GROUP-IB

Cyber Fraud Fusion

inception
Un evento de TrustDimension 2026

Acerca de Group-IB

Group-IB es un creador de soluciones de ciberseguridad que se dedica a investigar, prevenir y combatir delitos informáticos.

1,550+
Investigaciones exitosas en casos de cibercrimen mediante tecnología avanzada

500+
Empleados en todo el mundo

600+
Clientes corporativos

60
Países

$1 bln
Ahorrados por nuestros clientes corporativos gracias a nuestras tecnologías

 # 1
Proveedor de retención de respuesta ante incidentes

120+
Patentes y aplicaciones

11
Centros de Resistencia contra el Crimen Digital únicos en el mundo

Colaboraciones a escala global

INTERPOL EUROPOL AFRIPOL

Con el reconocimiento de los principales especialistas del sector

FORRESTER Aité Novarica kuppingercole

Gartner IDC FROST & SULLIVAN

FROM GLOBAL TO GLOCAL
INTELIGENCIA DE AMENAZAS EN TIEMPO REAL EN REGIONES CLAVE

GROUP-IB

De la inteligencia de amenazas a la inteligencia de fraude

Cyber Fraud Fusion

Un evento de TrustDimension 2026

¿QUÉ ES CYBER FRAUD FUSION?

GROUP-IB

Gartner

Emerging Tech: Security — Cyber-Fraud Fusion Is the Future of Online Fraud Detection

Published 7 September 2023 - ID G00790000 - 16 min read

By Analyst(s): Dan Ayoub, Pete Redshaw

Initiatives: Emerging Technologies and Trends Impact on Products and Services

> Organizations worldwide have begun merging cybersecurity and fraud prevention teams. This trend will grow through the remainder of the decade. Product leaders must prepare now to lead this shift in positioning and portfolio, outcompete peers, differentiate in the market, and address buyer demands.

Analysis

Trend Description

Cyber-fraud fusion is an emerging trend in online fraud prevention that combines:

- Cyberthreat intelligence
- Identity and access management
- Information security
- Fraud operations and TTPs

Gartner

Cyber-Fraud Kill Chain Has Emerged

The final example of cyber-fraud fusion occurring today includes the introduction of the cyber-fraud kill chain. This represents an emerging methodology and framework that is applied to online fraud prevention and that combines many best practices and well-defined TTPs typically leveraged in cybersecurity for online fraud prevention. The goal is to leverage the cyber-fraud kill chain to improve response and security when a threat is detected so that platform rules and policies can be crafted in a holistic manner.

Forward-leaning OFD vendors are already beginning to apply concepts from traditional cybersecurity frameworks to online fraud prevention. As of today, Gartner is aware of two vendors (Group-IB and ThreatFabric) that have implemented this framework as a form of "fraud intelligence" within their platforms. Gartner has also witnessed several organizations investing in new systems that interface with existing OFD platforms to create the ability to examine the TTPs utilized by adversaries in carrying out specific scams. These TTPs are mapped against relevant portions of the scam and compared with the MITRE ATT&CK Framework, allowing for policies and rules to be crafted to interrupt scams and fraud at multiple places within the user journey.

Strategic Planning Assumption

By 2028, 20% of large enterprises will shift to cyber-fraud fusion teams to combat internal and external adversaries targeting the organization, up from less than 5% today.

CYBER FRAUD FUSION EN ACCIÓN

GROUP-IB

Group-IB CERT has identified a new phishing scam in Brazil where cybercriminals use rogue mobile base stations to send SMS messages to steal personal and financial data

Group-IB's specialists discovered several web open directories with Python scripts allegedly used to brute force email accounts in order to get unauthorized access to SMTP servers of Brazilian companies

Group-IB CERT has identified a new phishing scam in Chile targeting users via SMS messages to steal personal and financial data

Group-IB's threat intelligence team discovered hundreds of LNK files used in a recent Coyote banking trojan campaign allegedly disseminated via WhatsApp targeting Brazilian Windows users

Breve descripción de las tendencias regionales:

