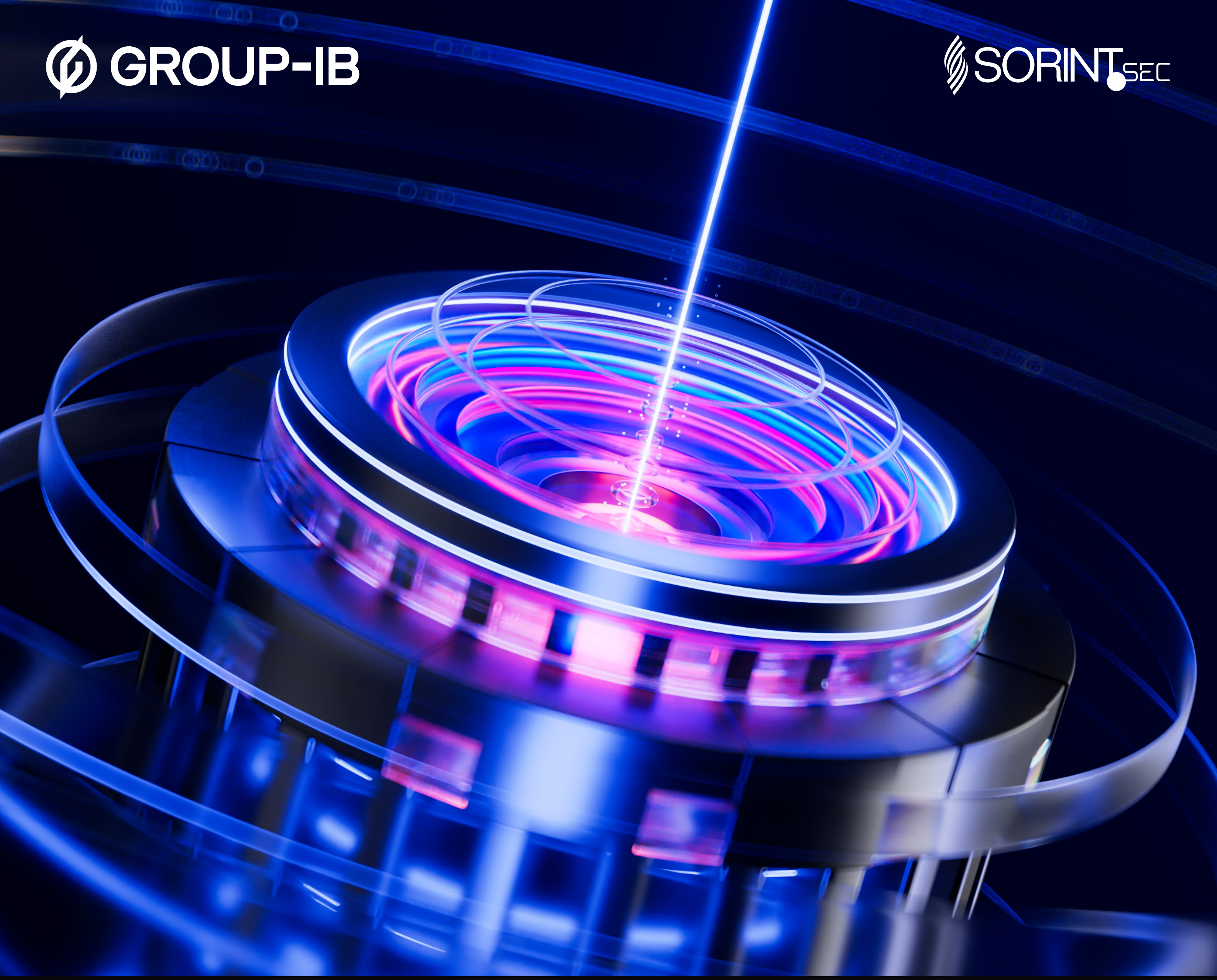

SUCCESS STORY

GROUP-IB X SORINT.SEC

Building joint expertise to enhance critical infrastructure security and facilitate seamless cybersecurity technology adoption for businesses globally

About Sorint.SEC

Industries Served	Multiple
Founding Year	2014
Company size	1200+ employees
Solutions	Cyber security protection services, SOC as a service

As cyber incidents continue to surge, companies struggle to adapt to the evolving demands of business security and resilience. Here is where cybersecurity partners like Sorint.SEC offers highly tailored services to help businesses enhance their cybersecurity suite. Since 2014, Sorint.SEC offers customer-oriented cybersecurity services bolstered by its state-of-the-art Security Operation Center (SOC). Sorint.SEC lends proactive cyber support through their portfolio of services - real-time monitoring of networks, systems, and endpoints, detection of threats, incident handling, and response.

