IRONCHIP

INFORME ANUAL

TOP 8 CASOS DE FRAUDE DETECTADOS POR IRONCHIP

Informe Fraude 2024

ÍNDICE

INTRODUCCIÓN

Integración de la Localización en la Detección de Fraude: Eficiencia Mejorada y Validación en Procesos Críticos

La incorporación de la localización en los sistemas de detección de fraude ha demostrado ser un factor clave para mejorar la precisión en el perfilamiento de usuarios y la identificación de comportamientos fraudulentos. Al analizar datos de localización, las organizaciones pueden detectar patrones anómalos que indican actividades sospechosas, permitiendo una respuesta más rápida y efectiva.
Según un informe de Gartner, se estima que para 2028, el 20% de las empresas adoptarán equipos especializados en CyberFraud o implementarán estrategias colaborativas para combatir amenazas digitales, frente a menos del 5% que ya lo han hecho hasta la fecha.

En procesos críticos como el onboarding y la verificación de identidad (KYC), la localización desempeña un papel determinante. La capacidad de verificar la congruencia entre la ubicación del usuario y su historial de actividad permite a las empresas identificar riesgos potenciales y validar la autenticidad de las transacciones de manera más efectiva. Esta mejora en el perfilamiento de usuarios no solo aumenta la fiabilidad del sistema, sino que también contribuye a reducir el fraude de forma significativa, proporcionando un enfoque más robusto y proactivo en la protección contra amenazas.
En este contexto, soluciones como Ironchip han demostrado ser efectivas. Su tecnología de Location Based Security (LBS) utiliza inteligencia artificial para analizar las ondas electromagnéticas de una ubicación específica, creando una firma única asociada a una geolocalización no basada en GPS, denominada "zona segura". Esta zona se integra para acceder a sistemas o servicios como una capa adicional de seguridad, validando el acceso seguro del usuario con un dispositivo asociado a esa ubicación.

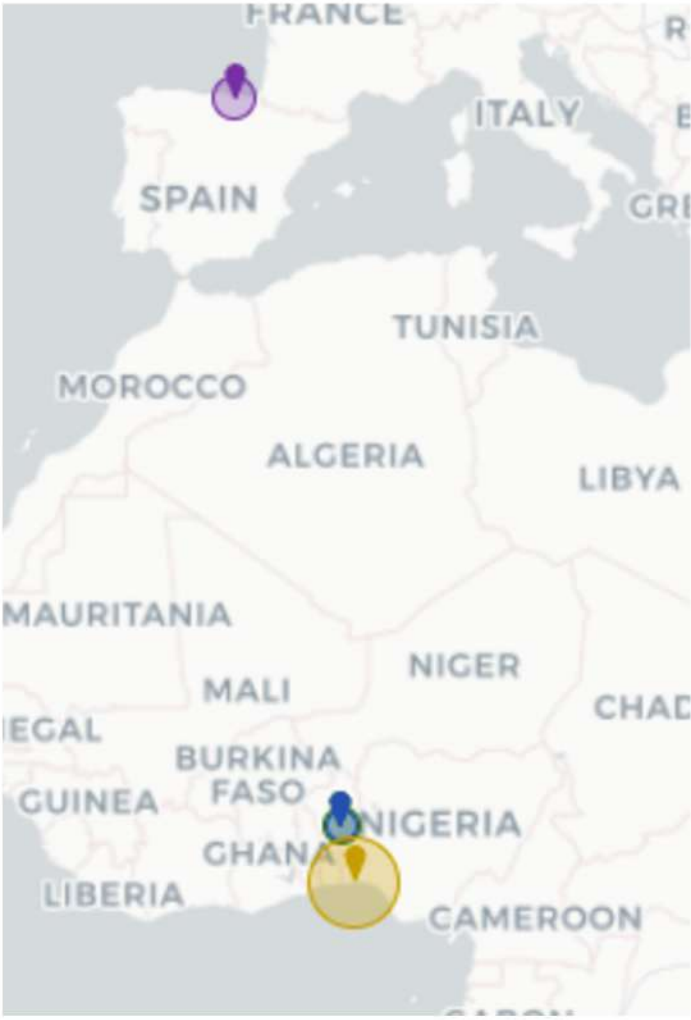
Al integrar la localización en los procesos de detección de fraude y verificación de identidad, las organizaciones pueden lograr una mayor precisión en la identificación de usuarios legítimos y actividades fraudulentas, fortaleciendo así la seguridad y reduciendo riesgos asociados.

01

GPS MANIPULADO / VIAJES IMPOSIBLES

Es totalmente habitual que los hackers que atacan a instituciones financieras utilicen técnicas como VPNs para ocultar su dirección IP o aplicaciones como Fake GPS para manipular la ubicación GPS y simular que están en una zona de actividad habitual del usuario legítimo. Estas técnicas son parte de su arsenal para eludir sistemas de seguridad y dificultar la detección.

¿Cómo ocurre?



Técnicas Comunes de los Atacantes:

- **Uso de VPNs para ocultar la IP real:**

Los atacantes recurren a redes privadas virtuales (VPNs) para redirigir su tráfico a través de servidores en ubicaciones preseleccionadas, lo que les permite:

a. Enmascarar su verdadera ubicación geográfica.
b. Simular accesos desde regiones que coincidan con el historial del usuario legítimo.

- **Falsificación de coordenadas GPS:**
-

Las aplicaciones de spoofing de GPS alteran las coordenadas reportadas por el dispositivo, simulando que el atacante se encuentra en una zona de confianza. Esto se utiliza para:

a. Evitar alertas basadas en localización.
b. Imitar patrones de acceso del usuario objetivo.

- **Manipulación de redes y proxies:**

Los hackers utilizan redes públicas, proxies o cambios rápidos entre Wi-Fi y datos móviles para disimular su actividad. Esto introduce inconsistencias difíciles de rastrear en sistemas que dependen únicamente de datos superficiales.

01

GPS MANIPULADO / VIAJES IMPOSIBLES

El Enfoque de Ironchip: Más Allá de la Localización

Ironchip no se limita al análisis básico de localización GPS. Su enfoque combina una amplia variedad de variables para determinar si una ubicación es legítima o manipulada.

- **Correlación Multivariable de Localización:**
    - GPS: Validación de coordenadas geográficas reportadas por el dispositivo.
    - Red y proveedor de servicios: Identificación del ISP y validación de que coincide con patrones históricos.
    - Hardware del dispositivo: Detección de alteraciones en el comportamiento del dispositivo, como aplicaciones de spoofing instaladas.
    - Entorno físico: Detección de discrepancias entre las señales de red y la ubicación reportada.