01

El equipo CERT de Group-IB identificó una estafa dirigida a bancos de Argentina, que utiliza anuncios falsos para hacerse pasar por canales de contacto oficiales

Estos anuncios, que suelen diseñarse para a
mediante ofertas de beneficios y descuentos,
WhatsApp donde los estafadores utilizan la ir
información personal y bancaria confidencial.
confianza que infunden las marcas reconocid
tendencia más amplia que tiene como objetiv
de Argentina

02

El CERT de Group-IB ha identificado un sofisticado esquema de estafas dirigido a compañías de seguros y sistemas de pago de Colombia

La estafa implica un proceso que consta de var
fraudulentos que se hacen pasar por marcas le
utilizan bases de datos públicas de licencias de
usuarios de la autenticidad del sitio, mostrando
vehículo. Aquellas víctimas cuyo seguro ha ven
sitio, en el que se les solicita que brinden infom

UNIQUE MISSION-DRIVEN UNIFIED PLATFORM

GROUP-IB

Creamos una plataforma única que integra productos para la ciberseguridad, la protección de la marca, la lucha contra el fraude y todos nuestros servicios, incluidas las investigaciones, la auditoría, la formación, el análisis forense digital y la respuesta a incidentes

UNIFIED RISK PLATFORM

Threat Intelligence & Digital Risk Protection

- Knowledge about threats — Threat Intelligence — Breach detection
- Vulnerabilities detection — Attack Surface Management — AI Investigation Graph
- Scam protection — Digital Risk Protection — AI detection and Auto-response

AI Driven Killer features

Fraud protection

- Web protection — AI to detect malware and scam
- Mobile protection — AI to detect malware and scam
- Real time prevention — Continuous session monitoring

AI Driven Killer features

Services

- Investigations and Incident response
- Audit & Consulting
- Managed Detection and Response and Takedown

20 years of experience and supportive technologies

Extended Detection and Response

- Network protection — Network Traffic Analysis — AI detecting threats in covert channels
- Malware behavioural analysis — Malware Detonation Platform — AI anti-evasion detection
- Email protection — Business Email Protection — AI text analysis and user behaviour simulation
- PC and servers protection — Endpoint Detection and Response

AI Driven Killer features

Killer features

Protection modules enrich other modules and experts

AI-Powered Predictive Analytics

Intelligence Data Lake

Intelligence Data Lake real time enriched with detection modules and human experts

Experts enrich with unique knowledge

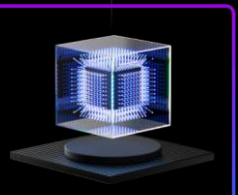
INCIDENT RESPONSE

INVESTIGATIONS

EXPERTS

COMPUTER EMERGENCY RESPONSE TEAM

THREAT RESEARCHERS



AI DRIVEN ANALYTICS

Notation:

AI Artificial Intelligence

DIVERSAS FUENTES DE INTELIGENCIA

OPEN-SOURCE INTELLIGENCE

- Paste sites
- Code repositories
- Exploit repositories
- URL sharing services

MALWARE INTELLIGENCE

- Detonation platform
- Malware emulators
- Malware configuration files extraction
- Public sandboxes

DATA INTELLIGENCE

- C&C server analysis
- Darkweb card shops
- Phishing and malware kits
- Compromised data-checkers

HUMAN INTELLIGENCE

- Malware reverse engineers
- Undercover dark web agents
- Regional specialists
- Embedded managed service teams

SENSOR INTELLIGENCE

- ISP-level sensors
- Honeypot network
- IP scanners
- Web crawlers

VULNERABILITY INTELLIGENCE

- CVE list
- Exploit repositories
- Dark web discussions
- Threat campaigns mapping

LAW ENFORCEMENT AND SECURITY PARTNERS

- Operations with Interpol and Europol
- Local law enforcement investigations
- CERT community partners
- Technology partners

FRAUD INTELLIGENCE

- Web channel fingerprinting
- Digital biometrics
- Hosting detection
- Multi-account monitoring

