NUVOL
Cybersecurity services

CASO DE ÉXITO

Validación Continua de Controles: 2 años midiendo la postura de seguridad real

Sector Bancario | LATAM

PICUS

Una institución financiera líder en LATAM implementó Breach and Attack Simulation con Nuvol para saber, con certeza, si sus controles realmente funcionan.

2+	6	Banca
Años de Servicio	**Controles Validados**	**Sector**
Contrato Renovado	EDR + SIEM + NGFW	Institución líder en LATAM

El Desafío

La institución contaba con un ecosistema de controles de seguridad maduro: NGFW, EDR y SIEM operativos, pero carecía de visibilidad real sobre si dichos controles funcionaban efectivamente frente a amenazas actuales.

Las evaluaciones periódicas de penetración no eran suficientes para medir la postura de seguridad de forma continua, especialmente ante un panorama de amenazas en constante evolución para el sector bancario en LATAM.

- Controles instalados pero no validados: no existía certeza de que el EDR o el SIEM generarán alertas correctas ante técnicas de ataque reales.
- Pentesting periódico insuficiente: las evaluaciones puntuales dejaban ventanas de meses sin visibilidad sobre cambios en la postura de seguridad.
- Evolución constante del threat landscape bancario: nuevos TTPs dirigidos al sector financiero en LATAM sin mecanismo de validación continua.
- Brecha entre herramientas y efectividad real: inversiones significativas en tecnología sin métricas objetivas de su rendimiento operativo.

La solución

Nuvol implementó Picus Security BAS (Breach and Attack Simulation) sobre la infraestructura de controles existente del banco, integrando validación continua y automatizada al ciclo operativo del equipo de seguridad.

Componente	Tecnología	Valor entregado
Validación de controles	Picus SCV - Security Control Validation	Validación continua sobre EDR, SIEM y NGFW contra técnicas MITRE ATT&CK; reales.
Simulación automatizada	Campañas recurrentes por perfil de riesgo bancario	Malware, movimientos laterales, abuso de credenciales y phishing dirigido simulados de forma recurrente.
Detección de brechas	Módulo de detección Picus	Verifica que el SIEM genera alertas correctas ante cada técnica simulada — no solo que bloquea.
Ciclo de remediación	Integración con flujo interno del banco	Hallazgos priorizados, remediación aplicada y re-validación automática tras cada corrección.

Resultados e impacto

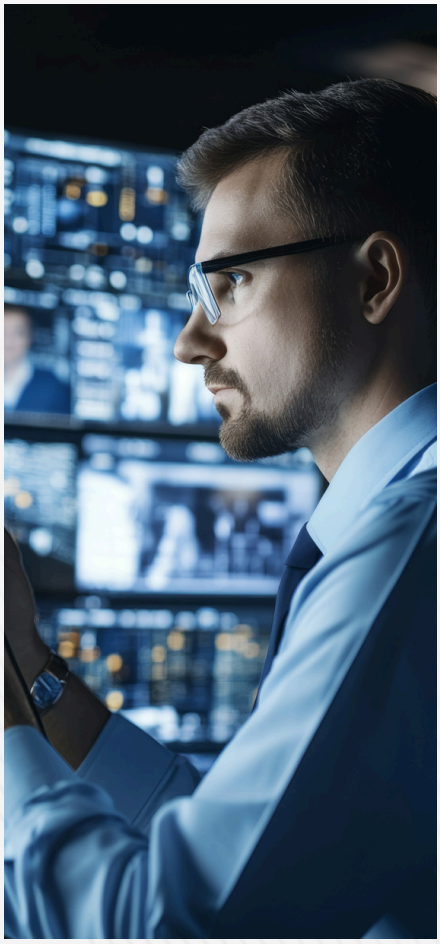
Visibilidad real por primera vez: Técnicas de ataque conocidas que lograban evadir los controles fueron identificadas y documentadas — riesgos que el banco no tenía en su radar de prioridades.

Postura de seguridad medible y en mejora continua: A lo largo de los 2 años de servicio, el equipo de seguridad cuenta con métricas objetivas de evolución — no percepciones, sino datos.

