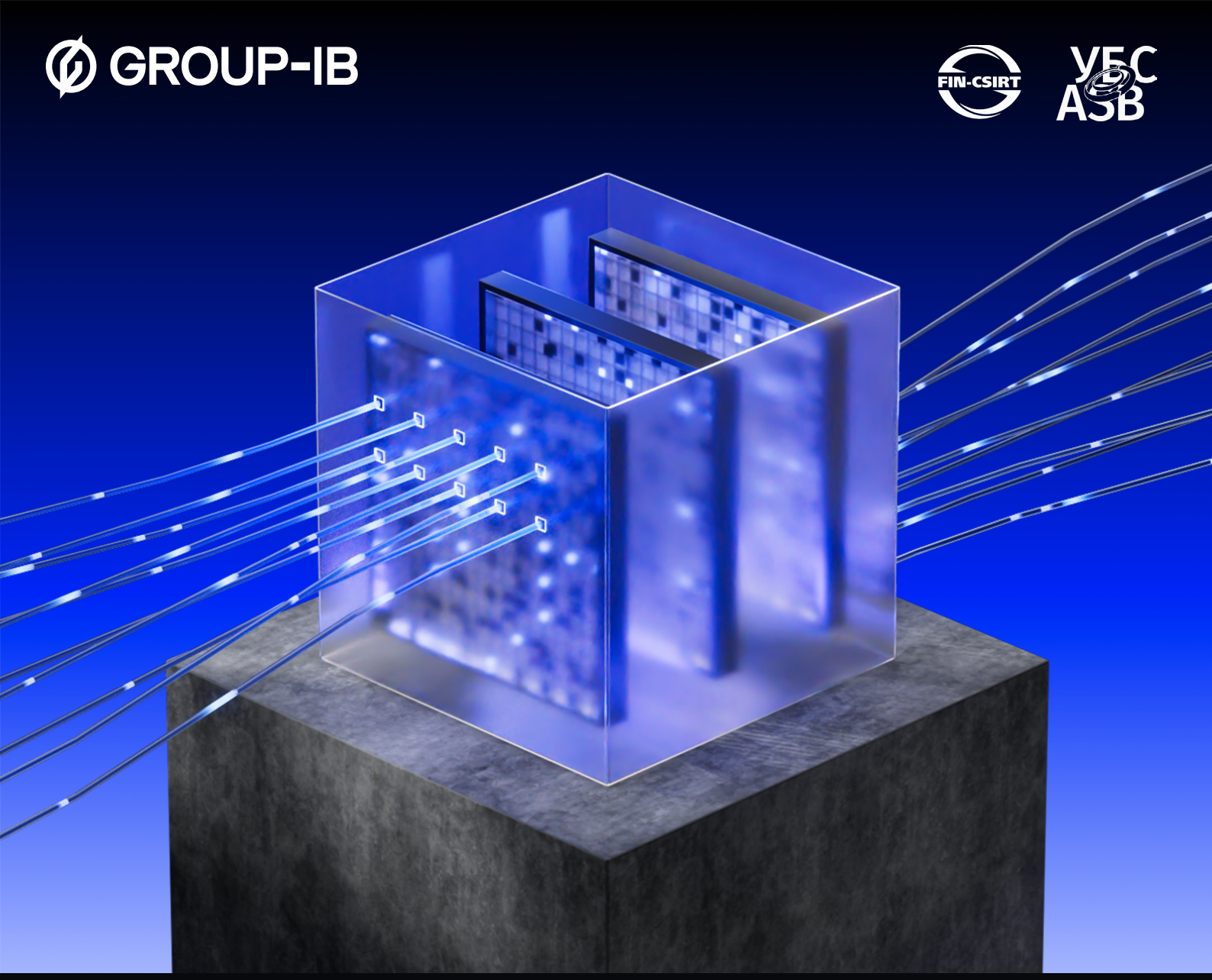
GROUP-IB

FIN-CSIRT

VFC ASB



SUCCESS STORY

GROUP-IB × FIN-CSIRT

Boosting visibility and cyber resilience for Serbia's financial sector

About FIN-CSIRT

Country	Serbia
Founded	2021
Members	20+ (banks, payment institutions, insurance companies)
Industry	Cybersecurity services
Group-IB solution	Attack Surface Management (ASM)

FIN-CSIRT (Financial Sector Computer Security Incident Response Team) is Serbia's first sector-specific CERT, dedicated to improving the cybersecurity posture of the country's financial sector. Acting as a vital link between public and private financial institutions, FIN-CSIRT works together with stakeholders both locally and internationally to build robust cyber resilience and help them safeguard against the ever-evolving cyber threat landscape.

FIN-CSIRT focuses on enhancing cybersecurity in the financial sector by exchanging knowledge among members, preventing and responding to incidents, and raising awareness among financial service users.

Background

European countries remain a prime target for cybercriminals — based locally or in other parts of the world — on account of their developed economy and limited awareness of some types of cybercrime among the general population. At the same time, the region's large number of hosting providers and data centers make it a hotspot for malicious infrastructure.

