Evaluación de resistencia cibernética

Una evaluación de riesgos complementaria para medir la exposición de los datos y poner a prueba su pila de seguridad con respecto a las últimas tácticas y técnicas profesionales de los adversarios.

Con tantas rutas de ataque, debe estar atento a todo lo que sucede. La resistencia cibernética requiere un enfoque en el que se asumen las vulneraciones. Necesita ver más allá de los puntos finales: los datos compartidos, las aplicaciones SaaS, el DNS y el Directorio Activo. **Nuestra evaluación lo ayuda a responder con confianza estas preguntas:**

¿Puedo detectar una vulneración?

¿Puedo investigar incidentes y recuperarme rápidamente?

¿Puedo proteger mis datos almacenados en la nube y de forma local?

Nuestro equipo hará lo siguiente:

- Evaluar sus capacidades de detección de amenazas frente a los adversarios modernos
- Clasificar los datos confidenciales y medir la sobreexposición y el acceso que no cumple las regulaciones
- Documentar las fallas en la detección, la postura frente a la estrategia Zero Trust y las prioridades en cuanto a la remediación
- Preparar y educar a su equipo para manejar incidentes avanzados

¿Cómo funciona?

LANZAMIENTO
Instalar la Plataforma de seguridad de datos Varonis

SEMANA 1
Período de aprendizaje de IA

SEMANA 2
Simulación del atacante

SEMANA 3
Revisión de la resistencia

SEMANA 4
Resumen de la evaluación

El equipo de primera clase detrás de la simulación de los atacantes.

Desde para prevenir el ransomware hasta para atrapar a los usuarios internos maliciosos, las marcas más importantes del planeta confían en nuestros expertos de primera clase para identificar, investigar y detener ataques.

Lea su investigación

Reduzca su riesgo sin tomar ningún otro.

Obtenga un documento detallado que incluye fortalezas, debilidades y recomendaciones prácticas. Nuestro equipo trabajará codo a codo con el suyo para revisar toda la actividad y los resultados utilizando su pila de seguridad existente.

Vector de ataque	Etapa de la cadena de eliminación	Detecciones	Gravedad	Explotación
Descarga de archivos maliciosos	Entrada inicial	No se detecta	Mediana	Exitosa
Escaneo de SPN	Reconocimiento	No se detecta	Baja	Exitosa
Análisis de vulnerabilidad local	Reconocimiento	No se detecta	Mediana	Exitosa
Enumeración de cuenta de usuario	Reconocimiento	Se detecta	Baja	Falló
Kerberoasting	Explotación	Se detecta	Mediana	Falló
Lista del administrador de credenciales	Explotación	No se detecta	Mediana	Falló
Password spraying	Movimiento lateral	Se detecta	Mediana	Falló
Ejecución de ransomware	Negación de servicio	Se detecta	Alta	Exitosa
Túnel DNS	Exfiltración de datos	No se detecta	Alta	Exitosa
Algoritmo de generación de dominios	Contra el análisis forense	No se detecta	Baja	Exitosa

¿Cómo solicito una Evaluación de resistencia cibernética?

Comuníquese con su equipo de cuentas de Varonis para solicitar una llamada para analizar su resistencia cibernética con nuestro equipo de análisis forense.

Contáctenos