

Resumen

El Módulo de Resumen es el apartado principal que presenta una evaluación completa y consolidada de todos los riesgos asociados a una sesión específica. Proporciona una vista integral que combina múltiples análisis para determinar la autenticidad y nivel de riesgo de la interacción del usuario.

COUNTRY	DATE	SCORE	USER	CSID	DURATION	BRAND	CHANNEL	ISP	KNOWN DEVICE	IP	IP AGE	IP COUNTRY AGE	USERS ON MUID TW	DEVICE AGE	USER AGE	CONTEXT
	30/6/2025, 18:20:20	994	UNPROTECTED_167397343	87c5989b-e588-4fc7-8881-ba50b1795bf2	211	SMP	samsung exynos9611 (ANDROID)	SLINC	✗	66.85.52.56	0	0	0	0	147	AUTH_PAGE,LOGIN,LOGIN_PASSWORD,TRANSPRO_ORIGEN
	30/6/2025, 10:30:57	994	UNPROTECTED_3CE8800337	33de322e-e659-4285-a160-b4ae942d736b	75	SMP	Emulator (IOS)	WI-NET TELECOM S.A.C.	✗	38.25.16.17	0	0	0	0	214	AUTH_PAGE,LOGIN,LOGIN_PASSWORD,OPERACIONES,TRANSFEREN
	26/6/2025, 11:55:02	933	UNPROTECTED_117916500	cfe31330-31b0-48a4-a2dc-486dbdc0284b	1730		Emulator (ANDROID)	Datacamp Limited	✗	102.38.199.7	0	0	0	0	263	
	26/6/2025, 11:55:02	895	UNPROTECTED_117916500	cfe31330-31b0-48a4-a2dc-486dbdc0284b	2695		Emulator (ANDROID)	Datacamp Limited	✗	102.38.199.7	0	0	0	0	263	

Device Risks

85

845

Fraud

Location Risks

87

865

Fraud

Behavioural Risks

68

684

Data collection phase

Integrated Score

99

994

NAME	VALUE	AGE	COUNTER	RELATIVE PREVALENCE	INDICATION STRENGTH
ua browser family	Interbank%20UAT	214	1	0.0%	1000
c network		214	1	2.1%	168
language	es	214	1	98.1%	1
ua os family	iOS	214	1	100.0%	0
Show More					
NAME	VALUE	FRAUD COUNTER	RELATIVE PREVALENCE	INDICATION STRENGTH	
Show More					

AUTH,LOGIN,LOGIN_PASSWORD

UserID UNPROTECTED_3CE8800337	Session ID 1751297457...	Device age 0	Users on this device (last week) 0
Device type iOS-Device	Browser Interbank%20UAT	Device First appearance Date 2025-06-30,15:30:57	Device Source IOS
Timezone America/Lima	MUID 1751297457...	Platform iOS 0	Brand SMP

DEVICE RISKS

Qué significa: Evalúa todos los riesgos relacionados con el dispositivo físico utilizado para acceder a la plataforma.

Valor mostrado: 85/845 Fraud

- 85: Score de riesgo del dispositivo en escala 0-100
- 845: Número total de casos de fraude detectados previamente con características de dispositivo similares

Parámetros que analiza:

- Modelo, marca y especificaciones del dispositivo
- Sistema operativo y versión
- Configuraciones de seguridad del dispositivo
- Identificadores únicos (IMEI, MAC address, etc.)
- Historial de actividad fraudulenta del dispositivo
- Configuraciones sospechosas o modificaciones
- Presencia de software malicioso o herramientas de hacking
- Edad del dispositivo en la plataforma

Cómo contribuye al Integrated Score: Aporta aproximadamente 25-30% del peso total al score final. Un dispositivo con alto riesgo puede elevar significativamente el score integrado.

LOCATION RISKS

Qué significa: Analiza todos los aspectos relacionados con la ubicación geográfica y contexto de red desde donde se realiza el acceso.

