IRONCHIP

Fight Against Identity Threats

www.ironchip.com

1. **Ironchip**
    - ¿Quiénes somos?
    - Certificaciones
2. **Nuestra tecnología y productos**
    - Location intelligence
    - La localización aplicada a la identidad
    - Detección de fraude por localización
    - Casos de fraude.
3. **Módulo antiphishing**
    - Detección de sites
    - Scanning de credenciales

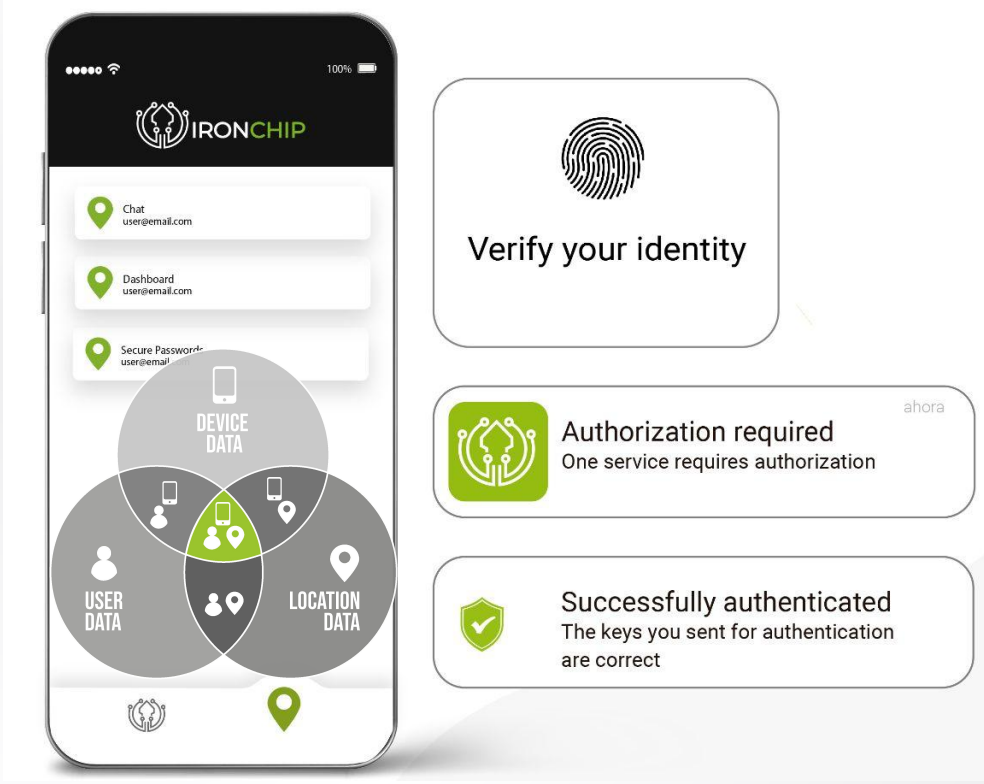
IRONCHIP

¿Quiénes somos?

Ironchip es una compañía de ciberseguridad global, especializada en protección de identidad digital y detección de fraude de nueva generación.

Con una **tecnología única en el mundo,** las soluciones de Ironchip ofrecen al cliente una **protección integral de la identidad** de todos sus servicios y recursos, así como también los de sus colaboradores.

Nuestra **tecnología de localización inteligente,** ofrece una trazabilidad, visibilidad y control en tiempo real de todos los usuarios, accesos y recursos, garantizando a las compañías una **seguridad 360.**



IRONCHIP

Ciberseguridad en nuestro ADN

En Ironchip, la **seguridad** no es solo una palabra, es nuestro **compromiso**. Por eso, nos sentimos orgullosos de contar con el aval de los más exigentes organismos de **certificación**.

Nuestras soluciones han sido certificadas con el nivel ALTO, la máxima calificación posible, por las entidades más prestigiosas del sector.

El gobierno de España avala la compañía mediante su inversión, convirtiendonos en empresa clave estratégica a nivel nacional.

