Análisis de enlaces

El módulo de Link Analysis es un sistema avanzado de análisis de relaciones y conexiones que identifica vínculos entre usuarios, dispositivos, sesiones y patrones de comportamiento. Su función principal es detectar redes de actividad relacionada, identificar cuentas múltiples operadas por la misma entidad, y descubrir patrones de fraude coordinado mediante el análisis de conexiones y similitudes comportamentales.

Objetivos Principales

Objetivo	Descripción	Aplicación
Detección de Redes de Fraude	Identificar grupos de cuentas operadas por la misma entidad	Prevención de fraude masivo
Análisis de Dispositivos Compartidos	Detectar múltiples identidades usando el mismo dispositivo	Control de identidad única
Identificación de Patrones Similares	Encontrar sesiones con comportamiento idéntico o muy similar	Detección de automatización
Mapeo de Conexiones	Visualizar relaciones entre usuarios, dispositivos y sesiones	Investigación forense
Análisis de Familias de Dispositivos	Identificar dispositivos conocidos y sus relaciones	Control de dispositivos autorizados

Arquitectura del Sistema

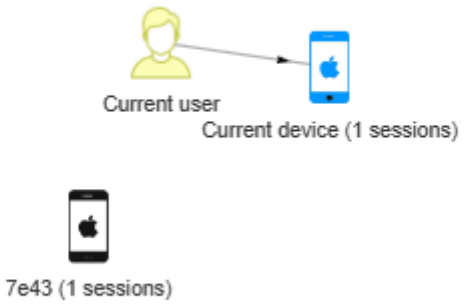
Componentes Principales

Componente	Función	Descripción
Graph View	Visualización gráfica de conexiones	Muestra relaciones entre usuarios y dispositivos
Sessions with Similar Behaviour	Tabla de sesiones relacionadas	Lista detallada de actividad vinculada
Link Detection Engine	Motor de detección de vínculos	Algoritmos de correlación y análisis
Relationship Mapping	Mapeo de relaciones	Sistema de identificación de patrones

Graph View - Vista Gráfica de Conexiones

La vista gráfica proporciona una representación visual de las conexiones identificadas entre el usuario actual, sus dispositivos y otros elementos relacionados. Utiliza algoritmos de grafos para

mostrar relaciones complejas de manera intuitiva.



Elementos del Grafo

Elemento	Representación Visual	Descripción	Información Mostrada
Current User	Icono de persona (amarillo)	Usuario actual bajo análisis	Punto central del análisis
Current Device	Teléfono azul	Dispositivo utilizado en la sesión actual	Número de sesiones activas
Related Device	Teléfono negro	Dispositivos adicionales vinculados al usuario	Identificador y conteo de sesiones
Connections	Líneas conectoras	Relaciones identificadas entre elementos	Tipo y fuerza de la conexión

Interpretación de Conexiones

Tipo de Conexión	Descripción	Nivel de Riesgo	Interpretación
Usuario-Dispositivo Único	Un usuario conectado a un solo dispositivo	Bajo	Patrón normal de uso
Usuario-Múltiples Dispositivos	Un usuario conectado a varios dispositivos	Medio	Posible uso legítimo múltiple o cuenta compartida
Múltiples Usuarios-Un Dispositivo	Varios usuarios usando el mismo dispositivo	Alto	Posible fraude o uso no autorizado
Red Compleja	Múltiples conexiones entrecruzadas	Muy Alto	Red sospechosa de actividad coordinada

Métricas del Grafo

Métrica	Descripción	Ejemplo en Imagen	Interpretación

Device ID	Identificador único del dispositivo	7e43	Código de identificación del dispositivo relacionado
Session Count	Número de sesiones por dispositivo	(1 sessions)	Cantidad de sesiones registradas en cada dispositivo
Connection Type	Tipo de relación identificada	Línea directa	Relación directa entre usuario y dispositivo

Sessions with Similar Behaviour - Sesiones con Comportamiento Similar

Esta tabla presenta una lista detallada de todas las sesiones que han sido identificadas como relacionadas o similares a la sesión actual, basándose en algoritmos de análisis comportamental y detección de patrones.

