

# Métricas Principales (Top Row)

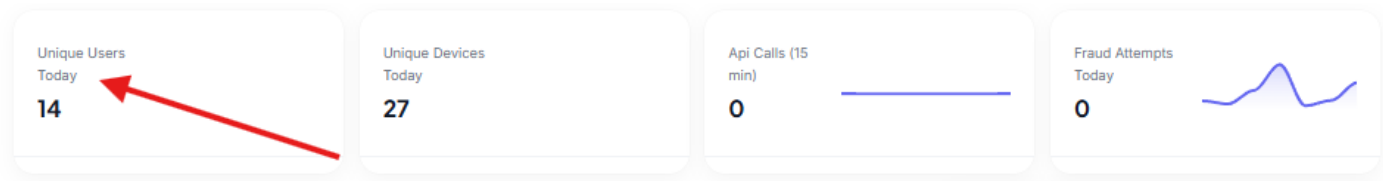
El Dashboard ADO-STS está estructurado en **3 secciones principales** que proporcionan una vista integral del estado de seguridad:

## SECCIÓN 1: MÉTRICAS PRINCIPALES

### Ubicación en Dashboard

**Parte superior del dashboard** - Cuatro indicadores principales mostrados como tarjetas de KPIs

#### 1.1 Unique Users Today



**¿Qué muestra?** Número total de usuarios únicos que han iniciado sesión en el sistema durante las últimas 24 horas.

#### ¿Para qué sirve?

- Monitorear el volumen de actividad diaria de usuarios
- Detectar picos anómalos de actividad que podrían indicar ataques masivos
- Establecer líneas base de actividad normal

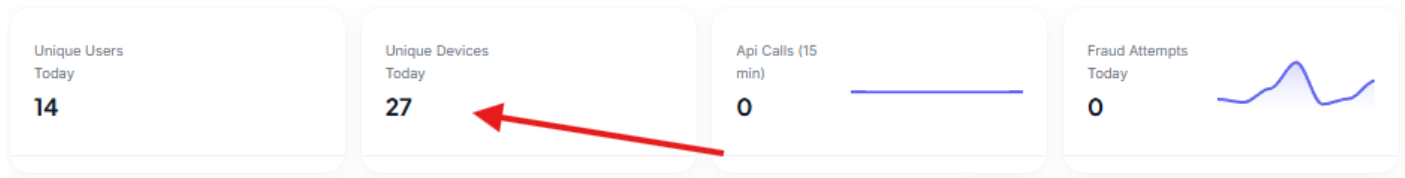
#### ¿Cómo interpretarlo?

Escenario	Interpretación	Acción Requerida
Valor muy bajo	Posible problema técnico o día festivo	Verificar sistema y calendario
Valor normal	Operación estándar según patrones históricos	Continuar monitoreo
Pico súbito	Posible ataque DDoS o evento promocional	Investigar causa y preparar escalamiento

#### Factores que influyen en esta métrica:

- Horarios comerciales y días de la semana
- Campañas promocionales o marketing
- Eventos especiales o lanzamientos
- Ataques coordinados o actividad bot

## 1.2 Unique Devices Today



**¿Qué muestra?** Cantidad de dispositivos únicos (identificados por device fingerprint) que han accedido al sistema en las últimas 24 horas.

**¿Para qué sirve?**

- Identificar el uso de múltiples dispositivos por usuario
- Detectar device farming (granjas de dispositivos)
- Monitorear la diversidad tecnológica de los usuarios