- **Detección de Inconsistencias:**

Ironchip analiza patrones de conexión para identificar anomalías como:

- Ubicación GPS que no coincide con la dirección IP del dispositivo.
- ISP asociado con listas negras de actividad fraudulenta.
- Cambios sospechosos de red (por ejemplo, de una conexión doméstica habitual a un servidor VPN en otra región).

- **Inteligencia Adaptativa:**

Mediante algoritmos de machine learning, Ironchip aprende y adapta continuamente los patrones habituales de los usuarios legítimos, detectando accesos no autorizados basados en pequeñas anomalías.

02

PUNTOS CALIENTES

Gestión Ágil de Ubicaciones Sospechosas y Prevención de Ataques Coordinados

En el panorama actual de la ciberseguridad, es común que grupos organizados de ciberdelincuentes (mafias digitales) lancen ataques masivos desde ubicaciones específicas hacia múltiples objetivos, como bancos y usuarios finales. Estos ataques, que suelen originarse desde un único punto geográfico, aprovechan la infraestructura local para enmascarar sus operaciones.

Ironchip ofrece una solución avanzada para identificar patrones de comportamiento asociados a estas actividades, permitiendo no solo detectar dichas ubicaciones, sino también bloquearlas de forma ágil y eficiente, fortaleciendo las estrategias de defensa de las instituciones financieras y otros sectores.

02

PUNTOS CALIENTES

Cómo Ironchip Detecta y Responde a Ataques Coordinados

- **Análisis del Tráfico de Red por Localización:**

Ironchip monitoriza continuamente el tráfico asociado a ubicaciones geográficas específicas. Mediante algoritmos avanzados, es capaz de:

  - Detectar picos anómalos de actividad en tiempo real.
  - Identificar accesos recurrentes desde zonas inusuales o de alto riesgo.
  - Correlacionar patrones de comportamiento con actividades maliciosas conocidas.

- **Detección de Ataques Basados en Ubicación:**

Las mafias digitales a menudo concentran sus operaciones en un área geográfica concreta para lanzar ataques distribuidos. Ironchip analiza:

  - Conexiones simultáneas provenientes de una única ubicación hacia múltiples objetivos.
  - Variaciones de las redes utilizadas (ISP, proxies, VPNs) en esa zona.
  - Datos históricos de accesos maliciosos registrados en esa ubicación.
  -

- **Bloqueo Ágil de Localizaciones:**

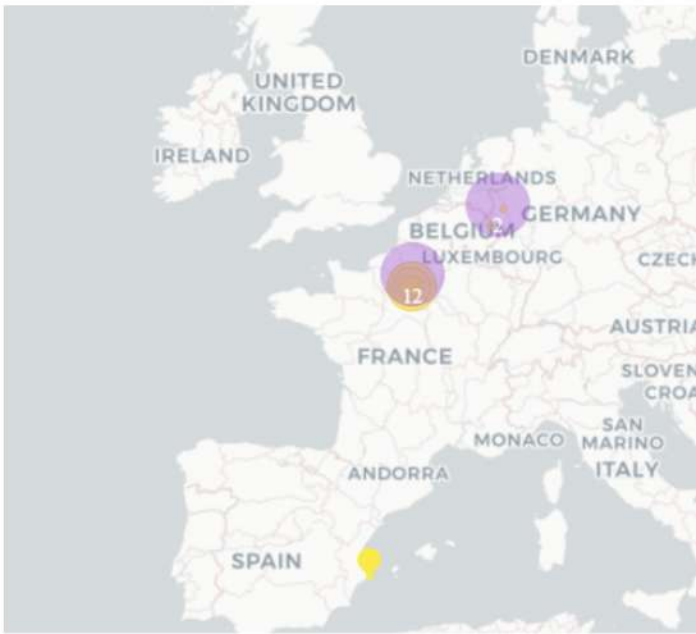
Una vez identificada una ubicación como sospechosa, Ironchip permite:

  - Bloquear automáticamente todas las conexiones provenientes de esa área geográfica.
  - Crear reglas de restricción temporal o permanente asociadas a la ubicación.
  - Configurar notificaciones en tiempo real para alertar a los equipos de seguridad.

- **Inteligencia Adaptativa:**

Ironchip utiliza machine learning para actualizar continuamente su base de datos de ubicaciones sospechosas. Esto incluye:

  - Incorporar nuevas zonas de riesgo detectadas a nivel global.
  - Adaptarse a patrones dinámicos de los atacantes, como cambios en puntos de origen.



03

LOCALIZACIÓN PRECISA

Localización Precisa de Atacantes y Uso de Evidencias Judiciales

Gracias a su avanzada tecnología de mapeo de ondas internacional, Ironchip no solo detecta intentos de fraude, sino que es capaz de identificar con precisión la ubicación física de los atacantes. Esta capacidad única combina inteligencia de localización con análisis de señales de red, permitiendo:

- **Identificación de Orígenes de Ataques:**
  - Mapeo detallado de ondas: Ironchip utiliza una base de datos global de patrones de señales (GPS, red y entorno) para correlacionar accesos sospechosos con ubicaciones geográficas reales.
  - Validación de autenticidad: Se detecta si las señales de ubicación son manipuladas mediante VPN o aplicaciones como Fake GPS, verificándolas contra datos históricos y en tiempo real.

- **Bloqueo de Localizaciones Maliciosas:**
  - Una vez identificada una ubicación como origen de actividades fraudulentas, se puede proceder al bloqueo inmediato de todas las conexiones provenientes de esa zona.
  - La solución permite automatizar este proceso, minimizando riesgos y evitando la propagación de ataques hacia múltiples objetivos.

