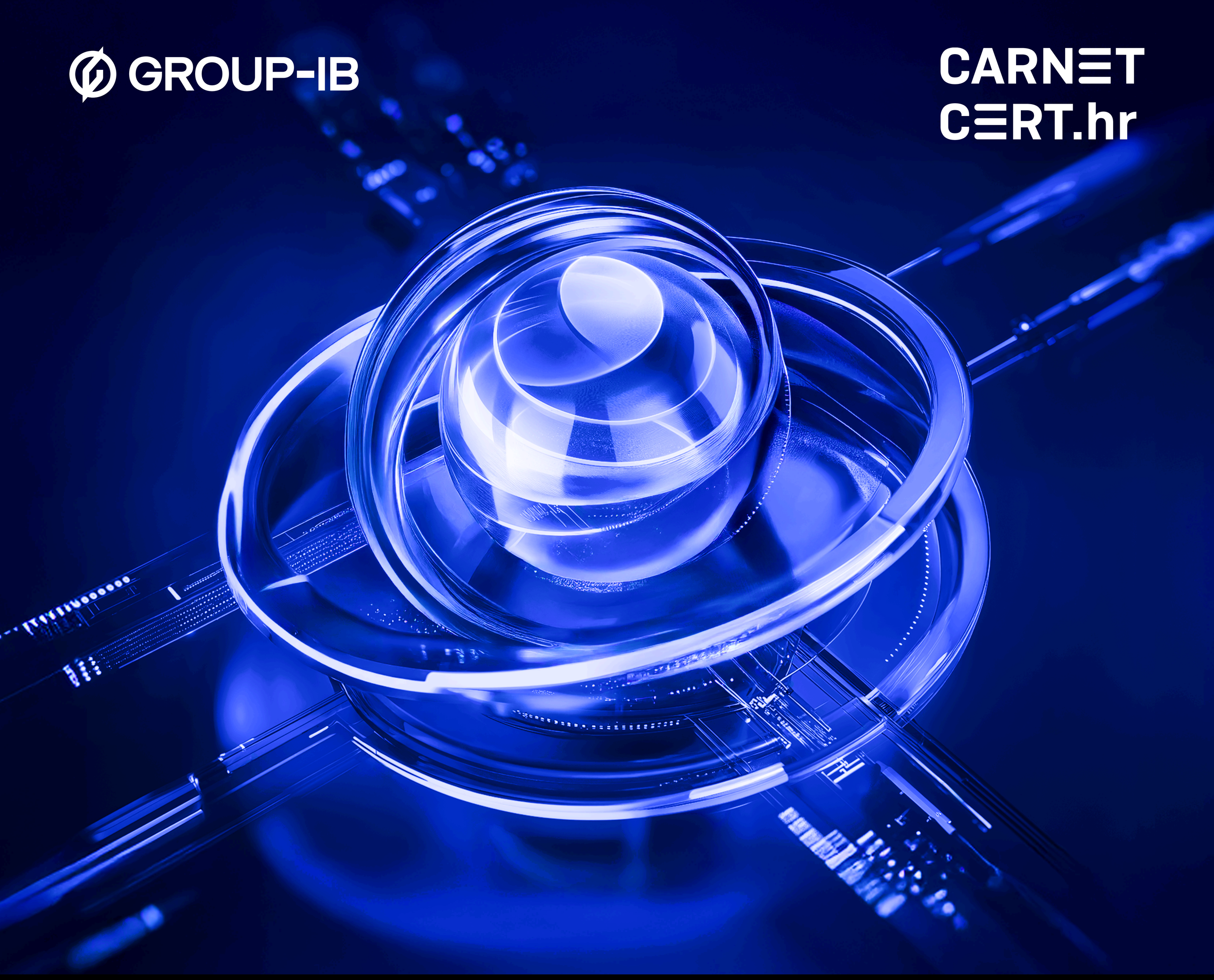

Success story

Group-IB x Croatian National CERT

Enhancing cybersecurity across the nation’s critical sectors with real-time intelligence

About National CERT

Industry	Government, National cybersecurity
Year founded	2007 (CERT.hr under CARNET)
Country	Croatia
Scope	National CERT for Croatia, covering over five regulated sectors and millions of users
Website	cert.hr

Background

CERT.hr, Croatia's National Computer Emergency Response Team, was founded in 2007 as part of the Croatian Academic and Research Network - CARNET. Its mission is to prevent, detect, and respond to cybersecurity incidents affecting public information systems, including in key sectors such as banking, education, digital infrastructure, and financial services.

