Construyendo un SOC escalable

para TEK Soluciones Tecnológicas

kaspersky cybersecurity true to business

TEK Soluciones Tecnológicas

Desarrollado con tecnología de Kaspersky, se convirtió en el primer SOC de propiedad empresarial con tecnología de Kaspersky en Sudamérica, lo que le permitió a TEK adoptar un modelo operativo unificado.

Cómo TEK amplió la protección a más de 7400 endpoints y aceleró la detección de amenazas con un SOC unificado

TEK Soluciones Tecnológicas transformó su enfoque de ciberseguridad mediante la implementación de un SOC plenamente operativo, lo que permitió mejorar los tiempos de detección y respuesta, fortalecer la visibilidad en todos los entornos y crear una oferta escalable de SOC como servicio.

>12 Años
De experiencia

+1000
Empresas atendidas

+30
Marcas aliadas

Creación de un SOC con intención comercial

TEK Soluciones Tecnológicas es un proveedor colombiano de ciberseguridad e infraestructura TI que ofrece servicios de protección y operaciones de seguridad a organizaciones en todo el país.

En 2025, TEK evolucionó de un modelo de protección tradicional de endpoints hacia la implementación de su propio SOC para detección, correlación y respuesta en tiempo real. El SOC fue diseñado como una base escalable para una oferta de SOC como servicio (SOCaaS), orientada a organizaciones que no cuentan con capacidades internas de operaciones de seguridad.

De las carencias de visibilidad a la claridad operativa

La decisión de TEK respondió a una brecha común en el mercado: las organizaciones contaban con herramientas de seguridad, pero no con la capacidad de convertir los datos en contexto. Existían alertas, pero sin correlación no era posible entender la progresión de los ataques, la causa raíz ni la relación entre incidentes. Esto limitaba la velocidad de respuesta y aumentaba el riesgo operativo.

TEK enfrentaba las mismas limitaciones a nivel interno: herramientas fragmentadas, visibilidad limitada entre entornos y dificultades para correlacionar incidentes entre sistemas.

La conclusión fue que las mejoras incrementales no eran suficientes. TEK necesitaba evolucionar de herramientas aisladas hacia operaciones de seguridad unificadas, con el objetivo de reducir el MTTD y el MTTR mediante un modelo integrado de detección y respuesta.

«

No solo buscábamos un proveedor de soluciones para endpoints. Buscábamos la base tecnológica para construir un SOC real.

Mauricio Restrepo
CEO de TEK

La elección de la plataforma adecuada

Para lograr ese cambio, TEK necesitaba algo más que una solución para endpoints. Necesitaba una plataforma que pudiera soportar un SOC completo.

Dos factores fueron decisivos en la toma de decisión:

La profundidad de la inteligencia global sobre amenazas

La flexibilidad de Kaspersky SIEM

En conjunto, le proporcionaron a TEK lo que antes le faltaba: una visión unificada de los eventos de seguridad en todo el entorno.

Otro aspecto igual de importante fue que la arquitectura admitía un modelo operativo único en el que la telemetría, el análisis y la respuesta trabajaban conjuntamente. Al consolidar las funciones en una única plataforma, TEK redujo la dependencia de herramientas fragmentadas y creó una base escalable tanto para la protección interna como para los servicios externos.

Un SOC diseñado para operaciones integradas

TEK adoptó un enfoque deliberado para construir un ecosistema unificado en lugar de implementar componentes aislados.

- Kaspersky SIEM recopiló datos de telemetría de todo el entorno para permitir la correlación y el análisis en tiempo real.
- Una capa de concienciación sobre seguridad agregó simulaciones de phishing, capacitaciones y medición de la madurez del usuario.

El resultado no fue solo un conjunto de herramientas, sino un SOC totalmente operativo. Al integrar datos de red, infraestructura y nivel de servicio, TEK creó un modelo en el que los eventos podían entenderse en contexto en lugar de analizarse de forma aislada. La detección de comportamiento complementó el análisis basado en reglas, mientras que la visibilidad centralizada facilitó una respuesta más rápida y coordinada.

Kaspersky SIEM

Una solución SIEM de última generación y alto rendimiento diseñada para la recopilación, el análisis y la correlación centralizados de eventos de seguridad de la información procedentes de diversas fuentes, con el fin de identificar.

Kaspersky Security Awareness

Una cartera de productos de capacitación que aumenta la alfabetización digital entre los empleados de todos los niveles y fomenta una cultura donde la seguridad es responsabilidad de todos.

