Company story, products and services portfolio overview

Group-IB – one of the global leaders in providing attribution-based Threat Intelligence, best-in-class anti-APT and anti-fraud solutions

Tim Bobak

Regional Lead, UK & MEA
bobak@group-ib.com

Group-IB at a Glance

600+
Protected Customers
all over the World

1000+
Successful Investigations
of Hi-tech Cybercrime Cases

60 000+
Hours of Hands-on
Incident Response

450+
Employees Worldwide

Recognized by Top Industry Experts

Forrester · IDC · Gartner

Official Partner

Europol · Interpol

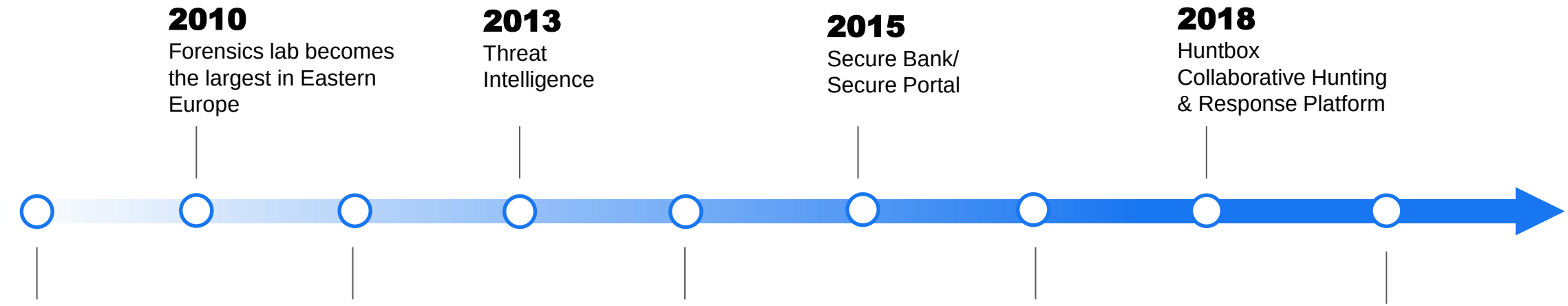
Recommended by

OSCE · SWIFT

Some of Our High-end Clients

Deutsche Bank · Raiffeisen Bank · HSBC · Commonwealth Bank · Sony

Our Story



Media coverage: theguardian Bloomberg Forbes REUTERS Esquire The Washington Post CNN The Register InformationWeek DARKReading SC MAGAZINE

Technologies with Detective DNA

Threat Intelligence

High-fidelity threat intelligence data
& best-in-class custom research

Adversary-centric threat detection and proactive threat hunting

Threat Detection System (TDS)

Huntbox | Sensor |
Polygon| Huntpoint

Advanced fraud detection and user authentication

Secure Bank Secure Portal

Next-gen intellectual property protection

Brand Protection

Anti-Piracy | Anti-Scam
Anti-Counterfeit

Services that give us the view from the battlefields

- Security & Risk Assessment
- Red Teaming Testing
- 24/7 CERT-GIB
- Internal & External Threat Hunting
- Incident Response
- Digital Forensics & Malware Analysis
- Hi-tech Crime Investigations
- Cyber Education