Estructura de Datos de la Tabla

Columna	Descripción	Tipo de Dato	Función

COUNTRY	País de origen de la sesión	Bandera/Código país	Identificación geográfica
DATE	Fecha y hora de la sesión	DateTime	Timestamp de la actividad
SCORE	Puntuación de similitud/riesgo	Numérico	Medida de similitud comportamental
USER	Identificador del usuario	String	ID de usuario (enmascarado)
REASON	Razón de la vinculación	String	Criterio de similitud detectado
KNOWN FAMILY	Dispositivo de familia conocida	Boolean (X/✓)	Indica si el dispositivo es reconocido
CSID	Identificador de sesión específico	String alfanumérico	ID único de la sesión
DURATION	Duración de la sesión	Numérico (segundos)	Tiempo total de la sesión
BRAND	Marca/Plataforma utilizada	String	Identificación de la plataforma
CHANNEL	Canal de acceso	String	Método de acceso utilizado
ISP	Proveedor de servicios de internet	String	Compañía de internet utilizada
KNOWN DEVICE	Dispositivo conocido	Boolean (X/✓)	Indica si el dispositivo está registrado
IP	Dirección IP (parcial)	String numérico	Identificación de red (enmascarada)
UNKNOWN DEVICE	Estado de dispositivo desconocido	Boolean (X/✓)	Marca dispositivos no registrados
IP AGE	Edad de la dirección IP en días	Numérico	Tiempo desde primer registro de la IP
IP COUNTRY AGE	Edad de IP en el país específico	Numérico	Tiempo de asociación IP-país
USERS IN MUD LV	Usuarios en nivel MUD	Numérico	Contador de usuarios en mismo nivel de riesgo
DEVICE AGE	Edad del dispositivo en días	Numérico	Tiempo desde primer registro del dispositivo
USER AGE	Edad del usuario en días	Numérico	Tiempo desde creación de la cuenta
CONTEXT	Contexto de navegación de la sesión	String	Secuencia de páginas/acciones realizadas

Análisis de Datos de la Tabla

Información de País y Ubicación

País Detectado	Bandera	Interpretación	Nivel de Atención
México	□□□□	Todas las sesiones desde México	Concentración geográfica sospechosa
Consistencia de Ubicación	Misma bandera	Actividad coordinada desde misma región	Posible red de fraude local

Análisis de Puntuaciones (SCORE)

Rango de Score	Ejemplo	Interpretación	Acción Recomendada
700-800	789, 770, 795, 772	Similitud muy alta en comportamiento	Investigación inmediata
500-600	569	Similitud moderada-alta	Monitoreo intensivo
100-200	123	Similitud baja-moderada	Monitoreo estándar
0-50	20	Similitud mínima detectada	Revisión periódica

Análisis de Usuarios

Patrón de Usuario	Ejemplo	Descripción	Implicación
UNPROTECTED_3C00190012	Usuario tipo 1	Cuenta sin protecciones adicionales	Mayor vulnerabilidad
UNPROTECTED_100190011	Usuario tipo 2	Diferentes variantes de cuentas desprotegidas	Patrón de cuentas similares
UNPROTECTED_175534809	Usuario tipo 3	Numeración secuencial o generada	Posibles cuentas automatizadas

Razón de Vinculación

Razón	Descripción	Algoritmo Utilizado	Nivel de Confianza
behaviour	Comportamiento similar detectado	Análisis de patrones de interacción	Alto
device	Mismo dispositivo utilizado	Fingerprinting de hardware	Muy Alto
network	Misma red o ISP	Análisis de infraestructura	Medio
temporal	Patrones temporales similares	Análisis de timing	Medio-Alto

Estado de Dispositivos y Familias

Campo	Valor	Significado	Implicación de Seguridad
KNOWN FAMILY	X (No)	Dispositivo no pertenece a familia conocida	Mayor riesgo de dispositivo nuevo/sospechoso
KNOWN DEVICE	X (No)	Dispositivo no registrado previamente	Dispositivo potencialmente malicioso
Combinación XX	Ambos negativos	Dispositivo completamente desconocido	Riesgo muy alto

Análisis de Infraestructura Técnica

Campo Técnico	Valor Detectado	Interpretación	Nivel de Riesgo
BRAND	SMP	Todas las sesiones usan la misma plataforma	Consistencia sospechosa
CHANNEL	Emulator (IOS)	Todas desde emulador de iOS	Uso de herramientas de automatización
ISP	WI-NET TELECOM S.A.C.	Mismo proveedor de internet	Concentración geográfica/infraestructura
IP Range	38.2.x.x	Mismo rango de direcciones IP	Red coordinada

