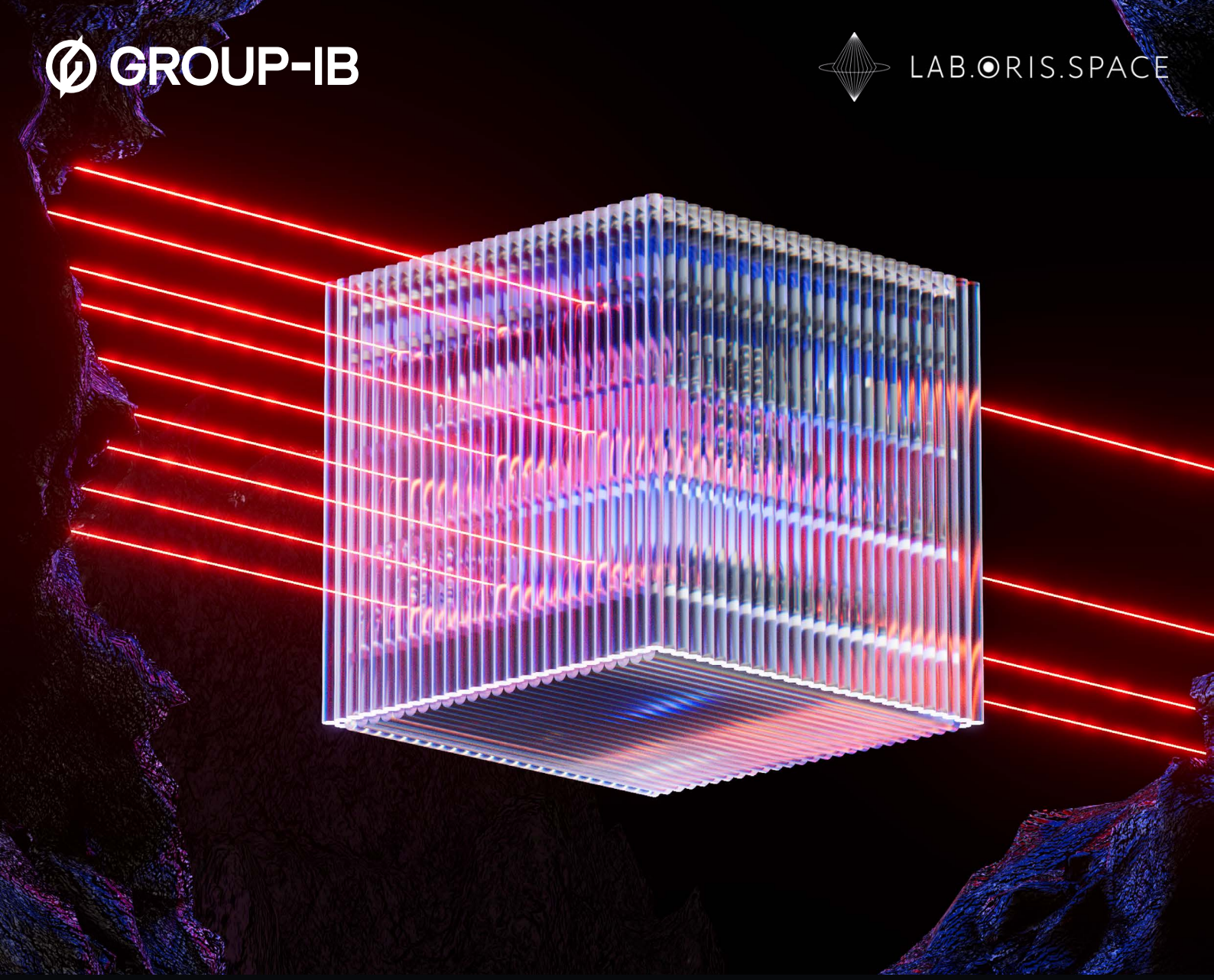
GROUP-IB

LAB.ORIS.SPACE



SUCCESS STORY

GROUP-IB X ORIS LAB

Software security assessment through penetration testing

About Oris Lab

Industry	Blockchain
Year founded	2013
Solutions	Secure reception and transmission of textual and structured information Crypto custody service Crypto WorkFlow Business process management system Safina (application server)

Since 2021, Oris Lab has been part of Astana Hub, an international technological cluster for IT startups.

Oris Lab is a software company based in Kazakhstan specializing in unique fintech solutions that combine blockchain with traditional finance.

The Oris Lab team brings together seasoned financial experts and IT specialists, each with many years of experience in banking, brokerage, and related fields. By merging the accumulated knowledge and capabilities provided by blockchain technology, the company supplies the international market with solutions that provide complete protection for crypto assets.

Context

Oris Lab's key objective is to ensure the highest level of security for user and customer data.

The cryptocurrency and blockchain sectors are becoming increasingly appealing to not only investors and enthusiasts but also threat actors. As attackers improve their techniques and methods, the number of breaches in the cryptocurrency industry grows. Evidence shows that even a service with an excellent reputation can fall victim to a hacker attack and lose all the user funds that it stores.

To protect assets from threat actors, cryptocurrency storage and management services (called "custodians") have been created. Oris Lab offers a comprehensive solution in this field.

To make sure that its products are secure and to eliminate potential vulnerabilities, Oris Lab requested a penetration test to be conducted for the following interrelated software products: Black Box, Safina, and crypto custody service.

Black Box is the core of Oris Lab's information system for managing crypto assets. It consists of subsystems for encrypting and storing keys, interacting with blockchains, and determining rules for using private keys.

Safina is an application server that ensures interaction between the system and the outside world through dedicated applications.

Crypto custody service brings together Black Box, Safina, and the business process management system.