IRONCHIP

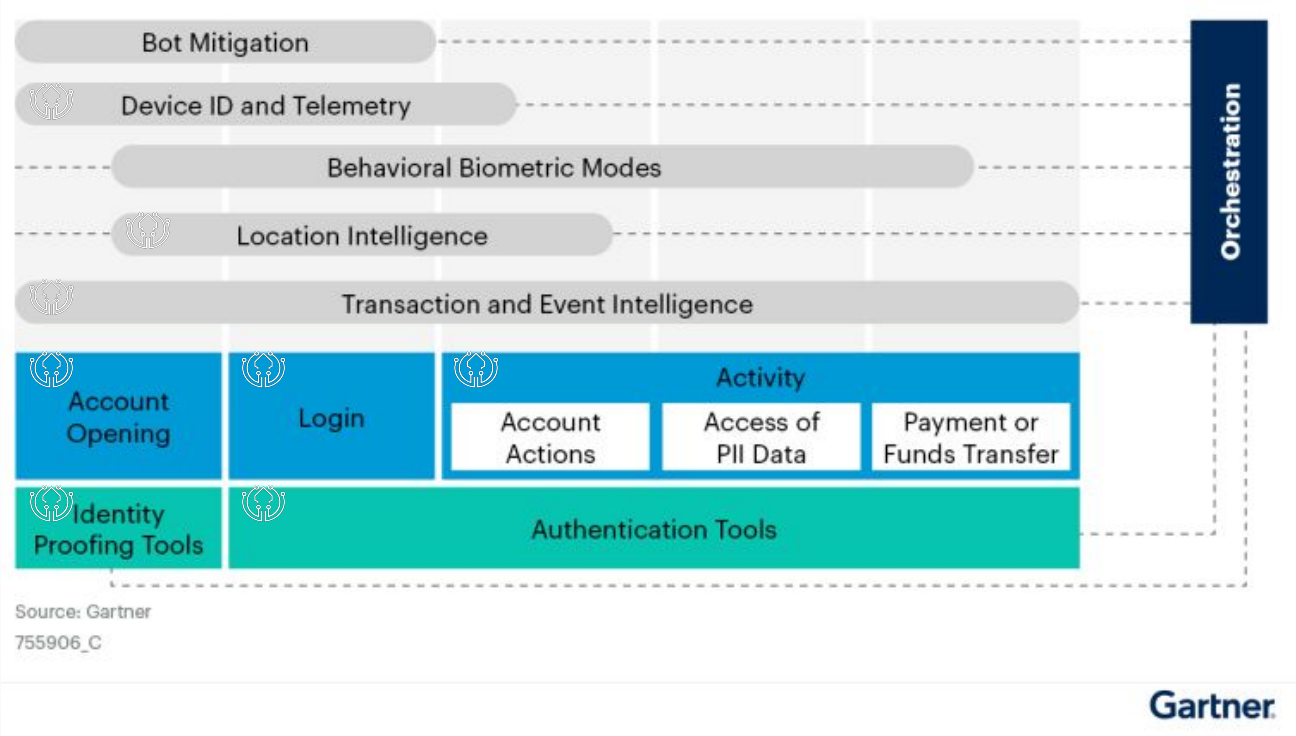
Tecnología

www.ironchip.com

Location intelligence

Location identity proof

Alcance de las capacidades de Online Fraud Detection a lo largo de un recorrido digital típico del cliente.



Tecnología de detección basado en localización

Transacciones seguras por comportamiento

IRONCHIP

Zonas de operaciones habituales

La **mayoría** de los procesos de identidad tienen lugar en **ubicaciones confiables**.

Ubicación No Confiable

El **92%** de los ataques ocurren de forma remota, desde una ubicación en la que el usuario nunca ha estado.

El **99%** de los estafadores cometen fraude desde la misma ubicación al menos en dos ocasiones.

La localización por operaciones

Tipos de transacciones protegidas

82%

Registro de usuario - KYC

El 92% de los usuarios se registran en una aplicación desde lugares habituales.

74%

E-commerce

El 74% de las compras se realizan desde lugares habituales.

66%

Inicio de sesión

El 68% de los inicios de sesión se realizan desde lugares habituales

90%

Transacciones +10.000€

Más del 90% de las transacciones de altos importes desde lugares habituales

¿Cómo funciona?

Transacciones seguras y localizadas

¿Que es una Zona Segura?

Una zona segura es un **lugar único, habitual e infalsificable** para cada usuario.

¿Cómo se genera una zona segura?

Una zona segura se genera usando una IA, tras captar y analizar las siguientes señales cada vez que un usuario opera una aplicación móvil o web.

- **Señales móviles: 2G, 3G, 4G o 5G.**
- **Señales WIFIs alrededor y WIFI favorito.**
- **GPS e IP.**
- **Geolocalización basada en latencias.**
- **ISP contratado y conexión a antenas móviles.**
- **SIM nativa y en uso.**
- **Suplantaciones de localización vía red VPN y TOR.**