ENDPOINT INTELLIGENCE

- Windows and Linux clients
- Android and iOS SDK
- Machine learning analysis
- Malware detonation

NETWORK INTELLIGENCE

- Email package scanners
- Open protocol and encrypted traffic analysis
- Traffic metadata
- Network log collection

MARKETPLACE INTELLIGENCE

- Mobile app store scanning
- Advertisement research
- Marketplace analysis
- Messengers & social media monitoring

BRAND INTELLIGENCE

- Search engine & domain name monitoring
- Cloud storage scanning
- Dark web mentions detection
- Scam campaigns mapping

AUDIT

- Penetration testing
- Compliance audit
- Application assessment
- Social engineering testings

SERVICES

- Endpoint threat hunting
- Host-level artifact collection
- TTP and IoC identification
- Malicious behavior detection

DFIR

- Digital evidence collection
- eDiscovery
- Kill chain reverse engineering
- Transaction analysis

CYBER FRAUD FUSION GROUP-IB FRAUD MATRIX

Proporcionamos una hoja de ruta completa para la protección contra el fraude

Threat Intelligence & Digital Risk Protection

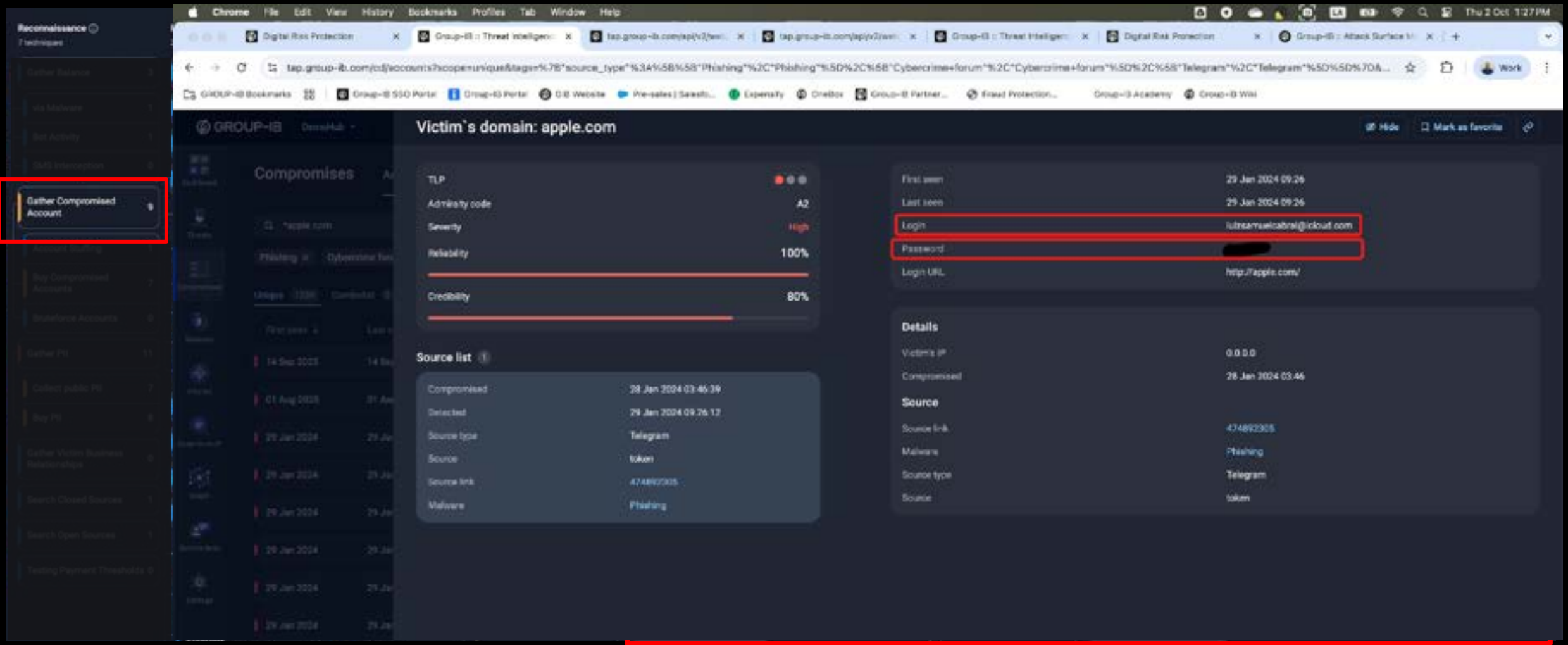
Fraud Protection

Podemos detener el ataque, en cada paso

CYBER FRAUD FUSION GROUP-IB FRAUD MATRIX

Proporcionamos una hoja de ruta completa para la protección contra el fraude

Threat Intelligence

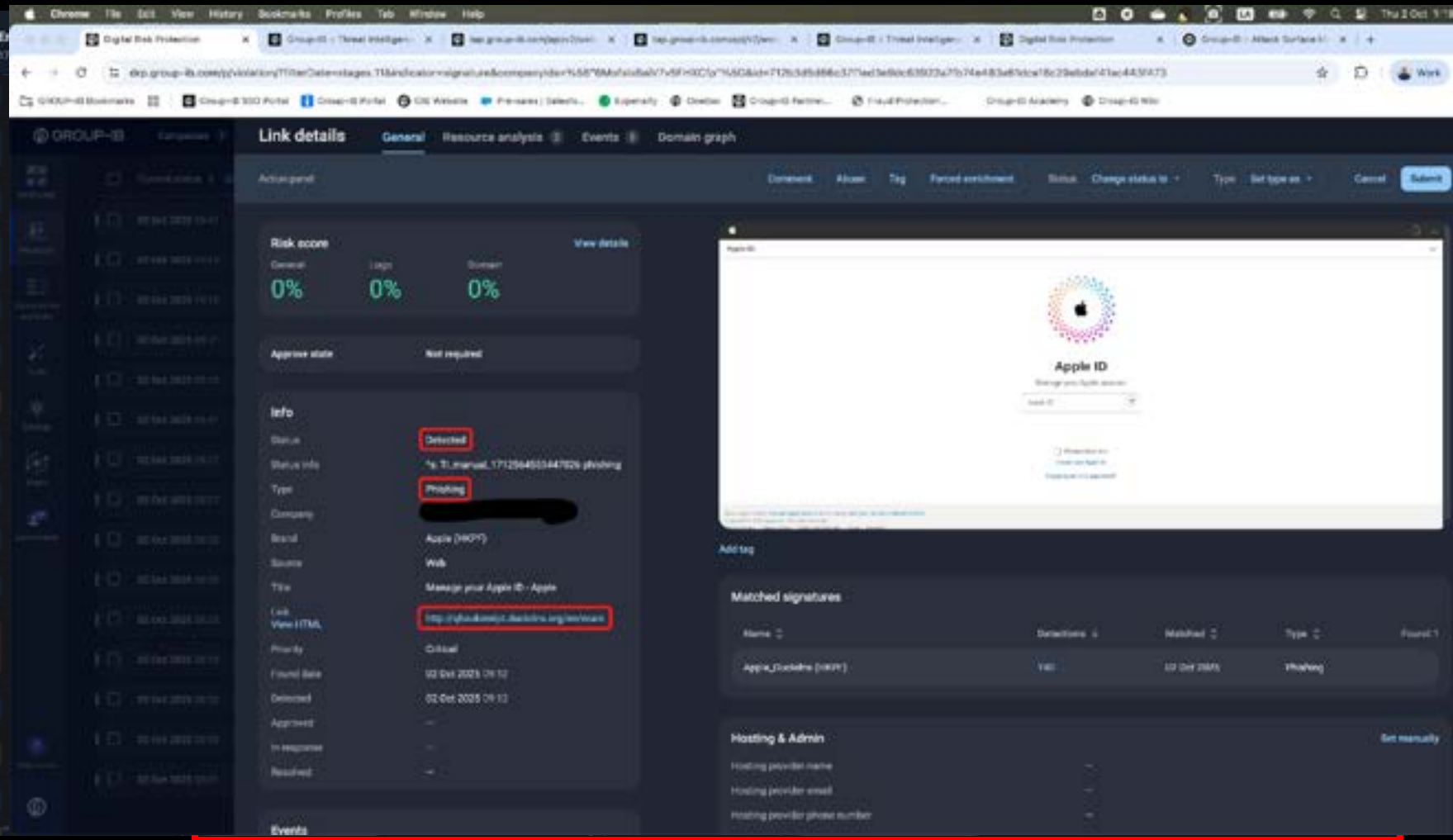


Podemos detener el ataque, a cada paso

