NUVOL
Cybersecurity services

CASO DE ÉXITO

De cero visibilidad a defensa activa: SOC as a Service para empresa de logística en México

PROFICIO™

Una empresa de logística en México con operaciones críticas de transporte y distribución llevaba años operando sin visibilidad real de lo que ocurría en su infraestructura. No había forma de saber si estaban siendo atacados, qué tecnologías generaban más eventos de riesgo, ni cuánto tiempo tardaban en responder a un incidente. Hoy, dos años después de implementar SOC as a Service con Nuvol y Proficio, tienen respuesta activa, métricas de madurez y un equipo de seguridad que sabe exactamente qué está pasando — en tiempo real.

+2
Años de Servicio
Contrato Activo y Renovado

24/7
Monitoreo MDR
365 días al año

Logística
México

El Desafío

La empresa operaba con herramientas de seguridad instaladas pero sin correlación central. Cada tecnología funcionaba en su propio silo — Fortinet, Microsoft y otras plataformas generaban eventos que nadie analizaba de forma unificada.

Sus principales retos:

- Sin correlación central de eventos — cada tecnología operaba en silos sin visibilidad unificada.
- Imposibilidad de medir tiempos de respuesta — sin métrica de MTTD ni MTTR establecida.
- Sin reporte ejecutivo — el board no tenía visibilidad del estado real de la seguridad.
- Logs sin priorización — volumen de eventos sin clasificación por severidad ni impacto.
- Sin capacidad de Active Defense — respuesta 100% manual y reactiva ante incidentes.
- Superficie de ataque en expansión — nuevas rutas, proveedores y sistemas integrados sin monitoreo.

La solución

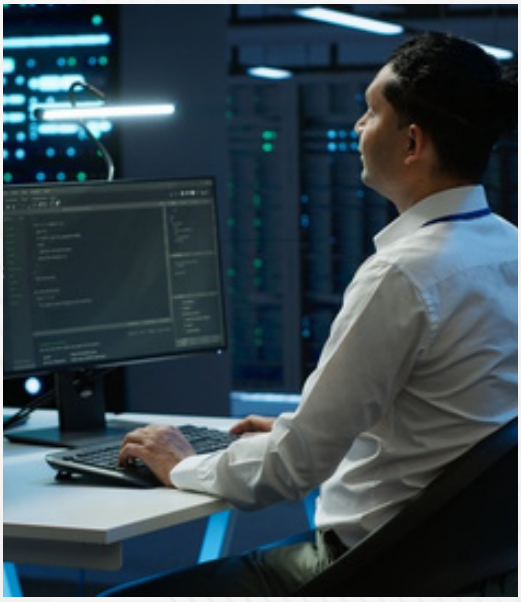
Nuvol diseñó e implementó un programa de SOC as a Service con Proficio, integrando las plataformas tecnológicas existentes en una arquitectura de visibilidad centralizada. La solución integra seis componentes clave.

Capa	Tecnología / Servicio	Valor entregado
Monitoreo 24/7	SOC as a Service · Proficio MDR	Detección y respuesta continua follow-the-sun. Cobertura global sin turnos nocturnos degradados.
Correlación de eventos	Elastic SIEM	Integración de logs de todas las fuentes tecnológicas. Visibilidad unificada de toda la infraestructura.
Análisis y métricas	Splunk	Procesamiento de eventos, tipo de ataques detectados y métricas de incidentes para el board.
Gestión de incidentes	ServiceNow ITSM	Clasificación por prioridad y severidad, casos de uso, comparativo mensual y estatus de tickets.
Respuesta automatizada	SOAR – Active Defense	Timeline de ataques por país e IP, bloqueo automatizado y remediación sin intervención manual.
Optimización de logs	Nuvol + Proficio + Cliente	Depuración de fuentes de log: identificación de lo que realmente aporta vs lo que genera ruido.

Resultados e impacto

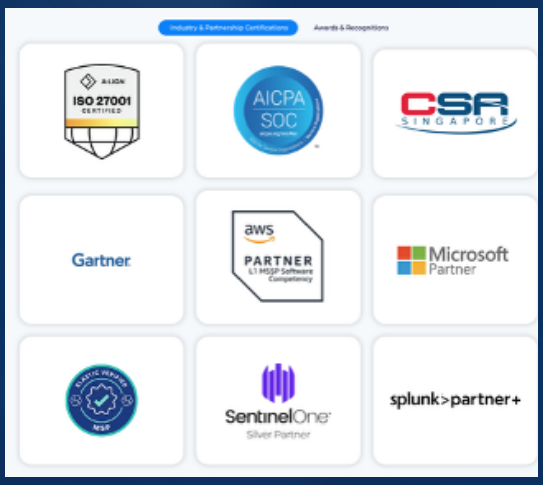
Visibilidad de seguridad completa desde el día 1:

- Elastic SIEM: Ingesta de logs por tecnología visible en tiempo real — Fortinet y Microsoft identificados como principales fuentes.
- ServiceNow: Clasificación de todos los eventos por prioridad (Bajo, Medio, Alto, Crítico) y severidad.
- Splunk: Métricas de eventos vs incidentes — mide efectividad del filtrado y correlación.
- Splunk: Tipo de ataques detectados en el período con mapeo a técnicas MITRE ATT&CK.



CASO DE ÉXITO
LOGÍSTICA

Cumplimiento y Certificaciones



Respuesta validada — Active Defense con SOAR

- Timeline de ataques por país e IP — visibilidad geográfica de amenazas activas.
- Bloqueo automatizado de IPs maliciosas sin intervención manual.
- Las pruebas de simulación de ataques confirmaron que el SOC detecta y responde dentro de SLAs.
- Tiempo de contención dramáticamente reducido vs modelo de respuesta manual anterior.

Optimización del programa — segundo año

- Depuración de fuentes de log: identificación de qué logs realmente aportan valor vs los que generan ruido.
- SOC más eficiente con menor ruido, mejor MTTD y reportes más accionables para el equipo directivo.
- Comparativo mensual de eventos — tendencia histórica visible mes a mes para el board.
- Top 3 incidentes por categoría y severidad — permite focalizar esfuerzos de remediación.

"Las pruebas de simulación de ataques confirmaron que el SOC responde. Ya no operamos a ciegas — sabemos qué está pasando, cuándo pasó y qué se hizo al respecto." ***— Equipo de TI · Empresa de logística · México***

Por qué Nuvol

- Equipo técnico estable dedicado al cliente
- Visión integral: estrategia + operación
- Servicio en español con conocimiento local
- CSM dedicado — acceso directo al experto
- Respuesta en tiempo real sin escalar tickets
- Partner certificado Proficio en MX, PA y CO

Conversemos sobre cómo Nuvol puede ser su aliado estratégico de ciberseguridad.

info@cybernuvol.com México - Panamá - Colombia +(52) 55 9124 0158