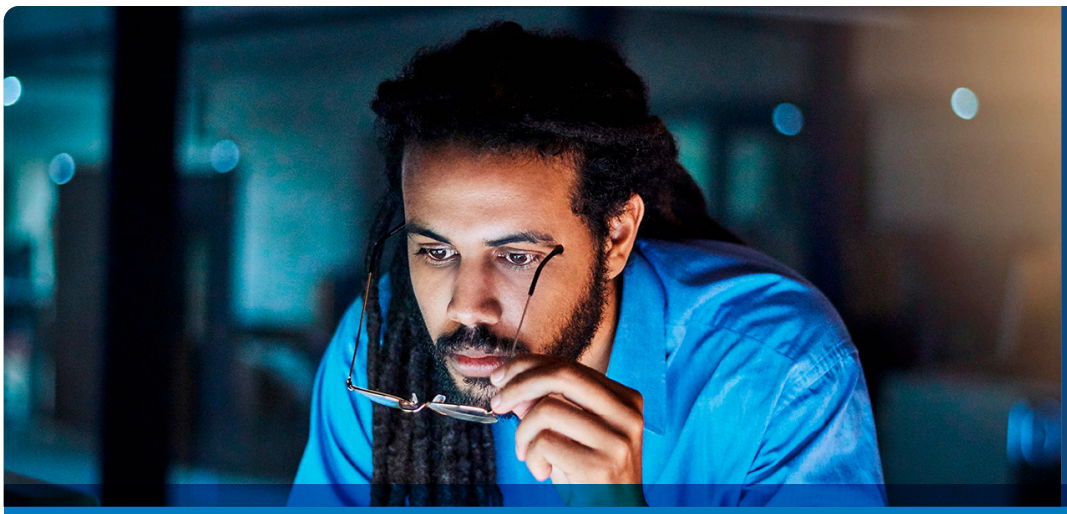
Validar los controles y las políticas de seguridad para cerrar los vectores de ataque



Simule las técnicas que emplean los atacantes para el acceso inicial, la ejecución de archivos maliciosos, el robo de datos, etc.

Gestión de pruebas de intrusión y de simulación de ataques

Dell valida sus controles de seguridad y sus políticas en toda la cadena de eliminación

Las organizaciones cuentan con cientos de controles de seguridad, desde los puntos finales hasta las puertas de enlace web y de correo electrónico. Los controles suelen ser complejos y difíciles de gestionar, y un fallo de configuración puede dar lugar a una exposición de riesgo. Los atacantes intentan beneficiarse de aquellos controles desconfigurados o desactualizados.

Para poner a prueba y validar la eficacia de sus controles de seguridad, la gestión de pruebas de intrusión y de simulación de ataques de Dell reproduce fielmente los ataques del mundo real.

El servicio combina lo siguiente:

- Simulaciones mensuales automatizadas de vulneraciones y ataques (BAS) para confirmar que sus controles funcionan correctamente.
- Prueba de intrusión anual, en la que expertos cualificados intentan sortear las defensas de los activos y datos críticos.

Simulaciones de ataque para probar los controles de seguridad

Los profesionales de seguridad de Dell utilizan tecnología de BAS avanzada para probar los diferentes vectores de ataque; por ejemplo, para intentar colocar malware en un punto final o para acceder sin autorización a la información de un servidor web. Los evaluadores de Dell aplican las BAS para simular ataques en toda la cadena de eliminación[1] de amenazas, incluidas las TTP[2] de ataque más actuales.

La tecnología BAS es segura para entornos de producción y se actualiza continuamente con la información de amenazas, los ataques y las conductas más actuales.

Las pruebas de intrusión analizan las rutas hacia objetivos de alto valor

Incluso con simulación de ataques, algunos atacantes tienen la habilidad para navegar por el entorno, sortear los obstáculos y alcanzar los datos valiosos. Aquí es donde entran en juego las pruebas de intrusión.

Principales beneficios:

- Utilizar simulaciones exhaustivas de brechas y ataques para detectar controles de seguridad mal configurados susceptibles de ser aprovechados
- Tener en cuenta los problemas y debilidades de reciente aparición con simulaciones mensuales
- Inspeccionar de cerca las rutas de alto riesgo hacia activos o datos muy valiosos con una prueba de intrusión anual
- Elaborar informes de resultados de pruebas, tendencias trimestrales y actividad reseñable para ayudarle a mejorar el estado de su seguridad
- Obtener rápidamente información estratégica acerca de amenazas de alto riesgo con pruebas ad hoc

Las pruebas de intrusión son un complemento a la BAS: en lugar de probar controles individuales o conjuntos de controles, las pruebas de intrusión se centran en las rutas vulnerables o de alto riesgo que conducen a un entorno. Los evaluadores de intrusión de Dell pueden emular las diversas técnicas, e incluso las diferentes cargas útiles, que los atacantes utilizan para tratar de alcanzar un objetivo concreto, como capturar un sistema de alto valor o robar o desactivar un conjunto de archivos concreto. Al igual que los atacantes, un evaluador de intrusión experimentado puede desplazar, reorientar y adaptar las técnicas para alcanzar su objetivo.

Aplicar información de pruebas para mejorar el estado de seguridad

Dell Technologies Services le ofrece informes mensuales sobre los problemas de control de seguridad para corregirlos en función de los resultados que se obtienen al ejecutar las secuencias de la BAS. Cada trimestre, Dell revisará las tendencias de las diversas simulaciones de ataque, notificará la actividad reseñable observada en su entorno de tecnología informática y analizará las recomendaciones para mejorar el estado de su seguridad.

Funciones principales

Simulación de vulneraciones y ataques (BAS)

- Ejecutar simulaciones automatizadas de vulneraciones y ataques mensualmente en función del entorno del cliente
- Validar controles de seguridad en el perímetro y los componentes de infraestructura interna, incluida la puerta de enlace web, la puerta de enlace de correo electrónico y los puntos finales
- Actualizar continuamente la herramienta de BAS con la información de amenazas, los ataques y las conductas más actuales
- Modificar el flujo de trabajo de la simulación en función de las simulaciones previas y los factores del entorno de seguridad
- Ejecutar simulaciones ad hoc para los problemas de seguridad detectados recientemente en función de la inteligencia de amenazas y la evaluación de Dell

Pruebas de intrusión

- Ejecutar pruebas de intrusión anuales en un subconjunto definido de puertas de enlace web, API, dispositivos móviles, direcciones IP externas e internas y configuraciones de cloud
- Ejecutar nuevamente pruebas de intrusión después de solucionar los problemas hallados en la primera prueba (opcional)

Informes y revisión

- Proporcionar informes mensuales sobre las simulaciones de vulneraciones y ataques llevadas a cabo
- Entregar informes y revisiones trimestrales de las tendencias y la actividad reseñable observadas en el entorno de tecnología informática del cliente
- Aportar recomendaciones para mejorar el estado de seguridad general

Incorporación

- Llevar a cabo reuniones de introducción al servicio
- Revisar las listas de control previas a la participación llevadas a cabo por el cliente
- Revisar el entorno de tecnología informática del cliente
- Activar la aplicación de BAS para el cliente
- Proporcionar asistencia para la implementación de agentes

Póngase en contacto con su representante de ventas hoy mismo.

[1] "Full kill chain" engloba una serie de amenazas externas, entre otras, el phishing, las puertas de enlace web, etc., la vulneración de puntos finales, los movimientos laterales para obtener credenciales o distribuir el ataque, la filtración de datos, etc.
[2] "TTP": tácticas, técnicas y procedimientos