Construindo um SOC escalável

para a TEK Soluciones Tecnológicas

kaspersky cybersecurity true to business

TEK Soluciones Tecnológicas

Além de ser o primeiro SOC privado com tecnologia Kaspersky na América do Sul, posicionou a TEK como detentora de modelo operacional unificado.

Como a TEK ampliou a proteção em mais de 7.400 endpoints e acelerou a detecção de ameaças com um SOC unificado

A TEK Soluciones Tecnológicas transformou sua abordagem de cibersegurança construindo um SOC totalmente operacional, melhorando os tempos de detecção e resposta, fortalecendo a visibilidade entre os ambientes e criando uma oferta de SOC como serviço.

>12 Anos
De experiência

+1000
Empresas atendidas

+30
Marcas parceiras

Construção de um SOC para fins comerciais

A TEK Soluciones Tecnológicas é uma empresa colombiana de serviços de TI e cibersegurança que viabiliza operações de proteção e segurança a empresas de todo o país.

Em 2025, a TEK fez a transição da abordagem de segurança centrada em endpoints para a construção de seu próprio centro de operações de segurança, o SOC, possibilitando detecção, correlação e resposta em tempo real. O SOC foi projetado como uma base escalável para uma oferta de SOC como Serviço, para oferecer suporte a organizações sem recursos internos de operações de segurança.

Das lacunas de visibilidade à clareza operacional

A decisão da TEK foi motivada por uma lacuna comum no mercado: as organizações tinham ferramentas de segurança implementadas, mas não tinham capacidade de transformar dados em contexto. Havia alertas, mas sem correlação, eles não explicavam a evolução dos ataques, qual era a causa raiz, nem a conexão entre os incidentes. Isso limitava a agilidade da resposta e aumentava o risco operacional

Internamente, a TEK enfrentava as mesmas restrições: ferramentas fragmentadas, visibilidade limitada entre ambientes e dificuldade na correlação de incidentes entre os diferentes sistemas.

Por fim, as melhorias graduais não bastaram. A TEK precisava migrar de ferramentas para operações, reduzindo o MTTD e o MTTR por meio de um modelo unificado de detecção e resposta.

Não buscávamos apenas um provedor de endpoints. Buscávamos a base tecnológica para a construção de um SOC de verdade.

Mauricio Restrepo
CEO, TEK

Kaspersky SIEM

Uma solução SIEM de última geração e alto desempenho, projetada para coleta, análise e correlação centralizadas de eventos de segurança da informação de diversas fontes, com o objetivo de identificar incidentes cibernéticos e neutralizálos em tempo hábil.

Kaspersky Security Awareness

Um portfólio de serviços em treinamento que aumenta o conhecimento em cibersegurança entre os funcionários de todos os níveis e estimula uma cultura em que a segurança é responsabilidade de todos.

Kaspersky Professional Services

Um conjunto de serviços que apoia organizações na implementação e otimização das soluções Kaspersky de forma mais ágil e eficiente, garantindo máxima proteção e maior valor operacional.

Escolha da plataforma certa

Para realizar essa mudança, a TEK precisava de mais do que uma solução de endpoint. A empresa precisava de uma plataforma compatível com um SOC completo.

Dois fatores moldaram a decisão:

A profundidade da inteligência global de ameaças

A flexibilidade do Kaspersky SIEM

Juntos, possibilitaram aquilo que a TEK não tinha até então: uma visão unificada dos eventos de segurança em todo o ambiente.

Tão importante quanto, a arquitetura era compatível com um modelo operacional único em que telemetria, análise e resposta atuavam juntos. Ao consolidar funções dentro de uma única plataforma, a TEK reduziu a dependência de ferramentas fragmentadas e criou uma base expansível tanto para proteção interna quanto para serviços externos.

Un SOC diseñado para operaciones integradas

Um SOC construído para operações integradas.

- O Kaspersky SIEM recebia telemetria de todo o ambiente para possibilitar correlação e análise em tempo real.
- Uma camada de conscientização de segurança adicionou simulações de phishing, treinamentos e mensuração da maturidade dos usuários.

O resultado não foi apenas um conjunto de ferramentas, mas um SOC em plena operação. Integrando rede, infraestrutura e dados no nível do serviço, a TEK criou um modelo em que os eventos deixaram de ser vistos isoladamente para ser entendidos em contexto. A detecção comportamental complementou a análise baseada em regras, enquanto a visibilidade centralizada deu suporte à resposta mais rápida e coordenada.