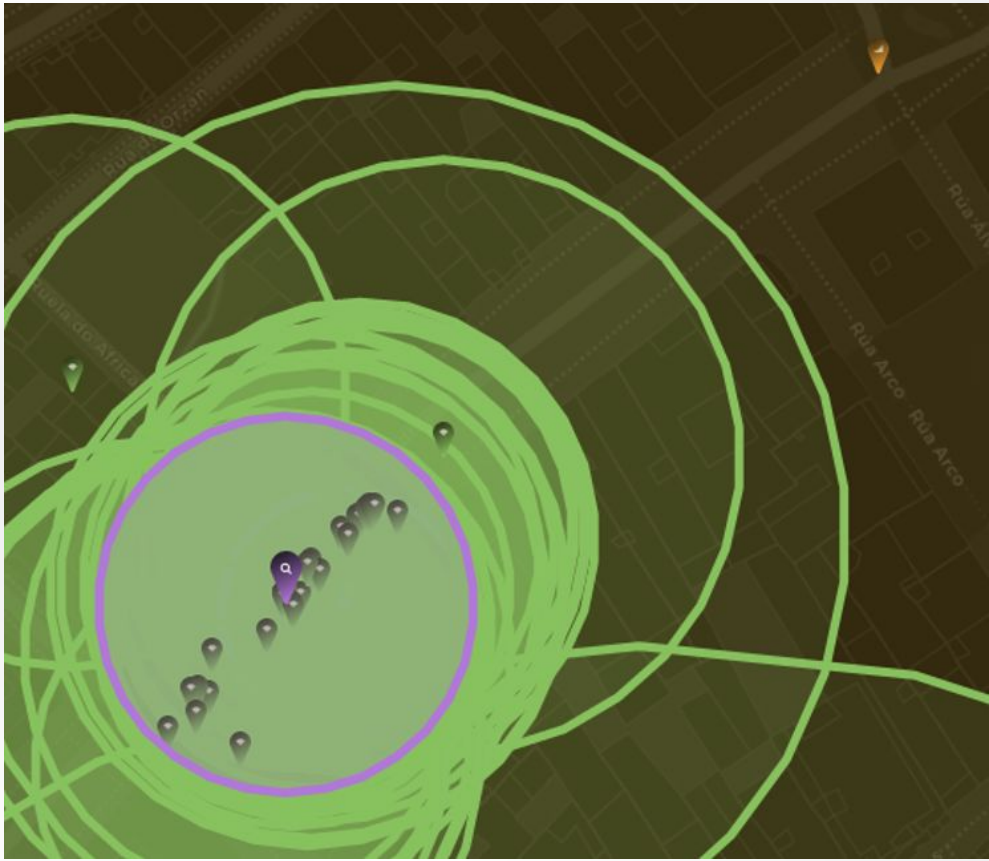


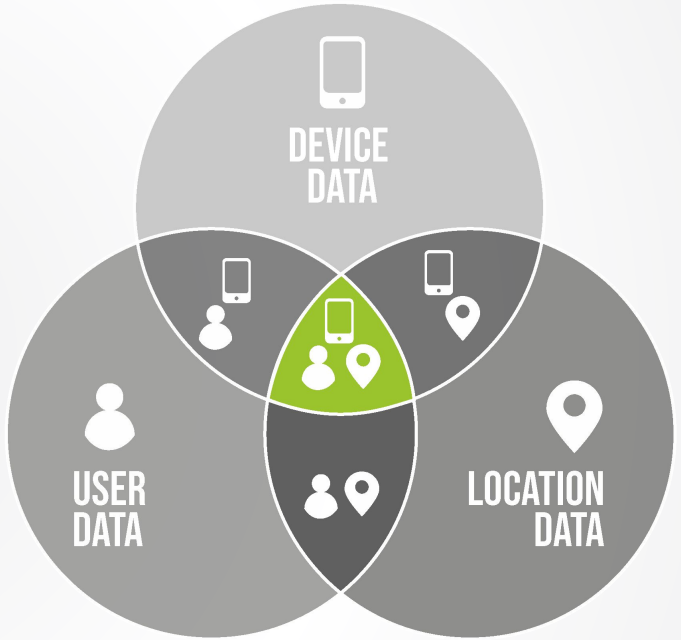
Image 1. Generated safe zone example with GPS, EM (2G, 3G, 4G, 5G) & IP signals.

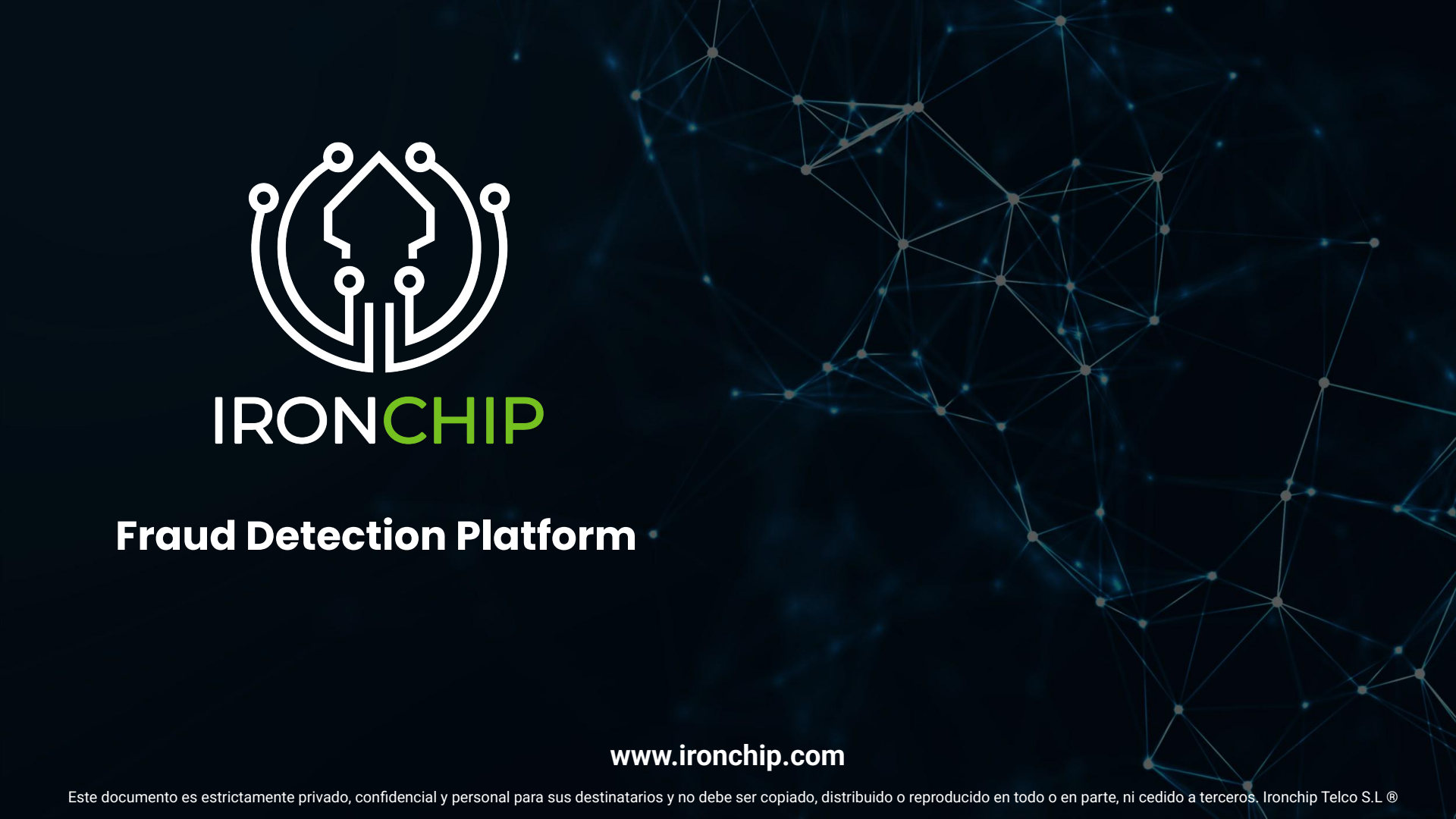
Comportamiento de usuario

Localización en el comportamiento

La vinculación entre el lugar y el dispositivo que integramos en nuestra tecnología, junto con la inteligencia artificial de localización basada en señales de redes móviles y WIFIS, junto con los datos del usuario, es fundamental para la **generación de patrones de comportamiento**.

Esta combinación permite entender el comportamiento del usuario y su ubicación de manera precisa, lo que resulta indispensable para una identidad segura en el futuro. La capacidad de **comprender dónde se encuentra el usuario y cómo interactúa con sus dispositivos** es inigualable, y representa la clave para garantizar la seguridad y la autenticación en los sistemas digitales.





