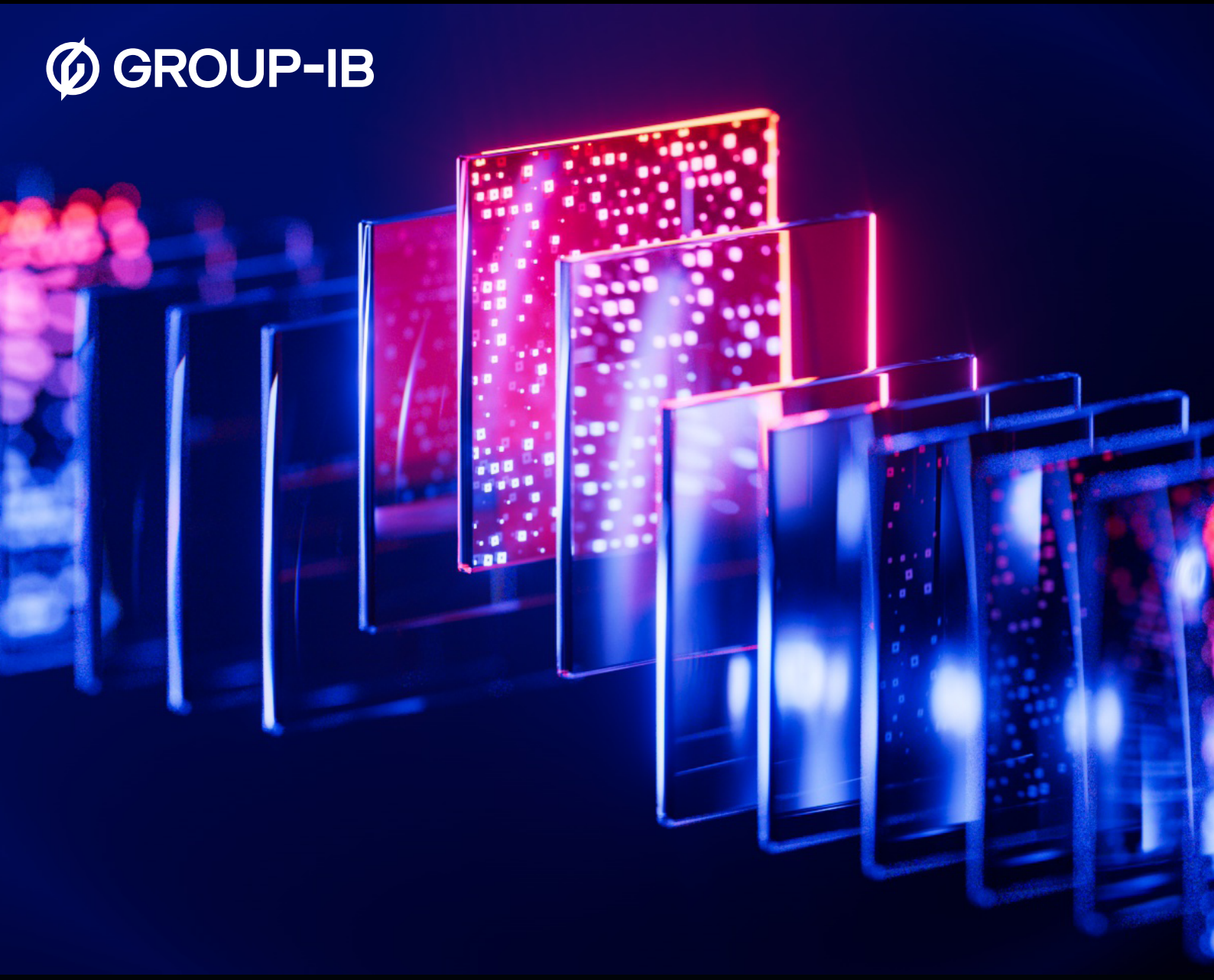
GROUP-IB



THREAT HUNTING

ADVERSARY HUNTING CODE: UNCOVER AND ELIMINATE UNKNOWN CYBER THREATS WITH GROUP-IB

Threats often lurk in the shadows, undetected, until they escalate into full-blown crises. The key to staying protected is to hunt them down—or risk being hunted. Learn how to do it the right way with Group-IB expert-curated and industry-proven approaches

01

Table of contents

02 Background

Since 2014, when Group-IB introduced its Threat Detection System (TDS), the solution has fundamentally enhanced the efficiency of incident response teams by providing a holistic view of an organization's network. Using this system for incident response and continuous monitoring has significantly reduced dwell time and improved threat detection capabilities. By 2018, while the "threat detection" approach had proven effective in addressing significant security challenges, it still left cybersecurity teams one step behind adversaries. Group-IB conducted research based on more than 1,400 incident response engagements to understand the most frequent cybersecurity gaps that led to successful cyber-attacks. The top three were **insufficient threat detection capabilities, lack of log management, and inadequate incident response actions**. In the most sophisticated cyberattacks, adversaries bypass available defenses by removing them or finding ways to evade detection logic.