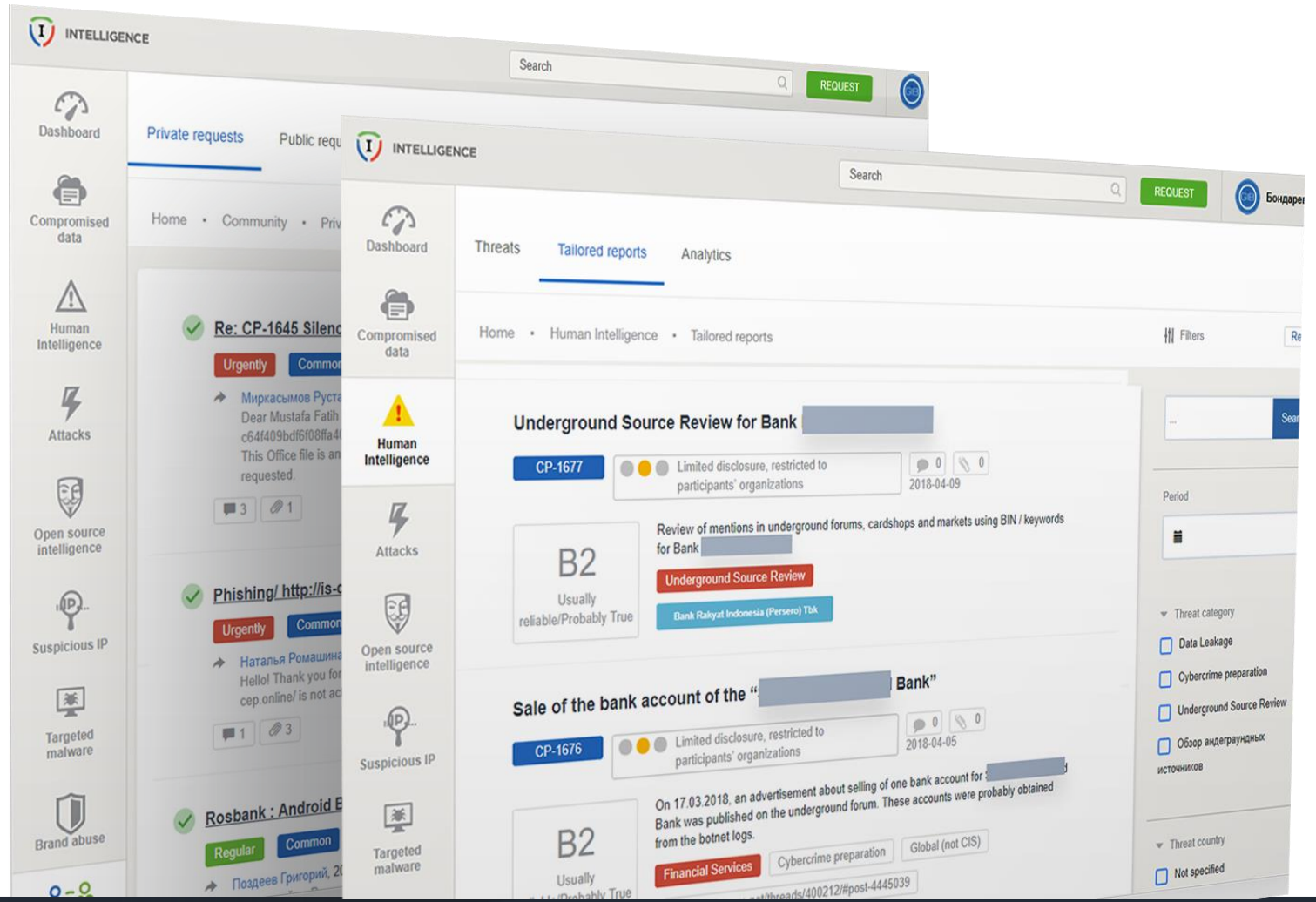
Threat Intelligence

Group-IB Threat Intelligence at a Glance

Attack attribution based on Threat Intelligence data

- Attacker management in lieu of indicator management
- Protection against attackers rather than irrelevant or general threats
- In-depth research into attackers instead of raw data analysis
- The most relevant data with up-to-date context

According to **Gartner, IDC, Forrester, Cyber Defense Magazine, and SC Media,** Group-IB is among the world's best Threat Intelligence providers



Use Cases

Combat advanced threats

Track advanced threat actors targeting or planning to target your industry, country & company

- timeline of targeted attacks
- targeted countries and sectors
- Tactics, techniques & procedures
- IoCs in convenient APIs & mapped to MITRE ATT&CK framework

Access the unknown

Monitoring of Deep and Dark Web, custom research

Empower your team

Dedicated analysts to solve complex cases

Prevent phishing

Detect, investigate and remove phishing

Become prepared

Actionable security briefs on potential threats

Detect data breaches

Identify compromised data enriched with context

Manage patches

Leverage vulnerability data to optimize patch management processes

Pivot strategy

Keep up with the constantly changing threat landscape

Enrich security stack

Improve your system's blocking and detection capabilities

Key Advantages of Threat Intelligence

- Built-in attribution tool
- Integration with built-in security solutions with STIX / TAXII, API/JSON support
- Personalized and the most relevant threat intelligence
- Collaboration with experts in various fields
- In-depth analysis of attackers
- Automated threat hunting, incident response, and malware research

Integrated into SIEMs & Threat Intelligence platforms

eclectic iq

THREATQUOTIENT

THREATCONNECT

ANOMALI

Threat Detection System

Threat Detection System at a Glance

TDS Huntbox is a ground-breaking security solution that combines managed detection & response with automated external threat hunting

