GROUP-IB

Edition 1

Intelligence. Action. Defense:

Your All-Hands E-Book On Operationalizing Cyber Threat Intelligence (CTI)

GROUP-IB.COM

Pavel’s Video Introduction

Before cyber threats strike, they always signal first. Early warnings are usually there, providing a critical window during which you can detect, prepare, and stop an attack. But how exactly do you detect and stop attacks before they happen? Hidden traces — signs buried in logs, alerts dismissed as false positives — often go unnoticed due to SOC backlogs or inefficient security controls. That’s why CTI is essential.
CTI isn’t just for IT teams in the backroom. It is for leadership to help with strategic decision-making and risk management.

It is for SOC & IR teams to help with threat triaging, proactive hunting & faster response.
But how is it done right? Definitely not by just collecting "boots-on-the-ground" data in the name of intelligence.

Define intelligence requirements	→ Know what to collect & how it aligns with business risks.
Enrich & analyze data	→ Risk-score IOCs, correlate threats, and eliminate noise.
Operationalize intelligence	→ Integrate CTI into SOC, XDR, SIEM, SOAR, and fraud detection tools.
Refine & optimize CTI	→ Use feedback loops, custom detections & intelligence-sharing networks to stay ahead.

Woah, woah, woah, slow down...
how do I build an effective CTI function step-by-step?

We’ve broken it all down for you.

Intended audience

Building a Cyber Threat Intelligence (CTI) program requires many different teams to work together. The following roles can benefit from this model and contribute to it.

Leadership & key decision-makers

CTI Directors & Team Leaders – Individual roles or part of larger teams (e.g., Cyber Defense Centers).

Cybersecurity Executives & Senior Leaders

- Chief Information Security Officer (CISO) – Responsible for an organization's information and data security
- Chief Information Officer (CIO) – Oversees information technology and computer systems
- Security Operations Center (SOC) Manager/Director – Manages teams that monitor and analyze security posture.
- Head of Fraud - Manages a Fraud Unit, which detects, investigates and prevents fraud incidents that impact customers
- Head of Risk – Oversees risk management strategies, ensuring threat intelligence is operationalized in a way that ensures proactive security and compliance

Intelligence and security practitioners

- Threat Intelligence Analyst – Gathers, processes, analyzes, and disseminates threat intelligence
- Incident Response (IR) Manager/Specialist – Manages a team or responds to security incidents
- CTI Team Lead/Manager – Manages a cyber threat intelligence team
- Cybersecurity Manager – Oversees security strategy and its implementation.
- Security Architect – Designs and implements security infrastructure
- Network Security Engineer – Implements and manages network security.
- Threat Hunters – Searches for TTPs within an organization’s environment and validates intelligence to enhance threat detection capabilities

Red team & Blue team

- Uses TI to simulate attacks and test defenses as a way of improving SIEM, security workflows, and more in order to enhance threat detection capabilities.

Risk, compliance and business resilience

- Risk and Compliance Manager – Manages risks and ensures regulatory compliance.
- Business Continuity Manager – Develops plans on how to sustain business operations during disruptions.
- Fraud Analyst – Compiles insights into evolving Techniques and Tactics (TTs) used by adversaries and develops strategies for strengthening detection and protection against fraudulent activities.

IT and infrastructure leaders

- IT Director – Oversees IT infrastructure and operations.

Cybersecurity stakeholders

- SOC Analysts, Incident Responders, Cybersecurity Researchers

By integrating insights from all these cross-functional roles, organizations can strengthen their CTI maturity, enhance their threat detection capabilities, and improve their resilience against evolving cyber threats.

Purpose of the e-book

As a domain, CTI continues to evolve all the while the threat landscape becomes increasingly complex. With threat feeds becoming increasingly extensive, enriched, consistent, and relevant, the challenges linked to operationalizing threat intelligence remain persistent. The transition between “not enough intelligence insights” to “a bit of an information overload” means that businesses still struggle to identify and act on relevant intelligence.