Developing a solid threat detection system is challenging due to several technology limitations.

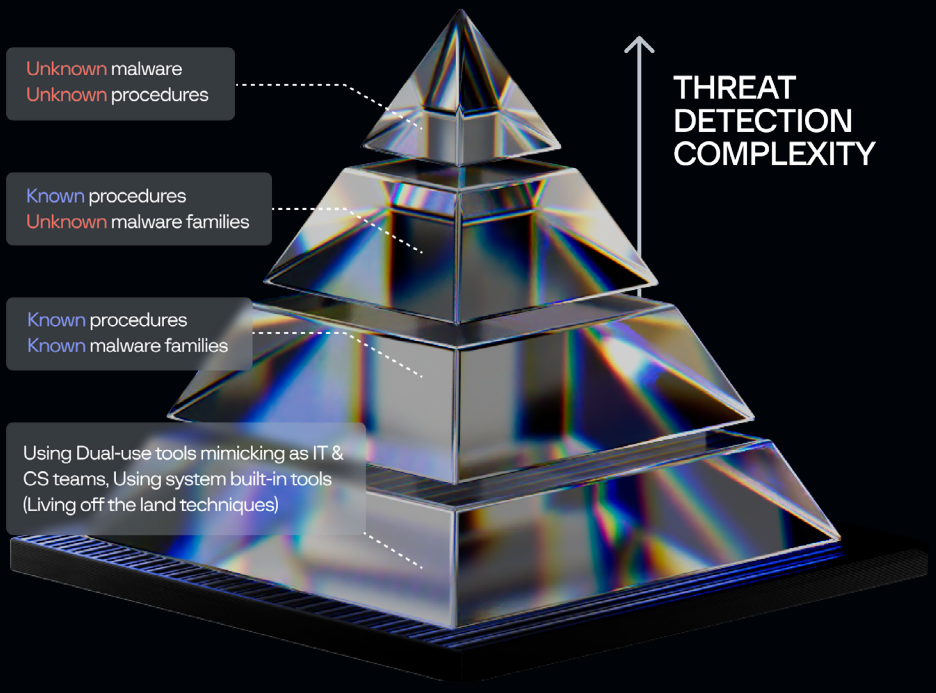


Figure 1. Complexity shift from known to unknown procedures and risks in threat detection

The cybersecurity industry brought SIGMA/YARA detection rules triggering on a single security event to spot dual-use tools (used by the IT team to check network reachability, the cybersecurity team to perform network discovery, and cybercriminals as well), built-in system binaries (known as "Living off the land" techniques), known procedures and known malware families. Adaptive weights scoring systems applied to various combinations of security events, activity baseline deviations, or trained machine learning models were created to capture the "unknowns."

So far, threat detection engines still generate a significant volume of false positives for the use cases mentioned in the figure, overwhelming security teams as they investigate each case. The most common method of reducing false positives is filtering by trusted applications or the activity patterns of IT and cybersecurity teams. However, this weakens defenses by allowing attackers to exploit these filters and remain undetected.

Given the inability to overcome the lack of threat detection mechanisms to spot adversaries' activities mentioned in the figure above, industry experts developed the threat hunting concept.

Anatoly Tykushin
Director, Cybersecurity Services, META

03

Introduction To Threat Hunting

Definition

Threat Hunting is a proactive manual or semi-automated process of searching through raw security controls' data on the assumption that threat actors have already breached the organization's surface and security controls have failed to automatically detect their activity.

Threat hunting improves proactive detection capabilities, taking an organization's risk management and mitigation to the next level. The quantifiable benefits of threat hunting are:

- Reduced intrusion dwell time (time between initial infection and attack discovery by the organization).
- Elimination of gaps in threat detection caused by lack of configuring, coverage, visibility
- Improved threat detection mechanisms by transforming threat hunting searches into detection rules with efficient noise reduction algorithms.
- Increased confidence in proper incident remediation during post-incident monitoring

Threat hunting is critical in spotting the "unknowns" where analysts search for threats that are not yet known or documented. This involves identifying the anomalies in infrastructure, misused permissions, configuration errors, data exfiltration, and emerging threat patterns that may not trigger traditional alarms. The threat hunting approach relies on knowledge of adversary tactics and a deep understanding of the environment to detect signs of compromise that automated tools could miss. It also goes beyond the network perimeter to uncover attackers' hidden infrastructure.

