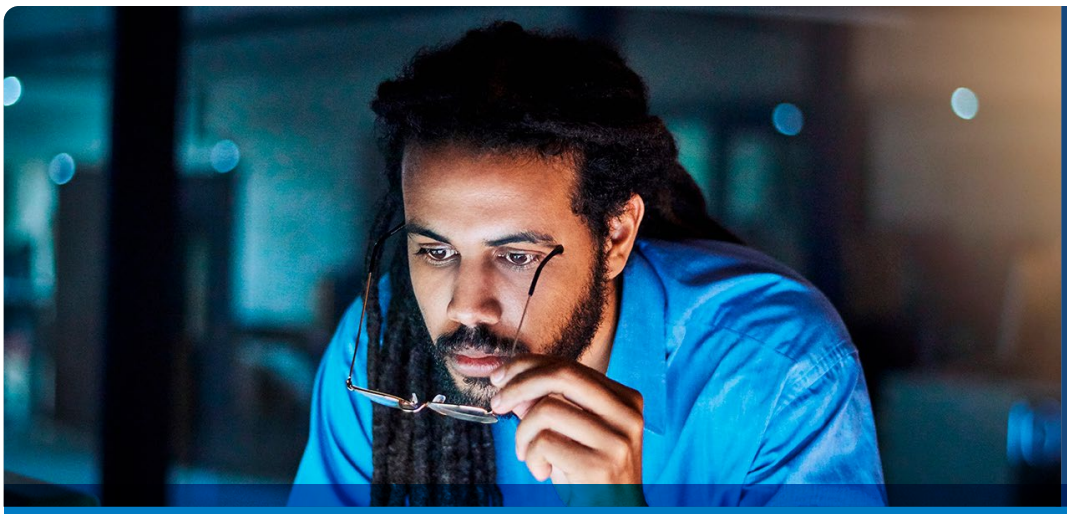
DELL Technologies

Valider les contrôles de sécurité et les stratégies pour contrer les vecteurs d'attaque



Simuler des techniques de cybercriminels pour l'accès initial, l'exécution de fichiers malveillants, le vol de données et bien plus encore

Pen Testing and Attack Simulation Management

Dell valide vos contrôles de sécurité et vos stratégies sur l'ensemble du processus d'attaque

Les organisations disposent de centaines de contrôles de sécurité, allant des points de terminaison aux passerelles Web et de messagerie. Les contrôles sont souvent complexes et difficiles à gérer. Une mauvaise configuration peut exposer à un risque. Les pirates cherchent à exploiter les contrôles vulnérables ou obsolètes.

Pour évaluer et valider l'efficacité de vos contrôles de sécurité, le service Dell Pen Testing and Attack Simulation Management imite les actions des menaces réelles.

Il combine les éléments suivants :

- Simulations mensuelles automatisées Breach and Attack Simulation (BAS) pour confirmer que vos contrôles fonctionnent correctement
- Test d'infiltration annuel dans lequel des experts tentent de franchir les défenses des ressources et des données stratégiques

Les simulations d'attaque testent les contrôles de sécurité

Les professionnels de la sécurité Dell utilisent la technologie BAS avancée pour tester différents vecteurs d'attaque. Ils essaient, par exemple, de placer un logiciel malveillant sur un point de terminaison ou d'obtenir des informations non autorisées à partir d'un serveur Web. Les testeurs Dell utilisent la technologie BAS pour simuler des attaques sur l'ensemble du processus d'attaque[1] pour connaître les menaces, mais aussi les TTP[2].

La technologie BAS ne présente aucun risque pour les environnements de production. Elle est continuellement mise à jour avec les dernières informations sur les menaces, les attaques et les comportements.

Le test d'infiltration évalue le chemin vers les cibles privilégiées

Même avec une simulation d'attaque, certains cybercriminels ont les compétences nécessaires pour parcourir l'environnement, et parviennent à contourner les obstacles pour accéder à des données précieuses. C'est là que le test d'infiltration intervient.

Principaux avantages :

- Détecter les contrôles de sécurité mal configurés qui pourraient être exploités à l'aide de simulations complètes de violations et d'attaques
- Tenir compte des failles et problèmes récents avec des simulations mensuelles
- Inspecter attentivement les chemins à haut risque vers des ressources ou des données précieuses à l'aide de tests d'infiltration annuels
- Générer des rapports avec les résultats des tests, les tendances trimestrielles et les activités notables pour vous aider à améliorer votre posture de sécurité
- Obtenir des informations rapides sur de nouvelles menaces à haut risque avec des tests ad hoc

Les tests d'infiltration complètent la technologie BAS. Au lieu de tester des contrôles individuels ou des ensembles de contrôles, les tests d'infiltration se concentrent sur les chemins vulnérables ou à haut risque dans un environnement. Les testeurs d'infiltration Dell peuvent imiter différentes techniques de cybercriminels et même différentes charges utiles pour atteindre un objectif spécifique, par exemple capturer un système précis, ou voler ou désactiver un ensemble particulier de fichiers. À l'instar d'un vrai pirate, un testeur d'infiltration expérimenté peut changer, modifier et adapter les techniques pour atteindre la cible.

Appliquer les informations tirées des tests pour améliorer la posture de sécurité

Dell Technologies Services partagera des rapports mensuels sur les problèmes de contrôles de sécurité à résoudre en fonction des résultats de l'exécution des séquences BAS. Chaque trimestre, Dell passera en revue les tendances des différentes simulations d'attaque, signalera les activités notables observées au sein de votre environnement IT et discutera des recommandations pour améliorer votre posture de sécurité.

Principales fonctionnalités

Breach and Attack Simulation (BAS)

- Exécuter tous les mois des simulations automatisées de violations et d'attaques en fonction de l'environnement du client
- Valider les contrôles de sécurité sur le périmètre et les composants de l'infrastructure interne, dont la passerelle Web, la passerelle de messagerie et les points de terminaison
- Mettre à jour continuellement l'outil BAS avec les dernières informations sur les menaces, les attaques et les comportements
- Apporter des modifications au workflow de simulation en fonction des simulations précédentes et des facteurs d'environnement de sécurité
- Exécuter des simulations ad hoc pour les problèmes de sécurité nouvellement découverts, en fonction de l'intelligence sur les menaces et de l'évaluation de Dell

Test d'infiltration

- Exécuter un test d'infiltration annuel dans un sous-ensemble défini de passerelles Web, d'API, d'appareils mobiles, d'adresses IP externes, d'adresses IP internes, de configurations Cloud
- Exécuter un nouveau test d'infiltration après avoir corrigé les résultats du premier test (en option)

Création de rapports et vérification

- Fournir des rapports mensuels sur les simulations de violation et d'attaque effectuées
- Partager un rapport trimestriel, et vérifier les tendances et les activités notables observées au sein de l'environnement IT du client
- Émettre des recommandations pour améliorer la posture de sécurité globale

Intégration

- Organiser une réunion de lancement du service
- Vérifier la check-list de pré-engagement effectuée par le client
- Vérifier l'environnement informatique du client
- Activer l'application BAS pour le client
- Fournir une assistance au déploiement d'agents

Contactez votre agent commercial Dell dès aujourd'hui.

[1] « Processus d'attaque » : menaces externes, notamment le phishing, les passerelles Web, etc., les points de terminaison compromis, les déplacements latéraux pour obtenir des informations d'identification ou propager l'attaque, l'exfiltration de données, etc.
[2] « TTP » : tactiques, techniques et procédures