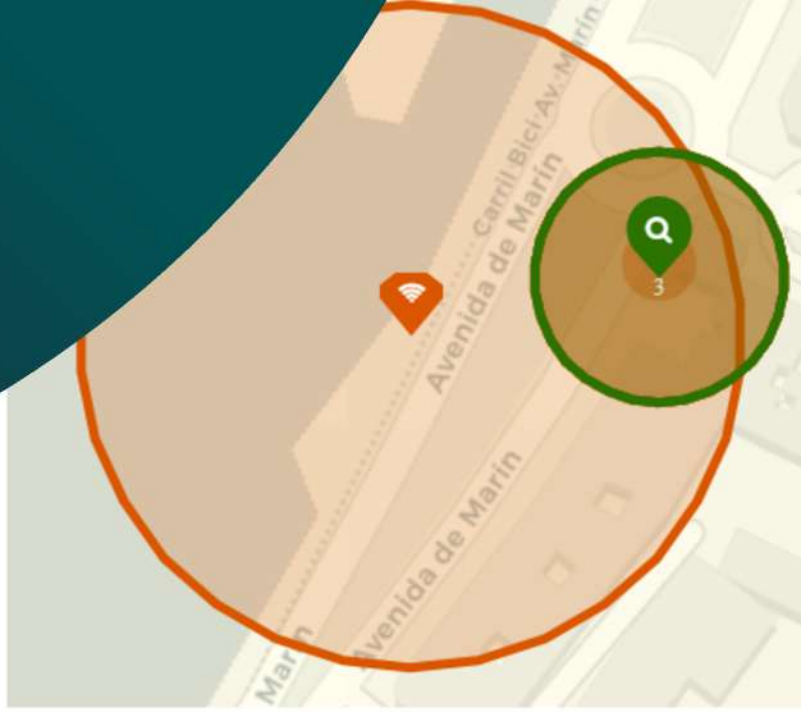
- **Soporte en Investigaciones Judiciales:**

En casos donde los atacantes pertenecen a bandas organizadas que operan desde ubicaciones fijas, la información recopilada por Ironchip ha sido:

  - Utilizada como evidencia judicial, proporcionando datos precisos sobre la ubicación de los cibercriminales.
  - Clave para colaborar con las autoridades en la identificación y desarticulación de redes de ciberdelincuentes.

03

LOCALIZACIÓN PRECISA

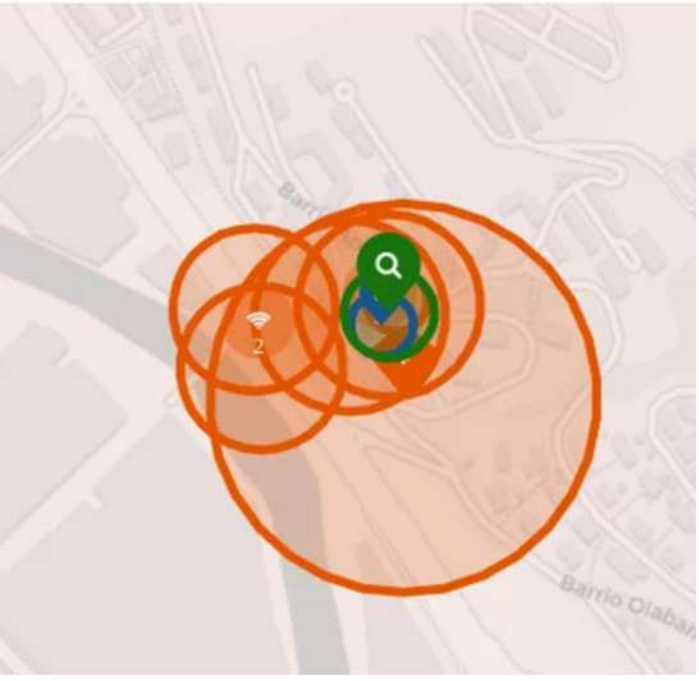


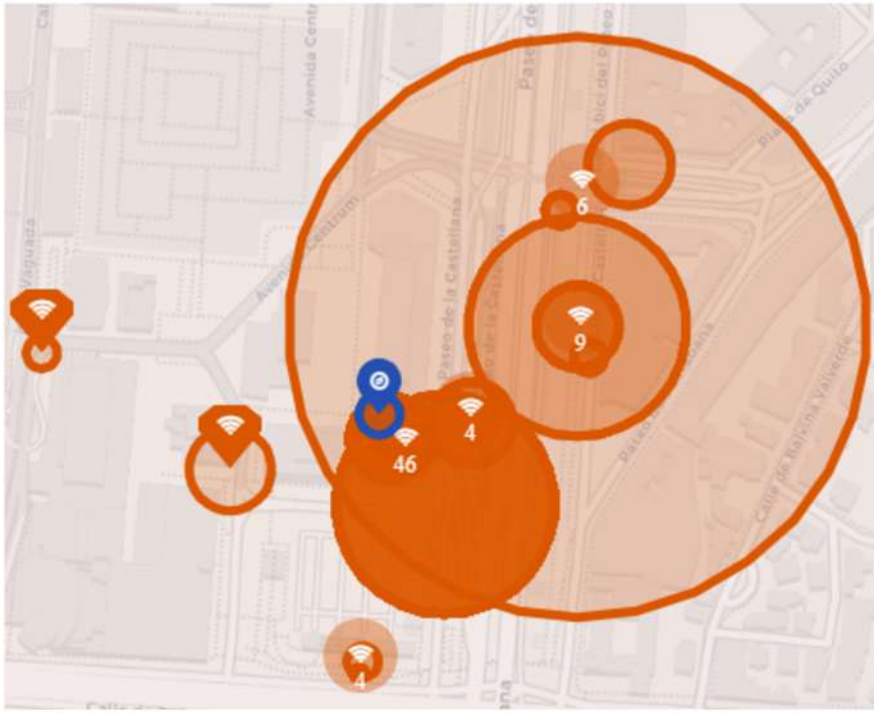
Tecnología Clave de Ironchip en la Detección

- **Mapeo Internacional de Ondas:**
  - Combina múltiples variables (GPS, red, entorno) para identificar patrones únicos de ubicación.
  - Permite una precisión superior al análisis basado únicamente en IP o GPS tradicionales.

- **Correlación Multivariable:**
  - Ironchip detecta inconsistencias entre IP, SIM, GPS y señales de red.
  - Identifica ubicaciones enmascaradas o manipuladas.

- **Automatización del Bloqueo:**
  - Una vez detectado un origen malicioso, se implementan bloqueos inmediatos.
  - Las reglas de bloqueo se adaptan en tiempo real, respondiendo a nuevos intentos de fraude.