Given the complexity and demands of their offering, possessing the right threat intelligence to promptly and accurately detect threats, along with their contextual information, is absolutely essential for Sorint.SEC.

The company's mission as a Cyber Security Service Provider is to make risk manageable and controlled. **They help businesses improve their security stance and offer complete support for its easy technology adoption and implementation to ensure protection isn't just advised but readily activated.**

But they don't stop there. Sorint.SEC works towards formidable cybersecurity, so they subject their cybersecurity controls to rigorous testing through Red Team activities, ensuring their effectiveness in real-world scenarios. This integrated approach, combining technological innovation, validation, and continuous monitoring, enables them to stay one step ahead of threats, providing organizations with the security, confidence, and resilience they need to survive and thrive in today's digital landscape.

Challenge

As a trusted partner in helping businesses with threat exposure management, Sorint.SEC remains steadfast in addressing and managing evolving cybersecurity challenges. Yet, in their pursuit of providing industry-leading services, they require contextual, relevant, and actionable threat intelligence. Despite collaborating with multiple vendors, Sorint.SEC faced challenges in accessing enriched and precise intelligence capable of outsmarting the dynamic landscape of cyber threats and adversaries for its customers.

> “ Delivering cybersecurity requires constant efforts to be on top of emerging threats. To remain vigilant, we require a continuous feed of updated insights into threat actors, tactics, techniques, procedures (TTPs), indicators of compromise (IOCs), and all the relevant information to safeguard against dangers proactively. Since our company's inception, we have collaborated with threat intelligence providers, and we found that Group-IB's solutions excel in helping us track malicious actors and stay consistently updated.

CLAUDIO COLOMBO

Alliance Director
Sorint.SEC

How did Sorint.SEC leverage Group-IB’s Threat Intelligence (TI) Platform?

After facing trials and tribulations with testing several CTI solutions, Sorint.SEC turned to Group-IB's proprietary Threat Intelligence (TI) as an intelligence-enabling platform for its clients. Real-time, updated, and contextual threat intelligence was a non-negotiable need for Sorint.SEC, leading them to choose Group-IB’s Threat Intelligence, **which offers:**

- The industry’s largest library of dark web data and monitors cybercriminal forums, marketplaces, and closed communities in real time to identify compromised credentials, sensitive information, stolen credit cards, fresh malware samples, access to corporate networks, and other critical intelligence that enables companies to identify and mitigate cyber risks before further damage is done.
- Unparallel insights into adversaries, attack tactics, and risk insights tailored to Sorint.SEC’s clients business’s landscape
- Network-graph interface to easily connect the missing dots between the attacker's identity, infrastructure data exfiltration, internal interactions, or network lateral movement.
- Insights from 60+ sources and internal threat research to understand attacks and attackers your business is most prone to. With comprehensive coverage, cyber risks can be reduced, and effective threat-hunting exercises can be conducted.
- Exclusive data collected by undercover operatives on the dark web and from Interpol, Europol, and Afripol, with whom Group-IB frequently collaborates to investigate cyberattacks.

Adding to the technology prowess, Group-IB’s industry-leading expertise and comprehensive research on global and regional threat landscapes made our offering more unique, end-to-end, and reliable. Another differentiating factor was the speed and quality of threat detection, solidifying Group-IB as their official provider.

Continuous improvement and expanded coverage were additional merits that contributed to Group-IB being the final choice of technology provider to ensure they remained ahead in protecting their customers.

Key undertakings

After partnering with Group-IB, Sorint.SEC's first major breakthrough was tracking, decoding, and mitigating an active threat for one of its significant customers. Upon detection of the threat, Group-IB provided the required tactical intelligence, including indicators of compromise, behavior of the threat actor, Techniques, Tactics, and Procedures (TTPs) employed for further investigation and to make informed response decisions.