Local internal threat hunting across corporate network

Huntpoint

Detection, response and forensics on hosts

Response

Polygon

Files & e-mails analysis in isolated environment

Prevention

Sensor

Network traffic analysis, anomalies and infections detection

Detection

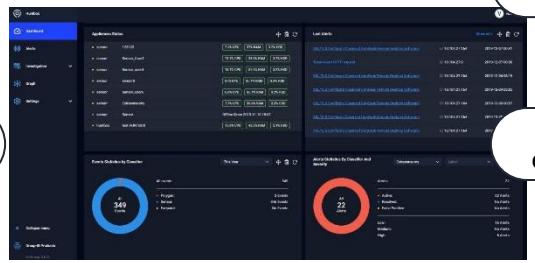
Indicators

Reports

Events

Huntbox

- Event correlation
- Retrospective analysis
- Automated threat hunting
- Streamlined response



Threat context

Hidden connections

Attacker's profile

IoC enrichment

Global external threat hunting & adversary infrastructure exposure

Threat Intelligence

Know the enemy

- Tactics, Techniques & Procedures (TTPs)
- Unique behavior patterns
- Anatomy of complex targeted attacks

Hidden infrastructure exposure

- Search algorithms based on specific behavior patterns
- Proprietary technologies of data gathering
- Historical data storage for retrospective analysis

4,2 bln
Ips and daily scanning of all IPv4 addresses

211 mln
SSH fingerprint

650 mln
Domains and historical data for 16 years

1,6 bln
SSL-certificates

TDS Modules

Managed detection & response 24/7

CERT-GIB

- Alerts monitoring
- Remote response
- Anomaly analysis
- Incident management
- Threat Hunting
- Critical threats analysis

Detecting infrastructure management & data analysis

TDS Huntbox

- Internal Threat Hunting
- External Threat Hunting
- Retrospective analysis
- Correlation & attribution
- Modules management
- Data storage
- Single interface

IoCs & events

Attacks detection & prevention

TDS Sensor

- Traffic analysis
- Anomalies detection
- Files extraction

TDS Polygon

- Isolated environment
- Files analysis
- Links analysis

TDS Huntpoint

- Events logging
- Threats detection
- Response at hosts

TDS Sensor

Advanced technology designed to analyze network traffic and identify anomalies & infected devices

In-depth inspection of traffic

Leverages machine learning algorithms and analyzes all types of channels: DNS, HTTP, Hop HTTP/HTTP, SMB

Analysis of encrypted traffic

Mechanisms designed to work with encrypted channels and extract files from them for analysis via ICAP

Detection of lateral movements

Detects pass-the-hash attacks, WMI, PsExec, admin shares

Unique signatures

Created based on proprietary data from unique sources & proprietary Threat Intelligence

TDS Polygon

Sophisticated sandboxing technology
that stays ahead of attackers

Unique sources

Knowledge of new attack tools thanks to investigations, incident response, and our own unique research

Advanced anti-evasion techniques

Advanced social engineering detection rules and realistic emulation of real-life environments

Regularly updated classifier

Verdicts on whether an object is dangerous based on a classifier powered by Threat Intelligence

TDS Huntpoint

Unparalleled visibility across endpoints
& streamlined response

Comprehensive data collection

Collects and processes information about all events on hosts

Control of devices & apps

Manages access to apps, removable devices, and data storage

Streamlined response

Stops attackers in real time by isolating the host or blocking the malicious process

Retrospective analysis

Gathers historical data and forensic details to quickly uncover the roots of attacks

TDS Huntbox

Single decision-making & alert management platform with internal & external threat hunting capabilities

Unified interface

Manage all components of the framework and choose flexible configuration options

Incidents

Correlate and group events into incidents to significantly reduce their processing time

Projects of any complexity

Manage any number of modules to implement complex infrastructure projects

Flexible supply options

ISO image format for installation on servers with relevant specifications

Hybrid

Flexible, mixed type of installation to meet individual requirements

Stand-alone solution

On-prem to keep all data within the perimeter and ensure absolute confidentiality

