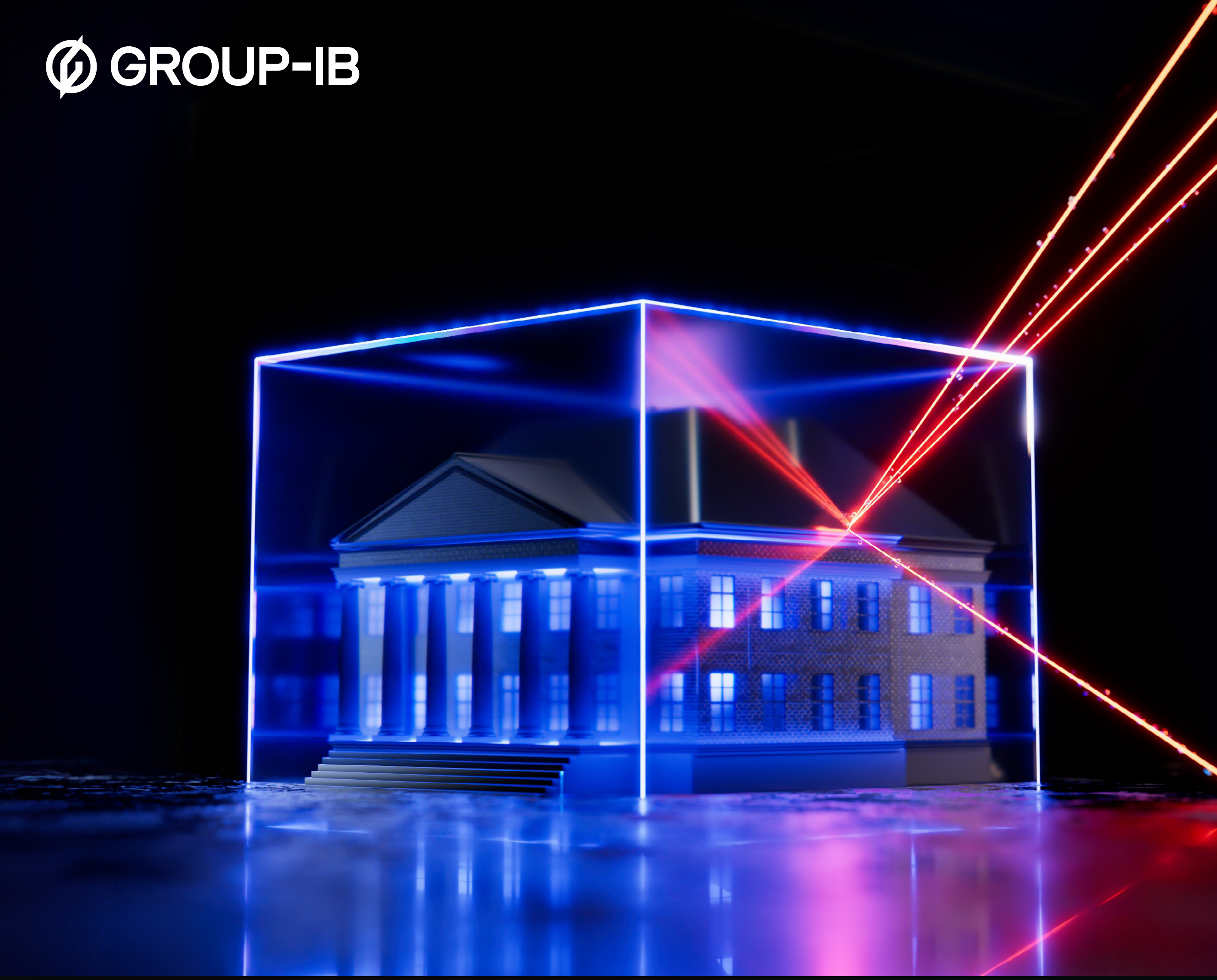
GROUP-IB



CASE STUDY

FINANCIAL CRIME

Combating financial crime for a tier-1 global bank using Group-IB Threat Intelligence (TI)

Introduction

Industry	FSI (Banking)
Region	Europe

Being a globally renowned bank means always upholding your fiduciary responsibility to support and protect everyone within your ecosystem - customers, associated businesses, and stakeholders.

While geographic expansion can bring significant business benefits, it exposes organizations to global cybersecurity challenges that, if left unevaluated, can disrupt operations indefinitely. In the world of finance, **cybersecurity is of paramount importance.**

Therefore, Group-IB empowers businesses with a powerful ecosystem of cybersecurity solutions. The company's mission is to secure operations, ensure compliance, and robustly defend financial institutions against emerging cyber threats.

Identifying the gap in the bank's existing cybersecurity

Modern banking demands **faster and more effective risk decisions.** Real-time threat detection and interdiction rely on the agility and preciseness of the generated threat insights.

The insights should be accurate, contextual, and actionable to help teams prioritize security tasks, and facilitate timely mitigation. It is also crucial to consolidate insights from the entire infrastructure into an actionable framework to ensure complete and across-the-board cyber protection.