CYBER FRAUD FUSION GROUP-IB FRAUD MATRIX

Proporcionamos una hoja de ruta completa para la protección contra el fraude

Digital Risk Protection

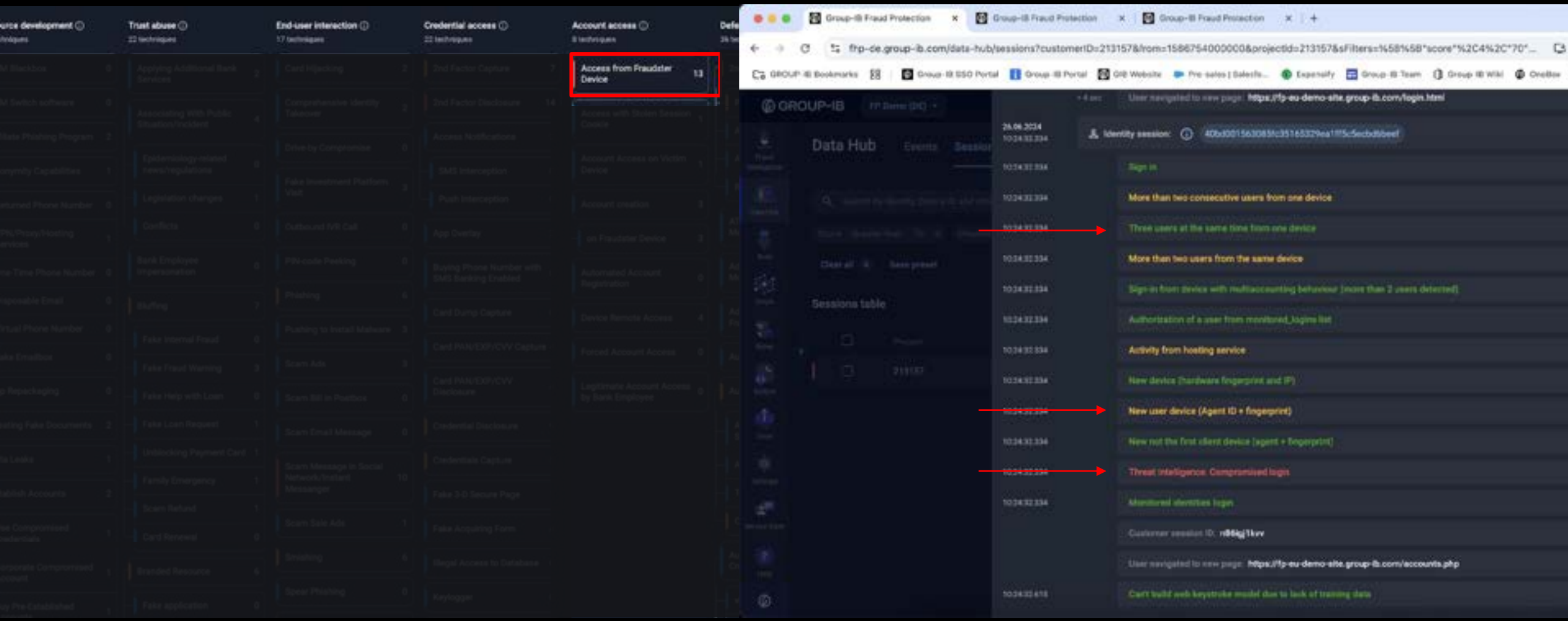


Podemos detener el ataque, a cada paso

CYBER FRAUD FUSION GROUP-IB FRAUD MATRIX

Proporcionamos una hoja de ruta completa para la protección contra el fraude

Fraud Protection



Podemos detener el ataque, a cada paso

CYBER-FRAUD FUSION: INTELIGENCIA DE AMENAZAS

GROUP-IB

THREATS & ACTORS

- More than 2.800 bad actor profiles
- Global cybersecurity threats feed with attribution
- Customizable Threat landscape
- Detailed information about threats and actors including IoCs and activity timeline