Ao construir um SOC, você não pode improvisar.

Mauricio Restrepo

CEO, TEK

Escala das operações de segurança na forma de serviço

Um dos resultados mais importantes foi que a mesma arquitetura podia ser levada aos clientes. Por meio desse modelo de SOC como serviço, os clientes obtêm monitoramento contínuo, correlação entre camadas, isolamento automatizado de sistemas comprometidos, além de investigação e emissão de relatórios forenses.

Rapidamente o modelo demonstrou ser escalável.

Em uma implementação no setor público, a TEK ofereceu suporte a um ambiente com mais de 7 mil endpoints, integrando o Kaspersky EDR Expert e o Kaspersky EDR Foundations ao seu SOC, sem construir uma infraestrutura nova.

Isso demonstrou tanto a flexibilidade quanto a eficiência operacional da plataforma.

Uma prova real do SOC

Um servidor crítico apresentou um uso de CPU e memória estranhamente alto, chegando perto de 90 por cento, sem qualquer causa operacional clara. Em um ambiente tradicional, esse evento teria sido tratado como um problema de desempenho. No SOC, tornou-se um alerta para uma investigação mais detalhada.

Ao correlacionar a telemetria por meio do Kaspersky SIEM, a TEK identificou um script de criptomineração oculto sendo executado no sistema. O servidor comprometido foi identificado em minutos e isolado para evitar propagação. Em seguida, a investigação descobriu o vetor do ataque antes da implementação da correção e dos aperfeiçoamentos de controle.

O valor do SOC ficou evidente durante um incidente envolvendo um cliente do setor público em Pereira.

O incidente fez mais do que validar a plataforma. Isso mostrou como a correlação e a detecção comportamental podem expor ameaças que o monitoramento tradicional pode não identificar, e como um SOC funcional pode transformar a detecção em ação decisiva.

Kaspersky CyberTrace

Uma Plataforma de inteligência de ameaças que integra dados de ameaças com soluções SIEM, ajudando analistas a usar inteligência de ameaças de forma mais eficaz em seus fluxos de trabalho de segurança.

Impacto operacional e estratégico

A plataforma melhorou a eficiência

Ao consolidar múltiplas funções de segurança dentro de uma arquitetura unificada, a TEK reduziu a complexidade, melhorou a escalabilidade e permitiu que grandes ambientes de clientes fossem integrados sem acréscimo de infraestrutura.

Aperfeiçoamento do desempenho operacional

Foi possível reduzir os tempos de detecção e reposta, aumentar a visibilidade, além de identificar e conter ameaças o quanto antes dentro do ciclo de vida do ataque, resultando em melhorias significativas tanto em MTTD quanto em MTTR.

A proteção foi aprimorada sem comprometer o desempenho

A TEK relata correlação estável, detecção comportamental eficaz e nenhum impacto notável no desempenho do sistema. Na visão da TEK, o nível de proteção entregue superou as expectativas.

Ao mesmo tempo, a TEK vem fortalecendo seus recursos de inteligência em ameaças, inclusive por meio da avaliação de tecnologias como o Kaspersky CyberTrace para melhorar a gestão de inteligência, correlacionar fontes com mais eficácia e apoiar a tomada de decisão mais ágil e fundamentada.

A próxima fase do crescimento do SOC

Agora, com o SOC em plena operação, a TEK tem se concentrado em expandir seus recursos enquanto mais organizações se conectam à plataforma. A prioridade é aumentar sua capacidade de analisar e correlacionar a telemetria de segurança em múltiplos ambientes de clientes. À medida que os dados aumentam, a TEK os utiliza para incrementar a detecção, gerar inteligência operacional prática e aperfeiçoar constantemente a defesa das organizações conectadas.

A próxima fase se concentrará em cobertura mais ampla, operações mais fortes e detecções e respostas ainda mais precisas em ambientes cada vez mais complexos. O objetivo de longo prazo é expandir ainda mais esse modelo, fornecendo a mais organizações o acesso a recursos de monitoramento avançado, detecção e resposta sem o custo e a complexidade da construção de uma infraestrutura própria de SOC.

kaspersky.com.br

#kaspersky
#truetobusiness