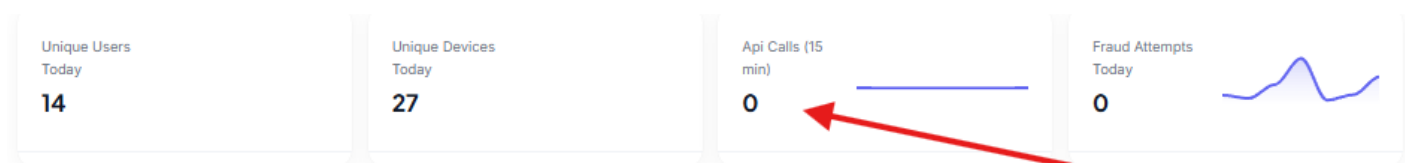
**¿Cómo interpretarlo?**

Relación Dispositivos/Usuarios	Significado	Nivel de Atención
Cerca de 1:1	Usuarios con dispositivo único	Normal
Mayor a 2:1	Uso multi-dispositivo o sharing	Monitoreo adicional
Muy alta (>5:1)	Posible device farming o bots	Investigación inmediata

**Lo que nos ayuda a identificar:**

- Usuarios que comparten dispositivos
- Actividad de bots usando múltiples dispositivos emulados
- Patrones de uso legítimo multi-dispositivo (BYOD)

## 1.3 Api Calls T5 min



**¿Qué muestra?** Número total de llamadas API realizadas al sistema ADO-STs en los últimos 5 minutos.

**¿Para qué sirve?**

- Monitorear la carga del sistema en tiempo real
- Detectar picos de actividad automatizada
- Evaluar el performance del sistema

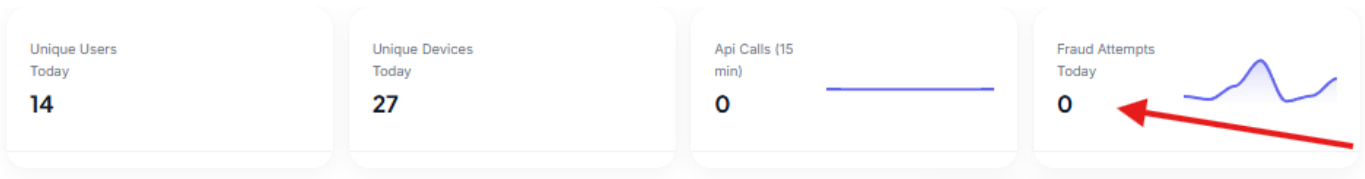
¿Cómo interpretarlo?

Volumen de Calls	Estado del Sistema	Acción
0-1,000	Actividad baja	Monitoreo normal
1,001-5,000	Actividad normal	Operación estándar
5,001-15,000	Actividad alta	Monitoreo de capacidad
>15,000	Sobrecarga potencial	Activar auto-scaling

Tipos de llamadas que incluye:

- Inicialización de sesiones
- Análisis de comportamiento en tiempo real
- Evaluaciones de riesgo
- Enriquecimiento de datos

1.4 Fraud Attempts Today



¿Qué muestra? Número de intentos de fraude detectados y bloqueados en las últimas 24 horas.

¿Para qué sirve?

- Medir la efectividad del sistema de detección
- Identificar tendencias de actividad fraudulenta
- Evaluar el nivel de amenaza diario

¿Cómo interpretarlo?

Número de Intentos	Evaluación	Consideraciones
0-10	Día tranquilo o excelente detección	Verificar que el sistema esté funcionando
11-50	Actividad fraudulenta normal	Monitoreo estándar
51-200	Actividad alta	Investigar patrones comunes
>200	Posible ataque coordinado	Activar protocolos de emergencia