04
LOCALIZACIÓN PAÍS POR RED MÓVIL

Identificación del País de Conexión Real mediante Análisis de Hardware y Señales de Red

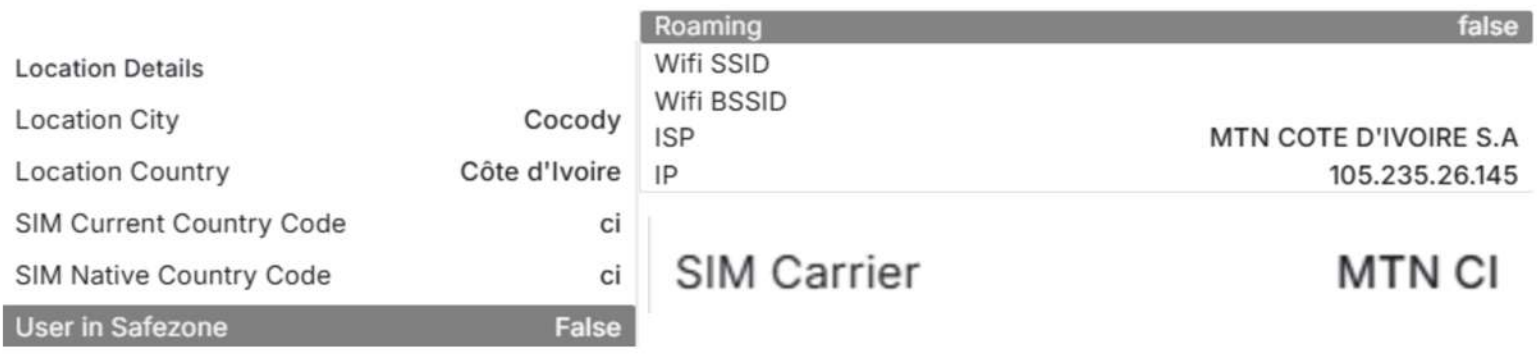
La tecnología de Ironchip permite detectar el origen real de una conexión incluso cuando los atacantes intentan enmascararlo mediante técnicas como la manipulación de GPS, VPN o proxys. Esto se logra gracias al conocimiento avanzado de componentes de hardware, como las SIM cards, las antenas telefónicas y otros elementos relacionados con las telecomunicaciones.

Cómo Ironchip Detecta el País Real de Conexión

Análisis de Componentes Hardware y Señales:
Información de la SIM: Cada tarjeta SIM incluye identificadores únicos, como el MCC (Mobile Country Code) y el MNC (Mobile Network Code), que indican el país y la red de origen.
Antenas Telefónicas: Ironchip analiza las conexiones con torres de telefonía móvil cercanas, verificando que la señal sea coherente con la ubicación reportada.
Señales de Red: La correlación de datos de red, como el ISP y la geolocalización asociada, refuerza la validación de la ubicación real.

Detección de Manipulaciones:
Simulación de Localización: Los atacantes a menudo utilizan herramientas como VPN o aplicaciones de GPS falso para aparentar que se conectan desde un país distinto.
Sin embargo, el hardware no es manipulable, y Ironchip puede identificar discrepancias entre la ubicación simulada y la información obtenida de la SIM, la red y las antenas.

Identificación de País Real:
Ironchip utiliza estos datos para determinar con alta precisión el país desde el que se origina la conexión.
Esta información es clave para evaluar si el acceso proviene de un país restringido o de alto riesgo.



05
DETECCIÓN DE VISHING Y FRAUDE AUTORIZADO

El fraude autorizado se caracteriza por el hecho de que el usuario legítimo, bajo manipulación psicológica, termina autorizando transacciones fraudulentas o proporcionando información sensible que compromete su seguridad. Este tipo de fraude ha aumentado considerablemente en los últimos años debido al uso de ingeniería social avanzada por parte de los atacantes.

Modalidades de Fraude Autorizado

1.- Autorización Bajo Coacción o Engaño:

En esta modalidad, el atacante:

- Se hace pasar por un representante del banco o un proveedor de servicios.
- Contacta al usuario legítimo, generalmente mediante una llamada telefónica.
- Utiliza tácticas de urgencia extrema o amenazas veladas para convencer al usuario de realizar una o varias transacciones rápidamente.
- Estas transacciones suelen ser transferencias bancarias, compras en línea o autorizaciones de acceso a la cuenta.

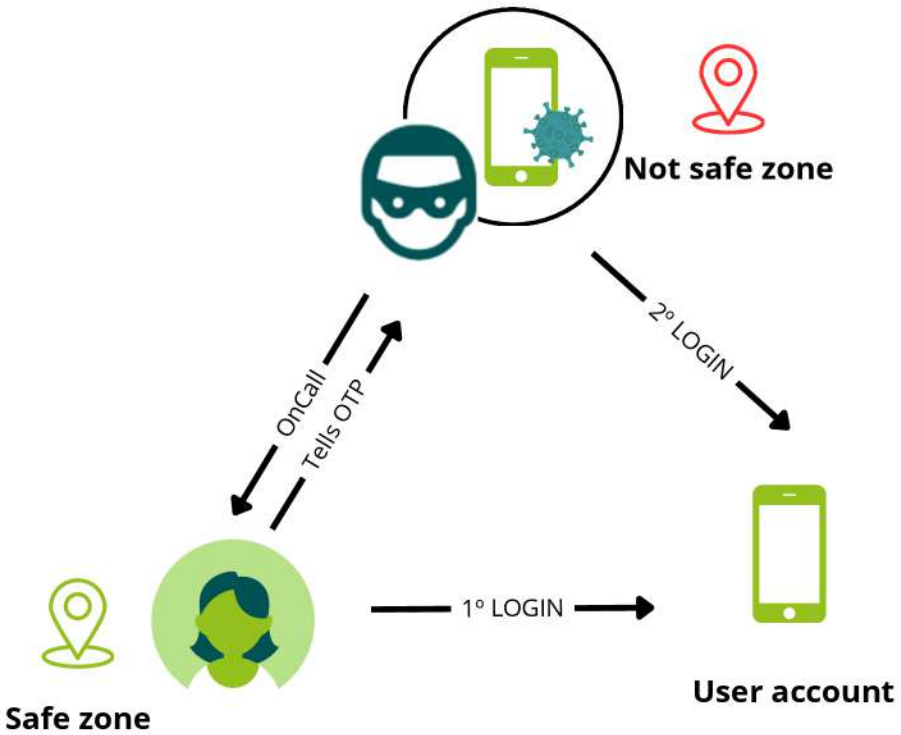
Ejemplo:
Un usuario recibe una llamada indicando que su cuenta está en riesgo de ser bloqueada. Bajo presión, el usuario autoriza múltiples compras o transferencias que benefician al atacante.

