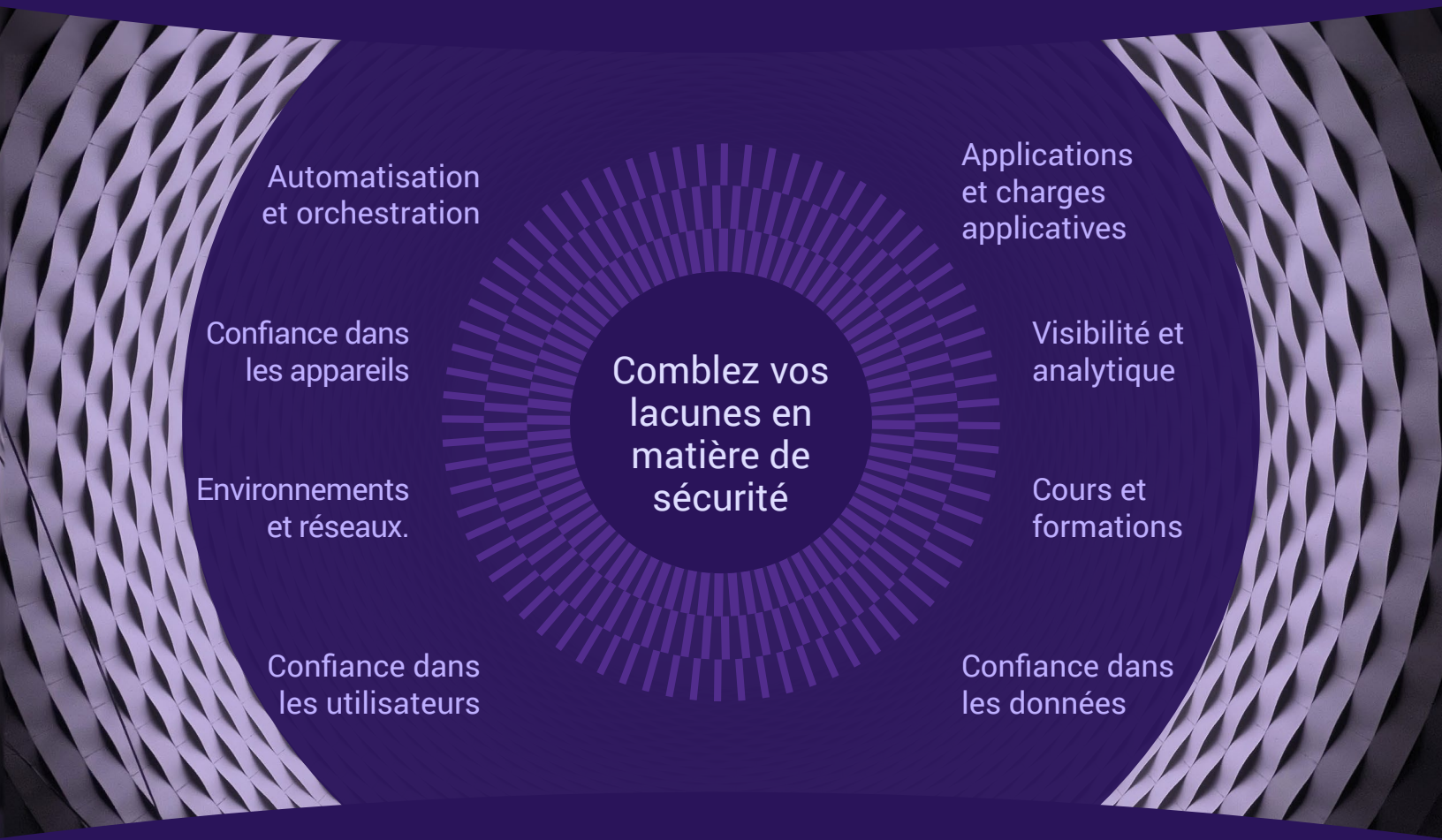
Sécuriser les systèmes d'IA générative

Bien que l'IA générative offre des avantages considérables en matière de sécurité, ses fonctionnalités peuvent être utilisées avec malveillance si elles ne sont pas suffisamment sécurisées.

- Garantissez la confidentialité et l'intégrité des données.
- Limitez les attaques conçues pour tromper les systèmes d'IA et provoquer des dysfonctionnements.
- Détectez et réagissez face aux utilisations inadéquates du système par une IA malveillante.
- Audits et limitation des biais et problèmes liés à l'éthique.
- Mise en œuvre de solides contrôles d'accès pour les systèmes d'IA.
- Protégez et effectuez des restaurations sécurisées de grands modèles de langage (LLM).

La cybersécurité moderne doit être intelligente, évolutive et automatisée

Dell Technologies peut vous aider à mettre en place une sécurité complète qui vous protège contre l'évolution des cybermenaces. À mesure que la technologie progresse, notre approche en matière de cybersécurité a toujours une longueur d'avance, car nous exploitons la puissance de l'IA et du ML pour protéger vos infrastructures numériques et préserver la confiance dans le domaine numérique. Quelle que soit votre stratégie en matière de cybersécurité, nous collaborerons afin de vous proposer plus qu'une simple protection de votre organisation grâce à des étapes qui vous permettent de rester agile et résilient.



DELL Technologies

Dell.com/SecuritySolutions

Demander que l'on vous rappelle

Chatter avec un conseiller en sécurité

Appelez le 1-800-433-2393