As cyber threats continue to grow across Europe and the Adriatic, CERT.hr's mission has become even more critical. In 2024 alone, Europe recorded an **18% rise** in state-sponsored attacks. Alongside these, ransomware operations, credential leaks, and phishing campaigns, have continued to put more pressure on national cybersecurity authorities like CERT.hr, which safeguard both local networks and essential infrastructure.

To keep pace with threats, CERT.hr's responsibilities have evolved well beyond traditional incident response. The team is now engaged in forensic investigations, real-time risk assessments, and compliance efforts aligned with the EU's **NIS2 Directive** and other regulatory requirements.

To support this expanded mandate, the team required a solution capable of delivering real-time, contextual threat intelligence that could be integrated with existing systems and that would enhance both technical and strategic decision-making. This led to the start of the CERT's collaboration with Group-IB.

Initial pain points

- Lack of reliable, real-time threat intelligence with context around malware, infrastructure, and dark web activity
- Limited in-house resources to handle the growing volume of increasingly complex incidents
- A need to enrich SIEM systems with intelligence to improve detection and reduce response time
- A requirement for forensic capabilities without adding manual overheads
- A critical need for integration with existing infrastructure and tools
- Legal and procurement constraints requiring cost-effective, fully compliant solutions

Why Group-IB?

Group-IB was selected through a public procurement process in which the company's solution met all the technical and support criteria while offering the best value under Croatian law.

What followed was a seamless deployment, supported by detailed onboarding, monthly check-ins, and fast resolution of any technical requests. Smooth integration with the SIEM was achieved via Splunk thanks to Group-IB's dedicated app. Group-IB's team worked closely with CERT.hr to help the organization not only operationalize threat intelligence but also tailor the platform's capabilities to the National CERT's unique mission and workflows.

Chosen solution

Group-IB Threat Intelligence

CERT.hr now uses Group-IB Threat Intelligence to monitor exposed infrastructure, malware campaigns, leaked credentials, and threat actor behavior in real time.

The platform's extensive database of malicious actors provides visibility into APT and ransomware activity, while grouping features make it possible for analysts to segment organizations across sectors, which allows for targeted monitoring.

All insights are embedded into internal briefings and daily CTI reports, strengthening CERT.hr's core mission as a national CSIRT.

Outcomes

With Group-IB Threat Intelligence integrated into its workflows, CERT.hr has made its operations more effective across several dimensions. The team gained visibility into previously undetected exposure points across its constituency, which has allowed analysts to detect early signs of credential leaks and infrastructure compromise with greater speed and precision.

By segmenting organizations by sector, CERT.hr sharpened its threat monitoring and response strategies to match the specific needs of each regulated domain. The platform's dark web monitoring capabilities also enabled early alerts about potentially exploited credentials, which has given the team time to intervene before incidents can escalate.

Access to structured, high-confidence intelligence about threat actors has allowed for more in-depth reporting and gave CERT.hr the ability to track adversary infrastructure more proactively. As a result, the team not only enhanced its day-to-day operations but also bolstered its strategic advisory role within Croatia's cybersecurity framework.

Success highlights

Seamless integration and fast onboarding

Real-time visibility into compromised accounts, leaks, and vulnerabilities across critical sectors

Quicker detection and response

Daily use of APT and ransomware intelligence to enrich internal reports and alerts

Stronger cybersecurity posture aligned with regulations and standards

Increased team capacity and expertise through ongoing support and monthly consultations

“

Group-IB’s product has met all our expectations. Our proactive roles and tasks have improved and our team has significantly expanded its capabilities in detecting anomalies and responding to incidents. We now have the information and tools to act faster, smarter, and with greater impact across our national constituency.

Ivan Šabić

Vice CEO of CARNET
and Head of National CERT

With Group-IB’s intelligence capabilities, CERT.hr has reinforced its national cybersecurity role with improved visibility, faster incident response, and greater alignment with regulatory obligations under Croatia’s Cybersecurity Act. The partnership has made the organization better equipped to protect digital infrastructure across sectors all the while strengthening collaboration between government, academia, and critical industries.

National regulations and industry requirements are tightening by the day. Group-IB solutions help you stay compliant, resilient, and ready for modern threats all the while meeting regulatory demands. Learn more

GROUP-IB

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

1,550+
Successful investigations of high-tech crime cases

500+
Employees

60
Countries

$1 bln+
Saved by our client companies through our technologies

#1*
Incident Response Retainer vendor

*According to Cybersecurity Excellence Awards

11
Unique Digital Crime Resistance Centers

Global partnerships

- INTERPOL
- EUROPOL
- AFRIPOL

Recognized by top industry experts

- Forrester®
- Aité Novarica
- kuppingercole ANALYSTS
- Gartner®
- IDC
- Frost & Sullivan

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