04 Threat Hunters

As mentioned before, threat hunting is an expert-driven approach. The expert or threat hunter is a seasoned engineer with solid experience in digital forensics, incident response, and log analysis, along with a reliable understanding of malware analysis, cyber threat intelligence, and network forensics.

When Should You Conduct Threat Hunting?

Threat hunting should be an iterative process, evolving based on new information, detection gaps, and threat landscape changes. A core principle of effective threat hunting is covering gaps in current alerting systems and manually searching for them.

A highly effective approach is to align your current detections to the MITRE ATT&CK framework, fuel it with cyber threat intelligence feeds, and focus your hunts on undercovered techniques. Mapping thousands of hunts' search hits can be time-consuming, but it provides valuable insight into gaps in your detection capabilities.

Threat hunting should be conducted at key times, such as post-incident investigation phases, new tools, processes, and organizational and operational changes, upon indication of anomalous activity, as part of regular security assessments, cyber threat intelligence provider notifications, and infrastructure audits. These are moments when an organization is more vulnerable or new attack vectors may arise, making proactive hunting crucial.

Executive Overview

Threat Hunting Use-Cases

Today, Threat Hunting at Group-IB has become an integral part of the Incident Response service, evolved into the standalone XDR solution's vendor-agnostic service, and has added a unique value to the managed cybersecurity service offering for the Group-IB Managed XDR product.

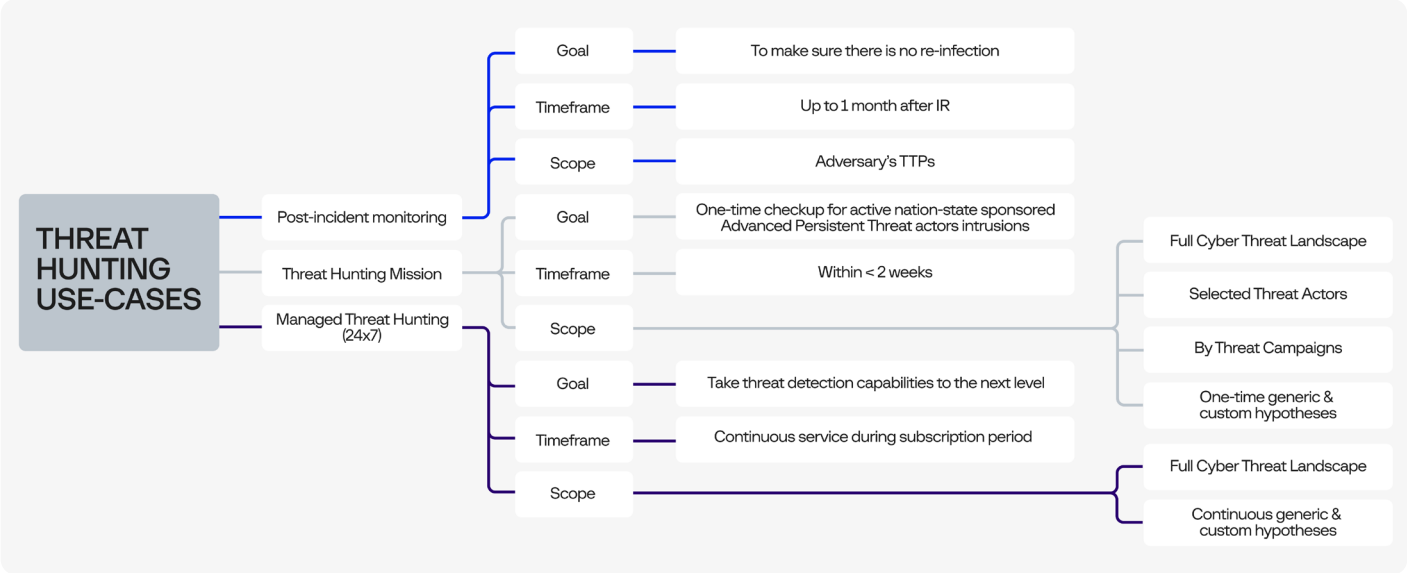


Figure 2. Use cases of threat hunting with scope, goals, and timeframes

There are three key use cases for threat hunting: post-incident monitoring, one-time threat hunting missions, and continuous, 24x7 threat hunting. Among these, customers and businesses **gain the most value from continuous threat hunting, also known as managed threat hunting**. This approach allows organizations to fully integrate the threat hunting process into their daily activities, ensuring that it aligns with business needs and operational specifics. By continuously monitoring for threats, managed threat hunting provides proactive defense and enables a seamless response to potential risks, delivering the highest level of security and adaptability for the client.