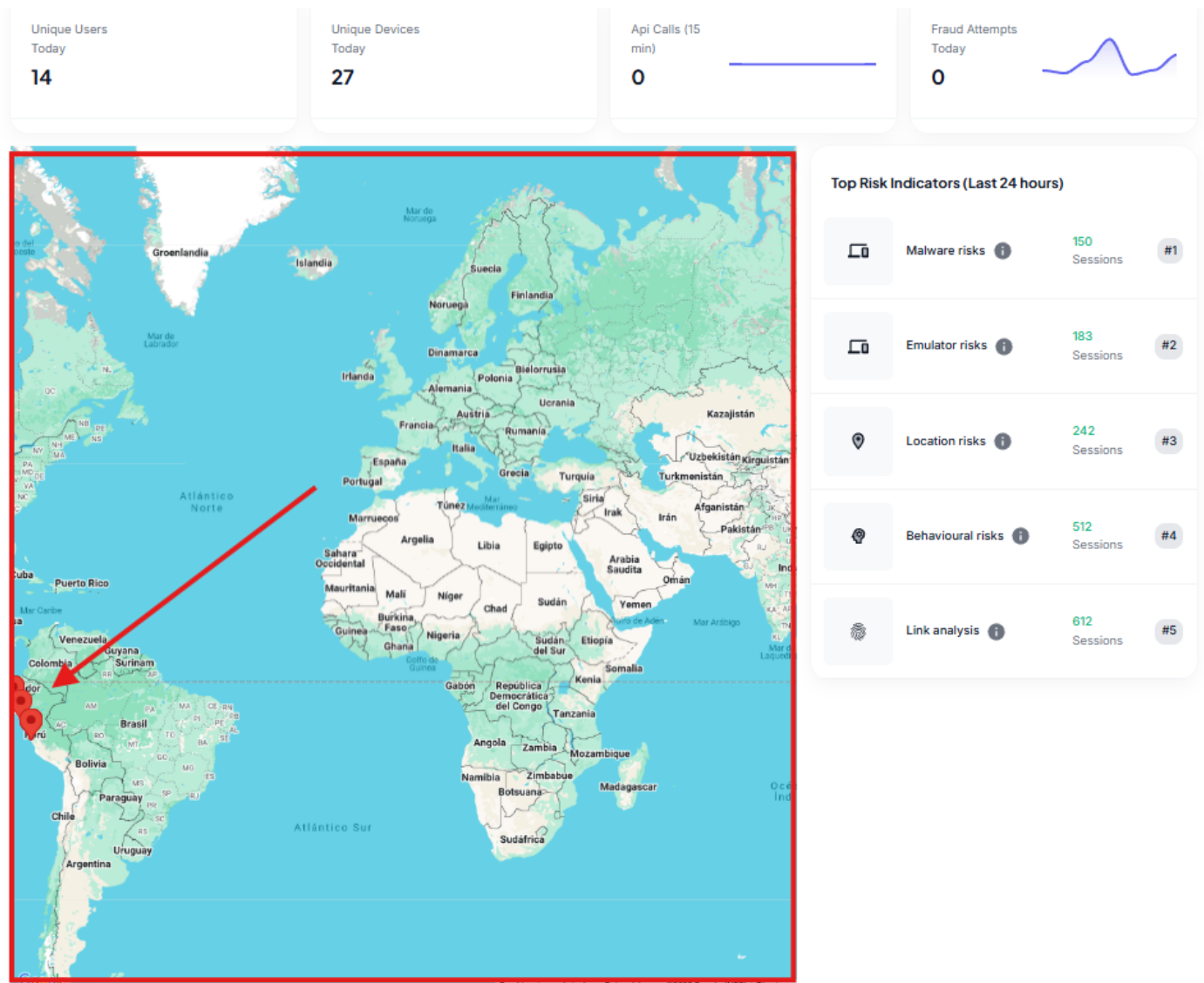
## Lo que cuenta como "intento de fraude":

- Sesiones con score de riesgo alto (>800)
- Actividad bloqueada automáticamente
- Casos confirmados manualmente por analistas

## SECCIÓN 2: VISUALIZACIÓN GEOGRÁFICA

### Ubicación en Dashboard

**Centro del dashboard** - Mapa mundial interactivo que ocupa la mayor parte de la pantalla



### ¿Qué muestra el mapa?

#### Representación visual de:

- Ubicación geográfica de todas las sesiones activas
- Distribución global de la actividad del sistema

- Concentraciones de riesgo por regiones
- Patrones de movimiento anómalos

## Elementos visuales en el mapa

Elemento	Descripción	Significado
Puntos de colores	Marcadores en ubicaciones específicas	Sesiones individuales con nivel de riesgo
Densidad de puntos	Concentración de marcadores	Volumen de actividad por zona
Líneas conectoras	Conexiones entre ubicaciones	Posibles viajes imposibles o conexiones sospechosas