Now more than ever, the financial sector in Europe is vulnerable to many types of cyberattacks, ranging from sophisticated APT (Advanced Persistent Threat) groups to organized crime syndicates and individual hackers. These threats exploit various vectors (including social engineering, phishing, and malware) to compromise sensitive financial data. The financial services were among the top five most targeted industries in 2023, Group-IB experts report.

With dependency on digital infrastructures in the financial sector only increasing, CSIRTs play a vital role in cyber resilience. Their responsibilities range from identifying and preventing security incidents to disseminating threat intelligence and supporting incident recovery. For FIN-CSIRT, protecting banks in Serbia against these emerging threats meant finding **a solution that could comprehensively monitor and manage the entire threat landscape**.

Challenges

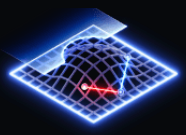
FIN-CSIRT's primary challenge was gaining visibility into the vast and complex cyber threat landscape affecting its members. The fact that the financial institutions under its protection differed in size and maturity meant that a flexible and scalable approach to threat management was needed. Existing solutions didn't give enough data and flexibility to manage the entire threat landscape.

At the same time, FIN-CSIRT faced increasing regulatory requirements, particularly around third-party monitoring (including critical vendors and the supply chain). Regulatory frameworks such as NIS2, DORA, National Bank Regulations, the Law on Information Security, and the Law on Personal Data Protection demanded rigorous oversight — further compounding the need for an adaptable, powerful solution.

Initial pain points

- Complex and fast-moving cyber threat landscape
- Different organization size and maturity level
- Lack of customizable and single-interface solutions
- Tightening regulatory requirements
- Limited staff and time resources
- Rising threats to the financial sector

FIN-CSIRT's solution of choice



Attack Surface Management

> Our main challenge was monitoring and timely reporting threats to our clients. Group-IB's solution provided us with a realistic view of our asset landscape, vulnerabilities, and relevant threat intelligence, making our proactive service more effective. Group-IB's customizable platform has been crucial in managing our operations efficiently.

DARKO SEHOVIC
Head of FIN-CSIRT

Why Group-IB?

FIN-CSIRT selected Group-IB's Attack Surface Management for its robust and comprehensive approach to cybersecurity. Attack Surface Management provided the much-needed visibility into external IT assets, enabling FIN-CSIRT to assess risks and prioritize remediation efforts. Group-IB's responsiveness during the pilot phase, combined with the flexibility of the Attack Surface Management platform, made it the perfect fit for FIN-CSIRT's needs.

Group-IB's Attack Surface Management helps FIN-CSIRT uncover all external IT assets belonging to its members and vendors, assess risks, and prioritize remediation efforts. By providing a clear view of the threat landscape, Attack Surface Management allows FIN-CSIRT to manage vulnerabilities efficiently and improve the overall security posture of its members.

> Attack Surface Management not only has ensured our regulatory compliance through monitoring third-party vendors but also strengthened our overall security posture. Our efforts help to mitigate risks associated with external partners, ensuring that both financial institutions and their clients are better protected against vulnerabilities arising from the supply chain. Through this approach, we have effectively built a robust, secure ecosystem that aligns with the growing regulatory demands, ultimately enhancing trust and security across the board.

DARKO SEHOVIC
Head of FIN-CSIRT

Outcomes

By partnering with Group-IB, FIN-CSIRT has significantly improved its capability to safeguard the financial sector in Serbia against sophisticated cyber threats, ensuring a safer and more resilient environment for all its members. Group-IB's Attack Surface Management capabilities enabled FIN-CSIRT and its members to reduce incident response times, meet stringent regulatory requirements, and provide actionable insights that enhanced security across the financial sector.

Key success factors	Success highlights
Real-time visibility into exposed assets and potential vulnerabilities	Enabled proper vulnerability management, leading to faster threat detection and mitigation.
	Facilitated compliance with regulatory frameworks such as NIS2 and DORA.
	Reduced incident response time significantly with improved threat awareness.
Customizable and user-friendly dashboard	Streamlined monitoring of all banks and critical vendors in a single interface.
	Reduced alert overload and manpower needed for incident management.
	Simplified collaboration and data sharing with its constituents to combat cyberthreats
Comprehensive risk assessment and contextual intelligence	Strengthened the overall security posture of financial institutions.
	Improved confidence across the financial sector, helping institutions stay ahead of evolving cyber threats.

FIN-CSIRT plans to deepen its collaboration with Group-IB, leveraging ASM for even more actionable insights. In the future, they aim to explore other solutions like Threat Intelligence, Digital Risk Protection and Fraud Protection to address new and emerging cyber threats to the financial sector.

GROUP-IB

Fight against cybercrime

GROUP-IB.COM
INFO@GROUP-IB.COM

APAC
+65 3159 4398

EU & NA
+31 20 226 90 90

MEA
+971 4568 1785