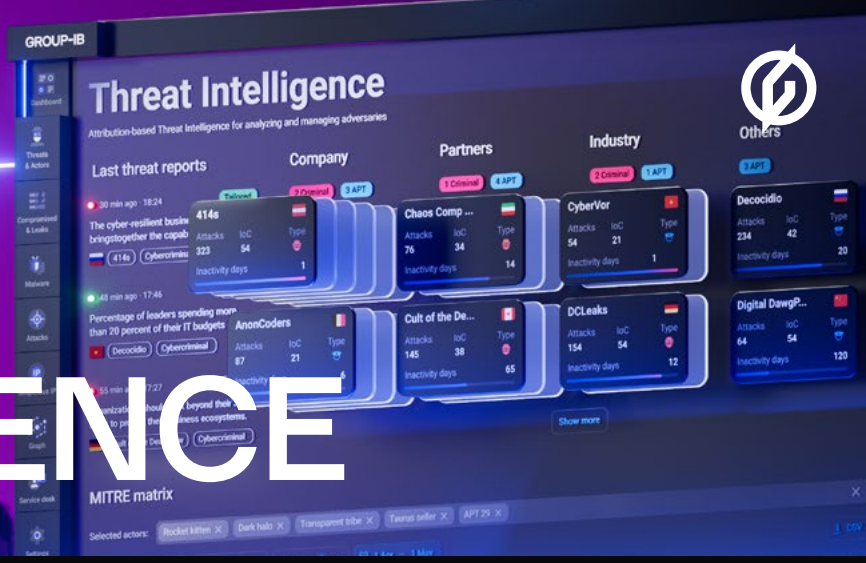
GROUP-IB

THREAT INTELLIGENCE



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 Manage XDR solutions.

The first line of defense shouldn't be your infrastructure; optimize your security and defeat attacks before they begin with knowledge of who, how and when you will be attacked.

Group-IB Threat Intelligence provides unparalleled insight into your adversaries. Integrate the intelligence to maximize 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 efficiency.

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

Key features

Graph interface

Investigate and research threats with an intuitive graphical interface. Use the Graph to easily explore the relationship between threat actors, their infrastructure and the tools they use at a glance and drill into the details with just a click.

Threat actor attribution

Easily understand threat actors' behaviors, preferred methods and infrastructure with insight into their activity in the MITRE ATT&CK format. The Unified Risk Platform tracks and logs their attacks in real-time; review these insights within Group-IB Threat Intelligence.

Compromised data detection

Discover compromised credentials, including VIP's personal accounts, payment card information and breach databases before they are used to launch attacks or cause financial damage. Alerts within can be created to inform you whenever a compromise for your organization is discovered.

Malware and vulnerability investigation

Use Group-IB Threat Intelligence to detonate suspicious files on the Unified Risk Platform or submit them to our reverse engineering team. Review in-depth analysis of the weaknesses targeted by malware and threat actors from the dashboard to prioritize patching.

Dark web insights

Group-IB's Unified Risk Platform has the industry's largest dark web database, access into intelligence with Threat Intelligence to discover illegal activities and monitor your organization is mentioned on the dark web. Create rules to inform you when a topic of interest is discussed.

Tailored threat landscape

Track threat actors easily with a customized threat landscape dashboard, giving you a single pane of glass to monitor their attacks. Use the landscape to track actors that target you, your industry, partners and those of interest.

Phishing detection and response

Configure the Unified Risk Platform with Group-IB Threat Intelligence to automatically detect and takedown malicious sites automatically to protect your brand and customers. Mitigate damage caused by phishing in record time thanks to CERT-GIB's super fast take down processes.

Comprehensive integrations

Enhance your existing security ecosystem easily with out-of-the-box integrations for the Unified Risk Platform with popular SIEM, SOAR and TIP solutions, or via API and STIX/TAXII data transfer to any tool in your security ecosystem.

Comprehensive intelligence powered by the Unified Risk Platform

Open-source intelligence

- Paste sites
- Code repositories
- Exploit repositories
- Social media discussions
- URL sharing services

Malware intelligence

- Detonation platform
- Malware emulators
- Malware configuration files extraction
- Public sandboxes

Sensor intelligence

- ISP-level sensors
- Honeypot network
- IP scanners
- Web crawlers

Human intelligence

- Malware reverse engineers
- Undercover dark web agents
- DFIR and audit services
- Law enforcement operations

Vulnerability intelligence

- CVE list
- Exploit repositories
- Dark web discussions
- Threat campaigns mapping

Data intelligence

- C&C server analysis
- Dark web card shops and underground markets
- Phishing and malware kits
- Compromised data-checkers
- Phishing data collection points

Operations with law enforcement

Extensive expertise and best practices knowledge has been gained by working alongside law enforcement specialists around the world, including Interpol and Europol, and granted Group-IB access to data that has never become public.

OUR MISSION IS TO FIGHT CYBERCRIME.
TO LEARN MORE GET IN TOUCH WITH
ONE OF OUR SECURITY EXPERTS

SINGAPORE
+65 3159-3798

AMSTERDAM
+31 20 226-90-90

DUBAI
+971 4 508 1605