DARKWEB

- Full access to our Dark web database
- Instant Messenger monitoring for Telegram and Discord
- Live translation of messages
- Unlimited Threat hunting rules to improve monitoring

COMPROMISES

- End user or employee compromised credentials
- Information leaked on public sources like Pastebin sites.
- Sensitive data leaked on code repositories like GitHub
- Corporate data leaked in public breaches

BANKING

- Compromised Bank Cards information
- Masked Bank Cards information

MALWARE

- Group-IB detonation platform
- Over 1.400 malware reports
- Malware configuration files
- Vulnerabilities feed
- Phishing kits

SUSPICIOUS INDICATORS

- Deface attacks feed
- DDoS attacks feed
- Phishing sites feed
- Malicious IPs used for: VPNs, Scanning, Thor nodes, Proxys

GRAPH

- Advanced Investigation Platform
- Visual Search engine for Group-IB Threat Intelligence data lake

CYBER-FRAUD FUSION: PROTECIÓN DE MARCA

GROUP-IB

Analyze your digital presence

Monitoring tools:
- Parsers
- Crawlers
- APIs

Monitoring path:
- Proxy scheduler
- User-agent scheduler
- Special/ dedicated accounts

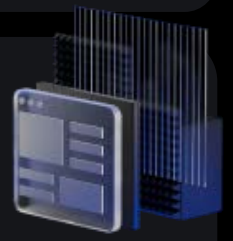
~3,000,000/day across all digital sources 24/7/365

ADVANCED FEEDS

- REFERRER LOGS
- DMARC/DKIM/SPF
- FRAUD PROTECTION SNIPPET
- CUSTOMER'S REPORTS
- C&C SERVERS
- BUSINESS EMAIL PROTECTION
- GRAPH ATTRIBUTION
- MALWARE CONFIGS

and more..

MONITORING SOURCES



- Domain names
- Databases of phishing resources
- Search engines
- Social media
- Mobile app stores
- Online classifieds and marketplaces
- Advertising
- Instant messengers
- Deep/dark web

DIGITAL RISK PROTECTION

DATA ANALYSIS

- Logo analysis
- Text recognition
- Image recognition
- Regular expressions
- Signature analysis
- Neural networks
- General score
- Domain name score

IDENTIFICATION, PRIORITIZATION

- Brand name mentions
- Violation determination
- Enforcement prioritization

AUTOMATED

HOW WE ENFORCE

1 NOTIFICATION

Identify the resource owner and request to remove the detected violation

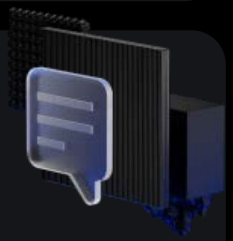
2 ESCALATION

Use partnership network to enforce the removal of the violation

3 CEASE-AND-DESIST

Obtain an official pre-trial order to take down the detected violation

RESPONSE



Comprehensive takedown procedure reaching an 85% pre-trial takedown rate on average

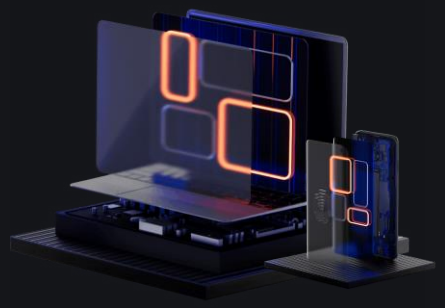
AUTOMATED & MANUAL

CYBER-FRAUD FUSION: PROTECIÓN DE FRAUDE

GROUP-IB

Protección continua en todos los canales digitales

Página Web o Aplicación Móvil



- Inteligencia de dispositivos
- Detección de bots
- Detección de malware
- Detección de acceso remoto
- Detección de llamadas telefónicas activas
- Integridad del SO
- Comprobación de ID global

