NUVOL
Cybersecurity services

CASO DE ÉXITO

Del Ruido a la Prioridad: SOC as a Service para un Banco Multi-Región

Sector Bancario | Institución Multiregión

PROFICIO™

Un banco con operaciones en múltiples regiones recibía un volumen de alertas imposible de gestionar internamente. Nuvol transformó ese ruido en inteligencia accionable — y lleva 4 años haciéndolo.

4+
Años de Servicio
Relación continua y activa

24/7
Cobertura MDR
Múltiples Regiones

Banca
Institución multi-región
Sector

El Desafío

Con operaciones distribuidas en diferentes regiones, el equipo de seguridad del banco enfrentaba un problema crítico: recibía un volumen de alertas tan alto que era imposible distinguir lo urgente de lo irrelevante. La fatiga de alertas paralizaba la respuesta efectiva ante incidentes reales, mientras que la falta de visibilidad holística impedía detectar patrones de ataque que atravesaban múltiples regiones.

- **Fatiga de alertas severa:** el equipo de seguridad recibía cientos de alertas diarias sin capacidad de triaje efectivo.
- **Sin visión holística:** cada región operaba con logs y herramientas independientes, sin correlación centralizada.
- **Incidentes críticos perdidos en el ruido:** amenazas reales se mezclaban con falsos positivos sin mecanismo de priorización.
- **Presión regulatoria multi-jurisdiccional:** el banco debía demostrar controles de seguridad ante reguladores en cada región donde operaba
- Equipo interno insuficiente para cobertura 24x7: fuera del horario laboral, la capacidad de respuesta era prácticamente nula.

La solución

Nuvol implementó SOC as a Service con Proficio, centralizando la visibilidad de seguridad de todas las regiones del banco en una plataforma unificada. El servicio incluyó tuning de casos de uso específicos para banca, reducción activa de falsos positivos y asignación de un equipo analítico dedicado con conocimiento del entorno del cliente.

Componente	Tecnología	Valor entregado
SIEM centralizado	Plataforma Proficio multi-región.	Logs de todas las regiones correlacionados en tiempo real en un único panel de control.
Triaje y priorización	Analistas Nuvol + Machine Learning	Reducción de falsos positivos y priorización de incidentes críticos para que el equipo interno actúe en lo que importa.
Casos de uso bancarios	Reglas específicas por sector	Detección de fraude, abuso de privilegios, accesos fuera de horario y movimientos laterales en entornos multi-región.
Equipo 24x7 dedicado	SOCs en San Diego, Barcelona y Singapur	Cobertura ininterrumpida con analistas que conocen el entorno del banco y escalan con criterio.

Resultados e impacto

Eliminación de la fatiga de alertas: El equipo de seguridad del banco pasó de gestionar cientos de alertas diarias a recibir únicamente los incidentes priorizados y accionables.

Visión holística por primera vez: Todas las regiones del banco centralizadas en un único panel, con correlación de eventos en tiempo real entre jurisdicciones.

Reducción de redundancias operativas: Casos de uso optimizados eliminaron las alertas duplicadas y los falsos positivos que consumían el tiempo del equipo interno.

NUVOL
Cybersecurity services

CASO DE ÉXITO
MULTIREGIÓN
BANCARIO

Equipo especializado disponible 24x7: El banco cubrió la brecha de cobertura nocturna y de fines de semana sin contratar personal adicional.

Cuatro años de servicio activo con evidencia de madurez operativa sostenida y renovación continua del contrato.

"Antes nos ahogábamos en alertas. Hoy nuestro equipo trabaja en lo que realmente importa - Nuvol y Proficio se encargan del resto."***CISO — Institución Bancaria Multi-Región, LATAM***

Por qué Nuvol

- Especialistas en detección y respuesta para el sector bancario
- Cobertura multi-región desde un único punto de gestión
- SLA de 30 minutos para incidentes críticos (P1)
- Reducción activa de falsos positivos desde las primeras semanas
- Equipo técnico senior con conocimiento profundo del entorno del cliente
- Reportes ejecutivos y operativos adaptados a cada audiencia

Servicios Detección y respuesta gestionadas:

1. **ProSOC MDR:** SOC como servicio 24/7 con tecnología SIEM alojada en Proficio
2. **ProSOC MDR para Microsoft**: Gestión de plataformas y SOC como servicio 24/7 con tecnología de Microsoft Sentinel
3. **ProSOC MDR para endpoint:** Protección contra amenazas en todos sus endpoints
4. **ProSOC MDR para Splunk:** Gestión de plataformas y SOC como servicio 24/7 con tecnología de Splunk
5. **ProSOC XDR:** Potente monitorización 24/7 SOC-as-a-Service impulsado por la plataforma SIEM

Cumplimiento y Certificaciones

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