Building a scalable SOC

for Tek Soluciones Tecnológicas

kaspersky cybersecurity true to business

TEK Soluciones Tecnológicas

Built on Kaspersky technology, it became the first enterprise-owned SOC powered by Kaspersky in South America, shifting TEK to a unified operating model

How TEK scaled protection across 7,400+ endpoints and accelerated threat detection with a unified SOC

TEK Soluciones Tecnológicas transformed its approach to cybersecurity by building a fully operational SOC – improving detection and response times, strengthening visibility across environments, and creating a scalable SOC-as-a-Service offering.

>12 Years
of experience

1000+
companies served

30+
partner brands

Building a SOC with commercial intent

TEK Soluciones Tecnológicas is a Colombian cybersecurity and IT services provider delivering protection and security operations across enterprises nationwide.

In 2025, TEK transitioned from endpoint-centric security to building its own SOC for real-time detection, correlation and response. The SOC was designed as a scalable foundation for a SOC-as-a-Service offering to support organizations without in-house security operations capabilities.

From visibility gaps to operational clarity

TEK's decision was driven by a common market gap: organizations had security tools in place, but lacked the ability to turn data into context. Alerts existed, but without correlation they did not explain how attacks progressed, what the root cause was, or how incidents were connected. This limited response speed and increased operational risk.

TEK faced the same constraints internally: fragmented tooling, limited cross-environment visibility, and difficulty correlating incidents across systems.

The conclusion was that incremental improvements were insufficient. TEK needed to shift from tools to operations, reducing MTTD and MTTR through a unified detection and response model.

We weren't just looking for an endpoint provider. We were looking for the technological foundation to build a real SOC.

Mauricio Restrepo
CEO, TEK

Kaspersky SIEM

A high-performance next-generation SIEM solution designed for the centralized collection, analysis and correlation of information security events from various sources, in order to identify cyber incidents and neutralize them in a timely manner.

Kaspersky Security Awareness

A portfolio of training products that increase cyber literacy among employees at all levels and foster a culture where security is everyone's responsibility.

Kaspersky Professional Services

A set of services that help organizations deploy and optimize Kaspersky solutions faster and more effectively, ensuring maximum protection and operational value.

Choosing the right platform

To make that shift, TEK needed more than an endpoint solution. It needed a platform that could support a complete SOC.

Two factors shaped the decision:

The depth of global threat intelligence

The flexibility of Kaspersky SIEM

Together, they gave TEK what it had previously lacked: a unified view of security events across the environment.

Just as importantly, the architecture supported a single operating model in which telemetry, analysis and response worked together. By consolidating functions within one platform, TEK reduced reliance on fragmented tools and created a scalable foundation for both internal protection and external services.

A SOC built for integrated operations

TEK took a deliberate approach, building a unified ecosystem rather than deploying isolated components.

- Kaspersky SIEM ingested telemetry from across the environment to enable real-time correlation and analysis.
- A security awareness layer added phishing simulations, training and user maturity measurement.

The result was not just a toolset but a fully operational SOC. By integrating network, infrastructure and service-level data, TEK created a model where events could be understood in context rather than in isolation. Behavioral detection complemented rule-based analysis, while centralized visibility supported faster, more coordinated response

When building a SOC, you cannot improvise.

Mauricio Restrepo

CEO, TEK

Scaling security operations as a service

One of the most important outcomes was that the same architecture could be extended to clients. Through this SOC-as-a-Service model, clients gain continuous monitoring, cross-layer correlation, automated isolation of compromised systems, and forensic investigation and reporting.

The model proved scalable quickly.

In one public sector deployment, TEK supported an environment spanning more than 7,000 endpoints, integrating both Kaspersky EDR Expert and Kaspersky EDR Foundations into its SOC without building new infrastructure.

That demonstrated both the flexibility and operational efficiency of the platform.

The value of the SOC became clear during an incident involving a public sector client in Pereira.

The incident did more than validate the platform. It showed how correlation and behavioral detection could expose threats that traditional monitoring might miss, and how a functioning SOC could turn detection into decisive action.

A real-world test of the SOC

A critical server showed unusually high CPU and memory usage – approaching 90 percent – without any clear operational cause. In a traditional environment, this might have been treated as a performance issue. Within the SOC, it became a signal for deeper investigation.

By correlating telemetry through Kaspersky SIEM, TEK identified a hidden cryptomining script running on the system. The compromised server was identified within minutes, isolated to prevent further spread, and investigated to determine the attack vector before remediation and control improvements were implemented.

Kaspersky CyberTrace

A threat intelligence platform that enables seamless integration of threat data feeds with SIEM solutions to help analysts leverage threat intelligence in their existing security operations workflows more effectively

Strategic and operational impact

The platform improved efficiency

By consolidating multiple security functions within a unified architecture, TEK reduced complexity, improved scalability, and enabled large client environments to be onboarded without additional infrastructure.

Operational performance improved

Detection and response times were reduced, visibility increased, and threats could be identified and contained earlier in the attack lifecycle, reflecting meaningful improvements in both MTTD and MTTR.

Protection improved without performance trade-offs

TEK reports stable correlation, effective behavioral detection and no observable impact on system performance. In TEK's view, the level of protection delivered has exceeded initial expectations.

At the same time, TEK is strengthening its threat intelligence capabilities, including evaluating technologies such as Kaspersky CyberTrace to improve intelligence management, correlate sources more effectively, and support faster, better-informed decision-making.

The next phase of SOC growth

With the SOC now fully operational, TEK is focused on expanding its capabilities as more organizations connect to the platform. A key priority is increasing its ability to analyze and correlate security telemetry across multiple client environments. As that data grows, TEK is using it to enrich detection, generate actionable operational intelligence, and continuously improve the security posture of connected organizations.

The next phase is focused on broader coverage, stronger operations, and more precise detection and response across increasingly complex environments. The long-term objective is to scale this model further, giving more organizations access to advanced monitoring, detection and response capabilities without the cost and complexity of building their own SOC infrastructure.

www.kaspersky.com

#kaspersky
#truetobusiness