Análisis de Dispositivos y Edades

Campo	Valor Observado	Descripción	Interpretación de Riesgo
UNKNOWN DEVICE	X (Todos marcados)	Todos los dispositivos son desconocidos	Muy Alto - Dispositivos nuevos o temporales
IP	38.25.16.17	Misma dirección IP para todas las sesiones	Crítico - Concentración de actividad
IP AGE	290 días (mayoría), 0 días	IP conocida por 290 días, nueva actividad	Medio - IP establecida con nuevo uso
IP COUNTRY AGE	290-326 días	IP asociada al país por varios meses	Bajo - Asociación geográfica estable
USERS IN MUD LV	0 (Todos)	Sin usuarios en mismo nivel MUD	Información - Nivel de riesgo único
DEVICE AGE	0 días (Todos)	Todos los dispositivos son completamente nuevos	Crítico - Dispositivos creados específicamente
USER AGE	290-326 días	Usuarios con diferentes antigüedades	Medio - Cuentas no recién creadas

Análisis de Contexto de Navegación

Patrón de Contexto	Secuencia Observada	Interpretación	Nivel de Automatización
Flujo Completo	AUTH_PAGE,LOGIN,LOGIN_PASSWORD,OPERACIONES,TRANSFERENCIAS,TRANSPAC_ORIGEN,TRANSPAC_DESTINO	Proceso completo de transferencia	Alto - Secuencia muy específica
Flujo Parcial	AUTH_PAGE,LOGIN,LOGIN_PASSWORD,OPERACIONES,SERVIC,SERVIC_BUSC,SERVIC_DATOS,SERVIC_MON	Acceso a servicios específicos	Alto - Navegación dirigida
Flujo Simplificado	AUTH_PAGE,LOGIN,LOGIN_PASSWORD	Solo proceso de autenticación	Medio - Acceso básico
Consistencia	Patrones repetitivos exactos	Mismas secuencias de navegación	Crítico - Comportamiento no humano

Patrones de Riesgo Identificados

Patrón 1: Concentración Temporal

Característica	Valor Observado	Interpretación
Fecha	30/6/2025	Todas las sesiones el mismo día
Horario	17:15-17:28	Ventana temporal de 13 minutos
Frecuencia	7 sesiones	Alta concentración de actividad

Patrón 2: Uniformidad Técnica

Aspecto	Consistencia	Nivel de Sospecha
Plataforma	100% SMP	Extremadamente sospechoso
Emulador	100% iOS Emulator	Indica automatización
ISP	100% mismo proveedor	Red coordinada
Dispositivos	100% desconocidos	Dispositivos nuevos/temporales

Patrón 3: Similitud Comportamental

Métrica	Observación	Implicación
Scores Altos	6 de 7 sesiones >500	Comportamiento muy similar
Duración Variable	0-86 segundos	Diferentes tipos de actividad
Razón Común	Todas por "behaviour"	Algoritmo detecta patrones idénticos

Patrón 4: Infraestructura Centralizada (Nuevo Análisis)

Factor	Valor Crítico	Interpretación	Nivel de Alerta
IP Única	38.25.16.17	Todas las sesiones desde la misma IP	CRÍTICO
Dispositivos Edad 0	100% dispositivos nuevos	Creados específicamente para esta actividad	CRÍTICO
IP Age vs Device Age	IP: 290 días, Dispositivos: 0 días	IP conocida pero dispositivos nuevos	ALTO
Contextos Repetitivos	Secuencias de navegación idénticas	Automatización confirmada	CRÍTICO

Patrón 5: Perfil de Usuario Sospechoso

Característica	Observación	Significado	Riesgo
País de Origen	OM (Omán)	Concentración geográfica específica	MEDIO
User Age Variado	290-326 días	Cuentas no recién creadas	BAJO
MUD Level	Todos en 0	Mismo nivel de clasificación	INFORMACIÓN
Unknown Device	100% marcados	Ningún dispositivo reconocido	CRÍTICO

Interpretación de Resultados

Matriz de Riesgo por Patrones

Combinación de Factores	Nivel de Riesgo	Interpretación	Acción Recomendada
Múltiples dispositivos + Scores altos + Misma infraestructura	CRÍTICO	Red de fraude coordinada	Bloqueo inmediato de toda la red
Dispositivos desconocidos + Emuladores + Concentración temporal	ALTO	Ataque automatizado masivo	Investigación urgente
Comportamiento similar + Misma ubicación + Usuarios secuenciales	ALTO	Fraude organizado local	Escalación a equipo especializado
Scores moderados + Infraestructura mixta + Timing normal	MEDIO	Posible actividad coordinada	Monitoreo intensivo
Dispositivos conocidos + Scores bajos + Patrones normales	BAJO	Actividad legítima relacionada	Monitoreo estándar

Algoritmos de Detección de Vínculos

Algoritmo	Descripción	Factores Analizados	Peso en Decisión
Behavioral Similarity	Compara patrones de interacción	Timing, secuencias, errores	40%
Device Fingerprinting	Identifica características únicas del dispositivo	Hardware, software, configuración	35%
Network Analysis	Analiza infraestructura de red	IP, ISP, geolocalización	15%
Temporal Correlation	Busca patrones temporales	Horarios, frecuencia, duración	10%