05
DETECCIÓN DE VISHING Y FRAUDE AUTORIZADO

2.- **Obtención de Credenciales por Ingeniería Social:**
En esta variante, el atacante:

- Llama al usuario, haciéndose pasar por un agente del banco, y solicita datos personales o credenciales.
- Las excusas suelen incluir:
  - Necesidad de renovar contraseñas.
  - Confirmación de claves de acceso.
  - Validación de datos sensibles para evitar un supuesto problema de seguridad.

Ejemplo:
Al usuario se le solicita un código de renovación que, al ser compartido, permite al atacante tomar control de la cuenta bancaria.



05
DETECCIÓN DE VISHING Y FRAUDE AUTORIZADO

Cómo Funciona la Detección de Llamadas con Ironchip

1. **Monitoreo de Actividad en el Dispositivo:**
   - Ironchip utiliza información derivada de las interacciones del dispositivo, detectando si el usuario está actualmente en una llamada de voz, ya sea a través de la red móvil o de aplicaciones de VoIP como WhatsApp, Telegram o similares.
2. **Correlación de Contexto:**
   - La tecnología no solo identifica que el usuario está en una llamada, sino que correlaciona esta información con:
     - Ubicación del dispositivo.
     - Tipo de conexión activa (red móvil, Wi-Fi, VPN).
     - Patrones habituales de uso.
   - Si la llamada coincide con transacciones sospechosas o intentos de autenticación, se genera una alerta automática.
3. **Detección Multicanal:**
   - Ironchip no se limita a las llamadas tradicionales. La plataforma analiza actividad en aplicaciones como:
     - WhatsApp.
     - Telegram.
     - Skype.
     - Otras aplicaciones de mensajería VoIP populares.

Caso Práctico: Bloqueo de Fraude Durante una Llamada

1.- Un atacante contacta al usuario haciéndose pasar por el servicio de atención al cliente del banco.
2.- Durante la llamada, el atacante guía al usuario para realizar una transferencia desde la banca móvil.
3.- Cómo actúa Ironchip:

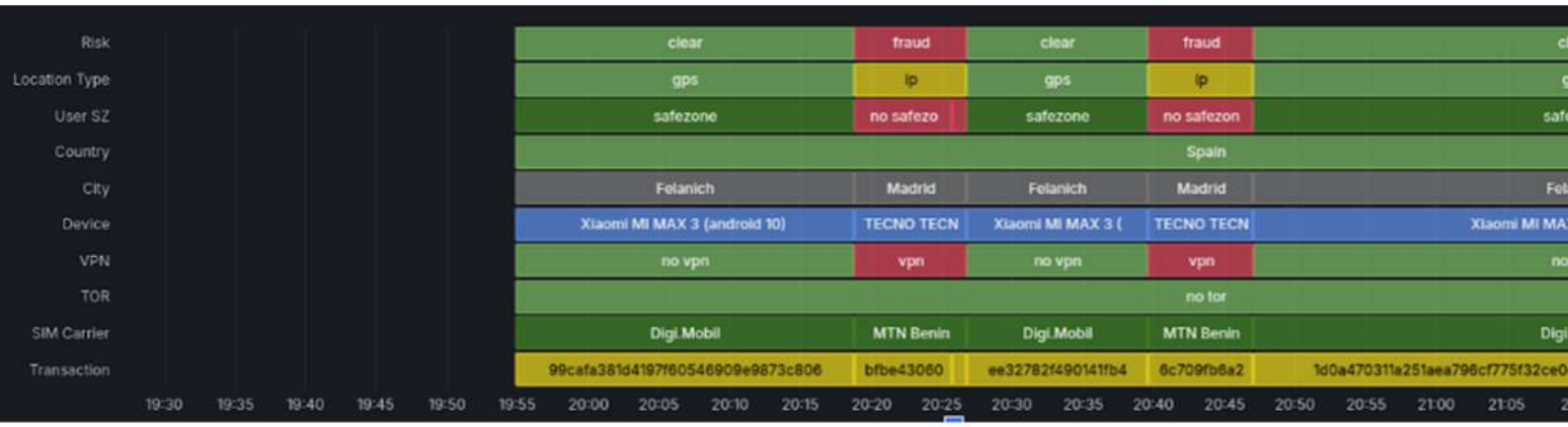
i. Detecta que el usuario está en una llamada mientras realiza la transacción.
ii. Correlaciona esta actividad con un cambio en la ubicación o red del dispositivo.
iii. La transacción es bloqueada automáticamente, y el usuario es notificado del intento de fraude.

06

DETECCIÓN DE MULAS

Análisis de Actividades Sospechosas Asociadas a Muleros

Un usuario que previamente mostró un comportamiento legítimo y consistente comenzó a exhibir anomalías significativas en sus conexiones, levantando sospechas de actividad fraudulenta. En la mayoría de sus interacciones previas, el usuario operaba desde ubicaciones seguras y con el GPS activado de manera constante, lo que permitía clasificar su actividad como confiable.