Análisis de Login & Password

- Biometría de inicio de sesión
- Comprobaciones antiphishing
- Huella digital del dispositivo
- Geolocalización
- Análisis del tipo de conectividad
- Autenticador sin contraseña

Monitoreo Continuo

- Comportamiento de la navegación en comparación con sesiones anteriores
- Detección de scripts
- Detección Man-in-the-Browser
- Detección de acceso remoto
- Llamada telefónica activa

Monitoreo de Transacciones

- Tarjetas bancarias comprometidas
- Cuentas Mula
- Análisis de vínculos de cuentas (AML)

*Todos los scripts, el tráfico y los datos están encriptados para evitar su interceptación por terceros. No se recogen datos de identificación personal (PII).

CYBER-FRAUD FUSION: PROTECIÓN DE FRAUDE

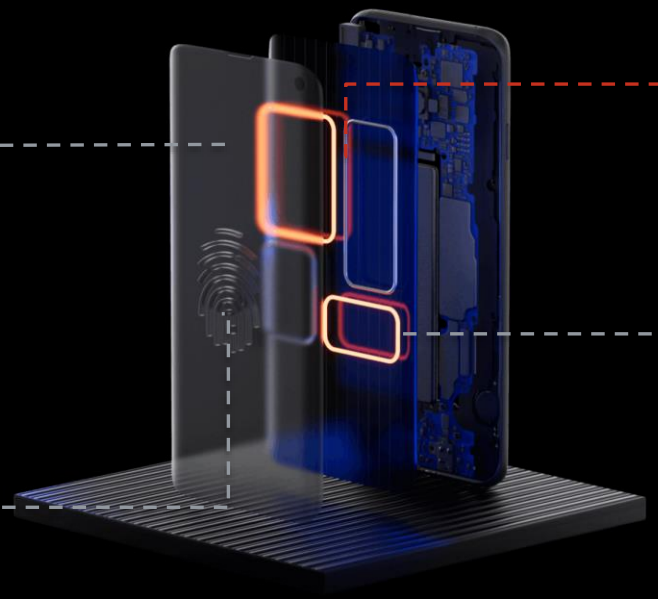
GROUP-IB

Perfiles completos de comportamiento de clientes

- Análisis del comportamiento
- Puntuación de onboarding
- Perfiles de geolocalización
- Detección de acciones de alto riesgo
- Perfiles de subredes IP
- Dispositivos y cuentas de confianza / bloqueados

Mapa de calor de desplazamiento de usuarios

Gráficos de pulsaciones de teclas de usuarios



Conexiones de dispositivos y cuentas de usuarios

Geolocalización de usuarios

Análisis detallado del entorno técnico del usuario

- Análisis de plataforma cruzada
- Detección de VPN/Proxy
- Detección de programas maliciosos
- Detección de bots
- Huella digital de dispositivo
- Detección de navegadores antidetección