Fraud Detection Platform

www.ironchip.com

Anomalous behaviour

Detected fraud behaviours

IRONCHIP

Detectamos los fraudes más avanzados

SIM SWAPPING

VISHING

PHISHING

SYNTHETIC IDENTITIES

MONEY MULE

Con un conjunto de métodos únicos

DEVICE FINGERPRINT

LOCATION INTELLIGENCE

DEVICE SWAPPING

TAMPERED DEVICE

TAMPERED APPLICATION

Instalación

SDK & API

Datasource SDK

Una librería iOS/Android/Javascript que puede integrarse en cualquier móvil/aplicación web para capturar la información necesaria.

Fraud detection API

Una HTTP API para solicitar resultado integrables con cualquier BPM o SIEM.

```
//  Login Operation

IronchipLBFraudSDK.executeTransaction("random_identifier_generated",
                                      "user_1234","login",null)


// Transfer Operation HashMap

HashMap <String, String> transferInformation = new HashMap<String, String>();
                                    transferInformation.put("Param_1", "XXX");
                                    transferInformation.put("Param_2", "YYY");
                                    IronchipLBFraudSDK.executeTransaction("random_identifier_generated",
                                    "user_1234","transfer",transferInformation)
```

03 Operaciones a proteger

Operación de KYC

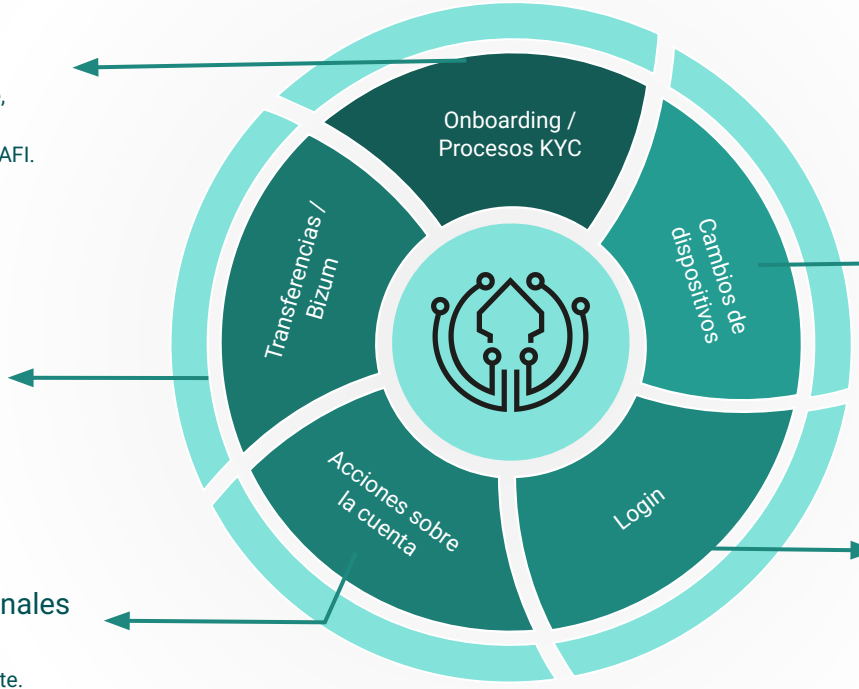
Operación opcionalmente bloqueante, usado para aprendizaje del usuario. Usualmente bloqueos desde países GAFI.

Operación de transferencia

Operación bloqueante, configurable en función de cantidades.

Operación de cambio de contraseña o datos personales

Operación habitualmente bloqueante.



Cambio de dispositivo o dispositivo habitual

Operación bloqueante, en algunos casos obligatoriedad de activación de la ubicación para asignar el dispositivo favorito, o cambio de dispositivo

Operación de Login

Operación habitualmente no bloqueante, utilizado para aprendizaje de las ubicaciones habituales de los usuarios.

03 Motor de reglas

IRONCHIP

Reglas de ubicación de riesgo

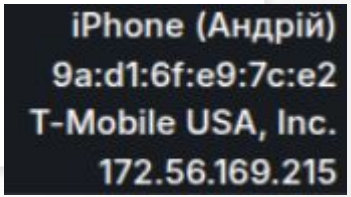
- Ubicaciones origen países GAFI.
- Conexión por red TOR o VPN.
- Si la geolocalización RF no coincide con GPS o SIM.
- Si existe proxy residencial.
- ISP de alto riesgo o en lista negra.
- Spoofing de ubicación.
- Carrier de la SIM difiere de la ubicación o del origen del ISP.
- Viajes imposibles.
- Red wifi pública. (high)
- Red wifi privada.
- Ubicaciones asociadas a ataques confirmados en otras entidades.
- IP en lista negra o de riesgo.

