kaspersky

Estimado Cliente,

Como parte de nuestro compromiso por mejorar el nivel de ciberseguridad de las organizaciones, hemos analizado la información que nos proporcionó y, en consecuencia, los distintos aspectos críticos que conforman su infraestructura, procesos y políticas de protección digital.

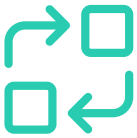
Tras la evaluación realizada, detectamos que el nivel actual de madurez en ciberseguridad de su compañía es un nivel avanzado.
Las organizaciones en esta etapa suelen presentar un enfoque estratégico y holístico de la ciberseguridad, con planes integrales y maduros alineados a los objetivos del negocio. Gestionan la seguridad de forma proactiva mediante tecnologías avanzadas de detección, respuesta y automatización, combinadas con procesos formales y una fuerte cultura organizacional en torno a la seguridad de la información y protección de sus activos.

Las tecnologías y procesos habituales en este nivel son:

Plataformas avanzadas de protección para estaciones de trabajo, servidores y dispositivos móviles (EDR avanzado o XDR).

Soluciones de visibilidad y control de red (NGFW, IDS/IPS, NDR) **y de protección de correo electrónico.**

Protección específica para entornos críticos: contenedores, aplicaciones web (WAF)**, cargas en la nube y servicios esenciales.**



Implementación de plataformas SIEM para correlación, análisis y gestión proactiva de eventos de seguridad.

SOC (Security Operations Center) **interno o externalizado, con monitoreo continuo** (24x7).

Consultoría avanzada y regular en ciberseguridad (Penetration Testing, Threat Hunting, Compromise Assessment).

Campañas de concientización periódicas y estructuradas para todo el personal, incluyendo la alta gerencia.

Procesos formales establecidos y documentados (plan de continuidad del negocio, playbooks de respuesta ante incidentes, gestión de crisis, etc.).

Entre los hallazgos más relevantes dentro de este tipo de organizaciones, destacamos:

- La ciberseguridad es considerada una prioridad estratégica por parte del management y la alta dirección.
- Cumplimiento de normativas y estándares internacionales de seguridad.
- Conciencia clara sobre cómo los riesgos de ciberseguridad impactan en el negocio y estrategias definidas para su gestión.
- Equipo especializado en TI y ciberseguridad con roles claramente definidos y métricas de desempeño periódicas.
- Presupuesto significativo y sostenido destinado a iniciativas de seguridad, alineado con los objetivos del negocio.

A pesar de estos avances, las organizaciones en un nivel avanzado no deben permanecer estáticas. La evolución continua implica optimizar procesos, anticipar amenazas emergentes y profundizar la automatización de la respuesta mediante analítica avanzada y capacidades predictivas. La ciberseguridad, en este nivel, se consolida como un pilar fundamental en la toma de decisiones estratégicas del negocio.

¿Cómo podemos ayudarlo?

Desde Kaspersky, estamos convencidos de que podemos acompañarlo en este proceso de optimización y evolución continua, poniendo a disposición un portafolio de soluciones y servicios acorde a su nivel:

EDR Expert:

Plataforma completa de protección para estaciones de trabajo, servidores y dispositivos móviles. Con capacidades integrales de control de postura y seguridad: navegación, periféricos, aplicaciones, vulnerabilidades. Incluyendo un EDR avanzado con capacidades de sandboxing, threat hunting, mapeo con el framework de MITRE y gestión de incidentes.

XDR Expert:

Solución empresarial de Extended Detection and Response (XDR) de nivel avanzado diseñada para ofrecer detección, investigación y respuesta coordinada y automatizada a amenazas cibernéticas complejas.

SIEM:

Plataforma de ciberseguridad que recopila, centraliza, correlaciona y analiza en tiempo real los eventos y registros (logs) que generan los diferentes sistemas, aplicaciones y dispositivos de una organización Correlación, gestión y análisis proactivo de incidentes de seguridad.

SOC Consulting:

Es el centro de operaciones de seguridad de una organización formado por un equipo que brinda servicios de consultoría y acompañamiento en la creación u optimización de un Security Operations Center.

Threat Intelligence:

Inteligencia de amenazas de clase mundial para anticipar ataques, identificar campañas APT y proteger activos críticos. Incluye monitoreo de activos externos, protección de marca, data feeds y cloud sandbox.

KATA NDR:

Solución avanzada de detección y respuesta en red para identificar ataques dirigidos y amenazas persistentes. Incluye DPI, análisis de las tablas de sesiones y visibilidad sobre la comunicación entre los diferentes activos y segmentos de la red.

Container Security:

Seguridad específica para entornos de contenedores y DevOps, con controles de imagen, despliegue y ejecución.

Incident and Response:

Servicios especializados para la gestión y contención de incidentes, con análisis forense y planes de remediación.

Con esta evaluación inicial, usted ya cuenta con un diagnóstico claro de su situación actual.

Nuestro equipo se comunicará a la brevedad para presentarle una propuesta técnica con el detalle y los alcances de cada solución, con el objetivo de avanzar juntos en un plan concreto para madurar la postura de ciberseguridad de su compañía.

Agradecemos nuevamente su confianza,

Atentamente,

Equipo Kaspersky

kaspersky