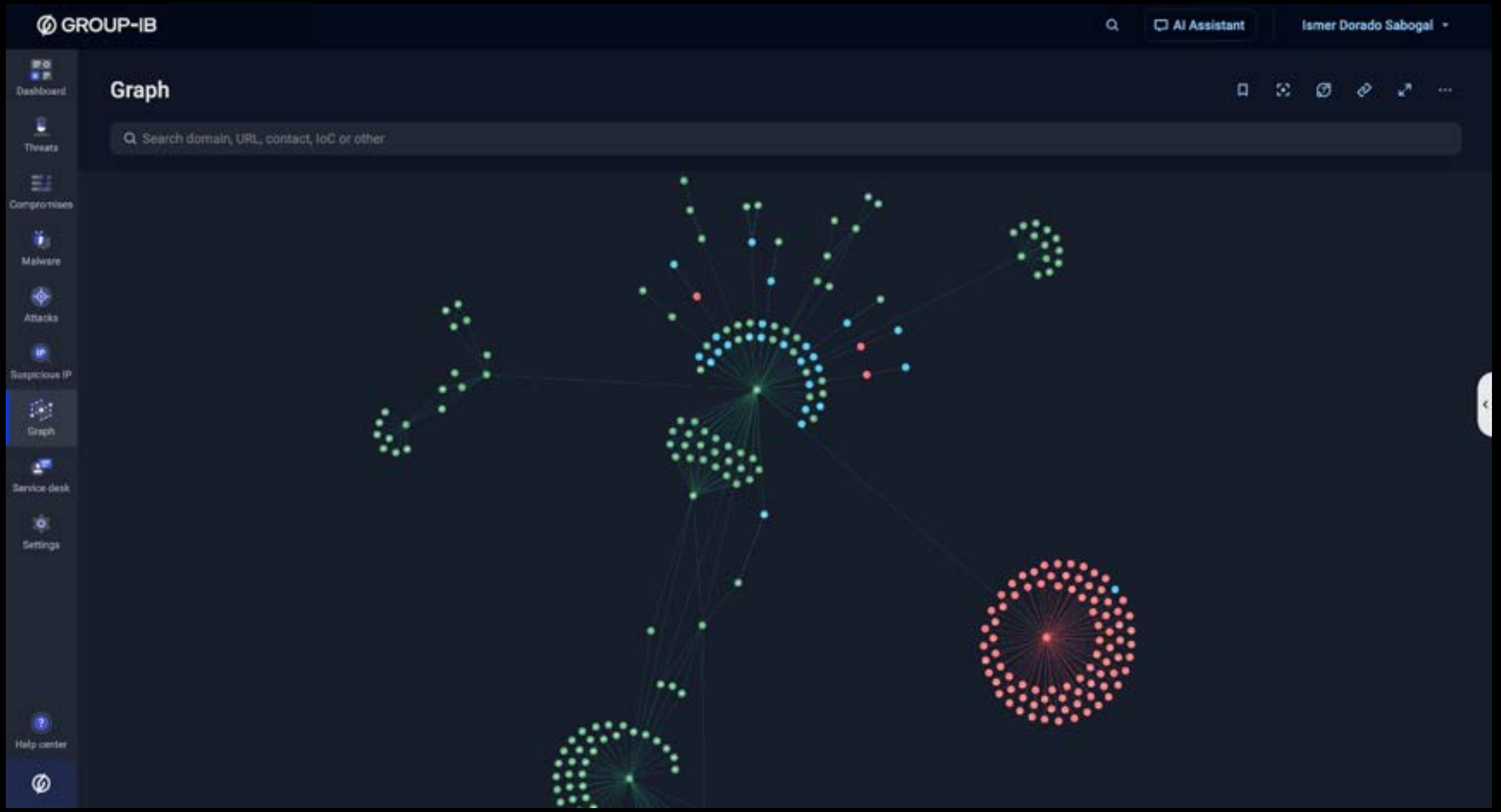
INTELIGENCIA CONTRA EL FRAUDE

Información sobre suplantación de identidad de dispositivos y redes	Dispositivos y credenciales de usuarios comprometidos	Información sobre esquemas de fraude	Direcciones IP e infraestructura de los estafadores	Páginas de *phishing* y sitios web fraudulentos	Perfiles de estafadores	Tarjetas de crédito y cuentas bancarias comprometidas

INTELIGENCIA DE LA WEB OSCURA | **INTELIGENCIA DE AMENAZAS A ESCALA REGIONAL** | **INTELIGENCIA SOBRE PROGRAMAS MALICIOSOS BANCARIOS** | **FUENTES DE INTELIGENCIA TÉCNICA** | **FUENTES DE INTELIGENCIA DE CÓDIGO ABIERTO**

CYBER-FRAUD FUSION: **GRAPH**

GROUP-IB




GROUP-IB
inception
Un evento de TrustDimension 2026
Muchas gracias