SUCCESS STORY

GROUP-IB × OSOM

Security testing of a crypto
wealth manager

About OSOM

INDUSTRY

Crypto Finance

ACTIVITIES

Crypto Wealth Manager using artificial intelligence to build portfolios

YEAR OF FOUNDATION

2018

OSOM is a member of FINTECH BELGIUM and Blockchain for Europe.

FINTECH
BELGIUM

BLOCKCHAIN
FOR
EUROPE

OSOM is a Belgian-Estonian wealthtech company proudly created by Polybius in 2018. OSOM strives to transform personal finance, allowing you to smartly manage and diversify exposure to Crypto in minutes.

To reach this goal, OSOM, the Crypto Wealth Manager, is EU-regulated and available in most countries. It offers an algorithmic portfolio construction solution called Crypto Autopilot to automatically manage and diversify your holdings, DeFi Earn to earn interest from lending in decentralized finance, a safe wallet and exchange.

Tracking over 200 cryptos and with an investable universe of nearly 100, the Crypto Autopilot is the best way to get access to an actively managed diversified portfolio of high-performing assets. With 2 stablecoins and 4 lending pools, DeFi Earn offers the best risk-reward profile of lending in DeFi.

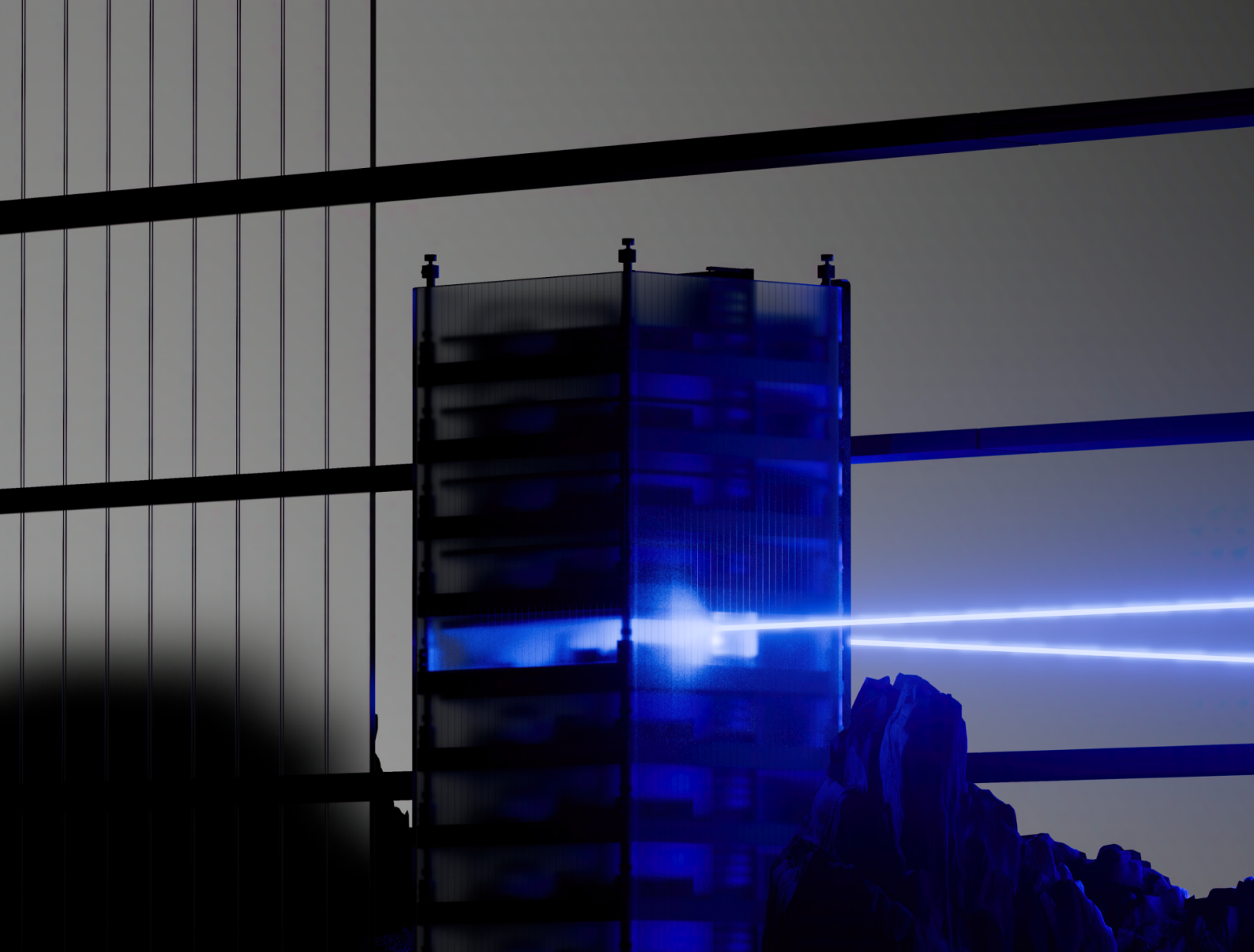| 6,000+	4+	3
happy users from over 100 countries	Stores and Trustpilot	awards in 2021