Irregularidades Detectadas

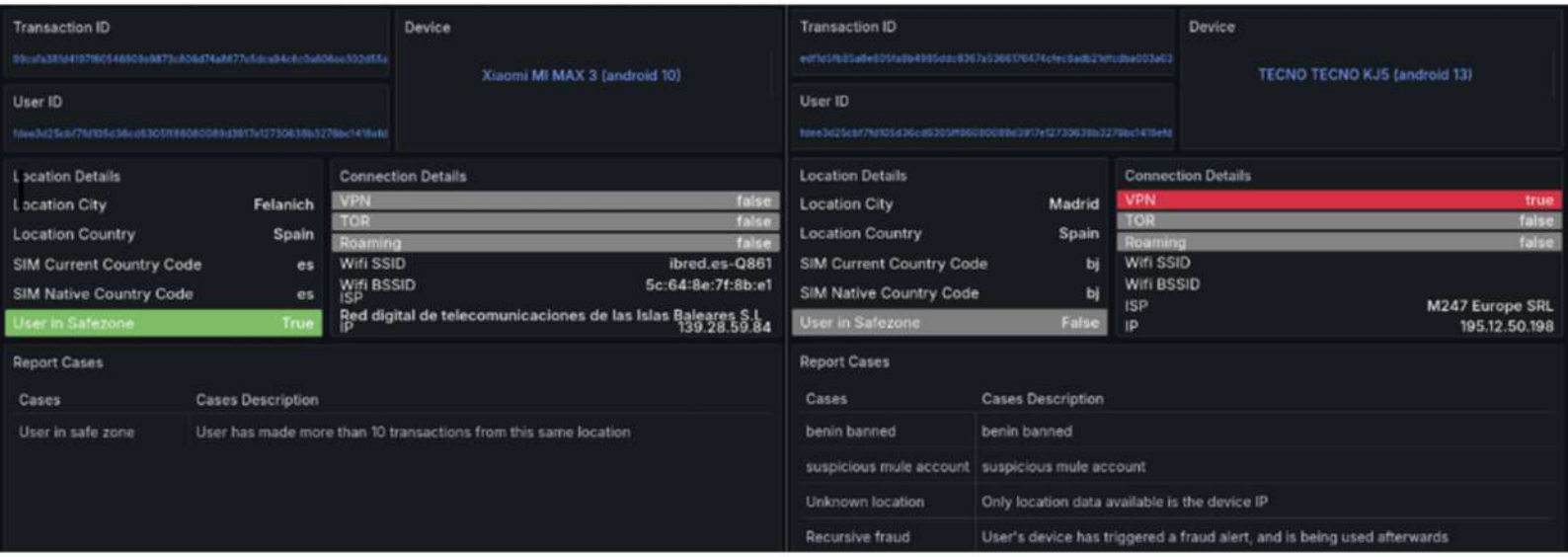
1. **Uso Repentino de VPN:**
   - Se observó el uso de una VPN por primera vez en el historial del usuario, lo que representa una desviación significativa de su comportamiento habitual.
2. **Cambio Anómalo de Ubicación y Proveedor Móvil:**
   - En un periodo muy breve, el usuario pasó de conectarse desde una ubicación segura en un país conocido a otra ubicación dentro del mismo país, pero utilizando una tarjeta SIM de un proveedor móvil extranjero.
   - Este cambio coincidió con la activación de la VPN, sugiriendo una posible manipulación intencionada de la ubicación.
3. **Incompatibilidad de Ubicaciones Físicas:**
   - La transición de ubicación fue demasiado rápida para ser físicamente posible, lo que indica el uso de tecnologías para simular la ubicación.
4. **Cambio de Proveedor de Internet:**
   - Se detectó un cambio repentino del proveedor de internet local a una conexión enmascarada mediante una VPN.

06

DETECCIÓN DE MULAS

Elementos Clave que Refuerzan la Sospecha

- Cambio de SIM: De un proveedor móvil local a un operador extranjero.
- Cambio de proveedor de internet: De un ISP local a una conexión VPN.
- Imposibilidad física de movimiento: La rapidez del cambio de ubicación no es plausible sin el uso de tecnologías para manipular la ubicación.



Conclusión

La detección temprana de patrones de fraude como cambios repentinos de ubicación, activación de VPN y uso de SIM extranjeras permite a Ironchip actuar de manera proactiva. Estas medidas no solo evitan pérdidas financieras, sino que también contribuyen a identificar y desmantelar redes de fraude organizadas, proporcionando información valiosa que puede ser utilizada como evidencia en investigaciones judiciales.

07
IDENTIDADES SINTETICAS/ NEW ACCOUNT FRAUD

Los atacantes frecuentemente utilizan el mismo dispositivo para simular múltiples cuentas fraudulentas. Ironchip ha logrado identificar hasta 25 usuarios asociados a un único dispositivo y, en un caso particular, 14 usuarios en la misma localización. La capacidad de generar reglas personalizadas de manera sencilla permite a las organizaciones limitar el número de dispositivos que un usuario puede activar, lo que contribuye a una detección más precisa y reduce el riesgo de fraude.

¿Cómo ocurre?

Los atacantes a menudo emplean redes de dispositivos interconectados, conocidas como botnets, para llevar a cabo actividades fraudulentas de manera coordinada. Estos dispositivos comprometidos pueden ejecutar transacciones desde diversas ubicaciones aparentes, crear una falsa sensación de legitimidad, o incluso acceder simultáneamente a cuentas desde múltiples dispositivos, dificultando la detección del fraude. Esta táctica permite a los atacantes realizar acciones que parecen dispersas y no relacionadas, cuando en realidad están siendo gestionadas de manera centralizada.

¿Cómo identificarlo?

La detección de este tipo de fraude implica un análisis exhaustivo de varios factores que ayudan a identificar patrones inusuales de comportamiento. Los principales métodos incluyen:

- **Análisis de Patrones de Conexión Simultáneos**: Si se detectan inicios de sesión en múltiples dispositivos en intervalos de tiempo muy cercanos, podría indicar que los dispositivos están siendo controlados por un atacante de forma remota.
- **Detección de Dispositivos que Comparten Credenciales**: Cuando dispositivos que no deberían estar asociados a una misma cuenta (por ejemplo, diferentes usuarios o dispositivos físicos) comienzan a compartir credenciales, se genera una señal de alerta.
- **Observación de Inconsistencias en los Tiempos de Acceso**: Acceder a la misma cuenta desde dispositivos o ubicaciones muy distintas en un corto período de tiempo es una señal de comportamiento sospechoso, ya que los usuarios legítimos suelen tener patrones más coherentes.