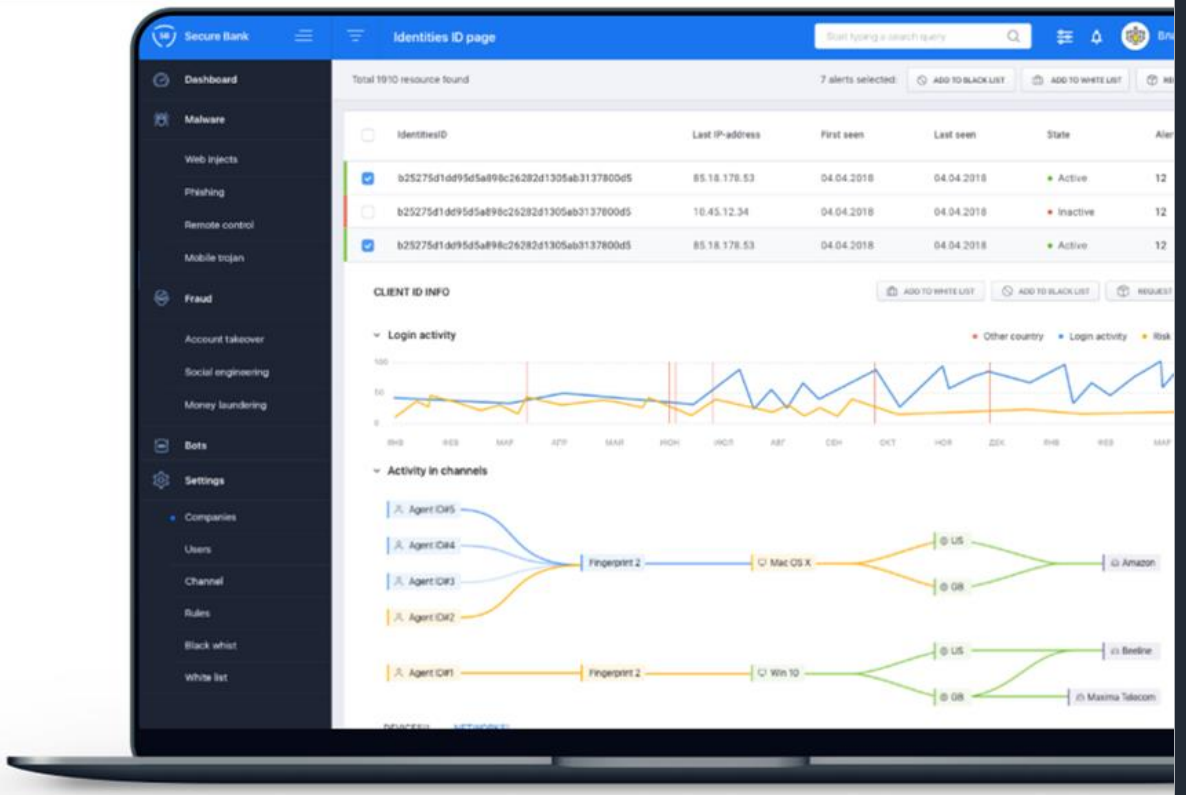
Secure Bank / Secure Portal

How Group-IB Secure Bank / Secure Portal Works

1. A light Group-IB Secure Bank / Secure Portal module runs seamlessly as JavaScript on your website pages or as an SDK in mobile apps.

2. Using proprietary technologies combined with unique threat intelligence data, it detects & prevents fraudulent activity in real time.

3. All fraudulent indicators are sent to your information security officers or analysts for retrospective analytics, prevention of future attacks, forensics & investigations.



Deployed instantly across the entire client base without affecting performance.

All scripts, traffic and data are encrypted to avoid interception by third parties.
No personal data and other confidential information collected.

Dedicated Group-IB anti-fraud analyst and incident response capabilities backed up by a team of world-class forensics experts.

Group-IB Secure Bank/Secure Portal

Client-side fraud prevention & digital identity protection

across sessions, platforms, and devices in real time for online portals & mobile apps.

Protecting end users of online & mobile banking, travel services, e-commerce, gaming & gambling portals, e-government, insurance services, and cryptocurrency projects.

Detecting fraud, social engineering attacks, payment attacks, money laundering, phishing, cross-channel attacks, etc**.**

Blocking malicious bot activity.

Decreasing number of false positives**, removing** extra authentication steps for a user.

Cutting business costs on risk protection practices.