This guide provides practical strategies to help security teams:

- Identify, assess, and mitigate threats relevant to their business with an effective CTI program
- Understand the different nuances of critical CTI functions and how to allocate resources to best maintain posture and to support business and strategic decisions
- Filter through an overwhelming number of alerts so that risks are prioritized effectively
- Enhance immediate protection through actionable intelligence
- Integrate threat intelligence into broader security operations, including anti-fraud operations, thereby creating an end-to-end defense strategy

Table of content

Introduction

Defense without intelligence is like staring into the abyss — eyes wide open yet blind to the enemy's identity, tactics, and timing. The result? A reactive and vulnerable security stance that leaves you exposed.

Your digital identity, assets, data, stakeholders, customers, and entire network could face devastating blows from cyber threats if you cannot detect and stop them before they occur. And if you're past that stage and actively experiencing a breach, having no context about what hit you could render retaliation efforts ill-informed and ineffective, leading to exhausted resources, overworked teams, and significant losses to your finances, reputation, and business integrity.

Such agony can result in long-lasting impacts, all of which could have been avoided with the right insights into your unique threat landscape. Combined with precision, intelligence can prove to be the most robust counter-strategy against modern threats.

In today's ever-shifting landscape, however, keeping up with developments is increasingly challenging. The complex task of mapping risks and aligning real-world threats with theoretical models outlined in frameworks often feels daunting.

Many companies invest in threat intelligence expecting clarity, but what they often get is noise. Why? Because they're consuming threat intel like a product as opposed to operationalizing it as a capability.

Our e-book is designed to be an all-in-one source on Cyber Threat Intelligence (CTI) — how relevant it is and how you can make intelligence actionable in order to stay ahead of cyber challenges specific to your region, industry, and business.

**The guide will be most useful to newly formed teams that have yet to establish their processes and structure. It may also prove valuable to existing threat intelligence team leaders, offering new insights or a different perspective on CTI. At Group-IB, we have often re-organized the CTI process and teams — it's always an evolving journey. Keep maturing your own workflows and processes because there is always room for improvement.

01
Section

Understanding Threat Intelligence

Strategic Insight for Leadership, Risk Managers

What is CTI and what are its components?

Cyber Threat Intelligence (CTI) is the process of systematically collecting, processing, analyzing, and disseminating information about cybersecurity threats, vulnerabilities, and adversaries. It involves gathering data from multiple sources, transforming it into meaningful information, and delivering it in a way that means it can be used to detect, respond to, and combat cyber threats proactively

CTI converts threat information into evidence-based intelligence that uncovers adversaries' intentions, motives, and capabilities. Such knowledge is essential for effective defense against all types of threats. By defining threat models and prioritizing threats, CTI helps organizations make informed investments in cybersecurity.

