Group-IB

THREAT HUNTING FRAMEWORK

Adversary-centric detection of targeted attacks and unknown threats.
Proactive local and global threat hunting.
Proprietary patented technologies.

Management of complex incidents

Automated and streamlined response

Threat research and incident response automation

Collaboration with best experts in common environment

GROUP-IB

Threat Hunting Framework

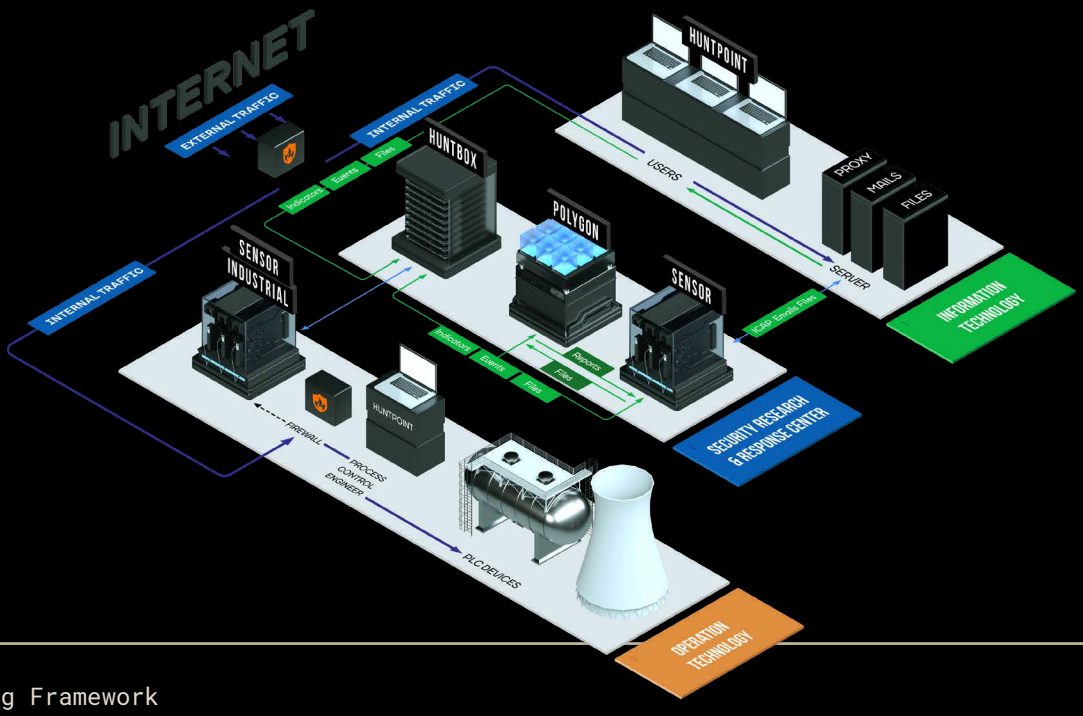
“Sees” more than others

Last decade		Group-IB Threat Hunting Framework
Reactive detection of known threats and passive approach to defense.	→	Detection of previously unknown threats based on Group-IB Threat Intelligence & Attribution. Proactive search for anomalies, hidden tunnels, and signs of communications with C&C server.
Manual event processing and correlation resulted in time lost. Threat hunting limited to local networks.	→	Automated correlation of events and alerts, and subsequent attribution. Global proactive threat hunting that exposes adversaries' infrastructure, TTPs, intent, and plans.
Absence of powerful analytical tools.	→	Proprietary tools: network graph analysis and malware detonation platform provide data enrichment, correlations, and analysis.
Correlation of events in different parts of infrastructure was poorly understood.	→	Full overview of the attack, in-depth management of incidents (up to Mutex/Pipes/Registry/Files).

Offers convenience and custom deployment options

On-prem	Cloud	Hybrid
Keeps all the data inside the perimeter for absolute confidentiality	Easily integrates with cloud services located in your country	Fits custom requirements for any type of business and goals

Becomes your local center for research, detection, and response



Threat Hunting Framework capabilities

Management of complex incidents

Discovers anomalies, hidden communication channels. Performs behavioral analysis for software and users, and event correlation.