Valor mostrado: 87/865 Fraud

- 87: Score de riesgo geográfico en escala 0-100
- 865: Casos de fraude asociados a patrones de ubicación similares

Parámetros que analiza:

- Coordenadas GPS versus geolocalización por IP
- Zona horaria configurada versus zona horaria real
- Proveedor de servicio de Internet (ISP)
- Tipo de red (celular, WiFi, VPN)
- Velocidad de desplazamiento imposible entre sesiones
- Ubicaciones inusuales para el usuario
- Países o regiones de alto riesgo
- Consistencia entre ubicación declarada y técnica
- Historial de ubicaciones del usuario

Cómo contribuye al Integrated Score: Representa aproximadamente 20-25% del peso en el cálculo final. Ubicaciones anómalas o de alto riesgo incrementan el score integrado.

BEHAVIOURAL RISKS

Qué significa: Mide los patrones de comportamiento del usuario durante la interacción con la plataforma para detectar anomalías.

Valor mostrado: 68/684 Data collection phase

- 68: Score de riesgo comportamental en escala 0-100
- 684: Indica que está en fase de recolección de datos comportamentales

Parámetros que analiza:

- Velocidad y ritmo de escritura (keystroke dynamics)
- Patrones de movimiento del mouse o gestos táctiles
- Presión aplicada en pantallas táctiles
- Tamaño del área de contacto del dedo
- Tiempo entre acciones y clicks
- Patrones de navegación únicos del usuario
- Secuencia de interacciones con la interfaz
- Movimientos del dispositivo durante el uso (acelerómetro)
- Comparación con perfil comportamental histórico del usuario

Cómo contribuye al Integrated Score: Aporta aproximadamente 20-25% del peso total. Comportamientos que no coinciden con el perfil del usuario legítimo aumentan el score de riesgo.

INTEGRATED SCORE

Qué significa: Es el score final consolidado que combina todos los análisis anteriores mediante algoritmos de inteligencia artificial para proporcionar una evaluación unificada del riesgo.

Valor mostrado: 99/994

- 99: Score simplificado en escala 0-100
- 994: Score detallado en escala extendida 0-1000

Cómo se calcula el Integrated Score:

Componentes principales (75-80% del peso):

- Device Risks: 25-30%
- Location Risks: 20-25%
- Behavioural Risks: 20-25%

Componentes adicionales (20-25% del peso):