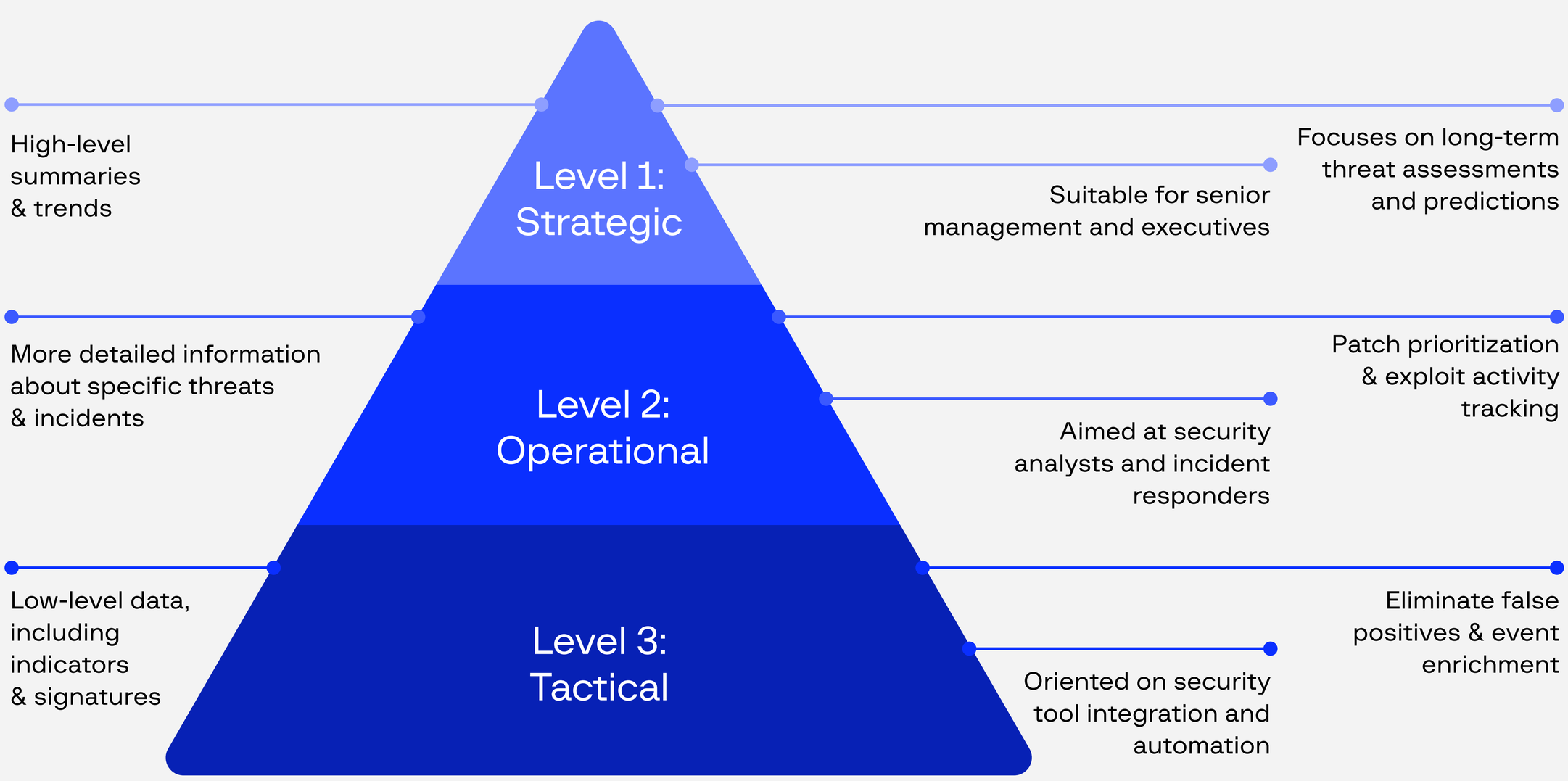
The building blocks of CTI:

- Data are pieces of information that function out of context. Data includes IP addresses and domain names, messages on dark web platforms, illicit shops, malware developers, command and control infrastructure, and more. Collected, processed, and analyzed data becomes information.
- Context is a set of circumstances and/or conditions surrounding a particular cybersecurity risk that may affect an organization's security posture.
- Intelligence results from data collection, processing, and analysis, allowing us to draw conclusions and make decisions.

> CTI is critical to building an organization’s risk profile and implementing security measures specifically tailored to address the unique threats and vulnerabilities that affect the organization. The next question is how to source such intelligence. Doing so begins with CTI feeds — structured flow of threat data that provide real-time insights into emerging risks.

Levels of threat intelligence

High-level distinctions between types of intelligence



Strategic intelligence (level 1)

Strategic intelligence provides critical foresight, enabling businesses to make risk-informed decisions by understanding threats to their departments. Such intelligence then feeds into risk and resource management processes.