## ¿Para qué sirve?

### Análisis geográfico para:

- **Detectar viajes imposibles:** Usuarios que aparecen en ubicaciones muy distantes en poco tiempo
- **Identificar hotspots de fraude:** Concentraciones anómalas de actividad sospechosa
- **Validar coherencia geográfica:** Verificar que la ubicación sea consistente con otros datos
- **Monitorear actividad global:** Tener vista panorámica de la operación mundial

## ¿Cómo interpretarlo?

### Patrones normales:

- Distribución uniforme según la base de usuarios
- Concentraciones en centros urbanos principales
- Actividad coherente con zonas horarias

### Patrones anómalos:

- Concentraciones súbitas en ubicaciones inusuales
- Múltiples sesiones desde coordenadas idénticas
- Saltos geográficos imposibles en tiempos cortos

# Funcionalidades interactivas

Función	Propósito	Caso de Uso
Zoom	Análisis detallado por región	Investigar actividad específica de una ciudad

Función	Propósito	Caso de Uso
Filtros temporales	Ver evolución histórica	Analizar patrones de ataque en el tiempo
Capas de información	Superponer diferentes tipos de datos	Correlacionar riesgo con ubicación

## SECCIÓN 3: TOP RISK INDICATORS (ÚLTIMAS 24 HORAS)

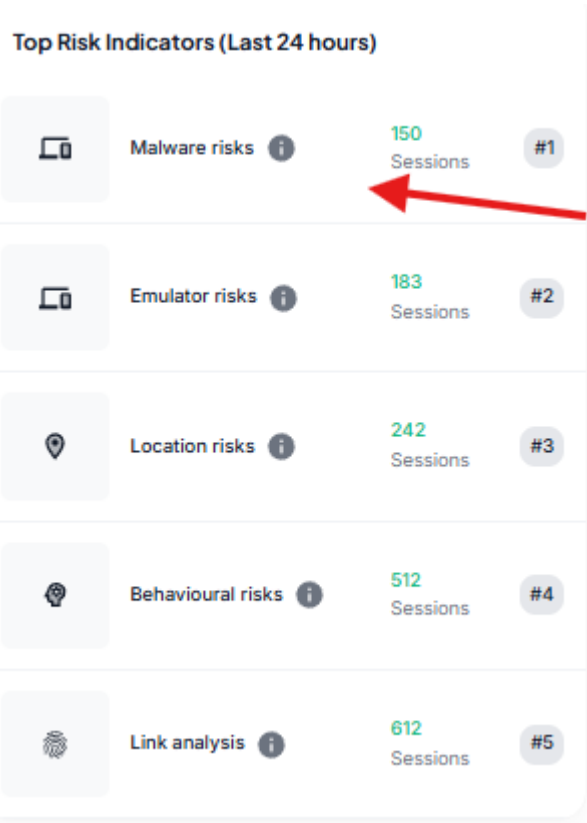
### Ubicación en Dashboard

**Panel lateral derecho** - Lista de los principales indicadores de riesgo detectados

¿Qué muestra esta sección?

