Identifique vulneraciones y establezca prioridades para prestarles atención inmediata

Obtenga una vista integral de las vulneraciones en una superficie de ataque en crecimiento

Vulnerability Management

Dell Technologies combina conocimientos expertos en seguridad con tecnología de análisis y priorización de vulneraciones

Más del 50% de las organizaciones han sufrido vulneraciones de datos provocadas por terceros, y el 44 % de ellas se produjeron en los últimos 12 meses.[1] Mientras tanto, la cantidad de vulneraciones que se publican sigue en aumento: en 2021, se publicaron casi 22 000 vulneraciones nuevas.[2] Dado que esta cifra sigue aumentando, resulta casi imposible para la mayoría de las organizaciones abordar todas ellas o determinar cuáles presentan las amenazas más importantes e inmediatas. Las organizaciones de TI necesitan un método para identificar las vulneraciones en sus entornos y priorizar las que se deben corregir primero.

Vulnerability Management

Gracias a Dell Vulnerability Management, los expertos de Dell pueden utilizar tecnología líder para analizar los entornos de TI regularmente, lo que ofrece una visión integral de las vulneraciones en los puntos finales, la infraestructura de red y los recursos de cloud. Un informe describe cada vulneración y le asigna una puntuación de prioridad que puede ser de nivel bajo, medio, alto o crítico. Los expertos de Dell utilizan el aprendizaje automático para identificar las vulneraciones que se están explotando de forma activa sin ningún control y que tienen más probabilidades de abordarse en el futuro próximo. Esto le ayuda a aplicar parches primero en las vulneraciones que comportan mayor riesgo y en los activos críticos.

El equipo de Dell ofrece trimestralmente revisiones, información sobre las tendencias de las vulneraciones y orientación sobre la programación de las medidas de aplicación de parches. Si trabaja con Dell, el estado de seguridad general de su organización mejorará notablemente.

Principales beneficios

- Mantener las defensas actualizadas con análisis y gestión de las vulneraciones regulares mensualmente.
- Obtener una imagen completa de las vulneraciones en los puntos finales, la infraestructura de red y la cloud.
- Saber qué vulneraciones críticas debe resolver antes de que puedan aprovecharse de ellas.
- Aplicar el conocimiento y la experiencia del equipo de seguridad de Dell en la identificación de vulneraciones y su priorización.
- Adaptar las medidas de aplicación de parches en función de lo que indique el informe personalizado, que clasifica las vulneraciones de la más a la menos crítica.
- Mejorar la estrategia del estado de seguridad con un plan de corrección trimestral.

Funciones principales

- Analizar los entornos de los clientes para buscar vulneraciones (puntos finales, redes e infraestructura y cloud).
- Realizar análisis como mínimo mensualmente en busca de vulneraciones, con análisis adicionales según acuerden el equipo de Dell y el cliente.
- Realizar análisis ad hoc dirigidos por Dell, por ejemplo, cuando se detecta una nueva vulneración importante.
- Identificar y crear un inventario de recursos que se coteje con las bases de datos de vulneraciones conocidas para buscar los puntos débiles y las actualizaciones necesarias.
- Proporcionar comentarios al cliente sobre la priorización de las vulneraciones de mayor riesgo para gestionar la aplicación de parches y orientarle al respecto.
- Realizar revisiones trimestrales para informar al cliente sobre las tendencias de las vulneraciones en su entorno y en el sector.
- Utilizar un servicio prestado por expertos en ciberseguridad de Dell certificados y con gran experiencia.
- Realizar análisis con una plataforma avanzada basada en aprendizaje automático
- Utilizar la solución bajo el modelo de subscripción con precios por niveles según el tamaño del entorno

Actúe de forma proactiva y empiece a analizar su entorno hoy mismo con Dell

Gracias a Dell Vulnerability Management, podrá centrarse en sus objetivos empresariales principales y dejar que nosotros nos ocupemos de la detección de las vulneraciones y establecer su nivel de prioridad. Dado que la frecuencia de las vulneraciones y los costes que originan no deja de aumentar, es primordial la gestión de Vulnerability Management, para ayudarle a mejorar de forma continuada el estado de seguridad de la organización.

Póngase en contacto con su representante de ventas hoy mismo.

[1]SecureLink (2021). "A crisis in third-party remote access security". Recuperado en agosto de 2022 en https://f6e9j5y4.rocketcdn.me/wp-content/uploads/2021/04/SL-Report-ThirdPartySecurity.pdf.
[2]Tenable (2021). "Threat Landscape Retrospective". Tenable. (2022, 13 de enero). Recuperado en agosto de 2022 en https://static.tenable.com/marketing/research-reports/Research-Report-2021_Threat_Landscape_Retrospective.pdf.