To distill data from various sources — such as trusted networks, geopolitical insights, and industry whitepapers — into actionable intelligence, Group-IB analysts produce monthly and quarterly threat reports tailored for boards and executive decision-making. The goal is to activate strategic intelligence with a clear view of:

- Intelligence insights into your operating region/regional reports
- Global monthly dispatches
- Global and local annual reports
- Dashboard widgets with quarterly trends and forecasts
- Real-time dynamic trends
- Threat landscape analysis and overview

Operational intelligence (level 2)

Operational intelligence is assimilated in the form of Tools, Techniques, and Procedures (TTPs), enabling teams to block malicious network and endpoint activity the moment it is first observed anywhere in the world.

What's more, operational intelligence helps security teams identify threats and neutralize them before they can be exploited. In the event of an active attack, it equips incident responders with crucial context — provided through Indicators of Compromise (IOCs) and attribution — and thereby makes investigations more effective.

Enable operational intelligence through complete visibility

- A knowledge database with information about cybercriminals and nation-state threat actors from the last 20+ years, including information such as threat actor profiles, malware profiles, MITRE ATT&CK, context and related attribution
- Public reports on current threats to information security from many different sources, including open sources made available by various cybersecurity vendors and extensive public research
- Knowledge base relating to malware families
- Ransomware data leak sites, featuring information about ransomware attacks and data leaks
- Graph tool, which provides a robust toolset for analyzing infrastructure used by threat actors or external customers, helping to identify potential or existing threats
- Malware detonation tool (comprehensive sandbox for sample research and analysis, also used in our XDR for email, network and endpoint protection)
- Research tool and highlights for dark web and instant messengers

Tactical intelligence (level 3)

Tactical intelligence involves a detailed analysis of IOCs to ensure more effective alert triaging and to distinguish high-priority threats from irrelevant noise. It also reduces response time by providing complete visibility into the cyber kill chain in the MITRE ATT&CK® matrix format, making it possible to quickly remove threats from your network.

Tactical intelligence is leveraged to update security controls based on internal and external threat data — for example, updating detection logic, adding rules to NGFWs, blocklisting, and taking down malicious resources. Group-IB Threat Intelligence helps to prioritize vulnerability patching for your technology stack with automated alerts, notifying you the moment vulnerabilities are discovered or actively exploited by threat actors.

Activate tactical intelligence with a clear view of:

- IoCs:
  - Malware database (CNCs and hashes)
  - Suspicious IPs like TOR and VPN nodes, public/SOCKS proxies
  - Attacks/Phishing
  - Attacks/DDoS
  - Attacks/Deface
  - Threat actors (CNCs, email addresses, hashes)
- Malware configurations files
- Malware Suricata rules
- Malware Yara rules
- SIGMA rules
- Vulnerabilities feed
- Legitimate tools used by threat actors
- Procedures filtered by MITRE ATT&CK in Threats
- Compromises & leaks feed

CTI feeds and data

Threat intelligence feeds are real-time streams of structured threat data delivered directly into an organization's security infrastructure. The feeds provide information about cybersecurity threats, vulnerabilities, indicators of compromise (IoCs), and other relevant data points.

CTI feeds usually consist of the following:

Type of data	Feed	Common formats
IoC (Indicators of Compromise)	• Domain names • Malicious URLs • IP addresses • Malware hashes • Malicious emails	csv json (custom or STIX 2.x objects) txt (for example, External Dynamic Lists) XML (custom, old STIX 1.x objects or OpenIOC)
Malware signatures	• Suricata/Snort rules • YARA rules • Sigma	YARA Suricata Snort Sigma
TTPs (Tactics, Techniques and Procedures)	MITRE ATT&CK heatmap	json
Reports	• Reports in text and picture formats • Can also include OSINT data (e.g., cybersecurity news)	pdf json images
Vulnerabilities	CVE, CVSS, Impact Subscore, Exploitability Subscore, Temporal score, PoCs	json
Compromises	• Compromised accounts • Compromised PII • Compromised bank card data • Public breaches	raw data json databases csv
Dark web	• Messages and threads on forums • Markets • Instant messengers	json

CTI feeds power a range of security functions. Between the source of threat intelligence and the ways of putting it into action for improved threat detection or response, there may be several layers of data enrichment, correlation, and automation — such as threat intelligence platforms (TIPs), SIEMs, and SOAR systems — to ensure that the information is filtered and validated. We'll expand on this in the sections below.

