CYBERSECURITY TECHCHECK

La rápida detección de una vulneración puede reducir las pérdidas hasta en un 32%.

¿Estás seguro de que le estás sacando el máximo provecho a tu sistema de ciberseguridad?

Nuestros años de experiencia combinado con las mejores prácticas de la industria y los estándares de los fabricantes, nos han permitido desarrollar **TechCheck**, un servicio que audita las plataformas de ciberseguridad, entregando visibilidad temprana y asegurando la continuidad de tu negocio.

TechCheck analiza la madurez actual de las configuraciones y políticas e identifica oportunidades de mejora, apuntando a garantizar el mejor desempeño y usabilidad de las herramientas de ciberseguridad.

CONTINUIDAD

Identifica y prioriza potenciales problemas antes de que se conviertan en fallas críticas.

OPTIMIZACIÓN

Logra la eficiencia de las herramientas de protección y asegura su aporte al negocio.

ACTUALIZACIÓN

Detecta brechas para asegurar que la protección esté al día en versiones y funcionalidades.

ESPECIALIZACIÓN

Nuestro especialistas se focalizan en maximizar la protección.

¿POR QUÉ REALIZAR UN TECHCHECK?

El 83% de los sistemas informáticos permanecen con la configuración inicial, lo que hace a las empresas 77% más vulnerables frente a las que mantienen sus sistemas actualizados.

TechCheck audita de forma profunda la infraestructura tecnológica para identificar oportunidades de optimización de configuraciones y versión, apuntando a garantizar el desempeño óptimo de las herramientas de protección y que cada componente de la infraestructura aporte valor real a las operaciones.

¿CÓMO FUNCIONA TECHCHECK?

El diagnóstico se ejecuta en sitio o mediante una conexión segura, con privilegios de auditoría con acceso a la configuración, registros de log e información de versiones.

Consideraciones: para plataformas de seguridad on-premise, el TechCheck no contempla el checkeo de vulnerabilidades sobre el servidor donde se encuentre alojada la consola de administración.

FASES DEL TECHCHECK

1. **RECONOCIMIENTO:** se indaga sobre la administración actual de la herramienta e información relevante de la red para personalizar el TechCheck,

2. **DIAGNÓSTICO:** teniendo acceso a la plataforma, se inicia la auditoría y se contrasta la información con nuestra línea base. Este diagnóstico se basa en cinco ítems: gobernanza y control, eficiencia y rendimiento, cobertura y efectividad, integración y conectividad, y actualización y mejora continua.

3. **INDICADOR FINAL:** puntaje del 0 al 100 que permite evaluar la madurez actual y visualizar puntos de mejora. Este indicador se basa en los 5 ítems establecidos en el diagnóstico.

4. **PROPUESTA DE OPTIMIZACIÓN:** se entrega un plan de mejoras concretas alineadas con los objetivos del negocio. En este punto el cliente puede enlazar los subcontroles del WSC con la usabilidad de la plataforma para tener una referencia de los controles CIS, lo que le permitirá compararse con los estándares y normas internacionales y apuntar a maximizar la inversión actual de ciberseguridad.

FASE DE DIAGNÓSTICO

Gobernanza y Control

Evalúa la capacidad de gestión, administración y cumplimiento de políticas para fortalecer la gobernanza y optimizar las configuraciones.

Eficiencia y Rendimiento

Analiza el uso de recursos y el desempeño general para identificar fallas en el flujo y mejorar la eficiencia operativa de la infraestructura.

Cobertura y Efectividad

Examina la capacidad de la plataforma para proteger todos los puntos de la red, y asegurar la protección integral y maximizar el uso de las funcionalidades.

Integración y Conectividad

Verifica que la herramienta maximice su integración con otras plataformas, alineándose con los requerimientos del negocio.

Actualización y Mejora Continua

Revisa que la plataforma esté actualizada, optimizada y preparada para responder a las amenazas más recientes.

METODOLOGÍA PROBADA

Nuestro equipo de Servicios Profesionales se rige bajo la metodología PGO (Preparar-Gestionar-Optimizar) de Widefense, lo que garantiza un proceso eficiente y una mejora continua en todos los proyectos.

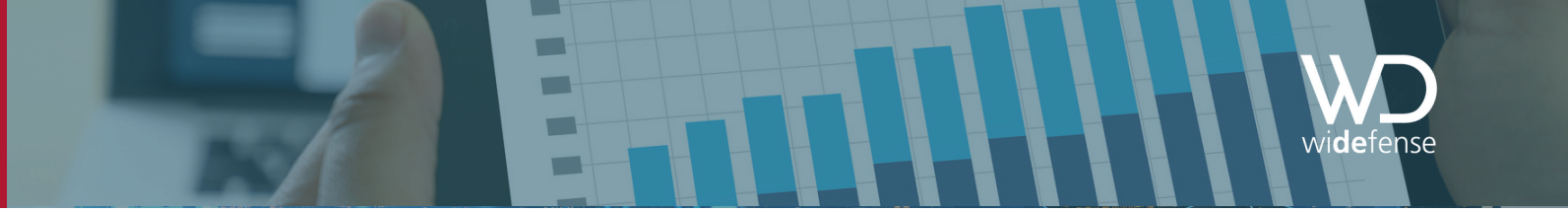
PREPARAR

Identificamos proactivamente configuraciones o políticas de riesgo en la infraestructura tecnológica, permitiendo anticipar posibles amenazas antes de que se conviertan en problemas críticos. Esto asegura la continuidad operativa del negocio y protege los activos más valiosos.

Entender los procesos del negocio nos permite elevar la seguridad del entorno apuntando siempre a obtener el máximo provecho de la plataforma, integrando tanto las políticas recomendadas por las marcas como por nuestro equipo de expertos. En la reunión inicial, es importante contar con la participación de todas las contrapartes involucradas en el producto a auditar para poder resolver todas las dudas.

GESTIONAR

Nuestros especialistas certificados analizan y auditan la configuración de las plataformas de ciberseguridad, garantizando que operen de manera eficiente y efectiva. Al mantener los sistemas actualizados y correctamente configurados, reducimos vulnerabilidades y mejoramos la usabilidad, permitiendo a las organizaciones enfocarse en sus objetivos empresariales con tranquilidad.



En paralelo a la revisión de la plataforma, nuestro equipo de profesionales va completando un informe basado en los cinco 5 ítems del diagnóstico para presentar al cliente en la siguiente fase. Además de los hallazgos, este informe contiene recomendaciones de buenas prácticas basadas en las sugerencias del fabricante y a las propias según nuestra experiencia y estudios de mercado.

OPTIMIZAR

Una vez listo el informe, el equipo comercial gestiona una reunión de todos los involucrados para poder presentar las conclusiones y el trabajo realizado. Las recomendaciones sostenidas en el documento dan pie a que el cliente pueda tomar decisiones sobre su herramienta con una base sólida y confiable apuntando siempre a maximizar el rendimiento de su plataforma de seguridad.

El informe incluye propuestas de mejora que incorporan tanto las tendencias del mercado como lo indicado por el cliente en la reunión inicial, lo que permite contar con un documento personalizado que validará las decisiones empresariales en post de mejorar los niveles de ciberseguridad.

Solicita tu TechCheck aquí o escribe a contacto@widefense.com para más información.