Reglas de dispositivo de riesgo

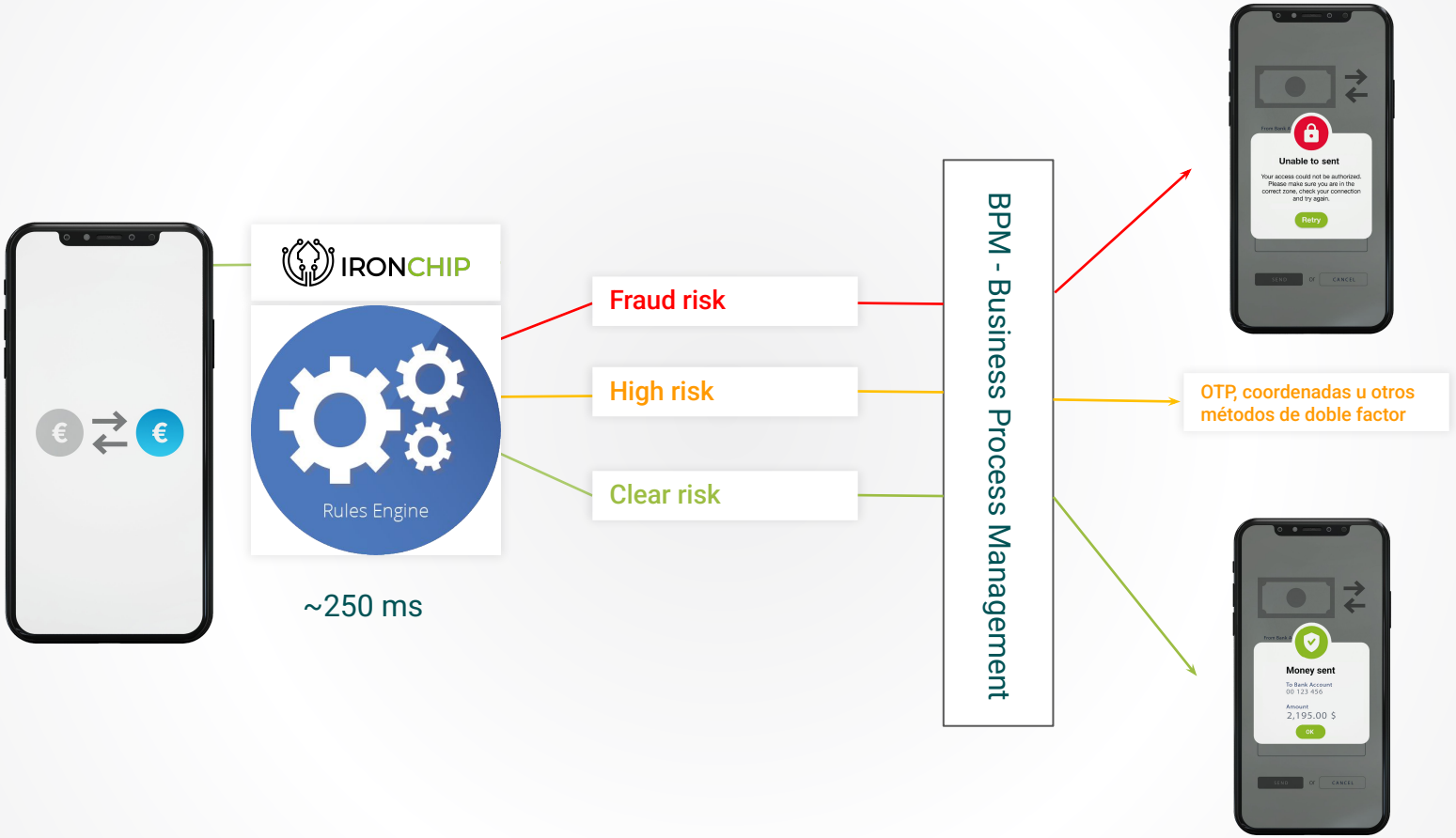
- Software malicioso instalado.
- Proceso de depuración o debugging activo.
- Dispositivo marcado en lista negra.
- Dispositivo de riesgo (ALPS, TECNO TECNO, INFINIX, Fairphone, Nothing, MobiWire).
- Dispositivo root/jailbreak.
- Desactualización del dispositivo en el historial de actualizaciones.
- Roaming inesperado.

Reglas de comportamiento

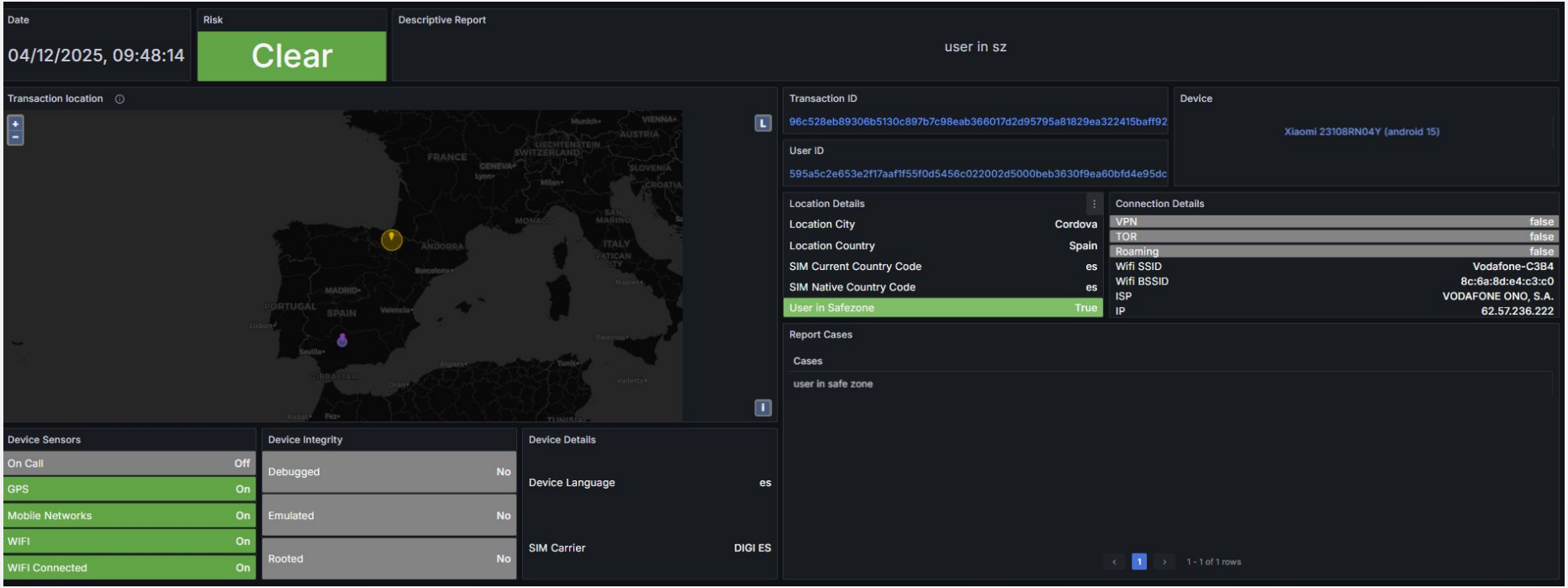
- Roaming + SIM virtual.
- Cambio de lenguaje sin cambio de dispositivo sin ubicación habitual.
- Transferencia en llamada o en redirección activa.
- Dispositivo asociado a + 3 usuarios.
- Lenguajes en cirilico desde ubicaciones de no uso.
- Múltiples conexiones en ventanas temporales pequeñas.
- Patrones consistentes con campañas de ataque conocidas.