> Once you build a structure around your intelligence and understand how it can be channeled to resolve issues and make decisions for different departments, the next step is understanding how this intelligence moves through your organization. The following section illustrates the flow of CTI across teams and processes.

Operational Insight for SOC Managers, CTI Leads

CTI data flows

Threat intelligence acts as a central hub for different security processes, either feeding them data from sources or collecting new data from them. These interconnected flows are often visualized in data diagrams to show the real-time movement of intelligence across platforms and teams.

Here's how CTI integrates across key security functions:

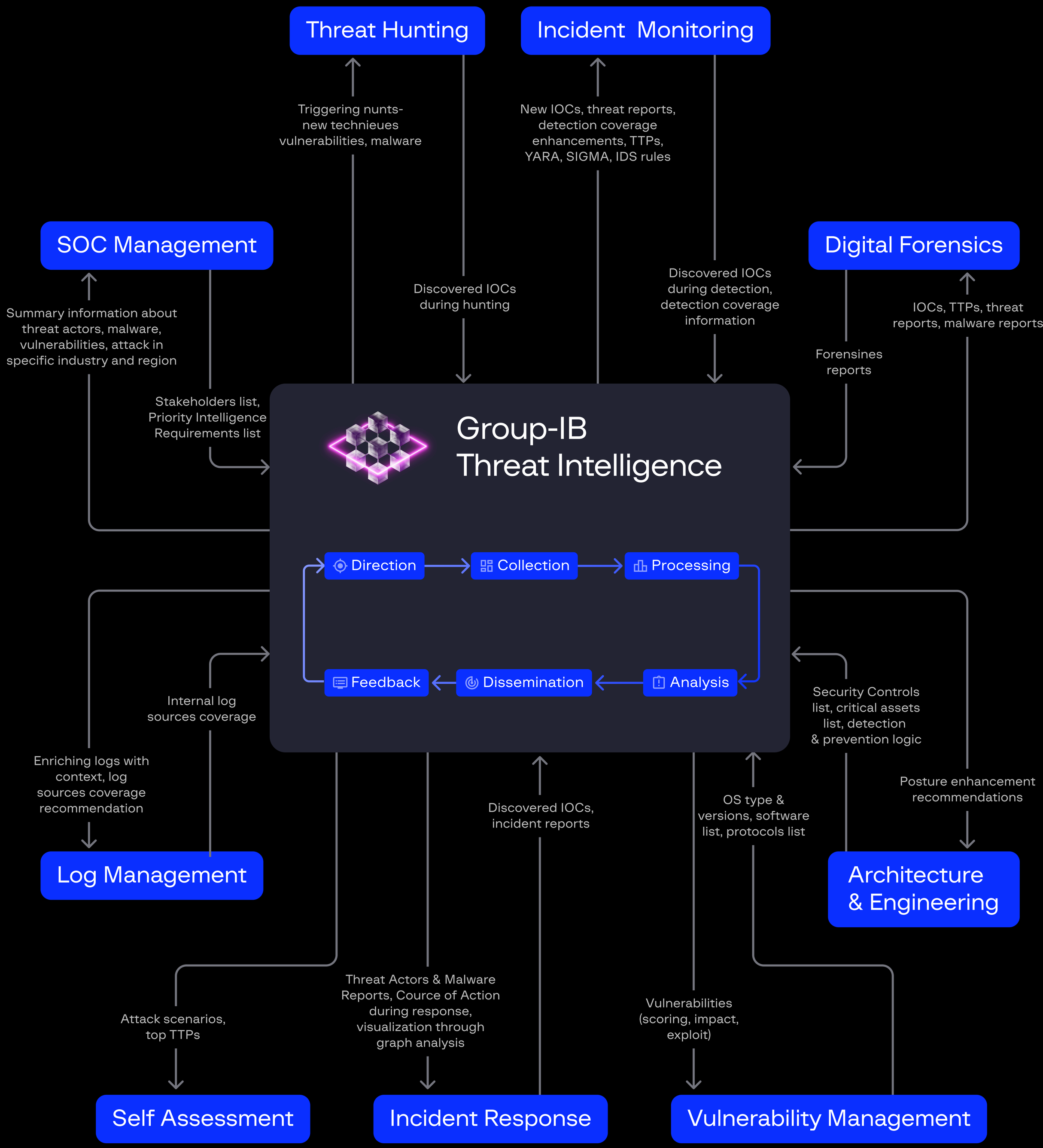
- **Log Management:** Enriches logs with contextual data about threats.
- **SOC Management:** Informs strategic and operational decisions using threat landscape insights, attacker infrastructure data, and region-specific TTPs.
- **Monitoring:** Ingests new IoCs, threat reports, and attribution data to ensure proactive detection.
- **Incident Response:** Leverages contextualized IoCs, threat reports, and TTPs to speed up investigations.
- **Threat Hunting:** Adds depth with enriched reports and TTP insights to support proactive hunts.
- **Self Assessment:** Provides threat actor attribution, readiness assessment, and exposure mapping for organizational risk management.
- **Vulnerability Management:** Prioritizes remediation based on threat intelligence aboutvulnerabilities, active exploitation, and assets most likely to be targeted..
- **Architecture & Engineering:** Guides control design, tech stack evaluation, and configuration hardening using emerging threat trends and attack paths.
- **Digital Forensics:** Enhances investigations with threat actor context, TTP mapping, all building credible evidence for the attack.