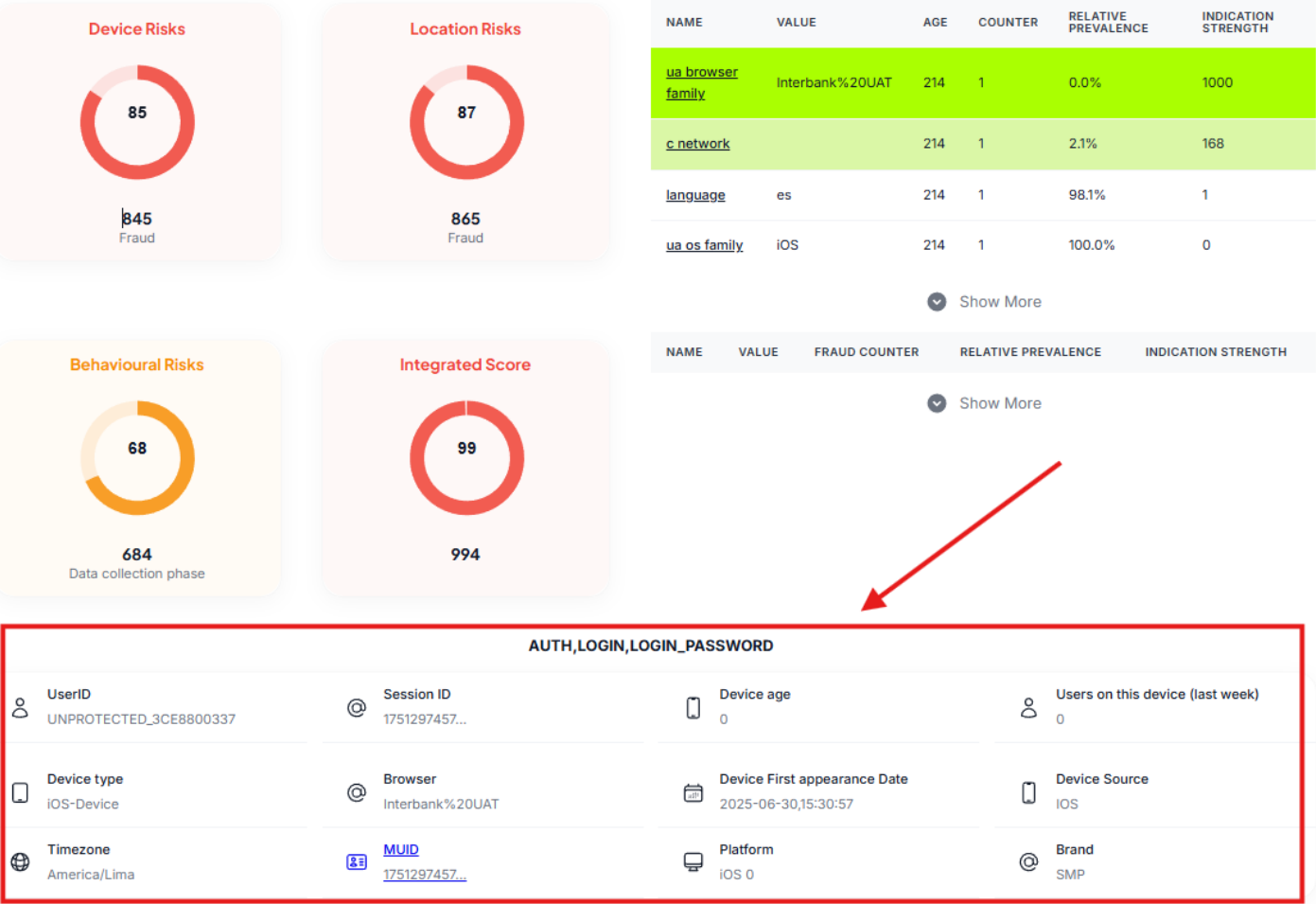
- Modelos de detección de malware: 5-8%
- Detección de bots: 5-8%

- Análisis de riesgo por actividad: 5-7%
- Análisis relacional y conexiones: 5-7%

Proceso de cálculo:

1. Cada componente genera su score individual
2. La IA aplica pesos dinámicos según el contexto
3. Se ejecutan modelos adicionales especializados
4. Se realiza análisis relacional con otras sesiones
5. Se aplica el modelo de machine learning final
6. Se genera el score integrado unificado

Escalas de interpretación: Cálculo del score de riesgo



Tipo de operación: AUTH,LOGIN,LOGIN_PASSWORD

UserID: UNPROTECTED_3CE8800337

Session ID: 1751297457

Device age: 0 (dispositivo completamente nuevo)

Users on this device: 0 (primer usuario en este dispositivo)

Características técnicas:

