Group-IB

THREAT INTELLIGENCE & ATTRIBUTION

A system for analyzing and attributing cyberattacks, proactive threat hunting, and protecting network infrastructure based on data relating to adversary tactics, tools, and activity

Threat Landscape Management

Cutting-edge analytical tools

Unique closed data sources

GROUP IB

Capabilities

Detects and stops attacks

Prevents threats that are missed by traditional security tools from harming your company

Understands the methods of advanced attackers

Determines whether the protected infrastructure can counteract relevant TTPs

Discovers insiders or leaks

Obtains information about possible data compromise or an insider's activity from closed sources

Identifies and blocks phishing sites

Stops threat actors who threaten your company or customers with brand abuse

Analyzes and attributes threats

Supplements and enriches indicators obtained from other systems with unique data

Strengthens and improves your team

Boosts efficiency by 30%, reduces costs, and engages external experts

Key features

1. Creation and management of personalized threat landscape in the interface
2. Advanced profiling of threat actors, including cybercriminals and nation-state groups
3. Access to unique data sets and wide range of closed sources
4. Tailored and personalized data for each specific company and industry
5. Extraction of company's data after compromise via phishing or malware attacks
6. Ready-to-go integration with SIEM, TIPs, and other systems via API/STIX

Leverage powerful analytical tools

The largest dark web database

Read messages and analyze profiles of attackers. Dig deep and enrich your own research.

Malware Detonation Platform

Detonate malware and malicious links for analysis in realistic virtual environments that are customized for each client.

Automated Graph analysis

Correlate and research events and indicators, empower your threat hunting and attribution with leading technology.

Data Sources

Human Intelligence

- Undercover agents in underground forums on the dark web
- DFIR services and joint operations with international law enforcement
- Experienced reverse engineers, malware analysts, TI analysts, and other professionals
- Certified CERT-GIB, information sharing within the cybersecurity community

Malware Intelligence

- ISP-level sensors
- Group-IB Threat Hunting Framework
- Group-IB Fraud Hunting Platform (anti-fraud solution)
- Honeypot network; SPAM traps, sinkholing
- Malware emulators
- External threat hunting system (internal product to identify malicious infrastructure and extract threat-related data)

Data Intelligence

- C&C-server analysis (botnet and phishing)
- C&C-servers of JS-sniffers
- Phishing data collection points and cardshops
- Configuration file analysis for auto-filler malware and phishing kits
- Compromised data-checkers

Open Source Intelligence

- Paste sites like Pastebin
- Code repositories like GitHub
- Messengers, social networks
- Vulnerabilities and exploits
- URL sharing services

Group-IB Threat Intelligence & Attribution architecture

group-ib.com ↗

Group-IB is a leading provider of advanced Threat Intelligence & Attribution, best-in-class anti-APT and anti-fraud solutions.

Group-IB is ranked among the best threat intelligence vendors in the world by Gartner, IDC, Forrester, Cyber Defense Magazine and SC Media.

We have provided professional development training to Europol, INTERPOL, law enforcement agencies and corporate security teams on four continents.

INTERPOL EUROPOL

Official partners

17 years	65,000+	1,200+	500+
of hands-on experience	hours of incident response	cybercrime investigations worldwide	world-class cybersecurity experts

→

Contact us to test Threat Intelligence & Attribution

info@group-ib.com

→

Get to know us

group-ib.com
twitter.com/GroupIB_GIB

→

Learn more about Threat Intelligence & Attribution

Intelligence-Driven Services

Strengthen your cybersecurity posture with services and advice from experienced specialists with 'boots on the ground' and access to one of the most advanced threat intelligence gathering infrastructures in the world.

Prevention

- Penetration Testing
- Security Assessment
- Compromise Assessment
- Red Teaming
- Incident Response Readiness Assessment
- Compliance Audit

Cyber Education

- Digital Forensics
- Incident Response
- Malware Analysis
- Threat Hunter

Response

- 24/7 CERT-GIB
- Incident Response
- Incident Response Retainer

Investigation

- Digital Forensics
- Investigations
- eDiscovery
- Financial Forensics