Overall, the data flow between CTI and other cybersecurity processes enables organizations to build a more resilient defense against cyber threats by leveraging timely, relevant, and actionable intelligence in order to detect, respond to, and mitigate security incidents effectively.

Depending on the setup, specialists collect, process, and store data in various formats throughout the cycle (either manually or in an automated manner). The data formats can be centralized (e.g., Threat Intelligence Platform) then distributed across systems, or fed into tools like SIEMs, TIPs, and SOAR platforms for real-time escalation and action.

> Turning data into actionable streams of intelligence — in order to ultimately defeat the adversaries who keep escalating their motives, TTPs and attack maneuvers — begins by understanding who they are. Once analysts analyze their digital footprints and attribute attacks to certain criminals, organizations can better understand what type of organization the group usually targets, how they operate, and how to defend against them.

CTI integration across key security components



Strategic Insight for Leadership, Risk Managers

Know your enemy: Categories of threat actors

Threat actors might be individuals, or they can form a syndicate of groups that operate maliciously in order to compromise and tamper with the security of the businesses, governments, and institutions they target. They can be financially or politically motivated and come from both beyond your organization (prolific threat actors behind multiple attacks or competitors performing espionage to uncover trade secrets) and within your organization (insider threats).

Understanding the types of threat actors and their goals could help businesses be aware of the main cybercriminals operating in their local landscape, their level of sophistication, and their motivations.