**Lista priorizada de los principales riesgos detectados en las últimas 24 horas, incluyendo:**

### 3.1 Malware Risks



**¿Qué detecta?** Presencia de software malicioso en los dispositivos de los usuarios que acceden al sistema.

**¿Para qué sirve?**

- Identificar dispositivos comprometidos

- Prevenir el uso de credentials robadas
- Detectar keyloggers y screen scrapers

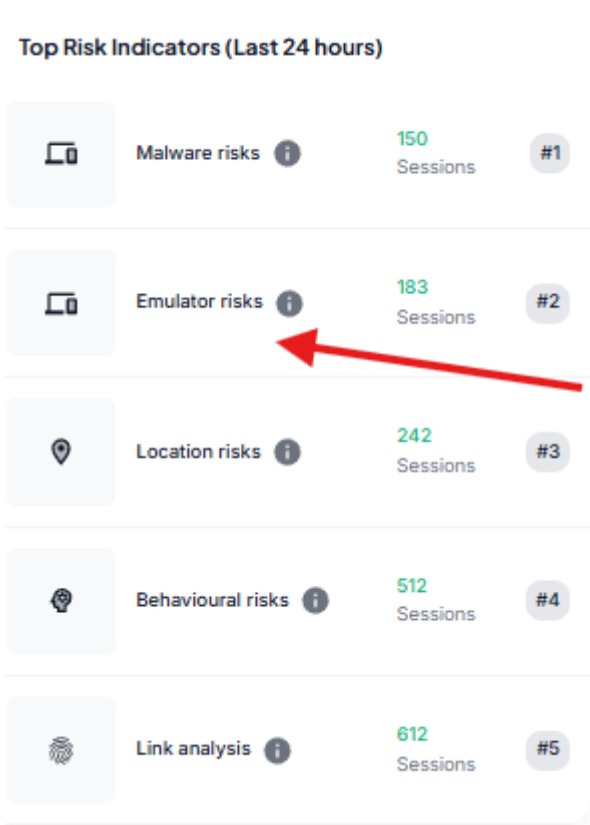
### ¿Cómo se presenta?

- Número de dispositivos con malware detectado
- Ranking por nivel de peligrosidad
- Tipos de malware más frecuentes

### Información que proporciona:

- Cantidad de detecciones de malware
- Tipos específicos encontrados (trojans bancarios, keyloggers, etc.)
- Dispositivos afectados y usuarios en riesgo

## 3.2 Emulator Risks



**¿Qué detecta?** Dispositivos emulados o virtualizados que pueden estar siendo utilizados para actividades fraudulentas.

### ¿Para qué sirve?

- Detectar device farming automatizado
- Identificar bots sofisticados
- Prevenir ataques masivos coordinados

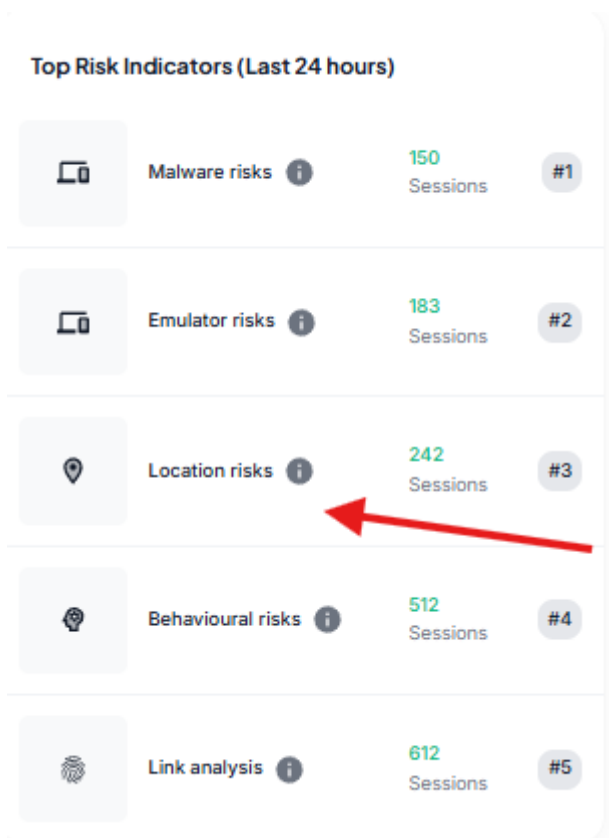
### ¿Cómo se presenta?