Malware detonation and analysis

Patented technology performs dynamic analysis of malware on virtual machines, and fully executes malicious code and extracts IoCs.

Collaboration with experts

Provides shared environment, remote incident response, digital forensics, and access to analysts and community.

Proactive threat hunting

Hunts on hosts and in network traffic within and outside the perimeter, while also analyzing adversaries' infrastructure.

Access to threat intelligence

Attributes scattered events to specific malware types and families or certain cybercriminal groups for efficient attack termination.

Unified security solution for IT and OT

A single system contains all the necessary tools for adaptive automation of research, threat hunting, and IR.

Automation and efficiency

Automatic incident investigation saves time on routine tasks.

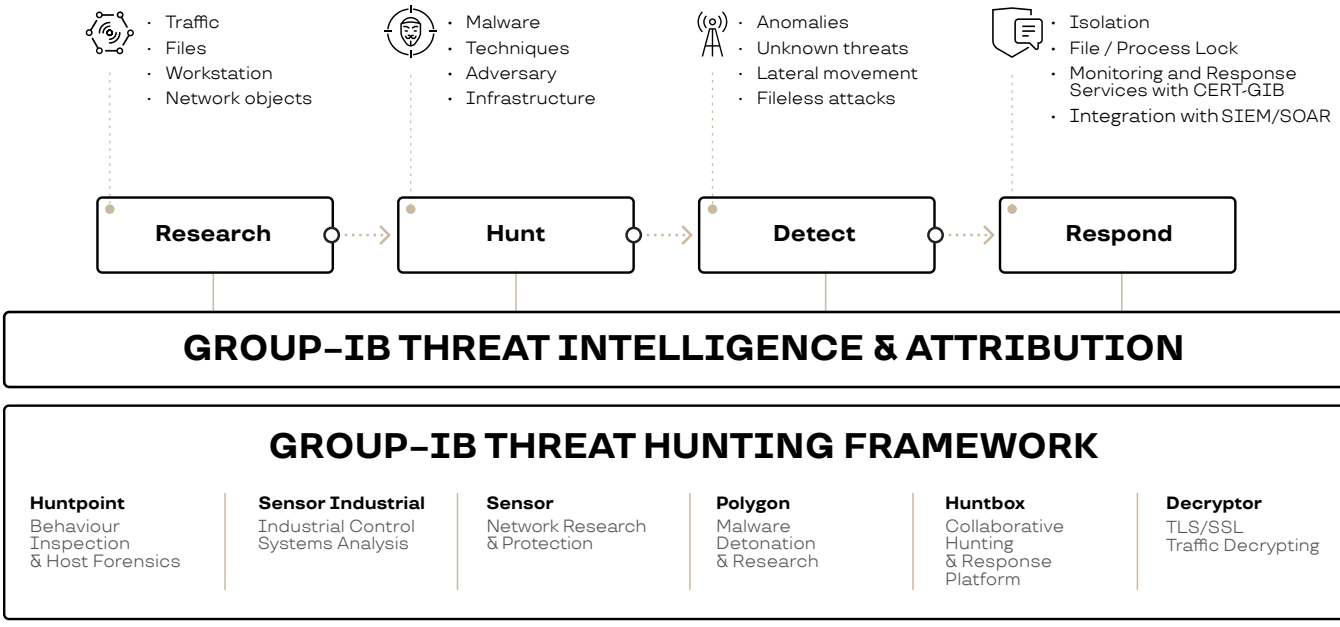
Business continuity

Low false positive rate prevents important business processes from stopping.

Ready-to-use integration

Adapted for SIEM, event and log-storage systems. Easy to set up and tune.

Threat Hunting Framework 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 Hunting Framework

thf@group-ib.com

→

Get to know us

group-ib.com
info@group-ib.com
twitter.com/GroupIB_GIB

→

Learn more about Threat Hunting Framework

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