Threat hunting is one of the most advanced methods for effectively utilizing your security intelligence, particularly through high-fidelity, high-value platforms like Group-IB Threat Intelligence. By tracking diverse sources and applying the right combination of methodologies, threat hunting streamlines responses and enhances overall security.

06

Managed Threat Hunting Overview

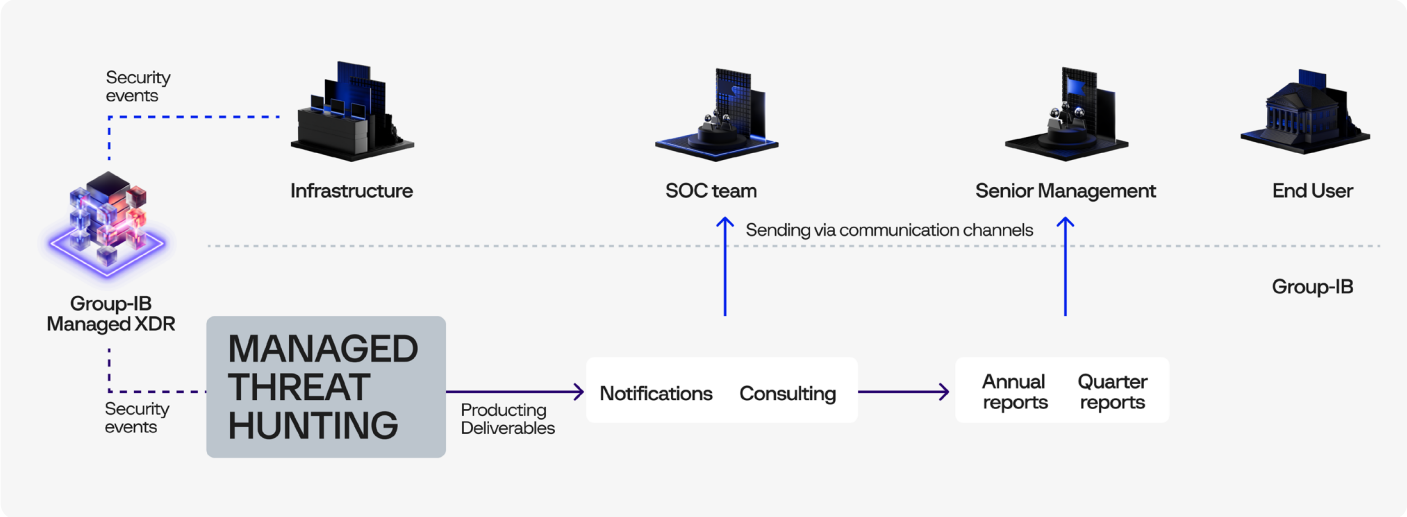


Figure 3. A macro-view at the managed threat hunting process

The high-level overview of the hunting process is as follows: It begins with telemetry collection via MXDR (Managed Extended Detection and Response) systems, which gather raw data from the endpoint and across the network. This raw telemetry is then subjected to threat hunts to identify potential threats. The collected data is further enriched by integrating additional information from various sources, improving the findings' context and accuracy. Expert analysis is then applied to this enriched data to identify potential security threats. A notification is sent to the client upon identifying a threat, and the Security Operations Center (SOC) team is consulted to address the issue. Finally, the results and findings are compiled into annual or quarterly reports to present to senior management, showcasing the effectiveness of risk management and the organization's security posture.

Key Managed Threat Hunting service consumers are:

- Cybersecurity (SOC) teams that get a triggered potential incident (hereinafter - Issue) notification message and consulting on validating the message or addressing the incident analysis efforts
- The senior cybersecurity management team receives quarterly and annual reports with key highlights about cyber threat landscape shifts and existing cyber defense gaps, as well as a summary and recommendations for improving cybersecurity resilience.