Kaspersky Professional Services

Un conjunto de servicios que ayuda a las organizaciones a implementar y optimizar las soluciones de Kaspersky de forma más ágil y eficiente, maximizando la protección y el valor operativo.

Al construir un SOC, no se puede improvisar.

Mauricio Restrepo

CEO de TEK

Ampliación de las operaciones de seguridad como servicio

Uno de los resultados más importantes fue que la misma arquitectura pudo extenderse a los clientes. A través de este modelo de SOC como servicio, los clientes obtienen supervisión continua, correlación entre capas, aislamiento automatizado de sistemas en riesgo e investigación y elaboración de informes forenses.

El modelo demostró ser escalable rápidamente.

En una implementación en el sector público, TEK brindó soporte a un entorno que abarcaba más de 7000 endpoints e integró tanto Kaspersky EDR Expert como Kaspersky EDR Foundations en su SOC sin necesidad de construir una nueva infraestructura.

Eso demostró tanto la flexibilidad como la eficacia operativa de la plataforma.

Una prueba real del SOC

Un servidor crítico mostró un uso inusualmente alto de CPU y memoria, cercano al 90 %, sin ninguna causa operativa clara. En un entorno tradicional, esto podría haberse tratado como un problema de rendimiento. Dentro del SOC, se convirtió en una señal para una investigación más profunda.

Al correlacionar la telemetría a través de Kaspersky SIEM, TEK identificó un script oculto de criptominería que se ejecutaba en el sistema. El servidor en riesgo fue identificado en cuestión de minutos, aislado para evitar una mayor propagación e investigado para determinar el vector de ataque antes de implementar las mejoras de remediación y control.

El valor del SOC se hizo evidente durante un incidente que involucró a un cliente del sector público en Pereira

El incidente hizo algo más que validar la plataforma. Demostró cómo la correlación y la detección de comportamientos podían revelar amenazas que la supervisión tradicional podría pasar por alto, y cómo un SOC en funcionamiento podía convertir la detección en acciones decisivas.

Kaspersky CyberTrace

Es una Plataforma de inteligencia frente a amenazas que facilita una integración perfecta de las fuentes de datos sobre amenazas con soluciones SIEM para ayudar a los analistas a aprovechar de manera más eficaz la inteligencia frente a amenazas de su flujo de trabajo de operaciones de seguridad existente.

Impacto estratégico y operativo

La plataforma mejoró la eficacia

Al consolidar múltiples funciones de seguridad dentro de una arquitectura unificada, TEK redujo la complejidad, mejoró la escalabilidad y permitió la incorporación de grandes entornos de clientes sin infraestructura adicional.

El rendimiento operativo mejoró

Se redujeron los tiempos de detección y respuesta, aumentó la visibilidad y se pudieron identificar y contener las amenazas en una etapa más temprana del ciclo de vida del ataque, lo que refleja mejoras significativas tanto en el MTTD como en el MTTR.

Se mejoró la protección sin comprometer el rendimiento

TEK informa de una correlación estable, una detección de comportamiento eficaz y ningún impacto observable en el rendimiento del sistema. Desde la perspectiva de TEK, el nivel de protección ofrecido superó las expectativas iniciales.

Al mismo tiempo, TEK está reforzando sus capacidades de inteligencia sobre amenazas, incluida la evaluación de tecnologías como Kaspersky CyberTrace para mejorar la gestión de la inteligencia, correlacionar las fuentes de manera más eficaz y respaldar una toma de decisiones más rápida y mejor fundamentada.

La siguiente fase del crecimiento del SOC

Ahora que el SOC está plenamente operativo, TEK se centra en ampliar sus capacidades a medida que más organizaciones se conectan a la plataforma. Una prioridad clave es aumentar su capacidad para analizar y correlacionar la telemetría de seguridad en múltiples entornos de clientes. A medida que aumenta la cantidad de datos, TEK los utiliza para enriquecer la detección, generar inteligencia operativa útil y mejorar continuamente la postura de seguridad de las organizaciones conectadas.

La siguiente fase se centra en una mayor cobertura, operaciones más sólidas y una detección y respuesta más precisas en entornos cada vez más complejos. El objetivo a largo plazo es ampliar aún más este modelo y brindarles a más organizaciones acceso a capacidades avanzadas de supervisión, detección y respuesta sin el costo y la complejidad de construir una infraestructura de SOC propia.

latam.kaspersky.com

#kaspersky
#truetobusiness