- Número de emuladores detectados
- Nivel de confianza en la detección
- Patrones de uso sospechosos

#### Indicadores que analiza:

- Inconsistencias en hardware reportado
- Patrones de sensores anómalos
- Características de virtualización

### 3.3 Location Risks



**¿Qué detecta?** Riesgos asociados con la ubicación geográfica y patrones de movimiento de los usuarios.

#### ¿Para qué sirve?

- Detectar viajes imposibles
- Identificar ubicaciones de alto riesgo
- Validar coherencia geográfica

#### ¿Cómo se presenta?

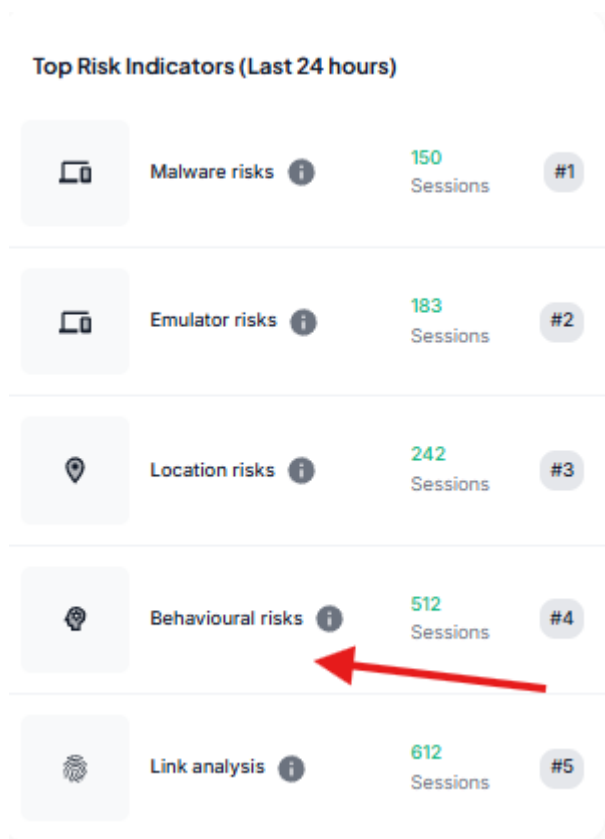
- Número de ubicaciones sospechosas
- Casos de viajes imposibles detectados
- Concentraciones anómalas por región



### Tipos de riesgos que identifica:

- Velocidades de viaje físicamente imposibles
- Ubicaciones en países de alto riesgo
- Inconsistencias entre IP y GPS
- Uso de VPNs o proxies para enmascarar ubicación

## 3.4 Behavioural Risks



**¿Qué detecta?** Patrones de comportamiento anómalos que no coinciden con el perfil normal del usuario o comportamiento humano típico.

### ¿Para qué sirve?

- Detectar account takeover (toma de cuentas)
- Identificar actividad automatizada (bots)
- Reconocer cambios súbitos en patrones de uso

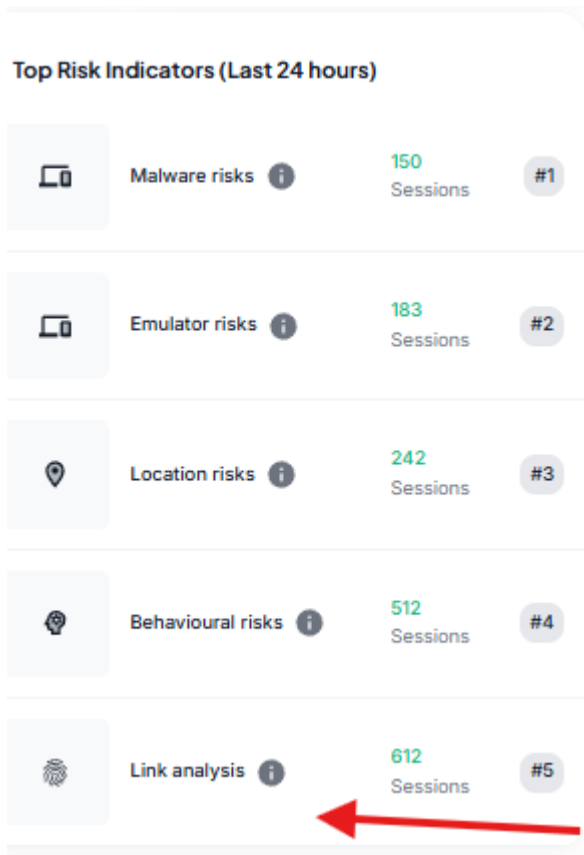
### ¿Cómo se presenta?