¿Cómo funciona?

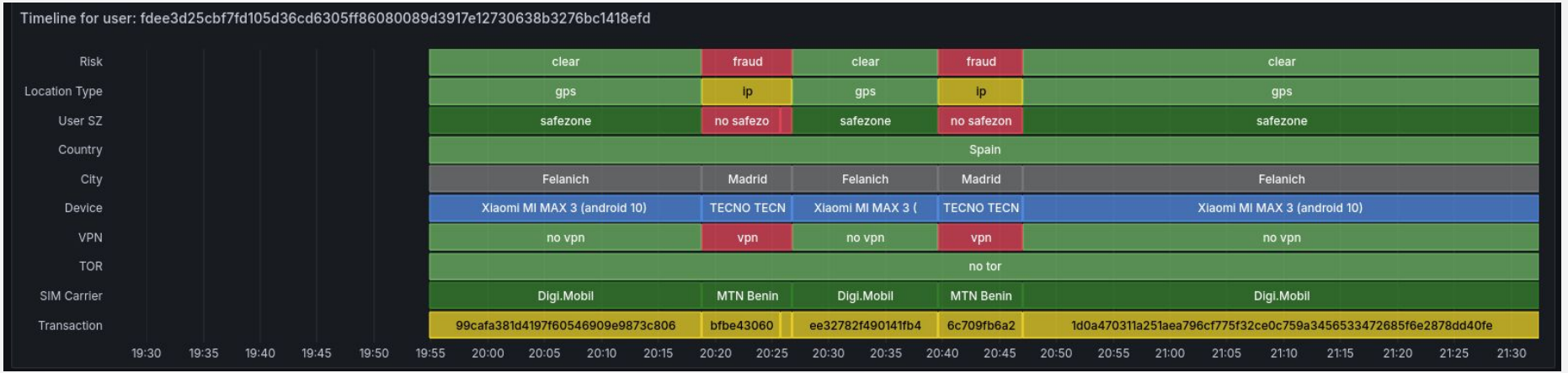


Comportamiento normal y seguro



03 Anomalous behaviour

Money Mule



Uso Repentino de VPN:

El 12 de septiembre se observó por primera vez una conexión a través de una VPN, específicamente NordVPN. Esto supone una desviación significativa del comportamiento habitual del usuario.

Cambio de SIM Carrier:

El dispositivo pasó de estar conectado en España a otra ubicación, también reportada como España, pero con una tarjeta SIM de origen en Benín. Esto fue posible mediante un cambio de proveedor de servicios móviles, de DiGI (España) a MTN Benin.

Viaje imposible:

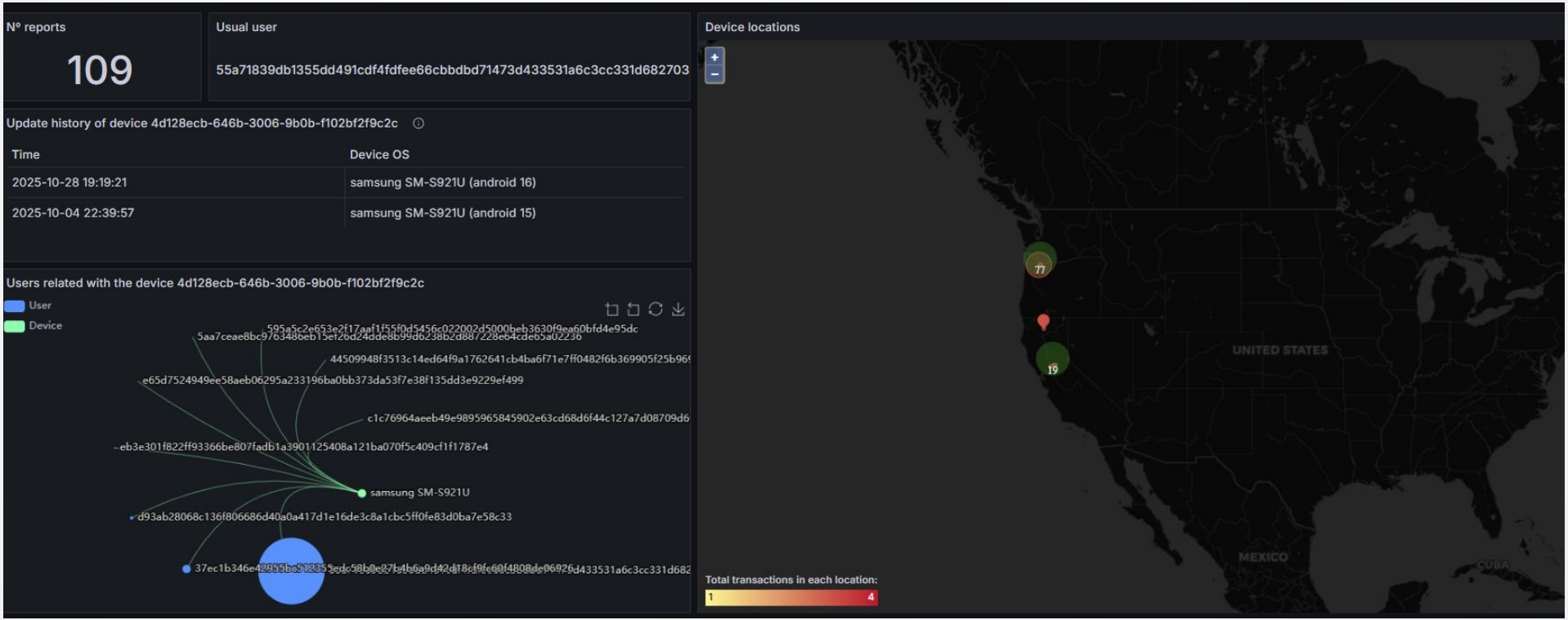
En 5 minutos viajo de España a Benin. Un cambio de ubicación tan drástico en tan poco tiempo es logísticamente imposible sin el uso de herramientas tecnológicas para manipular la ubicación.

