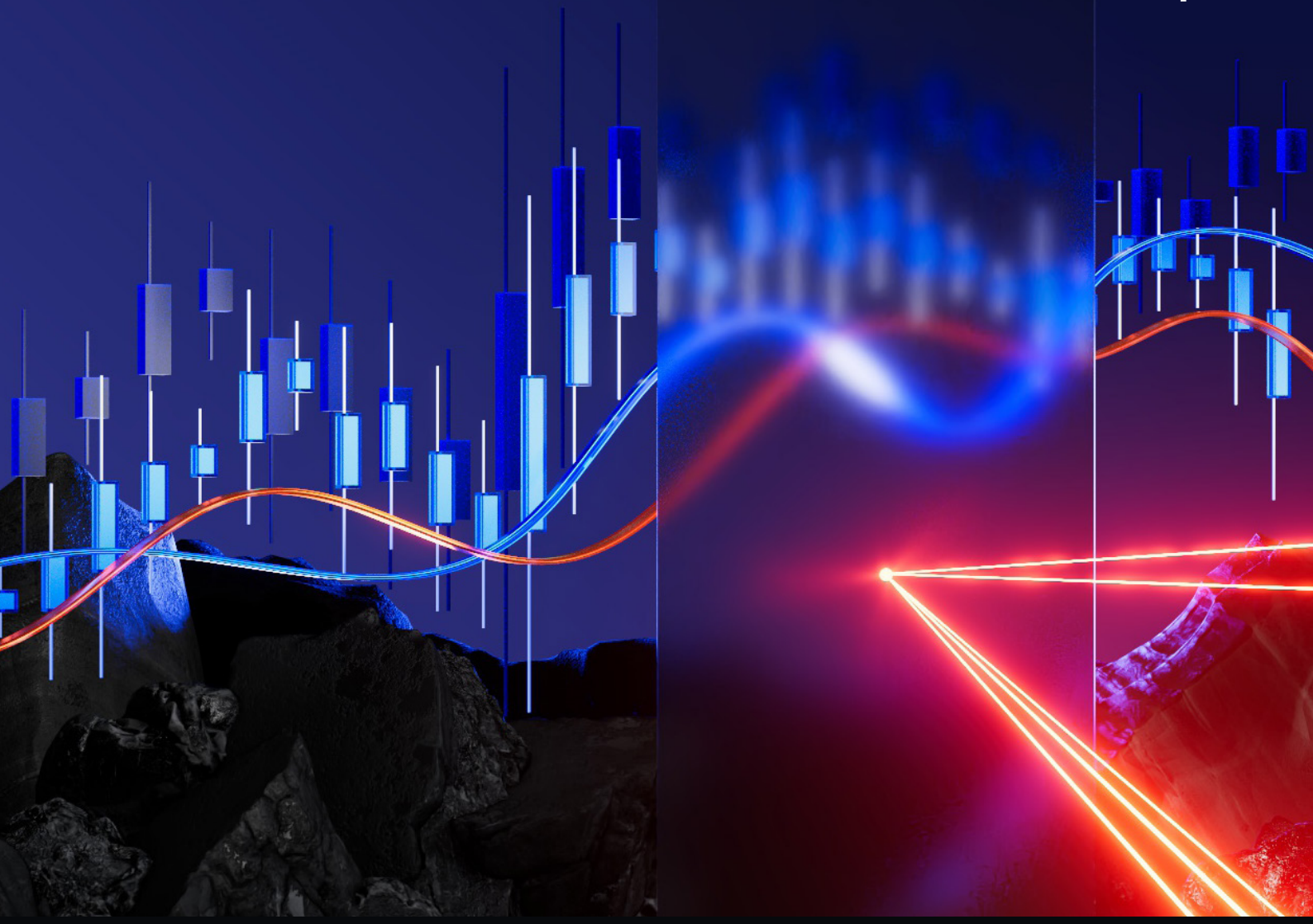
GROUP-IB

Libertex™ Group



SUCCESS STORY

SECURING INTERNATIONAL TRADING ON LIBERTEX GROUP

Group-IB's strategic Audit and Consulting Services

GROUP-IB.COM

Introduction

Industry	Online trading (financial services)
Size	700+ employees
Platform users	3M+ customers
Headquarters	Limassol, Cyprus

The sheer volume of transactions conducted every day on online trading platforms, combined with their complex nature, has made them a favorite target among hackers. Cybersecurity is at the forefront of how to address this growing issue. Whether customers are trading assets, fiat currency, stocks, or crypto, they rely on a secure layer of exchange that gives them the confidence to do business on a particular trading platform. Any blind spots in infrastructure security can quickly escalate into financial losses, data theft, customer distrust, and damage to business.

To mitigate this mounting challenge, Group-IB empowers businesses with the best-in-class cybersecurity solutions and services that underpin the company's mission to secure operations, ensure compliance, and defend the financial service sector against emerging cyber threats.

Analysis of Libertex Group's global-scale infrastructure

to uncover the full extent of vulnerabilities

As an international trading platform serving over 3 million users worldwide, Libertex Group is committed to offering comprehensive and effective cyber protection to its customers. The company is driven to safeguard its business operations and expand its user base, which has created the need for a comprehensive cybersecurity strategy that covers all aspects of online trading: access security, order placement, fund protection, and the technological infrastructure to go with all this.

