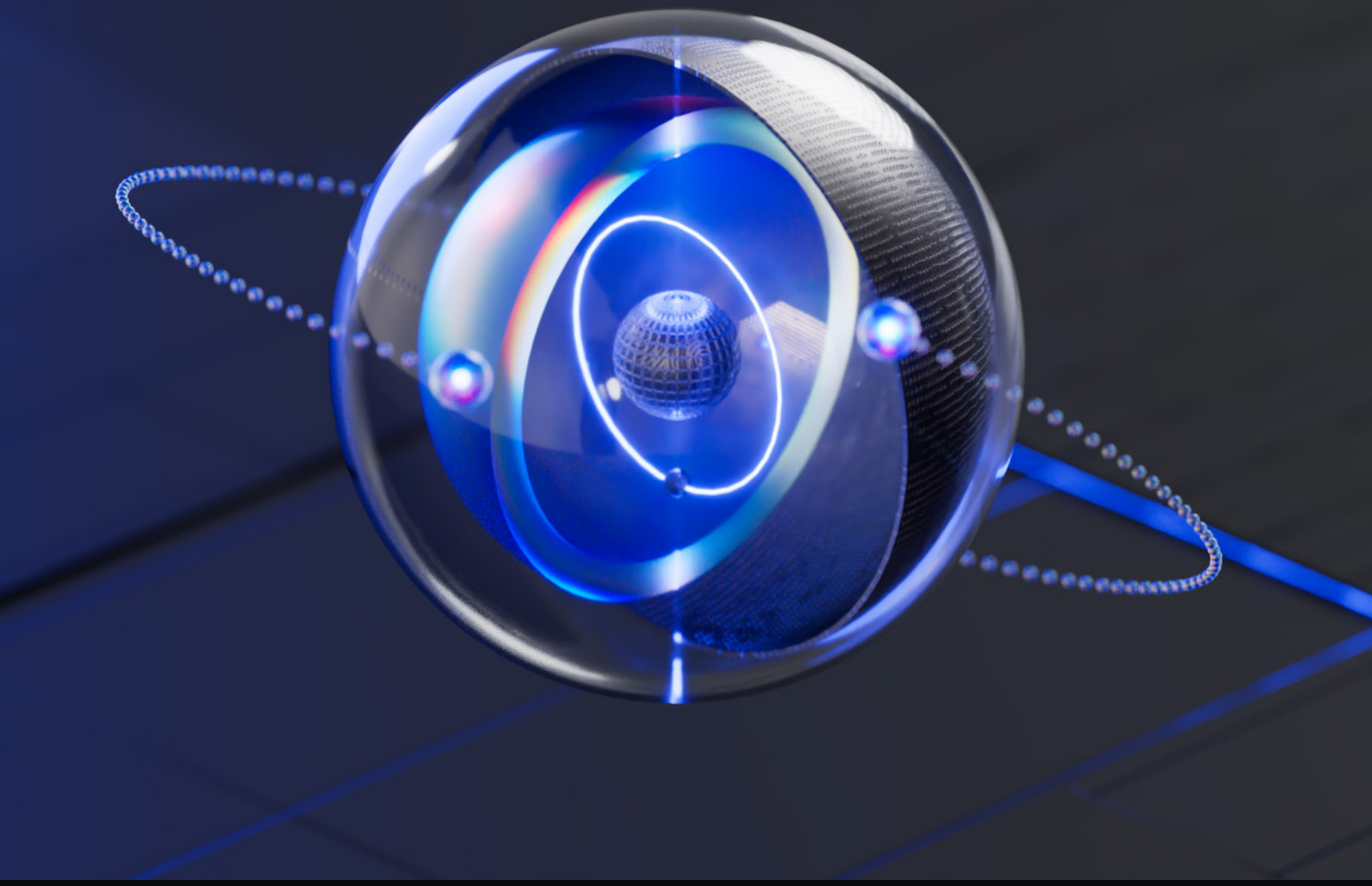
GROUP-IB

Security Lab
Prevent and protect



SUCCESS STORY

GROUP-IB X SECURITY LAB

Innovative solutions and joint expertise
for better customer protection

About Security Lab

Industry	Network security
Year founded	2011
Solutions	Analysis and development of solutions in the field

Security Lab was founded in 2011 as an organization dedicated to analyzing risks and developing solutions in the field of network security. With increasingly sophisticated cyber threats and a growing need for businesses to protect against them, Security Lab has quickly established itself as the go-to advisor for defending and optimizing companies' systems.