07

Threat Hunting Approaches

There are various threat-hunting techniques, each with varying levels of complexity. However, Group-IB primarily implements 2 types of threat hunting:

Cyber Threat Intelligence-driven

The threat hunting process is organized around the Tactics, Techniques, and Procedures (TTPs) reported by cyber threat intelligence providers. Using known TTPs patterns and generic hunts based on MITRE ATT&CK ® matrix techniques and sub-techniques, threat hunters can spot threat actors early in an attack and prevent them from causing damage to the system.

Hypotheses-driven

The threat hunting process is organized according to target infrastructure characteristics, normal activity baselines, key assets, guesses, and predictions about the attack methods that high-end adversaries use to achieve their goals.

Group-IB's threat hunters aren't just aligned with industry best practices—they've been directly involved in some of the most sophisticated intrusion investigations over the past 21 years. Combining **intelligence-driven** and **hypothesis-driven** threat hunting approaches, they tailor their expertise to each client's unique needs, operating without rigid, step-by-step methodologies. This creative freedom is crucial, allowing them to uncover threats that modern cybersecurity controls often miss.

08

Adversary Hunting Workflow

The adversary-hunting workflow consists of 5 crucial elements:

- **General preparations (Preparing for threat hunting):** It includes gathering comprehensive details about the environment where threat hunting will be implemented, determining relevant stakeholders, and establishing two-way communication channels.
- **Pre-hunting:** This step includes leveraging cyber threat intelligence to build a tailored cyber threat landscape and prepare hypotheses about potential threat actor activity.
- **Hunting:** Developing and running threat hunting searches (threat hunts) based on Pre-Hunting stage outputs.
- **Post-hunting:** It comprises of detecting anomalies and fine-tuning threat hunts to reduce noise and optimize the threat hunting approach.
- **Client notification:** Producing the deliverables of threat hunting for consumers: notifying about potential cybersecurity incidents, compiling and sharing periodical reports for visibility and cybersecurity posture improvements.

