Integración Avanzada de SDK

En esta sección se describen los campos adicionales necesarios para mejorar significativamente el rendimiento de la detección de fraudes, reducir los falsos positivos y fortalecer la capacidad de identificar actividades fraudulentas donde los atacantes no utilizan aplicaciones legítimas. Esta implementación representa una evolución crítica en la arquitectura de seguridad, proporcionando mayor granularidad en el análisis de comportamiento y patrones de uso.

Campos Requeridos

Para optimizar la eficacia del sistema de detección de fraudes, se deben agregar los siguientes campos a las llamadas de API:

Campo	Tipo	Descripción	Propósito de Seguridad	Ejemplo
Dirección IP	String	Dirección IP de origen de la sesión	Geolocalización, detección de VPN/Proxy, análisis de patrones geográficos	`192.168.1.100`
Fuente del dispositivo	Enum	Tipo de plataforma desde la cual se origina la petición	Identificación de canales no autorizados, detección de automatización	`android`, `ios`, `js`, `web`
ID del dispositivo	String	Identificador único y persistente del dispositivo	Tracking de dispositivos, detección de device spoofing	`abc123def456`
Beneficiario	String (Hash)	Objetivo de transferencia hasheado por seguridad	Análisis de patrones de transferencia, detección de mulas	`SHA256(account_id)`
Monto	Decimal	Cantidad de la transacción en moneda local	Detección de patrones de monto, análisis de velocidad	`1500.50`
Motivo de la API	Enum	Propósito específico de la llamada API	Contextualización del riesgo por tipo de operación	`login`, `transfer`, `register`

Campo	Tipo	Descripción	Propósito de Seguridad	Ejemplo
Tipo de transferencia	Enum	Categoría de operación financiera	Aplicación de reglas específicas por tipo de transferencia	`local`, `plin`, `international`

Beneficios de la Implementación

Esta integración avanzada proporcionará mejoras sustanciales en múltiples aspectos:

1. **Detección de Scripts Automatizados**

- Identificación precisa de sesiones que no provienen de aplicaciones legítimas
- Análisis de patrones de comportamiento no humano
- Reducción de ataques de fuerza bruta y automatización maliciosa

2. **Resolución de Problemas de CSID**

- Mejora significativa en la identificación de sesiones no encontradas
- Reducción de errores de tracking y seguimiento
- Mayor precisión en la correlación de eventos

3. **Reducción Drástica de Falsos Positivos**

- Mayor precisión en la detección mediante análisis contextual
- Refinamiento de modelos de machine learning con datos enriquecidos
- Optimización de umbrales de riesgo basados en contexto

4. **Identificación de Cuentas de Riesgo**

- Capacidad para detectar patrones sospechosos cross-account
- Análisis de redes de cuentas relacionadas
- Identificación temprana de esquemas de lavado de dinero

5. **Mejora en Debugging y Monitoreo**

- Facilita la resolución de problemas de integración
- Trazabilidad completa de transacciones
- Análisis forense mejorado para investigaciones

Funcionalidades Avanzadas de Detección de Fraudes

1. **Detección de Cuentas Mula**

Requiere añadir dos parámetros a las solicitudes que ya se envían al servidor: el monto de la transacción y el destino de la transacción (así como el tipo de transacción – transferencia nacional, internacional, P2P, etc.).

El resultado incluye:

- Una tabla de cuentas de alto riesgo
- Un gráfico 3D que muestra las conexiones entre las transferencias

Parámetro	Tipo	Descripción	Impacto
Monto de transacción	Decimal	Valor monetario de la operación	Detección de patrones de lavado
Destino de transacción	String (Hash)	Cuenta beneficiaria hasheada	Identificación de redes de mulas
Tipo de transacción	Enum	Categoría de operación financiera	Aplicación de reglas específicas

2. **Estafa por Voz**

Sistema que permite identificar si la llamada que recibió el cliente es del banco o no. Requiere integración con el servidor del banco.

Características:

- Verificación en tiempo real de llamadas entrantes
- Validación de números autorizados del banco
- Alertas inmediatas sobre llamadas sospechosas

3. **Detección de Malware Mediante Métodos Adicionales**

Objetivo: Reducir los falsos positivos

a. Detección de software malicioso que ya se ha comprobado que ha afectado al banco

b. Integración con un servicio verificado de Google para la detección de virus

Método	Descripción	Precisión Esperada
Firma conocida	Detección de malware previamente identificado	95-98%
Google Safe Browsing	Integración con servicio de Google	92-95%
Análisis comportamental	Detección de patrones maliciosos	85-90%

4. **Recepción de Información desde Redes Sociales**

Requiere que el banco agregue en algún lugar de la aplicación una opción como "Compartir por WhatsApp". Entonces, Google acepta recibir información sobre la cuenta de WhatsApp del usuario. Esto puede ayudar a detectar ataques de una persona específica con una tasa baja de falsos positivos.

Ventajas:

- Correlación cross-platform de identidades
- Reducción significativa de falsos positivos
- Detección de ataques de ingeniería social

5. **Sistema de Alertas**

Envía una alerta inmediata cuando hay un fraude confirmado (Falsos Positivos = 0)

La alerta puede enviarse por:

Canal	Tipo	Tiempo de Respuesta	Casos de Uso
A. Push Notification	Tiempo real	< 1 segundo	Monitoreo activo
B. Grupo WhatsApp	Inmediato	< 5 segundos	Equipos de respuesta
C. Correo electrónico	Inmediato	< 30 segundos	Documentación
D. Microsoft Teams	Tiempo real	< 3 segundos	Colaboración

Métricas de Impacto Esperadas

Antes vs Después de la Implementación

Métrica	Antes	Después	Mejora
Falsos Positivos	15-20%	5-8%	60-70% reducción
Detección de Fraudes	75-80%	90-95%	15-20% mejora
Tiempo de Respuesta	24-48 horas	1-5 minutos	99% mejora
Precisión General	82%	94%	12% mejora

Revision #4
Created 3 July 2025 16:18:42 by roger de avila
Updated 3 July 2025 17:34:32 by roger de avila