EARLY WARNING SYSTEM

THREAT INTELLIGENCE

MONITORING, ANALYSIS AND PREDICTION OF CYBERTHREATS

Threat Intelligence is a vital part of the security portfolio at every enterprise. Mitigating the consequences of cyber-attacks has been becoming increasingly more expensive and time consuming, as displayed in mass media. With the help of cyber intelligence, it's possible to predict cyber-attacks and prepare for them in advance.

We collect and analyze large amounts of unique and proprietary information to deliver tailored, trusted and actionable intelligence to predict risks, while preventing and mitigating any targeted attacks.

STRATEGIC INTELLIGENCE

Decision-making horizon: from months to years

Deep investigations of cyber security trends, attacks, cyber criminal groups, their tactics and tools

Annual, quarterly and monthly reports on cyberthreats and trends, key events and incidents in the cyber security sphere, predictions and prognoses from Group-IB experts

Tailored analytics on demand

Build your cyber security strategy based on predictions, made by world class experts

Maximize ROI on cybersecurity projects and initiatives, including incident response and support from your personal analysts

OPERATIONAL INTELLIGENCE

Decision-making horizon: from hours to weeks

New malware tools and services, cybercriminal community trends and actions, changes in tactics and tools of cyber criminals

Deep investigations of underground cybercriminal communities and forums

Hacktivists, their tactics, tools, profiles and attacks

Access to a closed global community forum of clients

Get operational notifications about new malicious software, targeting your business, infrastructure and your customers

Learn about data leaks, sale of databases, searches for insiders, and reconnaissance operations that are targeting your company

TACTICAL INTELLIGENCE

Decision-making horizon: from minutes to hours

Information on compromised accounts, banking cards, infected mobile devices plus rich context on each incident – time, tools, C2, relative cybercriminal groups

Configuration files of malicious software

Command and Control server information with rich context about them

Intelligence on DDoS, deface attacks

Suspicious IP address database (TOR, SOCKS, proxy)

Prevent cyber security incidents and cyber heists at your clients, stop cyberespionage operations targeting your employees and partners

Discover and detect malicious software and complex cyber-attack tools, that are not detected by antivirus software

Block connections to malicious nodes and detect suspicious activity in your network

IDC Gartner Forrester

Group-IB Threat Intelligence has been recognized by top industry researcher reports

"Having its base in Eastern Europe offers Group-IB the advantage of getting visibility on many threats originating from this region, and its local presence offers the ability to better infiltrate the many threat actors based in this region. Involved in the most high-profile investigations allows Group-IB to get more information about cybercriminals, their relationships and other intelligence".

«Competitive Landscape: Threat Intelligence Services, Worldwide», Gartner

THREAT INTELLIGENCE GIVES ANSWERS ON CORNERSTONE QUESTIONS

Who attacks you, your clients, companies that are similar to yours

How, using which tools and tactics those attacks are committed

What your clients or employees are already hit by cyber criminals

What do cybercriminals discuss at underground forums with respect to your company

How cybercriminals are able or already use your brand to achieve their goals

95%
of intelligence originates from exclusive sources

2000+
phishing links in a day discovered by Group-IB

EASY-TO-USE AND FUNCTIONAL USER INTERFACE

Cloud-based service

All the information can be easily accessed through web-based UI. See the notifications and get into details in a real time mode.

Personal analyst

You can address your questions and requests to dedicated expert analyst to get clarifications or to have a tailored operational report on threats and cyber criminals.

Reporting module

Use visualization tools and modules to work with statistics, see and track trends, make efficient decisions based on statistical analysis.

One-step integration

Include Group-IB Threat Intelligence into your existing processes and systems using STIX/TAXII technology using standard workflow.

Also available through your threat intelligence platform: ANOMALI eclectic iq

OPERATIVE DETECTION AND RESPONSE ON PHISHING ATTACKS

Discover 99% of domains, websites, mobile applications and SSL-certificates, that are using your brand, just in three hours.

Fast and efficient blocking of malicious websites in .RU, .РФ and in other 1100 domain zones.

Our private technology of discovering email addresses, that phishing attacks coordinators use to collect stolen information.

SUBSCRIPTION PACKS

Enterprise

40 HOURS OF PERSONAL ANALYST SUPPORT PER QUARTER

Access to a closed global community forum of clients
Tailored and general notifications about cyber threats
Analysis and information on malicious software
Compromised accounts and context on relevant threats
IMEI IDs of infected mobile devices
Information on DDoS attacks
Suspicious IP addresses
Phishing sites discovering and on-demand takedown procedure
Phishing kits
Deface

Financial

40 HOURS OF PERSONAL ANALYST SUPPORT PER QUARTER

Full capabilities of Enterprise pack
+ Compromised banking card data
+ Detailed information on malware, targeting your customers
+ Money mules section, including banking accounts, card numbers and other credentials, that cybercriminals use to transfer money acquired illegally

Ultimate

80 HOURS OF PERSONAL ANALYST SUPPORT PER QUARTER

Full capabilities of Financial pack
+ Discovering and response on fraudulent and malicious SSL-certificates, domain names, phishing web-sites and mobile applications, contextual advertising that misuse your brand
+ Extraction of phishing kits and making them able to be analyzed
+ Blocking of email addresses, that are used to collect stolen at phishing sites user credentials
+ Public leaks

START USING THREAT INTELLIGENCE RIGHT NOW

Get full access to information that helps to predict and mitigate cyber attacks – free 2 weeks trial

Use full functional of system during trial.
No installation is required – get all the information through web-interface or API. We start to deliver tailored data in one day after the start of subscription.
Get a personalized threat report after your trial.

Maximize your cyber security with your personal analyst:

- send malware samples for analysis,
- request additional information on actual threats (cyber-criminal groups, phishing emails, domain names and IP addresses),
- leverage your response procedures with Group-IB team – takedown phishing sites, block fraudulent mobile applications and much more.

CONTACT US
to activate your free 2 weeks trial
+7 (495) 984 33 64
ci@group-ib.com

LEARN MORE
about Group-IB threat intelligence capabilities
group-ib.com/intelligence

MEET GROUP-IB
one of 7 world's best threat intelligence providers according to Gartner
www.group-ib.com