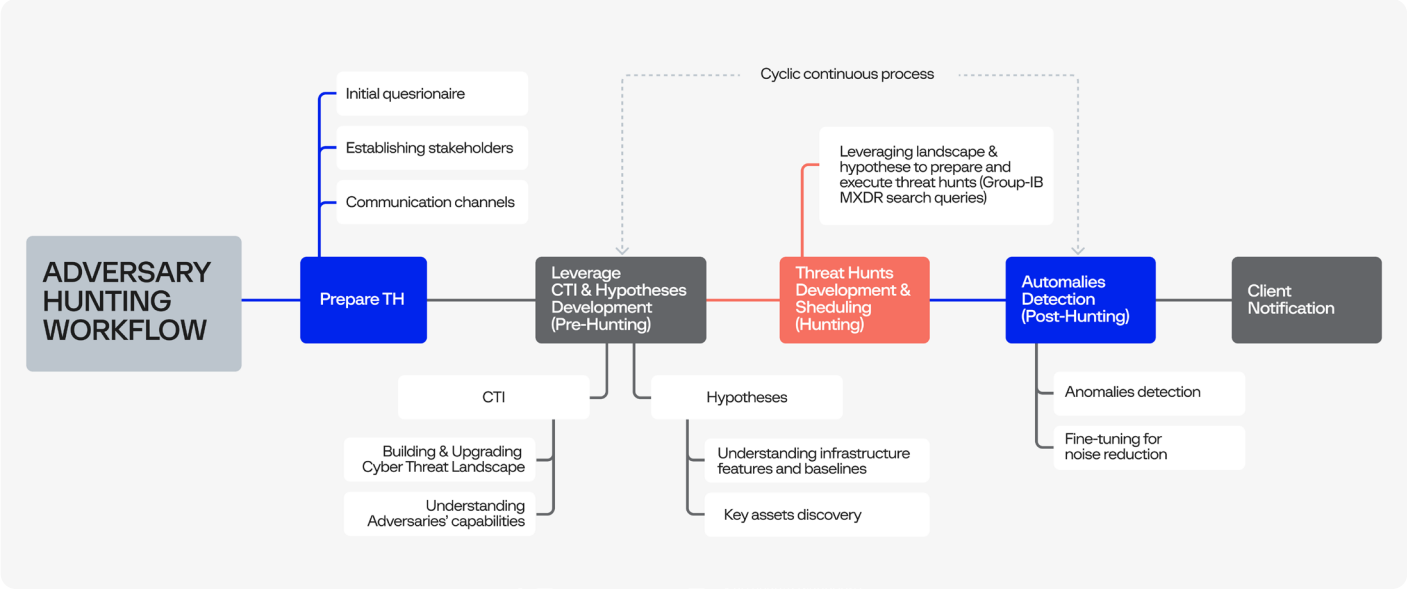


Figure 4. An overview of Group-IB experts-drafted Adversary-hunting workflow

09

Threat Hunts Development

Regular hunts lifecycle

Regular hunts are a periodic routine, enabling a proactive and cyclical approach to facilitate early detection of and response to an intrusion before its final goal is achieved. The main objective is to improve the overall cybersecurity posture by identifying and addressing potential traces of adversaries within the network. Unfortunately, it brings with it some challenges, including significant investment of time and resources, fighting against lots of false positives, fine-tuning the rules by allowing some known-good activity, and triggering additional investigation during the post-hunting phase.

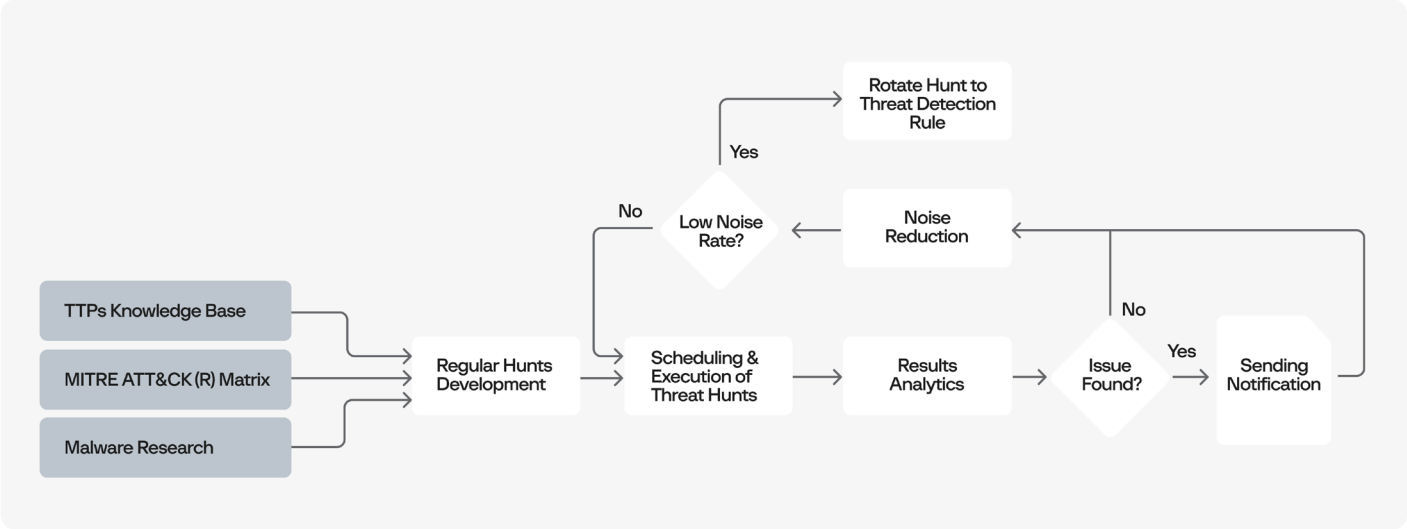


Figure 5. An overview of Group-IB regular-hunt lifecycle and how it eliminates potential threats

One-time hunts lifecycle

One-time hunts are conducted during threat hunting to identify and mitigate a specific threat or cybersecurity incident. These hunts are triggered when a particular threat needs investigation or when an incident has already occurred. One-time hunts enable an agile response, allowing teams to mitigate an intrusion before it causes significant damage. Best practices include establishing a process for consuming CTI (Cyber Threat Intelligence) related to emerging threats or campaigns, ensuring the necessary skills and tools are in place to hunt threats quickly, and regularly conducting post-hunt and post-incident reviews in lessons-learned sessions to improve the threat-hunting team's effectiveness.