Reduces
false positives & user notifications by **80%**

Protecting
100 000 000+
end users of major companies worldwide

Recognized
as a Representative Vendor in Online Fraud Detection by **Gartner***

Synergy of Advanced Anti-fraud Technologies & Intelligence

- Cross-channel analysis
- Behavioral analysis
- Device fingerprinting
- Adaptive authentication

- More than 16 years of technical experience in fighting cybercrime
- Proprietary machine learning and artificial intelligence technologies
- Unique data from Group-IB Threat Intelligence

- Bot detection and blocking
- Global user profiling
- Clientless malware detection
- Advanced rule engine

Integrates with:

RSA

SAS

GBG

Intellinx
Insider Threat Intelligence

Radar

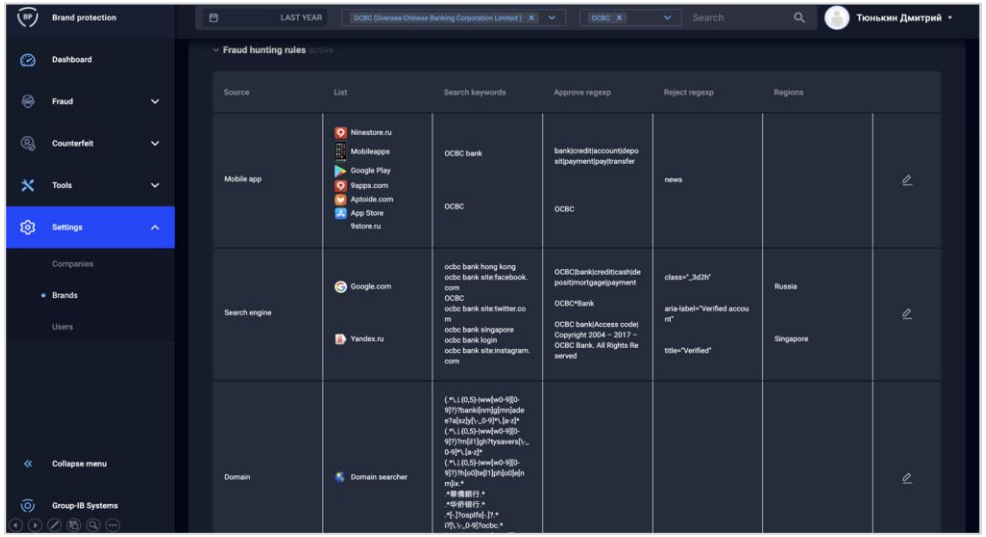
ArcSight
An HP Company

Brand Protection

Group-IB Brand Protection

Group-IB Brand Protection is a comprehensive solution designed to protect **intellectual property** and **brand name** of the customer against illegal use on the Internet.

Proprietary software



The platform combines the benefits of **machine learning** technology, **cybersecurity innovations** and **expertise of brand protection professionals** with broad law and IT experience.

50+

international brand protection professionals

8+

years of brand protection experience

350+

successfully protected brands

Analysis of Detected Infringements & Enforcement Prioritization

GROUP-IB

Resources for analysis

- Deep web
- Search engines
- Mobile app stores
- Contextual advertising
- Online classifieds and marketplaces
- Social media and opinion leaders
- Telegram channels
- Databases of phishing resources

Brand name mentions

Violation determination

Enforcement prioritization

Response

85% blocking
or help with filing lawsuit

Brand Protection Modules

ANTI-SCAM

- Fake partnerships
- Illegal advertising
- Fake mobile apps
- Phishing and fraudulent websites
- Fake accounts and groups on social media

ANTI-COUNTERFEITING

- Illegal sale of goods on the Internet
- Grey import
- Breaches of partnership agreements

ANTI-PIRACY

- Video content
- Software, computer games
- Books, newspapers, articles
- Music

Prevention of monetary and reputational losses in various industries:

- Luxury brands
- Electronics
- Alcohol
- Automotive
- Perfumes & Cosmetics
- Insurance
- Manufacturing
- FMCG
- Children’s products
- Sporting goods
- Media industry
- Construction

Services Portfolio

Group-IB Services at a Glance

Before the attack

- Penetration Testing
- Red Teaming
- Compliance Audit
- Compromise Assessment
- Incident Response Readiness Assessment (Pre-IR)

During the attack

- Computer Emergency Response Team (CERT-GIB)
- Incident Response
- Incident Response Retainer

After the attack

- Digital Forensics
- eDiscovery
- Hi-tech Crime Investigations

Cyber Education

- Programs for technical specialists
- Master classes for wide audiences
- Workshops for kids

CERT-GIB

CERT-GIB (Computer Emergency Response Team) — a round-the-clock computer security incident response team