Security Lab approach

Societal digital transformation leads to a surge in the number and severity of cyber incidents. To counter them, it is critical to address cybersecurity in all facets, focusing on such aspects of a company as the infrastructure, people, and corporate culture. Security Lab guides its clients through an analysis and awareness-raising process to help them adopt the same security culture, vision, and way of behaving and acting.

Security Lab SOC

Security Lab has a security operations center (SOC) offering managed detection and response services. They are intended to secure the client's information systems and provide incident response assistance, including operational support for in-depth cyber incident analysis.
In case of an alert, the Security Lab team will define the impact level, entities involved, and countermeasures to be implemented.

Why Security Lab and Group-IB partnered

> A highly skilled team of analysts is required to process the data provided by our MXDR solution and respond to incidents intelligently. After witnessing the level of professionalism and resources that Security Lab dedicates to building and continuously developing such a team, we made sure that our partnership will enable our customers to receive quality service and reliable protection.

VLADIMIR GOLIASHEV

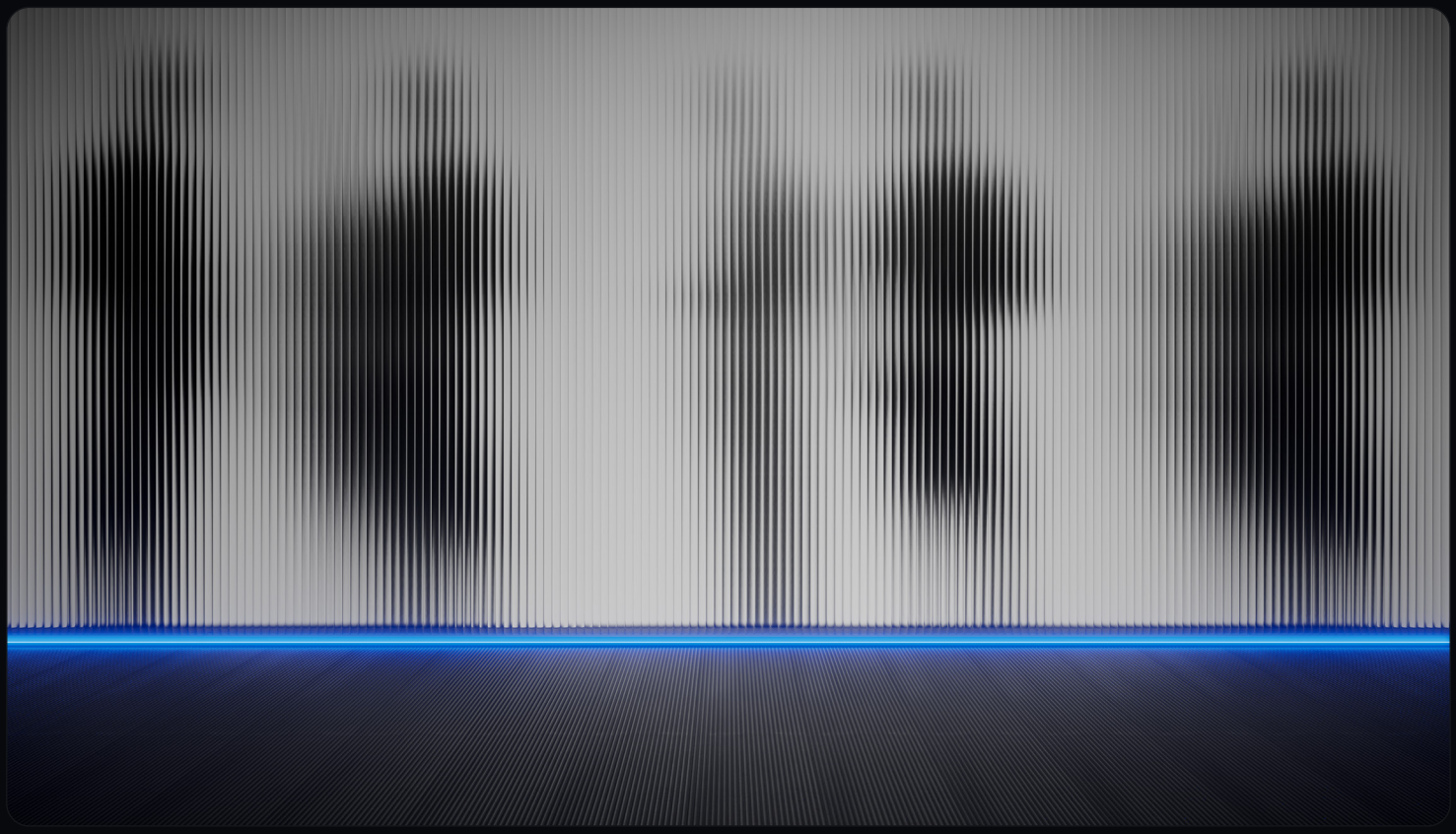
Director, MSSP & MDR Program

Security Lab sought a technological solution to deliver managed detection and response services that meet the most stringent standards. With the advanced sandbox technology, artificial intelligence, and machine learning algorithms Group-IB Managed XDR solution is a natural product to supplement these services. Thanks to advanced toolset bolstered with best-in-class threat intelligence, Group-IB solution enables Security Lab to identify the presence of a threat in the client's network before it results in a breach.