Cambio de ISP:

Además, se identificó un cambio de proveedor de internet. El usuario pasó de estar conectado a través de Red Digital de Telecomunicaciones de las Islas Baleares S.L. (España) a conectarse a través de NordVPN, lo cual coincide con la aparición de la tarjeta SIM de Benín.

03 Anomalous behaviour

ATO



Anomalous behaviour

Vishing para fraude autorizado

Detección de llamadas corrientes en operaciones de transacciones.

Detección de llamadas IP:

- Telegram, Discord, Watshapp…

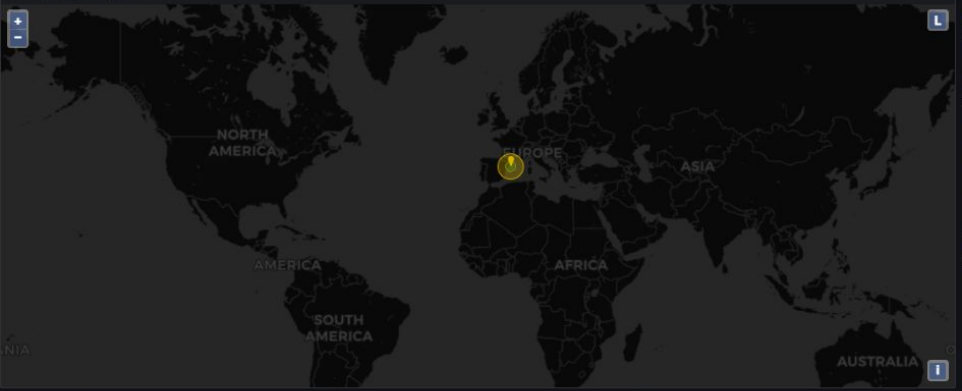
Redirección de llamadas y detección de Roaming.

03 Anomalous behaviour

Suplantación de ubicación o SIM virtuales

IRONCHIP

Date	Risk	Descriptive Report
09/12/2025, 17:55:07	Fraud	no gps - device swap - new device disable gps and enables vpn - new device disable gps



Transaction ID	Device
f25c4281d599041bc9f659d40eb6f77c5bcc47a99e6cc6a085f3fe9fe4f1c891	Xiaomi M2006C3MNG (android 11)

User ID
ee88f0356588ad570922db5d9b948a0a8590987c28a5c1aae002368aad685880

Location Details	
Location City	Barcelona
Location Country	Spain
SIM Current Country Code	ua
SIM Native Country Code	No value
User in Safezone	False

Connection Details	
VPN	true
TOR	false
Roaming	false
Wifi SSID	
Wifi BSSID	
ISP	PacketHub S.A.
IP	185.214.97.69

Report Cases

Cases
unknown location
device swapping

1 - 2 of 2 rows

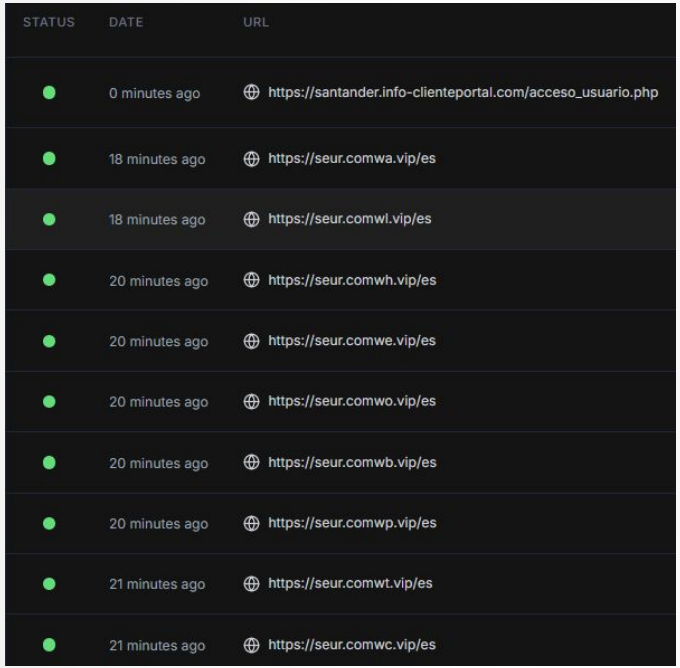
Device Sensors	
On Call	Off
GPS	Off
Mobile Networks	Off
WIFI	Off
WIFI Connected	Off

Device Integrity	
Debugged	No
Emulated	No
Rooted	No

Device Details	
Device Language	es
SIM Carrier	No value

Módulo phishing/smishing

Scanning de sites maliciosos



STATUS	DATE	URL
●	0 minutes ago	https://santander.info-clienteportal.com/acceso_usuario.php
●	18 minutes ago	https://seur.comwa.vip/es
●	18 minutes ago	https://seur.comwl.vip/es
●	20 minutes ago	https://seur.comwh.vip/es
●	20 minutes ago	https://seur.comwe.vip/es
●	20 minutes ago	https://seur.comwo.vip/es
●	20 minutes ago	https://seur.comwb.vip/es
●	20 minutes ago	https://seur.comwp.vip/es
●	21 minutes ago	https://seur.comwt.vip/es
●	21 minutes ago	https://seur.comwc.vip/es