Métricas de Confianza

Nivel de Confianza	Rango de Score	Descripción	Acción Automática
Muy Alto	800-1000	Vínculos casi certeros	Bloqueo automático
Alto	600-799	Vínculos muy probables	Revisión prioritaria
Medio	400-599	Vínculos probables	Monitoreo adicional
Bajo	200-399	Vínculos posibles	Seguimiento rutinario
Mínimo	0-199	Vínculos débiles	Solo logging

Casos de Uso del Sistema

Detección de Fraude Masivo

Indicador	Descripción	Ejemplo de la Imagen
Múltiples Cuentas	Varias cuentas UNPROTECTED creadas	7 usuarios diferentes
Misma Infraestructura	Mismo ISP y tipo de dispositivo	WI-NET TELECOM, Emulator iOS
Comportamiento Idéntico	Scores altos de similitud	789, 770, 795, 772
Concentración Temporal	Actividad en ventana corta	13 minutos el 30/6/2025

Caso Crítico: Red de Fraude con IP Centralizada (Análisis de Nueva Imagen)

Factor Crítico	Evidencia	Interpretación	Nivel de Alerta
IP Única	38.25.16.17 para 7 sesiones diferentes	Todos los ataques desde mismo punto	CRÍTICO

Factor Crítico	Evidencia	Interpretación	Nivel de Alerta
Dispositivos Vírgenes	Device Age = 0 en todos los casos	Dispositivos creados específicamente	CRÍTICO
Usuarios Comprometidos	User Age 290+ días pero dispositivos nuevos	Cuentas legítimas posiblemente comprometidas	ALTO
Automatización Confirmada	Contextos de navegación idénticos	Bots siguiendo scripts predefinidos	CRÍTICO
Objetivos Específicos	Rutas directas a TRANSFERENCIAS	Intención clara de fraude financiero	CRÍTICO

Conclusión del Caso: Red de fraude altamente organizada usando cuentas comprometidas, dispositivos desechables y automatización desde infraestructura centralizada para realizar transferencias bancarias fraudulentas.

Acción Inmediata Requerida:

1. Bloqueo inmediato de IP 38.25.16.17
2. Suspensión de todas las cuentas identificadas
3. Investigación forense de las transferencias realizadas
4. Notificación a autoridades competentes
5. Actualización de algoritmos de detección

Análisis de Dispositivos Compartidos

Escenario	Identificación	Riesgo	Acción
Familia Legítima	Dispositivos conocidos, usuarios relacionados	Bajo	Permitir con monitoreo
Cuenta Corporativa	Múltiples empleados, mismo dispositivo	Medio	Validar políticas
Fraude Coordinado	Usuarios no relacionados, dispositivos nuevos	Alto	Bloquear e investigar
Red Criminal (Nuevo)	Misma IP, dispositivos vírgenes, usuarios antiguos	CRÍTICO	Respuesta de emergencia

Investigación Forense

Capacidad	Descripción	Beneficio
Reconstrucción de Redes	Mapea conexiones completas	Identifica toda la red criminal
Análisis Temporal	Estudia evolución de patrones	Predice futuros ataques
Correlación de Evidencia	Vincula evidencia dispersa	Construye caso sólido

Beneficios del Sistema

Para Equipos de Seguridad

Beneficio	Descripción	Impacto
Detección Temprana	Identifica redes antes de que causen daño	Prevención proactiva
Análisis Masivo	Procesa miles de conexiones simultáneamente	Escalabilidad
Evidencia Visual	Gráficos claros para presentación	Comunicación efectiva
Automatización	Reduce trabajo manual de investigación	Eficiencia operativa

Para Prevención de Fraude

Beneficio	Descripción	Impacto
Detección de Patrones	Identifica nuevas técnicas de fraude	Adaptación rápida
Análisis Predictivo	Anticipa comportamientos futuros	Prevención proactiva
Correlación Avanzada	Conecta eventos aparentemente aislados	Detección sofisticada

Para Compliance y Auditoría

Beneficio	Descripción	Impacto
Documentación Completa	Registra todas las conexiones identificadas	Cumplimiento regulatorio
Trazabilidad	Rastrea origen y evolución de redes	Auditoría forense
Reportes Automáticos	Genera informes para reguladores	Eficiencia de compliance

---

Revision #2
Created 30 June 2025 14:53:50 by roger de avila
Updated 1 July 2025 13:08:38 by roger de avila