07

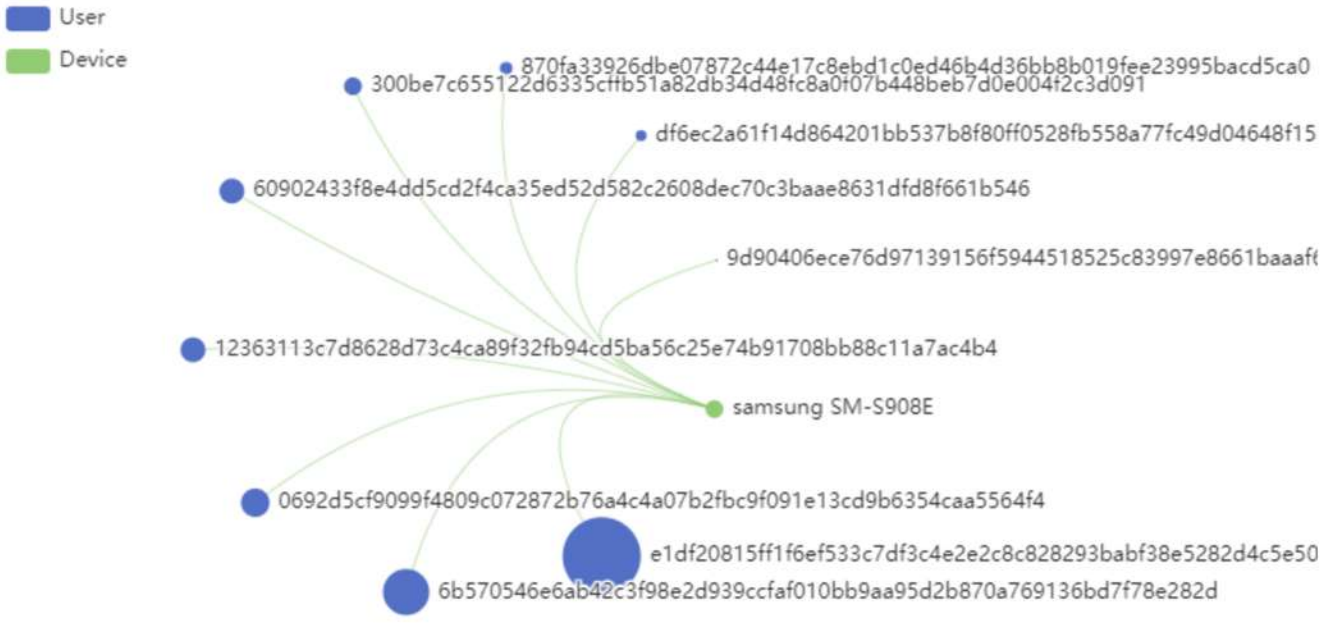
IDENTIDADES SINTETICAS/ NEW ACCOUNT FRAUD

Ironchip proporciona herramientas avanzadas para detectar este tipo de fraude, especialmente cuando se usan redes de dispositivos interconectados. Algunas de las técnicas clave incluyen:

- **Correlación de Dispositivos**: Ironchip correlaciona las huellas digitales de los dispositivos, creando un perfil único que puede identificar comportamientos anómalos incluso cuando los dispositivos están distribuidos entre diferentes entidades.

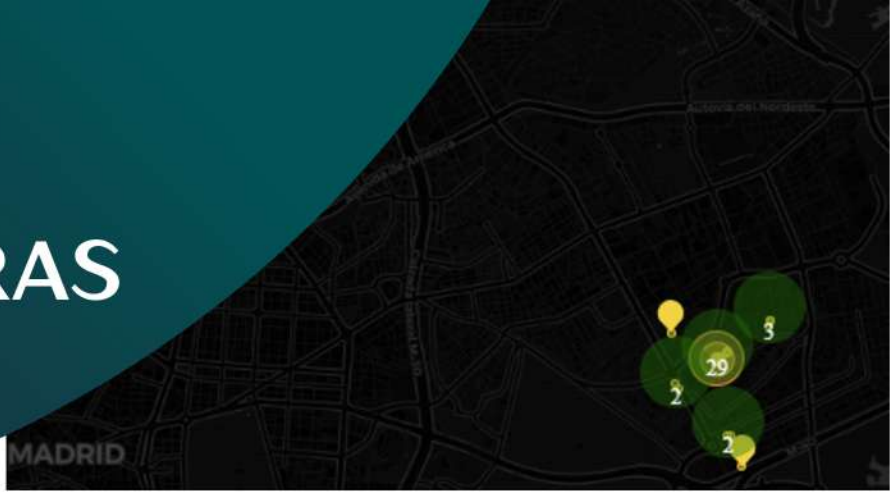
- **Limitación de usuarios por dispositivos**: Es habitual que las entidades bloqueen si un dispositivo es utilizado por más de **4 usuarios**. Aunque esta variable es personalizable, el éxito de esta limitación es superior a un 85%.

- **Lista negra de dispositivos**: Cuando un dispositivo fraudulento y distribuido es encontrado, es bloqueado y se introduce en la lista negra de dispositivos para evitar que sea utilizado en otro intento de fraude. Es recomendable, de forma paralela, introducir la zona generada por este fraudster en la lista de ubicaciones de riesgo.



08

ZONAS SEGURAS



Zona Segura: Una Herramienta Fundamental para Identificar Patrones de Comportamiento

Ironchip utiliza la zona segura como un parámetro clave para aprender y entender los patrones habituales de comportamiento de los usuarios. Esta funcionalidad permite establecer áreas geográficas asociadas con la operación legítima de cada usuario, basándose en la frecuencia y consistencia de sus conexiones desde esas ubicaciones.

- **Asociación de Lugares a la Confiabilidad:**

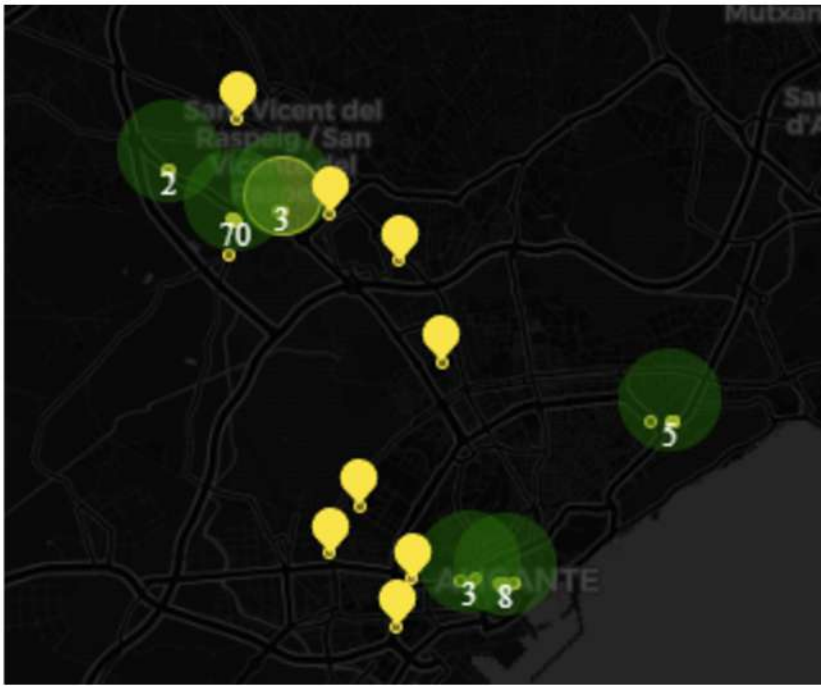
Ironchip evalúa el número de veces que un usuario opera desde un lugar específico y lo clasifica según su nivel de confiabilidad. Cuanto más frecuente sea la interacción desde una ubicación, mayor será la probabilidad de que esa zona sea considerada segura.