While Group-IB Managed XDR provides extensive capabilities to detect and prevent cyber threats, the expertise of the analysts who utilise these solutions is crucial.

The advanced Group-IB technologies combined with Security Lab analysts' experience and know-how allows the company to carry out the following activities:

- Identify the attack vectors for any occurring incident
- Determine the attack success and detect any persistences
- Verify any lateral movement and identify impacted systems
- Define the compromise duration and reconstruct the kill chain
- Identify whether an exfiltration has occurred and for what data
- Contain the incident to prevent further compromises



About the Group-IB solution

Group-IB Managed Extended Detection and Response (MXDR) is an intelligence-driven solution developed to reduce cyber risks for businesses by offering high-fidelity threat detection and immediate response capabilities. The tool provides complete visibility into operations happening inside the network, as well as on endpoints and servers.

The Managed XDR solution is powered by in-house advanced Threat Intelligence, which empowers it to detect threats that would otherwise go unnoticed. Unique data collected from various sources, including the dark web, enables attributing cyber incidents to specific threat actors and conducting cyber investigations.

Machine learning algorithms convert massive amounts of data into easily digestible data sets, while automation capabilities free up resources. All of this reduces the likelihood of alert fatigue, which is common among information security professionals, and allows SOC personnel to avoid missing threats that need to be addressed.

For better threat detection and protection, the Managed XDR solution may be reinforced with Group-IB Attack Surface Management. Such a software class provides a comprehensive view of the company's forgotten assets or shadow IT, assessing the risks associated with these assets and prioritizing security issues. This integration allows Managed XDR to identify threats with greater accuracy and eliminate the risk of attacks from touchpoints that the organization is unaware of.

Business impact

After implementing the Group-IB Managed XDR solution, Security Lab improved its visibility into customers' infrastructure and developed a new approach to covering every single attack vector. It enabled the company to offer its clients new opportunities for uplifting their overall security posture.

The Group-IB Managed XDR's simple and quick implementation process, as well as its accelerated investigation and response capabilities, enabled Security Lab to reduce the costs of managed detection and response services. By partnering with Group-IB, Security Lab got the opportunity to uplift its incident response services by requesting assistance from Group-IB's DFIR Laboratory.

Client security outcomes

Working with Group-IB Managed XDR is easy to start. Just after a couple of days, a client could begin with its managed detection and response services.

The solution implementation facilitated both containing and analyzing the incidents in the cybersecurity field. The combination of Group-IB Managed XDR capabilities and Security Lab expertise and orchestration improved the detection and response functionalities and created a strong point of differentiation for customers.

SIMONE CREVENNA

Sales Manager, Security Lab

“ We're proud to have a partner like Group-IB that shares the same vision and approach to cybersecurity. Collaborating with someone who has a similar outlook and passion for improving customer cybersecurity posture is crucial in today's constantly evolving threat landscape.

With the joint expertise and technologies of Security Lab and Group-IB, our customers benefit from a more comprehensive and effective solution. The latter provides better protection of critical assets, prevention of data breaches, and reduced risks of damage to a brand reputation.

MARCO STAITI

Gruppo Sogegross ICT Responsible, Security Lab customer

“ Trust in Security Lab determined our choice in favor of a solution provided by their partner – Group-IB Managed XDR. Through the centralized console, we have a global view of what is detected within our network. With Attack Surface Management – another Group-IB solution – we also can monitor our assets, even the forgotten ones.

CISO from Italian Shipping Company, Security Lab customer

“ Our company is recognized as a critical infrastructure, thus, our brand reputation and service continuity are fundamental assets to defend. The expertise of Security Lab applied to Group-IB services represents added value for the integrity of our company.

GROUP-IB

Security Lab
Prevent and protect

Preventing and investigating cybercrime since 2003

70K

hours of incident response experience

1,4K

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 Managed Extended Detection and Response (Managed XDR)

LEARN MORE

CONTACT US