Any security blindspots can significantly weaken the security posture of an organization. This exact challenge became the forefront issue for the bank, leading it to part ways with its previous Threat Intelligence (TI) vendor.

Initial Pain Points:

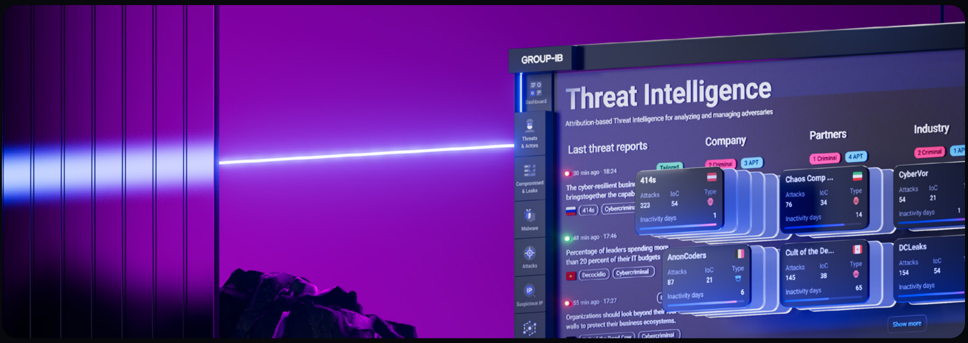
- Low context of Threat Intelligence which was mostly based on public sources and a lot of indicators were hidden.
- Poor operational Intelligence with a high level of false positives.
- Below-par risk advisory services
- Lack of critical insights to help evaluate and improve the cybersecurity posture.
- Extremely long incident response times and lack of support for phishing resources takedowns.
- Poor card and credential management

Bank's choice of arsenal to beat cybercrime

Group-IB Threat Intelligence (TI)

To beat the diversifying nature of the financial crime

- Industry's largest adversary-centric Threat Intelligence
- TI maps the tracks of threat actors to proactively elaborate the relevance, propensity, and the scope of threats to a business.



Group-IB Digital Risk Protection (DRP)

To comprehensively defend its digital presence

- AI-powered, all-in-one digital protection tool
- Digital Risk Protection (DRP) protects the business and its customers against brand-related scams by monitoring its digital footprint, detecting violations, and prioritizing and initiating appropriate takedown tactics.

Solutions offered

Group-IB Threat Intelligence

- Recognized as world's largest source of adversary-centric intelligence, Group-IB Threat Intelligence (TI) supports digital crime-nabbing operations of global businesses and law enforcement agencies.
- By seamlessly integrating Threat Intelligence into its existing infrastructure, the bank gained the ability to constantly profile threat actors, swiftly detect advanced attacks and techniques, flag network anomalies at their first indication, and respond to emerging threats with lightning speed.
- The context-rich data provided by Threat Intelligence (TI) helped the bank establish connections between credential attacks and understand the likelihood of account takeovers, and illegal money movements. This correlation capability helped minimize false positives in detection algorithms, reduce costs, and enable investigators to concentrate their efforts on real incidents.

GIB-CERT

(Computer Emergency Response Team)

- Recognized as first incident responders, Group-IB's CERT offers 24/7/365 threat triage.
- Group-IB's CERT also offers the quickest takedowns for phishing and non-phishing resources (malicious mobile applications, infected websites, compromised servers, etc.) to neutralize threats and protect the client’s brand and cash flow.

High-quality compromised Credit Card (CC) data

- Leveraging high-quality compromised credit card data offers robust fraud detection insights including information on money mules, and account activity.
- The data empowers banks to stop fraud in their tracks, saving millions of dollars.

Extended cybersecurity capabilities with Attack Surface Management (ASM) + Digital Risk Protection (DRP)

- More solutions were added to extend coverage and provide a truly unified risk management. The comprehensive anti-scam module was chosen as a natural complement.
- The choice was made on the basis of a thorough evaluation of the most suitable solution and DRP eventually emerged as the best product.

Success highlight

Quickest takedowns through Group-IB's CERT and DRP teams*

Improved customer experience and loyalty

Increased fraud detection

Improved detection of targeted threats

* 24 hours or even less, depending on the case

Conclusion

Acting as the first line of defense, Group-IB Threat Intelligence currently supports the global bank with insights on the broadest coverage of threats. With its across-the-board visibility, contextual threat information, and agile detection capabilities, Threat Intelligence (TI) coupled with Digital Risk Protection (DRP) and CERT's takedown capabilities empower the bank to effectively prioritize resources and strengthen its security stance against its most pressing cybersecurity challenges.

The unique insights into the threat landscape relieve the bank's SOC from the strain of continuous monitoring and investigation, enabling efficient alert management, and thus, bolstering the overall security posture. See Group-IB Threat Intelligence in action below.

Explore ↗

Unprecedented challenges require unbeatable solutions. Ground your cybersecurity on industry-leading Threat Intelligence.

Learn more ↗