- **Identificación de Cambios de Dispositivo en Zonas Seguras:**

Cuando un usuario legítimo cambia de dispositivo y opera dentro de su zona segura habitual, Ironchip reconoce esta acción como válida, minimizando las fricciones en la experiencia del usuario.

- **Refuerzo de Seguridad ante Operaciones Críticas Fuera de la Zona Segura:**

Si un usuario intenta autorizar una operación crítica desde fuera de su zona segura, el sistema puede activar automáticamente medidas adicionales, como dobles comprobaciones de seguridad o requerir una verificación de identidad más robusta.



08

ZONAS SEGURAS

Prevención de Ataques ATO (Account Takeover)

La implementación de zonas seguras también desempeña un papel crucial en la detección y prevención de ataques de toma de cuenta (ATO). Este tipo de fraude es particularmente peligroso, ya que los atacantes intentan suplantar al usuario legítimo para realizar transacciones o acciones maliciosas.

- Anomalías en Dispositivos y Ubicaciones:

Un comportamiento típico en los ATO incluye la presencia simultánea de dos dispositivos conectados desde ubicaciones muy alejadas entre sí, y fuera de las zonas seguras habituales del usuario. Esta situación es una señal clara de actividad sospechosa.

- Respuesta Adaptativa:

Ironchip puede detectar estas conexiones anómalas y activar respuestas automáticas, como:

- Bloqueo temporal del acceso.

Alertas en tiempo real al usuario legítimo.

- Restricción de operaciones críticas.

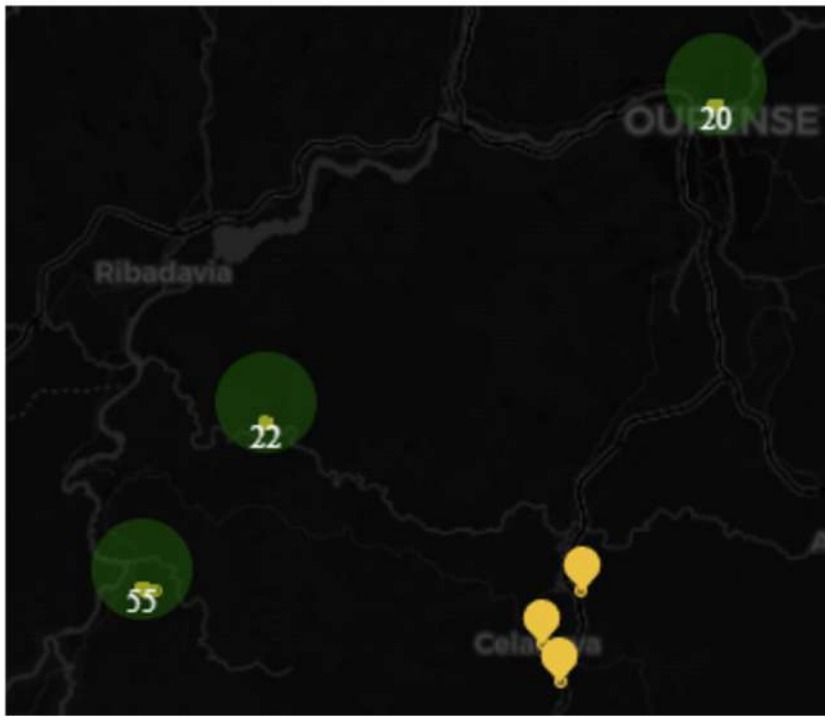
Ventajas Estratégicas de la Zona Segura

- Aprendizaje Adaptativo:

Ironchip no solo se limita a identificar ubicaciones, sino que aprende dinámicamente del comportamiento de los usuarios, adaptándose a cambios en sus patrones habituales.

Reducción de Falsos Positivos:

Al asociar ubicaciones confiables con los usuarios legítimos, se minimizan las interrupciones innecesarias en el acceso, mejorando la experiencia del cliente.
Protección Proactiva:
La detección de conexiones fuera de zonas seguras permite implementar medidas preventivas antes de que ocurra un fraude.



09

CONCLUSIONES

El fraude en el ámbito financiero ha evolucionado de manera significativa en los últimos años, adaptándose a las nuevas tecnologías y a las metodologías más sofisticadas. Uno de los paradigmas más preocupantes en la actualidad es el fraude autorizado, donde los atacantes logran manipular o engañar a usuarios legítimos para que autoricen transacciones fraudulentas. A menudo, esto ocurre a través de llamadas telefónicas, suplantación de identidad o incluso el uso de aplicaciones de mensajería, lo que permite a los delincuentes operar de manera sigilosa. En este contexto, el análisis del comportamiento y la localización del usuario se convierten en herramientas clave para detectar actividades inusuales o sospechosas, como conexiones provenientes de lugares no habituales o múltiples dispositivos operando simultáneamente desde ubicaciones distantes.

Ironchip se presenta como una solución avanzada y eficiente frente a estas amenazas, gracias a su capacidad para mapear y analizar patrones de comportamiento y ubicaciones de los usuarios. Al aprender de los lugares y dispositivos habituales de operación de un usuario, Ironchip puede identificar rápidamente si una operación crítica se realiza fuera de su zona segura, alertando a la entidad para que active medidas de verificación adicionales. Además, su capacidad para detectar el uso de VPNs, cambios de SIM o manipulación de localización permite bloquear conexiones fraudulentas antes de que se materialicen, protegiendo tanto a las instituciones financieras como a sus clientes. Esta solución no solo detecta fraudes en tiempo real, sino que también ofrece un enfoque adaptativo y dinámico que se ajusta a las amenazas emergentes.

Independientemente del tipo de fraude, hoy en día este crece de manera exponencial, impulsado por las nuevas tecnologías y las tácticas cada vez más sofisticadas empleadas por los atacantes. Para enfrentarlo de manera efectiva, es crucial contar con un abanico de herramientas de prevención que, como Ironchip, ofrezcan soluciones integrales y adaptativas. Solo con un enfoque multidimensional y una detección precisa en tiempo real, las organizaciones podrán proteger a sus usuarios y garantizar la seguridad de sus transacciones en un entorno cada vez más vulnerable.

IRONCHIP

FIGHT AGAINST IDENTITY THREATS!