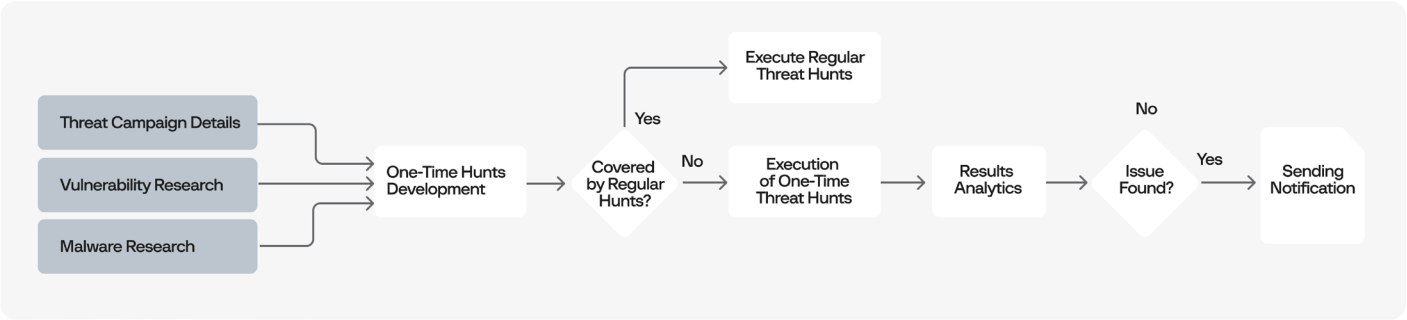


Figure 6. An overview of Group-IB one-time hunt lifecycle and how it eliminates potential threats

Anomalies detection

The workflow diagram below demonstrates the uniqueness of the Group-IB threat-hunting approach.

As input, our experts receive billions of security events daily (raw telemetry) from all assets covered with Group-IB XDR (Extended Detection and Response). The pre-developed one-time and regular hunts are applied to filter irrelevant events. Instead of triggering an alarm on a single event, our experts combine searching and aggregation algorithms, conducting post-enrichment with grouping techniques concatenating events such as user identity login, process creation, activity and termination, forensic triages, or using other log sources such as network traffic analysis (NTA) or next-gen firewalls (NGFW) to confirm if the actual breach has happened. The notification about the potential cybersecurity incident (issue) is sent to the client in case the threat hunter is suspicious of any threat.

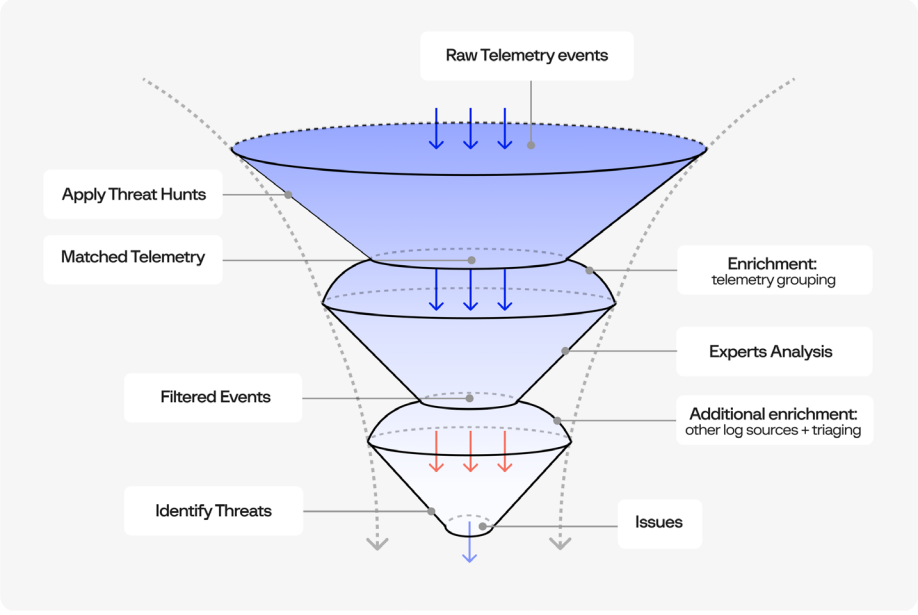


Figure 7. A demonstration of Group-IB threat hunting approach

10

How does Group-IB's approach to threat hunting stand out from other wide-range practices?

In today's threat landscape, defense practices must constantly evolve to identify and beat sophisticated threats, criminals' hyperactivity, and newer and unbeknownst means of disruptive behavior. There's a need to go both macro (Having a complete threat view of your industry and business landscape) and micro (Going more in-depth regarding telemetry collection, risk-based alerting, correlation, attack indicators, and analysis). As cybercriminals develop more deceptive tactics, defensive strategies must similarly advance. Group-IB's threat hunting practices combine a broad, industry-wide framework with a deep, detailed focus on specific indicators and risks.