Device type: iOS-Device

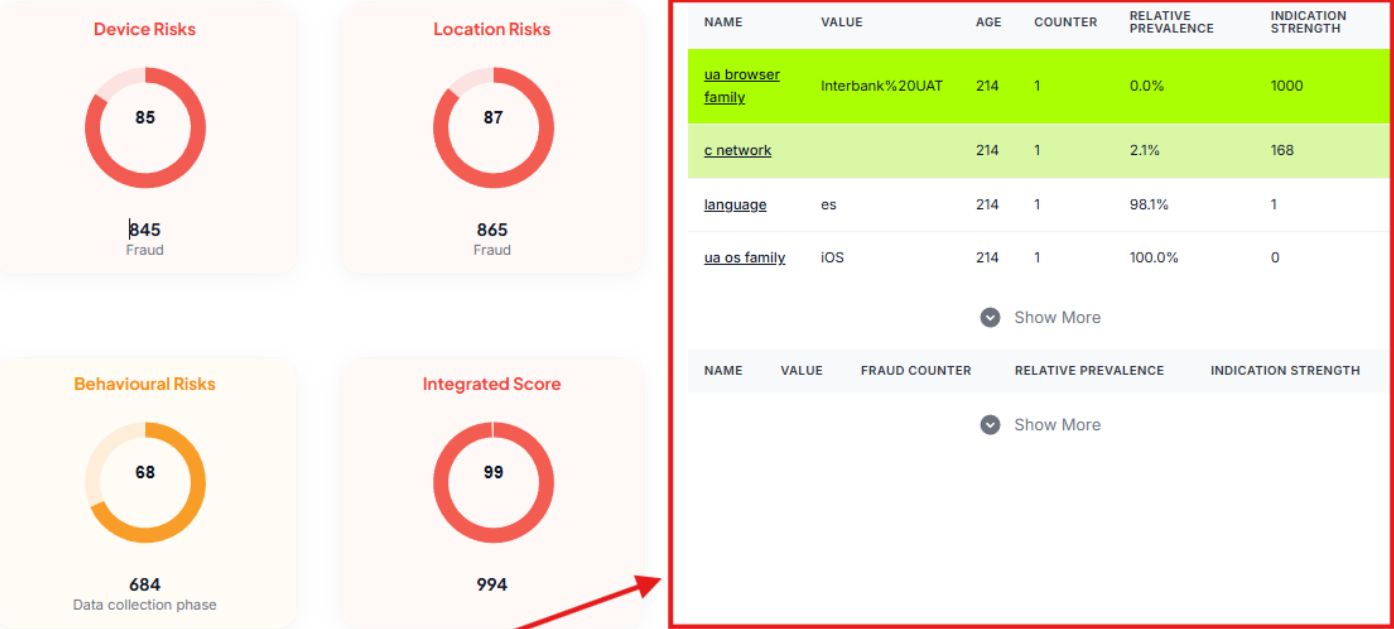
Browser: Interbank%20UAT (altamente sospechoso)

Timezone: America/Lima

Platform: iOS 0

Brand: SMP

Device First appearance: 2025-06-30,15:30:57



AUTH,LOGIN,LOGIN_PASSWORD

UserID UNPROTECTED_3CE8800337	Session ID 1751297457...	Device age 0	Users on this device (last week) 0
Device type iOS-Device	Browser Interbank%20UAT	Device First appearance Date 2025-06-30,15:30:57	Device Source IOS
Timezone America/Lima	MUID 1751297457...	Platform iOS 0	Brand SMP

TABLA DE INDICADORES DETALLADOS

Estructura y significado de cada columna:

NAME: Nombre del indicador específico analizado **VALUE:** Valor detectado para ese indicador **AGE:** Número de días desde la primera aparición de este valor **COUNTER:** Cantidad de veces que se ha observado este valor **RELATIVE PREVALENCE:** Porcentaje de frecuencia en la población total **INDICATION STRENGTH:** Fuerza del indicador de riesgo (0-1000)

Interpretación de colores:

- Verde: Indicadores normales con baja indication strength
- Amarillo/Naranja: Indicadores moderadamente sospechosos
- Rojo: Indicadores altamente sospechosos con alta indication strength

Ejemplo del caso mostrado:

ua_browser_family: "Interbank%20UAT"

- VALUE: Interbank%20UAT
- AGE: 214 días desde primera detección
- COUNTER: 1 (solo visto una vez)

- RELATIVE PREVALENCE: 0.0% (nunca visto en población normal)
- INDICATION STRENGTH: 1000 (máximo nivel de sospecha)

Este indicador muestra un navegador altamente sospechoso que imita la aplicación bancaria oficial pero con características técnicas anómalas.

Revision #4

Created 30 June 2025 14:53:13 by roger de avila

Updated 1 July 2025 12:25:10 by roger de avila