- Número de anomalías comportamentales
- Usuarios con cambios significativos en patrones
- Actividad que sugiere automatización

### Aspectos que monitorea:

- Cambios en velocidad de escritura
- Patrones de movimiento del mouse/touch anómalos
- Secuencias de navegación inconsistentes
- Timing no humano entre acciones

### 3.5 Link Analysis



**¿Qué detecta?** Conexiones y relaciones sospechosas entre usuarios, dispositivos, ubicaciones y comportamientos.

**¿Para qué sirve?**

- Identificar redes de fraude organizadas
- Detectar dispositivos compartidos sospechosamente
- Encontrar patrones ocultos de coordinación

**¿Cómo se presenta?**

- Número de conexiones sospechosas identificadas
- Redes de usuarios/dispositivos relacionados
- Patrones de coordinación detectados

**Tipos de conexiones que analiza:**

- Múltiples usuarios usando el mismo dispositivo
- Dispositivos conectados a las mismas redes WiFi/Bluetooth

- Patrones de comportamiento idénticos entre usuarios diferentes
- Secuencias de acceso coordinadas temporalmente

## Interpretación de cada indicador

Indicador	Valor Normal	Valor de Alerta	Acción Recomendada
Malware Risks	0-5 detecciones/día	>20 detecciones/día	Investigar dispositivos afectados
Emulator Risks	0-10 detecciones/día	>50 detecciones/día	Reforzar validación de dispositivos
Location Risks	0-15 casos/día	>100 casos/día	Revisar reglas geográficas
Behavioural Risks	0-20 anomalías/día	>200 anomalías/día	Ajustar modelos de comportamiento
Link Analysis	0-5 redes/día	>25 redes/día	Investigación de fraude organizado

## ¿Cómo usar esta información?

**Para priorización:** Los indicadores se ordenan por:

- Número de casos detectados
- Nivel de riesgo promedio
- Tendencia de crecimiento en las últimas horas

**Para investigación:** Cada indicador puede expandirse para mostrar:

- Casos específicos más relevantes
- Detalles de los usuarios/dispositivos afectados
- Recomendaciones de acción específicas

**Para reportes:** Esta sección proporciona un resumen ejecutivo de:

- Los principales tipos de amenaza del día
- Volumen de cada tipo de riesgo
- Tendencias comparativas con días anteriores

## Navegación e Interacción

### Funcionalidades del Dashboard

Elemento	Interactividad	Propósito
Métricas Principales	Click para detalles expandidos	Ver tendencias históricas y breakdowns

Elemento	Interactividad	Propósito
Mapa Geográfico	Zoom, filtros, overlays	Análisis geográfico detallado
Risk Indicators	Click para lista detallada	Investigar casos específicos

## Actualizaciones automáticas

Sección	Frecuencia de Actualización	Indicador Visual
Métricas Principales	Cada 30 segundos	Timestamp en pantalla
Mapa Geográfico	Cada 60 segundos	Pulso en nuevos eventos
Risk Indicators	Cada 5 minutos	Badge de "actualizado"

## Interpretación Integral del Dashboard

### ¿Qué nos dice un dashboard "saludable"?

- **Métricas principales:** Valores dentro de rangos históricos normales
- **Mapa geográfico:** Distribución esperada según base de usuarios
- **Risk indicators:** Números bajos y consistentes con tendencias históricas

### ¿Qué nos dice un dashboard "en alerta"?

- **Métricas principales:** Picos súbitos o valores inusualmente bajos
- **Mapa geográfico:** Concentraciones anómalas o patrones irregulares
- **Risk indicators:** Incrementos significativos en cualquier categoría

## Correlaciones importantes a observar

Correlación	Interpretación	Acción
Alto volumen de users + muchos emulators	Posible ataque bot masivo	Activar contramedidas automatizadas
Picos en API calls + location risks	Ataques desde múltiples ubicaciones	Revisar reglas geográficas
Behavioral risks + link analysis altos	Red organizada de fraude	Investigación profunda coordinada