The main challenge for Libertex Group was the limited availability of internal resources and the insufficient scope of the audits conducted by its previous vendors, who provided reports that lacked actionable insights. No vendor seemed able to offer the breadth of coverage that was necessary to give Libertex Group complete visibility over all vulnerabilities.

To address security concerns in a proactive way, Libertex needed a reliable partner who could support its cybersecurity efforts at all times through ongoing audits and high-impact recommendations.

In response to these needs, Group-IB stepped up and helped Libertex achieve end-to-end cyber protection.

Initial pain points:

- Limited visibility into network vulnerabilities
- Delayed response to security blind spots
- Limited scope of audits and assessments
- Lack of practical insights for addressing vulnerabilities, security concerns, attack paths, and operational techniques used by hackers, along with recommendations on how to mitigate them
- Inability to protect sensitive customer financial data from persistent threats
- Problems with ensuring regulatory compliance

Strengthening Libertex Group's infrastructure

through in-depth cybersecurity audits and assessments

Internal Penetration Testing

Group-IB penetration testing team simulated attacks to understand the extent to which threat actors can infiltrate and maintain persistence in Libertex's network and gain access to valuable assets.

Web Application Security Testing

Group-IB's experts evaluated Libertex's web application environment and configuration and conducted a manual and semi-automated analysis to identify maximum vulnerabilities.

External Penetration Testing

Group-IB penetration testing team evaluated Libertex's infrastructure perimeter to understand how threat actors could gain initial access to its network.

Compliance Assessment

Group-IB's compliance experts helped prioritize data protection needs based on PCI-DSS compliance, cost and business value, and associated risks.

Success highlight

Comprehensive visibility of the infrastructure to identify and prioritize vulnerabilities

Actionable insights to ensure effective and prompt risk mitigation

Constant security monitoring and updates to stay ahead of cyber threats

Fortified business operations through an improved cybersecurity posture

Solutions offered

Group-IB adopted a systematic approach to planning, implementing, evaluating, and improving Libertex's infrastructure and application security. Group-IB's offensive security team performed an in-depth assessment to highlight known and unknown weaknesses through the following services:

Internal Penetration Testing

Group-IB used a model involving an internal threat actor with initial access to the local network. The testing consisted of the following steps:

- Survey of internal network nodes to understand the customer's infrastructure
- Search for local network nodes and services that belong to critical information systems
- Finding vulnerabilities in manual and semi-automated mode, as well as their initial analysis
- Identifyingnetwork configuration and LAN system issues
- Determining attack vectors based on the vulnerabilities discovered
- Modeling the actions of a potential attacker to gain unauthorized access to critical information systems and exploiting any vulnerabilities found

External Penetration Testing

Group-IB used the "Black Box" testing model (i.e. simulated the actions of an attacker who has no data about the external infrastructure). The testing included the following steps:

- Reconnaissance on Libertex Group's infrastructure to provide an exhaustive inventory of all the information assets accessible from the public network
- Searching for network perimeter nodes and services that belong to critical information systems
- Survey of infrastructure, including an analysis of IP addresses, a scan of network perimeter nodes, and a study of external impact responses
- Determining attack vectors based on the vulnerabilities discovered
- External attack simulation to evaluate access to critical systems and data

Web Application Security Assessment

Group-IB used the "Grey Box" testing model (i.e. simulated an attack where the attacker has access to the web portal). The following steps were taken:

- Performing initial analysis of the application and the application's environment to understand business functions, technical features, and the application structure
- Identification of vulnerabilities in the web application through manual and semi-automated discovery
- Search for the web application's business logic flaws
- Threat modeling by exploiting the vulnerabilities identified

Compliance Assessment (PCI DSS)

Group-IB checked the company's processes and infrastructure against the best practices outlined by the PCI DSS framework. The assessment consisted of the following steps:

- Preliminary analysis, including the a review of the company's policies, procedures, system descriptions, and documentation
- Finalizing the audit plan based on the specific characteristics of the business
- Conducting an interview phase to gather information about business processes and security measures
- Reviewing the findings and assessing them against industry best practices

Conclusion

The Group-IB Audit and Consulting team worked closely with the Libertex Group's various security and IT teams, facilitating a seamless exchange of critical insights to enhance across-the-board cybersecurity measures. Through an expanded testing scope (including platforms, networks, and web-facing interfaces), Group-IB helped Libertex Group gain complete visibility over its perimeter and identified as many potential vulnerabilities as possible. Group-IB experts also provided guidance on how to ensure that all recommendations are implemented and strengthened on an ongoing basis.

What began as an initial collaboration evolved into a long-term partnership. Libertex now relies on Group-IB's industry expertise for regular audits and assessments, thereby continuously improving its cybersecurity resilience. Find out more about Group-IB Audit and Consulting services here:

Explore ↗

Mitigate threats before they turn into full-blown cyberattacks. Take your cyber resilience to the next level with Group-IB Audit and Consulting Services

Request a consultation ↗