DELL Technologies

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

Ne laissez pas les risques de sécurité entraver l'innovation

Évaluez votre niveau de cybersécurité

Découvrez votre objectif

Dans le paysage des menaces actuel, complexe et en constante évolution, les organisations qui souhaitent maintenir des pratiques de cybersécurité robustes se heurtent souvent à un manque de ressources et de connaissances. Or, faire progresser la maturité de la cybersécurité et de l'approche Zero-Trust est essentiel pour lutter contre l'évolution des cybermenaces, et protéger votre environnement sans entraver l'innovation.

Utilisez les listes de points à vérifier ci-après pour évaluer la maturité actuelle de votre cybersécurité. Connaître les points forts et les points faibles de la sécurité de votre organisation vous permet de prendre les bonnes mesures pour faire progresser votre maturité en matière de cybersécurité.

Sommaire

En savoir plus

Découvrez comment améliorer votre maturité en matière de cybersécurité et d'approche Zero-Trust.

Points à vérifier :

Réduction de la surface d'attaque

La surface d'attaque fait référence à tous les points ou zones d'un environnement qui peuvent être ciblés ou exploités par un cyberattaquant. Vulnérabilités logicielles, configurations incorrectes, mécanismes d'authentification faibles, correctifs non appliqués, droits d'utilisateur excessifs, ports réseau ouverts, sécurité physique médiocre, etc. Ces questions peuvent vous aider à déterminer comment réduire les failles de sécurité et les points d'entrée qu'un acteur malveillant peut exploiter.

Oui	Non	
☐	☐	Votre organisation réalise-t-elle régulièrement des évaluations, des tests d'intrusion ou des simulations de violation pour identifier les failles de sécurité et les points faibles des systèmes et des réseaux, afin d'apporter des mesures correctives et des améliorations en temps opportun ?
☐	☐	Votre organisation organise-t-elle régulièrement des formations sur la sécurité pour ses employés ?
☐	☐	Votre organisation utilise-t-elle l'authentification multifacteur (MFA) et les contrôles d'accès basés sur les rôles (RBAC) ?
☐	☐	Votre organisation a-t-elle mis en œuvre une segmentation du réseau pour isoler les ressources stratégiques et limiter l'accès entre les différentes parties de votre réseau ?
☐	☐	Votre organisation met-elle en œuvre des pratiques de codage sécurisées, effectue-t-elle régulièrement des tests de sécurité et des analyses de code, et utilise-t-elle les pare-feu d'applications Web (WAF) pour l'aider à se protéger contre les attaques courantes au niveau des applications et réduire la surface d'attaque des applications Web ?
☐	☐	Votre organisation choisit-elle des fournisseurs IT qui peuvent attester des processus et procédures de sécurisation de sa chaîne logistique ?
☐	☐	Votre organisation met-elle en œuvre des principes Zero-Trust pour remplacer la sécurité basée sur le périmètre traditionnelle ?
☐	☐	Votre organisation utilise-t-elle le principe du moindre privilège utilisateur pour que les comptes utilisateurs et système ne disposent que des droits d'accès minimaux nécessaires à l'exécution de leurs tâches ?
☐	☐	Votre organisation applique-t-elle régulièrement des correctifs à vos systèmes et logiciels ?
☐	☐	Les outils de sécurité de votre organisation utilisent-ils des fonctionnalités d'IA/ML pour identifier proactivement les failles de sécurité ?

Points à vérifier :

Détection et résolution des menaces

Détecter les cybermenaces et y répondre est un élément essentiel de toute stratégie de sécurité. Cela implique de surveiller et analyser 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. Ces questions peuvent vous aider à déterminer comment votre organisation identifie et traite activement les incidents de sécurité potentiels et les activités malveillantes au sein d'un réseau informatique, d'un système ou d'une organisation.

Oui	Non	
☐	☐	Votre organisation surveille-t-elle en permanence les activités du réseau et des systèmes à l'aide d'outils et de technologies de sécurité Extended Detection and Response (XDR), de systèmes de détection des intrusions (IDS), de systèmes de prévention des intrusions (IPS), de SIEM et d'analyse des journaux ?
☐	☐	Votre organisation analyse-t-elle les données collectées pour identifier des schémas, des anomalies ou des indicateurs de données compromises (IOC) et/ou des indicateurs d'attaque (IOA) pouvant révéler une cybermenace potentielle ?
☐	☐	Votre organisation a-t-elle déployé les outils de visibilité et de surveillance les plus récents pour des menaces potentielles et déclencher rapidement des alertes ?
☐	☐	Votre organisation surveille-t-elle le trafic réseau à la recherche de schémas inhabituels ou d'activités suspectes susceptibles d'indiquer qu'une cyberattaque est en cours ?
☐	☐	Votre organisation a-t-elle mis en œuvre des outils d'IA/ML pour aider à détecter les cybermenaces grâce à l'analyse en temps réel des schémas ou comportements de données inhabituels ?
☐	☐	Votre organisation a-t-elle envisagé d'implémenter une solution SIEM nouvelle génération pour mieux gérer les alertes de sécurité et commencer la corrélation des données d'événements de sécurité à partir de l'ensemble de l'écosystème IT ?
☐	☐	Votre organisation effectue-t-elle des tests et gère-t-elle les failles de sécurité pour hiérarchiser et traiter les failles existantes et répondre efficacement aux nouvelles ?
☐	☐	Votre organisation a-t-elle mis en place un plan de réponse aux incidents pour enquêter sur les incidents de sécurité confirmés et les atténuer ?
☐	☐	Votre organisation intègre-t-elle des outils SOAR (Security orchestration, Automation and Response) pour accélérer les actions de réponse aux incidents et réduire la propagation d'une cyberattaque ?
☐	☐	Le plan de réponse aux incidents de votre organisation prend-il en compte les politiques de confinement, les plans de communication, les exigences de conformité, l'analyse approfondie et le processus de récupération ?