Ciclo de remediación cerrado: Cada hallazgo genera una acción correctiva re-validada automáticamente, eliminando la incertidumbre sobre si el fix realmente funcionó.

Dos años de servicio ininterrumpido con alta satisfacción del equipo de seguridad, contrato renovado y expansión del alcance de los módulos activos.

Alineación a MITRE ATT&CK: Las simulaciones están mapeadas al framework estándar de la industria, facilitando la comunicación de riesgo con la Junta Directiva y auditores externos.



NUVOL
Cybersecurity services

"Finalmente tenemos certeza de que nuestros controles no solo están instalados — sabemos. que funcionan. Picus cambió cómo medimos la seguridad."

Gerente de Seguridad Informática — Institución Financiera, LATAM

Por qué Nuvol

- Especialistas certificados en Picus Security para LATAM
- Equipo técnico senior dedicado durante toda la relación
- Visión integral: validación + remediación + métricas ejecutivas
- Implementación sin disrupción sobre controles existentes
- Integración directa con el flujo operativo del cliente
- Acceso directo al experto — sin intermediarios ni rotación

¿Qué hace Picus BAS?

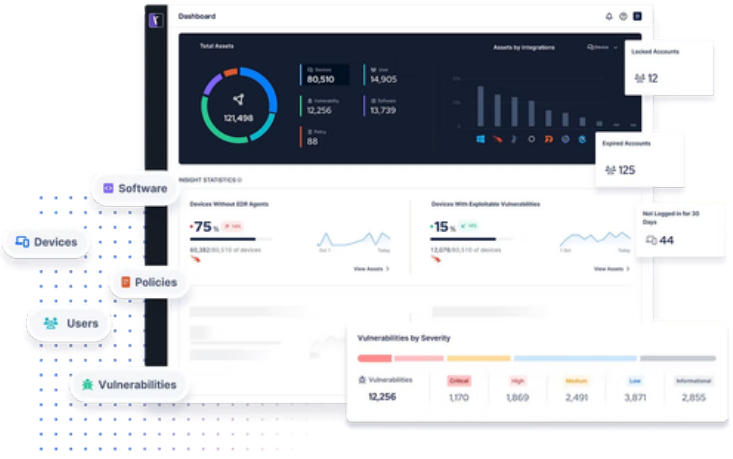
Simula ataques reales: Ejecuta miles de simulaciones de amenazas y técnicas de ataque para verificar si los controles de seguridad funcionan correctamente.

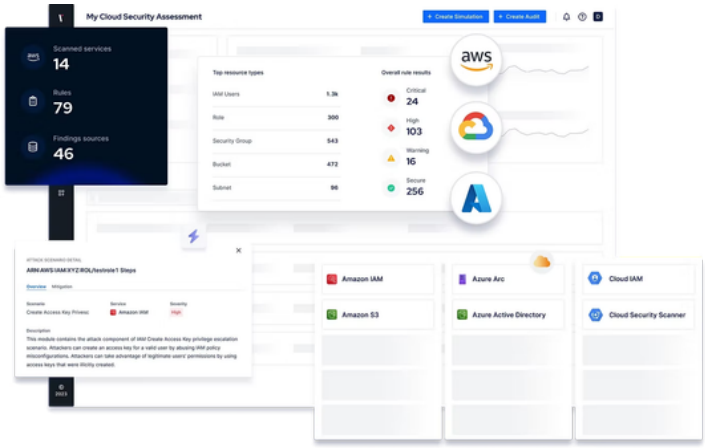
Válida controles de seguridad: Asegura que las herramientas de prevención y detección, como firewalls y sistemas de detección de intrusos, estén bien configuradas y sean efectivas.

Identifica brechas de seguridad: Permite encontrar vulnerabilidades y configuraciones erróneas en la nube y en el entorno de red antes de que sean explotadas por atacantes.

Valida la efectividad de las reglas de detección: Ayuda a los equipos de seguridad a mantenerse al día con la línea base de sus reglas de detección y automatiza los procesos de ingeniería.

Visualiza rutas de ataque: Muestra los pasos que un atacante podría seguir para comprometer los sistemas, revelando los puntos más críticos para el riesgo





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