- Incident monitoring, including distribution of malicious software, phishing, brand abuse, counterfeiting & piracy
- Full legal support on every stage of incident response and investigation
- Professional assistance from specialists with vast experience in response to cyber crime
- Prompt blockage of dangerous websites in the .RU, .РФ domains and more than 2500 other domain zones
- Close cooperation with CERT teams, domain registrars and hosting providers from all over the world
- Collection, analysis and preservation of digital evidences

Recognized as a competent organization of the Coordination Center for TLD RU (administrator of national top level domains .RU and .РФ)

Accredited member of FIRST and Trusted Introducer international associations

Member of OIC-CERT (Organisation of The Islamic Cooperation — Computer Emergency Response Teams)

Partner of IMPACT — International Multilateral Partnership Against Cyber Threats

Officially authorized by Carnegie Mellon University and licensed to use the “CERT” trademark in its name

Incident Response

DFIR teams responds to security incidents of varied complexity:

- Targeted attacks
- Unsanctioned access
- Financial crimes
- Data leakage
- Intellectual property theft
- State-sponsored attacks

STEP 1.
Network traffic analysis

TDS Huntbox implementation for network traffic monitoring and suspicious behavior detection missed by signature-based cybersecurity systems.

STEP 2.
Forensic analysis

Analysis of workstations and servers used by cybercriminals to identify the initial attack vector, applied tools and techniques, exploited vulnerabilities.

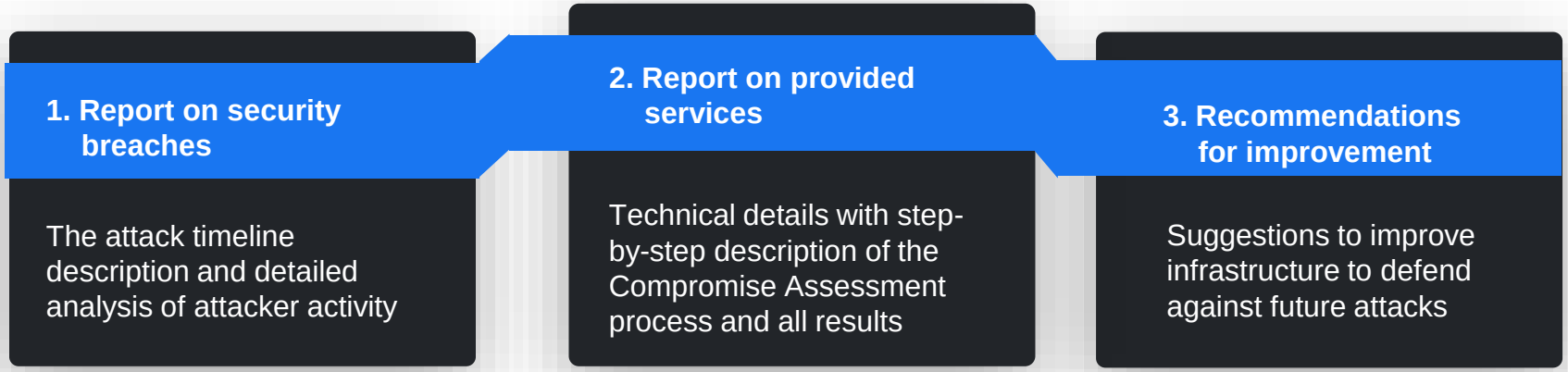
STEP 3.
Malware analysis

Basic or advanced static and dynamic analysis of malicious code discovered during an investigation to determine other affected assets and prevent further intrusions.

Compromise Assessment

Proactive detection of attack preparation and compromise within your IT infrastructure, assessing the scale of damage & identifying which assets in the network were attacked.

Service Deliverables:



As part of Compromise Assessment, our specialists will install a hardware and software solution called **Group-IB Threat Detection System (TDS) –** a comprehensive solution for adversary–centric detection and proactive threat hunting

Prerequisites:

Preparation for targeted attack

It takes hackers months to deploy malicious infrastructure to conduct an attack — in a completely unsuspicious way

Mergers & acquisitions

Integration with another business may pose risks hidden in new infrastructure: implants, backdoors, CVE

Unscrupulous competitors

Access to your trade secrets provides your rivals a competitive edge in the market

Preventing and investigating cybercrime since 2003

Tim Bobak

Regional Lead, UK & MEA
bobak@group-ib.com

www.group-ib.com
group-ib.com/blog

info@group-ib.com
+65 3159-3798

twitter.com/GroupIB_GIB
facebook.com/groupibHQ

linkedin.com/organization/1382013
instagram.com/group_ib