Points à vérifier :

Restauration après une cyberattaque

La restauration après une cyberattaque est le processus qui consiste à restaurer les systèmes, les réseaux et les données concernés afin de revenir à un état sécurisé et opérationnel à la suite d'un problème de sécurité. Elle implique de prendre des mesures pour atténuer les dommages causés par l'attaque, de reconstruire les services et les appareils compromis ou perturbés, d'analyser l'incident pour prévenir de futures attaques et de rétablir les opérations normales de l'organisation. Ces questions peuvent vous aider à évaluer si votre organisation est en mesure d'effectuer une restauration efficace après une cyberattaque.

Oui	Non	
☐	☐	Votre organisation a-t-elle mis en place des mesures de confinement des incidents pour isoler et contenir une cyberattaque ?
☐	☐	Votre organisation a-t-elle mis en place des processus pour la restauration des systèmes et/ou des appareils après la circonscription d'un incident ?
☐	☐	Votre organisation utilise-t-elle l'isolation des données, l'immuabilité ou un cybercoffre-fort pour protéger vos données ?
☐	☐	Votre organisation a-t-elle établi des procédures pour restaurer correctement les données au cas où ses données seraient compromises, chiffrées ou supprimées ?
☐	☐	Votre organisation utilise-t-elle des technologies d'IA/ML pour automatiser ou accélérer la restauration après une cyberattaque ?
☐	☐	Votre organisation évalue-t-elle continuellement l'incident et identifie-t-elle les domaines à améliorer après une attaque et une restauration ?
☐	☐	Votre organisation a-t-elle effectué une analyse approfondie pour comprendre la méthodologie d'attaque, déterminer l'étendue de la violation, identifier les systèmes et les données affectés et collecter des preuves pour vous aider à renforcer votre sécurité et à engager des actions judiciaires ou disciplinaires ?
☐	☐	Votre organisation sait-elle qu'il faut informer les parties concernées, telles que les clients, les partenaires et les fournisseurs, d'une cyberattaque et de tout impact potentiel sur leurs données ou leurs opérations ?
☐	☐	Votre organisation s'entraîne-t-elle à appliquer vos stratégies de restauration plusieurs fois par an pour renforcer la confiance concernant la restauration de votre activité et le respect de vos SLA ?
☐	☐	Votre organisation collabore-t-elle avec les prestataires de services pour aider à la restauration du fonctionnement de votre organisation ?

Renforcez la maturité de la cybersécurité et de l'approche Zero-Trust

En matière de cybersécurité, les départements IT doivent impérativement planifier le pire scénario en matière de cybersécurité et disposer de plusieurs couches de défense. Dans le paysage en constante évolution des menaces de cybersécurité, il est indispensable de continuellement renforcer les pratiques de sécurité et d'adopter les principes Zero-Trust. Cela inclut les points suivants :

Réduction de la surface d'attaque

Minimisez les failles de sécurité et les points d'entrée qui peuvent être exploités pour compromettre l'environnement.

Détection et réponse face aux cybermenaces

Identifiez et traitez activement les activités malveillantes et les incidents de sécurité.

Restauration après une cyberattaque

Restaurez le niveau de sécurité et de fonctionnement d'une organisation après un incident de sécurité.

En tirant parti de l'expertise des services professionnels et en collaborant avec des partenaires commerciaux de confiance, Dell peut aider les organisations à établir une posture de sécurité complète qui les protège contre l'évolution des cybermenaces. À mesure que la technologie continue de progresser, notre approche de la cybersécurité doit également protéger notre infrastructure numérique et maintenir la confiance dans le monde numérique.

DELL Technologies

À propos de Dell Technologies

Dell Technologies aide les organisations et les personnes à construire leur futur numérique et à transformer leur façon de travailler, de vivre et de se divertir. La société propose à ses clients la gamme de technologies et de services la plus complète et innovante du secteur à l'ère des données.

Pour en savoir plus, consultez le site
www.dell.com/securitysolutions