By taking a proactive approach, Sorint.SEC addressed surface-level issues for the customer, prepared them to withstand potential impacts in the next phase, and ensured they remained secure without experiencing any disruptions during the eradication of the threat.

Similar strategic, proactive interventions were made possible for their other clients by timely detecting threats and gaining complete context to dissolve or respond to them with Group-IB's Threat Intelligence solution.

Results

Sorint.SEC transformed its internal threat monitoring and exposure management as well of its customers, with Group-IB Threat Intelligence through:

Swift TI activation and seamless integration with Sorint.SEC's security processes and services.

Rapid threat detection for clients with time-bound and tailored remediation strategies.

Access to updated critical threat intelligence and unique research by Group-IB threat analysts, enabling proactive detection with unmatched speed and quality for Sorint.SEC.

Constantly monitored digital footprint for customers. Real-time detection and response with an improved mean time to action, reducing inconsistencies and increasing reliability.

Quotes

> Collaborating with Group-IB has been exceptionally efficient and empowering. Our relationship is founded on cooperation rather than a traditional client-provider dynamic. This collaborative approach ensures that information flows seamlessly between our teams, enhancing security services and better customer protection. It's truly a win-win-win situation.

GIUSEPPE LETIZIA

Execution Director
Sorint.SEC

> Through Group-IB's collaboration with Sorint.SEC, we've provided them with our proprietary Threat Intelligence (TI) to distribute critical, actionable, and timely insights, enriching their and their customers' understanding of the cyber threat landscape. Group-IB's TI integration into Sorint.SEC's service portfolio and its highly mature TI team make them well-positioned to offer tailored, high-quality services.

VLADIMIR GOLIASHEV

Director, MSSP
& MDR Program

Group-IB's Threat Intelligence Solution

Group-IB Threat Intelligence is a proprietary technology offering the industry's largest adversary-centric intelligence to inform and empower your cybersecurity strategies and decisions. Integrating Group-IB's Threat Intelligence maximizes the performance of every component of your security ecosystem. Equipping your team with Group-IB's strategic, operational, and tactical intelligence streamlines security workflows and increases security efficiency.

Benefits of Group-IB

Comprehensive sources

Maximize visibility with the industry's broadest coverage of intelligence sources continuously collected by Group-IB's Unified Risk Platform.

Extensive capabilities

Leave no question unanswered. Equip your team with the broadest range of research tools and analyst teams on the market.

Most trusted

Only Group-IB has cooperation agreements with Interpol, Europol and local law enforcement worldwide to identify and takedown threat actors.

Unlimited access

Reduce costs and potential bottlenecks with unlimited numbers of users and API usage. The team is on hand to help configure custom integrations.

Complete suite

For complete protection Group-IB's Unified Risk Platform also provides Attack Surface Management, Digital Risk Protection, and Managed XDR solutions.

Strategic intelligence

- Revolutionize risk management with bespoke on-demand, and regular monthly and quarterly threat reports written by analysts specifically for the board and executive business cases
- Enable growth with actionable threat intelligence before expanding into a new region / business line, and get industry-specific threats before digital transformation
- Lower the cost of cyber security by avoiding unnecessary purchases and postponing upgrades by maximizing the efficacy of your existing security investment

Operational intelligence

- Transform security and adapt instantly, use the insights to block malicious network and endpoint activity the moment it is first observed anywhere in the world
- Identify and remove weaknesses before they are exploited by conducting Red Teaming with detailed knowledge of threat actor's tools, tactics and processes
- Automate workflows and improve team efficiency by enriching your SIEM, SOAR, EDR and vulnerability management platforms with out-of-the-box integrations for Group-IB threat intelligence

Tactical intelligence

- Prioritize vulnerability patching for your technology stack with automated alerts that inform you the moment vulnerabilities are discovered or begin being exploited by threat actors targeting your industry
- Eliminate false positives and focus on legitimately risky events with a continuously updated database of system and network indicators of compromise for cybercriminals in your threat landscape
- Reduce response time with complete information about the cyber kill chain in the MITRE ATT&CK® matrix format, use the information to quickly remove them from your network

Preventing and investigating cybercrime since 2003

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