Group-IB's regular hunts are designed as a continuous, proactive effort tailored to your chosen model. By implementing threat hunting practices, CTI integration, sophisticated event correlation, human expertise, and continuous lifecycle improvement, Group-IB ensures a comprehensive security posture. Summarizing our approaches in key takeaways here:

- **Regular hunts** offer a structured lifecycle approach, focusing on ongoing threats. This approach fine-tunes detection rules, reduces false positives, and continuously refines techniques to improve cybersecurity posture.
- **One-time hunts** aim to quickly identify and mitigate specific threats or incidents in a time-bound manner, ensuring a swift response when needed.
- **Anomaly Detection and Event Correlation** are advanced features of Group-IB's threat hunting. Rather than triggering alarms on isolated events (a common limitation in other market solutions), Group-IB aggregates multiple events—such as user logins, process activities, and forensic data—to verify whether an actual breach has occurred. This significantly reduces false positives and enhances detection accuracy.

The powerful symbiosis of human expertise and cutting-edge technology sets Group-IB apart. While AI and automation play critical roles in threat detection, human-driven analysis adds a vital layer of intelligence. Threat hunting experts meticulously examine and interpret the aggregated data, providing insights that automated systems alone cannot achieve. This synergy between human expertise and technology results in more precise threat detection and a more resilient cybersecurity framework.

12 Conclusion

Threat hunting has evolved beyond traditional SOC operations and reactive responses, discovering specific tools and artifacts used by attackers and going beyond looking for basic indicators like domain names, hash values, or IP addresses. While automated alerting and logging serve as a foundation, they are often cluttered with false positives, noise events, or inaccurate insights. The key lies in using reliable, high-fidelity Threat Intelligence (TI) sources to search for specific indicators while concurrently aligning with predefined hunting methodologies and rules to build and refine your own hypotheses.

Group-IB's proprietary, adversary-centric Threat Intelligence empowers organizations by gathering data through active hunts, incident response efforts, and insights from the dark web and underground sources. This enriched intelligence improves understanding of industry-specific, company-focused, and third-party threats. It enhances hunting capabilities, enabling faster triage and in-depth analysis without relying on additional data feeds.

For advanced adversary detection,Group-IB's managed threat-hunting services can help detect early signs of intruder activity, reduce dwell times for incident response teams, establish new detection methods, and identify information gaps that lead to better defenses, new TTPs, and new hunts. Discover how Group-IB's Managed Threat Hunting, powered by expert hunters and Managed XDR technology, leverages endpoint, network, and cloud data to secure your environment and provide immediate remediation guidance proactively.

Threats often lurk in the shadows, undetected, until they escalate into full-blown crises. The key to staying protected is to hunt them down before they strike—or risk being hunted. Learn how to do it the right way with Group-IB.

Talk to experts →

About Group-IB

Group-IB is a creator of cybersecurity technologies to investigate, prevent and fight digital crime.

1,550+
Successful investigations of high-tech cybercrime cases

400+
employees

600+
enterprise customers

60
countries

$1 bln
saved by our client companies through our technologies

#1*
Incident Response Retainer vendor

120+
patents and applications

8
Unique Digital Crime Resistance Centers

* According to Cybersecurity Excellence Awards

Global partnerships

INTERPOL
EUROPOL
AFRIPOL

Recognized by top industry experts

FORRESTER®
Aité Novarica
kuppingercole ANALYSTS
Gartner
IDC
FROST & SULLIVAN

Technologies and innovations

Cybersecurity

- Threat intelligence
- Attack surface management
- Email protection
- Network traffic analysis
- Malware detonation
- EDR
- XDR

Anti-fraud

- Client-side anti-fraud
- Adaptive authentication
- Bot prevention
- Fraud intelligence
- User and entity behavior analysis

Brand protection

- Anti-phishing
- Anti-piracy
- Anti-scam
- Anti-counterfeit
- Protection from data leaks
- VIP protection

Intelligence-driven services

Audit & Consulting		• Security Assessment • Penetration Testing	• Red Teaming • Compliance & Consulting
Education & Training		• For technical specialists • For wider audiences	
DFIR	• Incident Response • Incident Response Retainer	• Incident Response Readiness Assessment • Compromise Assessment	• Digital Forensics • eDiscovery
Managed Services		• Managed Detection • Managed Threat Hunting	• Managed Response
High-Tech Crime Investigation		• Cyber Investigation • Investigation Subscription	

GROUP-IB

Fight against cybercrime

GROUP-IB.COM
INFO@GROUP-IB.COM

APAC
+65 3159 4398

EU & NA
+31 20 226 90 90

MEA
+971 4568 1785