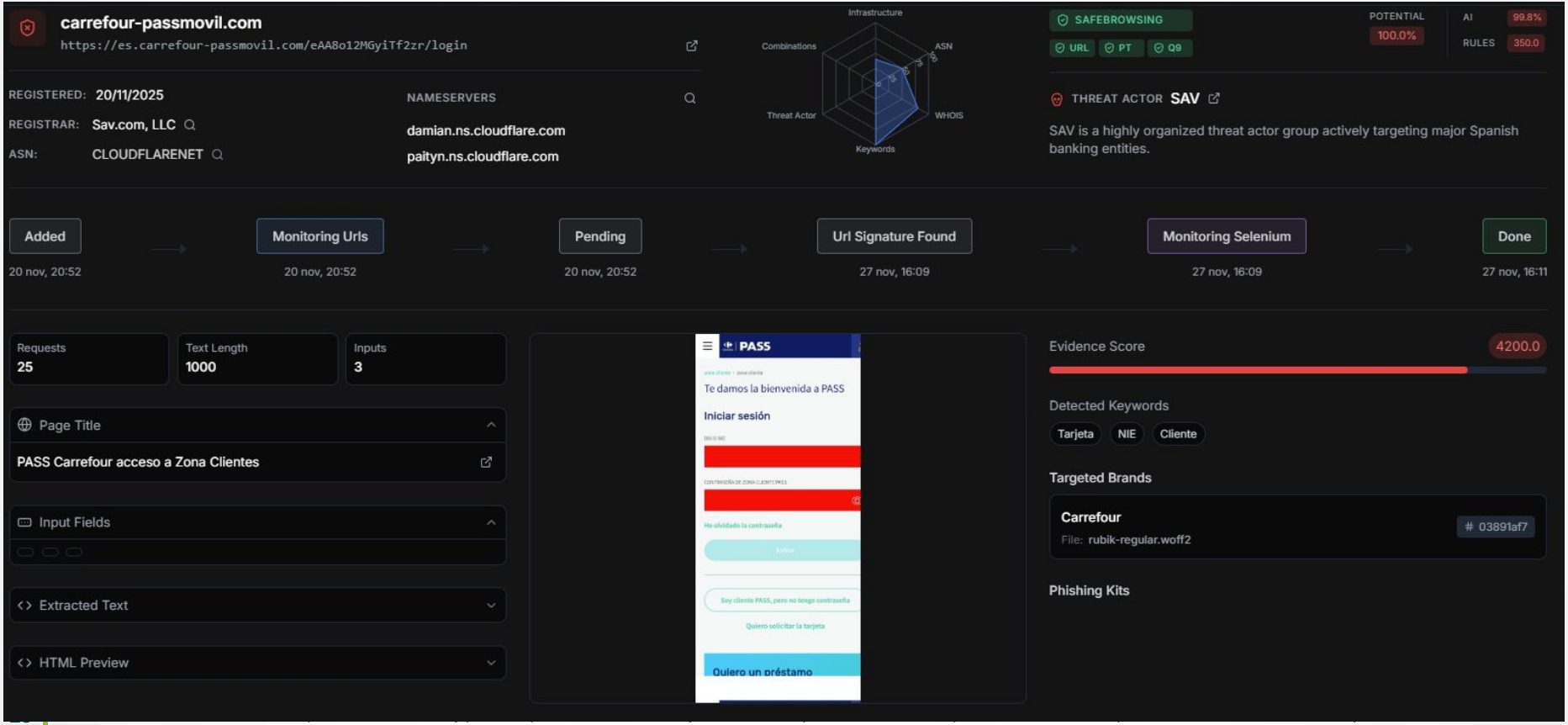
Nuestra tecnología de detección de phishing realiza un escaneo continuo de internet para identificar páginas que suplantan a entidades financieras. Cuando las localizamos, analizamos automáticamente sus vulnerabilidades, aprovechando que estas infraestructuras suelen ser débiles y poco seguras.

Cuando es posible, establecemos un sistema de monitorización que permite capturar en tiempo real la información que los atacantes intentan robar. Estos datos se notifican de inmediato a las entidades afectadas para bloquear accesos, resetear credenciales y prevenir el fraude.

Además, detectamos tarjetas comprometidas y rastreamos los canales donde los delincuentes centralizan la información robada —incluyendo bots de Telegram descubiertos a través de estas vulnerabilidades— para anticipar riesgos y reforzar la protección de los clientes financieros.

Módulo phishing/smishing

Perfilado de sites



Módulo phishing/smishing

credential & card scanning

IRONCHIP

Collected Credentials (59)

COLLECTION DATE	USER	PASSWORD	SOURCE	SITE ID
Dec 9, 2025 Collected: 08:59:18 AM Entered in DB: Dec 9, 2025 08:52:27 AM	[redacted]406L ID: 8192	[redacted]	carrefour karma_todo745f karma_todo745f@localhost	es.carrefour-passmovil.com
Dec 9, 2025 Collected: 02:42:58 PM Entered in DB: Dec 9, 2025 02:42:56 PM	[redacted]7994G ID: 8193	[redacted]	carrefour karma_todo745f karma_todo745f@localhost	es.carrefour-passmovil.com
Dec 9, 2025 Collected: 05:50:34 PM Entered in DB: Dec 9, 2025 05:36:57 PM	[redacted]7767m ID: 8199	[redacted]	carrefour karma_todo745f karma_todo745f@localhost	es.carrefour-passmovil.com
Dec 9, 2025 Collected: 08:12:05 PM Entered in DB: Dec 9, 2025 08:11:36 PM	[redacted]011Z ID: 8204	[redacted]	carrefour karma_todo745f karma_todo745f@localhost	es.carrefour-passmovil.com

IRONCHIP

Fight Against Identity Threats

Julen Martínez
julen@ironchip.com
+ 34 618438991

/

www.ironchip.com