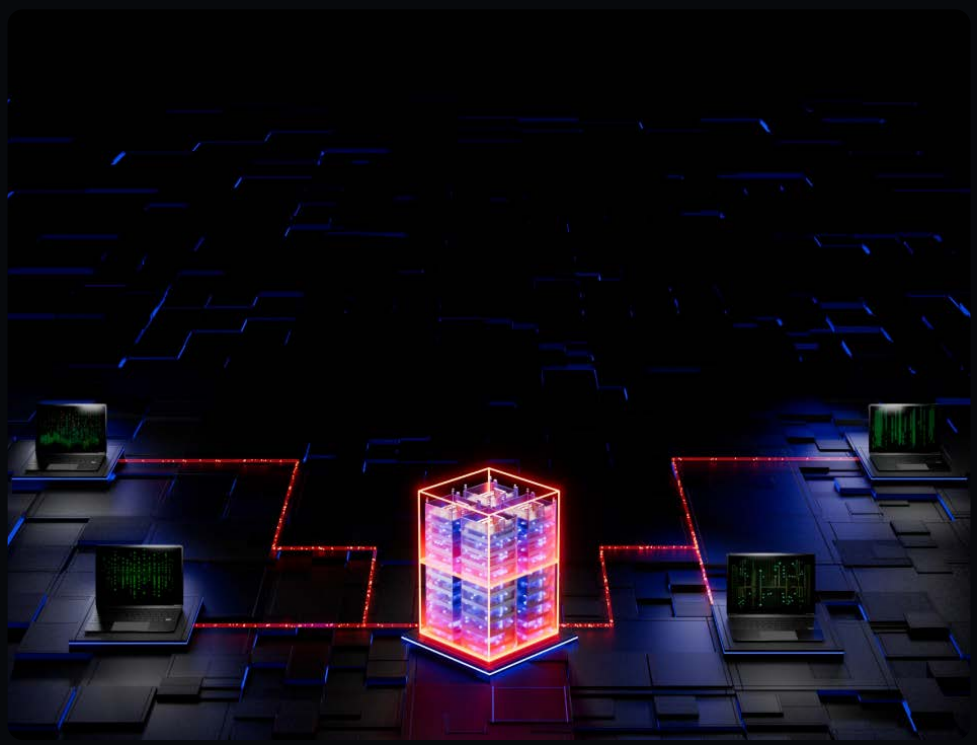
Why Group-IB?

Penetration testing service providers obtain information about the most vulnerable parts of the customer's infrastructure. Carefully choosing a provider is a matter of not just quality but also safety. In addition to an immaculate reputation, Group-IB's Audit & Consulting team has extensive expertise in the field.

> I have heard a lot of positive things about Group-IB from friends and colleagues. Even ChatGPT recommends it, and the number of tests and certificates that Group-IB's Audit & Consulting team has under its belt speaks for itself. Eventually I followed my intuition, and once again it did not let me down.

ALEXANDR KOLOKHMATOV

CEO, Oris Lab



Group-IB's solution

Group-IB's Audit & Consulting team conducted a comprehensive penetration test and assessed Oris Lab's security systems and external infrastructure. In addition, at the customer's request, Group-IB experts tested the possibility of gaining access to crypto wallet data.

The penetration test was carried out using the black box method, which means that Group-IB specialists independently conducted external reconnaissance and identified resources for the test. Within 25 days, Group-IB's team had tested the security of Oris Lab resources against internal and external attacks.

The penetration test included the following stages:

- Collecting information: Conducting reconnaissance and gathering data about available applications
- Searching for and analyzing vulnerabilities: Checking network services and applications for vulnerabilities
- Exploitation and post-exploitation of vulnerabilities: Modeling attacks against the entities in question
- Reporting: Analyzing and structuring the results

Result

- A multi-vector penetration test showed that Oris Lab has effective security measures and policies in place. The detected vulnerabilities were promptly eliminated as per Group-IB's recommendations.
- The Black Box crypto key storage successfully passed all tests. The project demonstrated that it is impossible to gain unauthorized external access to the core of Oris Lab's information system.
- Group-IB's Audit & Consulting team also detected non-critical vulnerabilities in legacy applications. After learning that such shadow assets are potentially dangerous, Oris Lab made the decision to discontinue support for them.

> "Group-IB's team provided a detailed report with an analysis of systems and processes. They identified vulnerabilities and made recommendations on how to eliminate them. The results of the external penetration test showed that our security measures and policies are effective. The detected weaknesses were promptly eliminated and the recommendations on how to enhance the system's security will be taken into account for future improvements.

NIKOLAY VINOKURTSEV

Security Engineer, Oris Lab

> "Oris Lab's team studied Group-IB's recommendations on how to enhance the security of Oris Lab's systems. The recommendations will be taken into account when integrating solutions for developing and modernizing our software suite. Oris Lab appreciates Group-IB's professionalism and hopes to work closely together in the future.

ALEXANDR OZEROV

CTO, Oris Lab

GROUP-IB

LAB.ORIS.SPACE

Preventing and investigating cyber-crime since 2003

70K

hours of incident response experience

1,3K

investigations worldwide

Group-IB is a leading provider of high-fidelity adversary tracking and threat detection, and best-in-class anti-APT and online fraud prevention solutions.

We hunt down real cybercriminals, catch them before they can harm your business, and provide evidence that puts them in jail. We also train security professionals around the globe.

Our clients include banks, financial institutions, oil and gas companies, telecoms, IT and cloud service providers, e-commerce and FMCG companies, and fintech and blockchain startups. We especially enjoy working with the next generation of cybersecurity specialists who share our passion for threat hunting.

Discover Group-IB Audit & Consulting services

LEARN MORE

CONTACT US