Background

Companies operating in the financial sector traditionally remain the most attractive target for attackers. Market participants have to take a very careful approach to ensuring the security of their infrastructure, especially the security of applications that their customers work with.

The past year has been a real challenge for companies: pandemic and the resulting need for a mass transfer of staff to remote work only complicated the work of maintaining the organization's information security. The ever-increasing number of methods and ways of attacks targeting infrastructure and information systems poses a serious threat to the financial sector.

Regular security testing of web-applications has been relevant for financial institutions before, but in 2020's this became a vital necessity. Customers are willing to trust their money to secure companies. And the way to confirm the security of web-application is to go through an independent security analysis. This type of work allows you to detect vulnerabilities and lacks of various levels of risk, as well as to determine the current level of security of applications and protection systems used.

OSOM requested a planned security analysis of the "app.osom.finance" web-application from Group-IB.

Why you chose Group-IB

Group-IB is one of the biggest players on the market with a great feedback from customers. The main factors for us were the number of services they offer, quality, feedback, and price

Dmitri Ahmarov, CTO OSOM

Group-IB services

Group-IB service
Web application security analysis

The web application security analysis service includes a complex of actions aimed at researching applications, finding and exploiting various levels' impact vulnerabilities, formation of attack vectors and modeling the actions of an attacker to implement unauthorized actions. Such as escalating privileges, gaining access to sensitive data, calling a denial of service, stealing money, and other data activity related to integrity, confidentiality, and availability.

The objective was to conduct a comprehensive independent vulnerability testing and security assessment of the web application app. osom.finance and its existing defense mechanisms. The Customer provided Group-IB experts with two accounts and had a test card issued for making payments, so that the application was tested from all perspectives.

During the analysis, not only the application itself was tested, but also its environment, including the API. In addition to finding the technical vulnerabilities of the application, check of lacks in the business logic also has been tested.

The "Gray box" was selected as the test model. This test model is more detailed and comprehensive than the "Black box" model. As initial conditions, the Contractor's specialists had at their disposal the accounts of roles provided in the application, which made it possible to imitate a potential attacker with various access rights to the system.

Results

Report of analysis
Report including detailed findings and recommendations

During the cooperation between OSOM and Group-IB the following results were achieved:

→ as a result of engagement, no critical issues were found. Discovered vulnerabilities mostly refer to lack of necessary security mechanisms which may potentially give a offender an ability to manipulate account's balances and use brute-force in order to compromise user accounts;

→ OSOM was recommended to integrate into the application's lifecycle processes that detect and eliminate vulnerabilities at development stages, use best secure coding practices, checklists and enhance protective mechanisms linked to user accounts management.

We are very satisfied with the results provided by Group-IB, especially that we do not have really critical issues. They did their job in time and shared with us the detailed report with the conclusions and possible solutions which is really helpful.

Dmitri Ahmarov, CTO OSOM

About Group-IB

Group-IB is a creator of cybersecurity technologies to investigate, prevent and fight digital crime.

1,400+
Successful investigations of high-tech cybercrime cases

300+
employees

600+
enterprise customers

60
countries

$1 bln
saved by our client companies through our technologies

#1[*]
Incident Response Retainer vendor

120+
patents and applications

7
Unique Digital Crime Resistance Centers

* According to Cybersecurity Excellence Awards

Global partnerships

INTERPOL

EUROPOL

AFRIPOL

Recognized by top industry experts

FORRESTER®

Aité Novarica

KUPPINGERCOLE ANALYSTS

Gartner.

IDC

FROST & SULLIVAN

Fight against cybercrime