tenable

mdtel

10 COSAS QUE DEBES HACER Y QUE DEBES EVITAR

PARA ELABORAR TU PROGRAMA DE GESTIÓN DE VULNERABILIDADES BASADA EN EL RIESGO

Con la gestión de vulnerabilidades tradicional, el número de vulnerabilidades detectadas suele ser tan grande que resulta difícil mantenerse al día con todas ellas y es complicado saber cuáles son las que representan el mayor riesgo para la organización.

Es aún más complicado si confías exclusivamente en las puntuaciones CVSS para determinar qué vulnerabilidades reparar primero. Esto se debe a que las puntuaciones CVSS no tienen en cuenta el riesgo real, y la gestión de vulnerabilidades tradicional no te brinda una visión completa de su superficie de ataque moderna. Esto deja puntos ciegos que pueden poner a tu organización en riesgo.

Hacer evolucionar tu gestión de vulnerabilidades tradicional hacia un programa de gestión de vulnerabilidades basada en el riesgo, puede ayudarte a priorizar qué vulnerabilidades debes corregir primero y brindarte más información sobre todos los activos y los riesgos asociados a lo largo de su superficie de ataque.

A continuación, incluimos algunas cosas que debes hacer y las que debes evitar si deseas agregar un abordaje basado en el riesgo a tu programa de gestión de vulnerabilidades.

Lo que debes hacer	Lo que debes evitar
Detecta las brechas en tus procesos actuales de gestión de vulnerabilidades, por ejemplo, los posibles puntos ciegos, y crea planes para subsanarlas a fin de mejorar su postura general en el área de seguridad.	No asumas que tu programa es lo "suficientemente bueno". Evalúa la madurez de tu programa en el área de seguridad para garantizar que sus métricas de riesgo se basen en datos de suma credibilidad.
Identifica y mapea todos tus activos, no solo la TI tradicional, sino también dentro de sus entornos móviles y en la nube, TO, contenedores y aplicaciones web.	No te enfoques solo en los activos que están dentro del alcance del cumplimiento. Evalúa todos tus activos críticos para el negocio.
Incluye todos tus activos y vulnerabilidades dentro del contexto completo, de modo que puedas enfocarte en lo que más importa primero.	No confíes únicamente en las puntuaciones CVSS para priorizar qué vulnerabilidades corregir primero. Para priorizar la corrección, comprende el contexto completo de cada vulnerabilidad, incluyendo la criticidad de los activos afectados y una evaluación de la actividad actual y la probable actividad futura de los atacantes.
Realiza una evaluación continua de todos los activos conocidos, y detecta y evalúa de inmediato todos aquellos que sean nuevos.	No solo detectes y evalúes tus activos en busca de vulnerabilidades. Emplea una solución más completa para poder priorizar cada vulnerabilidad en función del riesgo para el negocio, adopta las medidas de corrección adecuadas y mide los indicadores clave de rendimiento (KPI).
Adopta un abordaje estratégico proactivo con respecto a la gestión de vulnerabilidades para enfocarte en el riesgo real para el negocio, y no en la atención que los medios de comunicación prestan a una vulnerabilidad en particular.	No te enfoques únicamente en tus activos locales y de TI tradicional. Identifica y mapea todos tus activos, incluyendo aquellos móviles, en la nube, en contenedores y de TO.
Usa el aprendizaje automático para unir de manera espontánea los datos de vulnerabilidades y la criticidad de los activos con inteligencia de amenazas y exploits, de modo que puedas medir y priorizar las vulnerabilidades con el contexto del riesgo para el negocio.	No intentes analizar manualmente las decenas de miles de datos de seguridad que necesitas para evaluar las vulnerabilidades junto con el contexto. Utiliza la automatización del aprendizaje automático para determinar rápidamente, en cuestión de segundos, el riesgo para el negocio de cada vulnerabilidad.
Enfócate en el 3 % de las principales vulnerabilidades que representan el mayor riesgo para tu organización en los próximos 28 días.	No pierdas el tiempo en vulnerabilidades que no representan ningún riesgo. Enfócate en las vulnerabilidades y los activos que representan el mayor riesgo para tu organización.
Corrige las vulnerabilidades que representan el mayor riesgo para tu organización.	No bases las decisiones de corrección en información vieja y obsoleta de escaneos periódicos y poco frecuentes. Asegúrate de que tu inteligencia de seguridad sea tan dinámica como el escenario de las amenazas.
Usa métricas basadas en el riesgo para determinar el nivel de eficiencia y eficacia del equipo de seguridad.	No midas el éxito según el número de vulnerabilidades corregidas o el número de sistemas a los que se les colocaron parches. Identifica y aborda los activos y las vulnerabilidades que plantean un riesgo real para tu organización, para asegurarse de reducir la mayor cantidad de riesgos con el mínimo esfuerzo.
Utiliza el análisis de vulnerabilidades basado en el riesgo y otros informes de inteligencia para comunicar de manera eficaz tu postura en el área de seguridad a las principales partes interesadas, de una manera que comprendan.	No seas reactivo y lucha por abordar cada nueva vulnerabilidad que aparece en los titulares de las noticias. Un abordaje basado en el riesgo te ayudará a maximizar la eficacia y la eficiencia para que puedas enfocarte en lo que más importa.

¿Listo para reducir los riesgos, maximizar la eficiencia y poner foco en lo que más importa? ***mdtel*** puede ayudarte a adoptar un abordaje basado en el riesgo para tu programa de gestión de vulnerabilidades.

Aprende cómo hacerlo