Threat actors	Motivation	Resources	Recent associated attacks
Nation-state APTs State-sponsored advanced persistent threat (APT) actors conduct intrusions and malicious campaigns with various objectives such as financial gain, espionage, sabotage, and disinformation. Such threat actors target governments, businesses, and other entities. Their objectives often include damaging critical infrastructure, waging war, gaining illicit access to classified data or intelligence, and pursuing other goals of national significance.	Various motivations	Huge resources provided by governments or certain governmental departments Highly sophisticated attacks	**Lazarus attack on Bybit (February 2025):** The Lazarus group, a cybercrime organization with North Korean origins, carried out a sophisticated attack on the Bybit cryptocurrency exchange, resulting in the theft of approximately $1.5 billion in digital assets. The attackers used a combination of social engineering tactics and malware to gain access to a developer's workstation, drain the exchange's cold wallet, and launder funds through meme coins, etc.
Ransomware and extortion Adversaries such as RaaS and extortion groups, which either provide resources to affiliates or conduct double extortion or extortion attacks, are usually motivated by financial gain.	Financial gain and data exfiltration. Such threat actors are usually motivated by hunting (targeted attacks) and personal reasons such as ideological differences and espionage.	Huge resources provided by governments or certain governmental departments Highly sophisticated attacks	**End of double extortion, beginning of extortion-only attacks?** On January 1, 2025, Hunters International launched a new project called World Leaks, marking a shift from double extortion to extortion-only attacks. Collaborating criminals get a custom-built exfiltration tool that automates data theft within victim networks.
Insider threats Insider threats, which can be premeditated or unintentional, are caused by individuals within an organization — such as employees, contractors, or business partners — who harm the organization's assets, systems, or reputation.	Such threats can arise from negligence or inadequate cyber hygiene, or be entirely intentional. Motivations vary: financial incentives, sabotage, or even coercion by external parties	Their motivations vary: financial incentives, sabotage, or even coerced actions by external parties	**Cyberattack on the British Library (2024):** The British Library experienced a cyberattack, which highlighted the risks associated with insider threats and the need for robust internal security measures.
Hacktivists Hacktivists have various goals and are often driven by a political or social agenda. They usually aim to generate attention by defacing websites, conducting DDoS attacks, leaking confidential data, phishing, and more.	Unauthorized access, financial or ideological incentives, or simply disruptive behavior.	They use low-cost tools and botnets, and often seek support from like-minded individuals.	In June 2025, "Predatory Sparrow" compromised Nobitex, a leading Iranian cryptocurrency exchange, threatening to release its source code & internal data within 24 hours. Blockchain analysis showed around $90 million was “burned” by sending crypto to unspendable addresses.
Organized cybercrime Organized crime groups operate like businesses and are involved in various criminal activities such as fraud, carding, scams, access brokers, data breaches, investing in advanced tools, recruiting skilled personnel, and even offering cybercrime-as-a-service to less skilled or motivated cybercriminals, including leaked data, phishing toolkits, and ransomware-as-a-service.	Financial motivation is the primary driver	They have significant resources, including custom malware, exploit kits, and money laundering networks	Group-IB's investigation into the threat actor behind aliases ALTDOS, DESORDEN, GHOSTR, and 0mid16B revealed a series of high-profile data breaches (Asia, others). He targeted internet-facing Windows servers holding personal data, exfiltrated it, and in some cases encrypted it. Goal? financial extortion.

For CTI Analystsm Threat Hunters, Detection Engineers

How attackers operate: Techniques, Tactics and Procedures (TTPs)

The MITRE ATT&CK® framework is considered the industry standard to describe tactics and techniques used by attackers. Group-IB maps these patterns using a combination of the **MITRE ATT&CK framework**, evolving fraud schemes generated using the **Group-IB Fraud Matrix**, in-house research from real-world investigations, and extensive source-intelligence.

Whenever an event or activity is reported, it is attributed to a specific threat actor, (organized cybercrime, nation-state APTs). Threat actors tend to have recognizable **patterns**: they use similar tools, techniques, and infrastructures (like IP addresses, malware strains, or impersonated websites), but they might have distinct behaviors, preferred methods, and infrastructure.

Cybercriminals attack mapped to MITRE ATT&CK® framework

Tactic	Technique		
Resource Development	Obtain Capabilities		
Initial Access	Exploit Public-Facing Application	Valid Accounts	
Execution	User Execution	Command and Scripting Interpreter	
Persistence	Valid Accounts		
Privilege Escalation	Valid Accounts		
Defense Evasion	Indicator Removal	Impair Defenses	
Credential Access	Brute Force	Exploitation for Credential Access	
Discovery	Network Share Discovery		
Lateral Movement	Exploitation of Remote Services	Remote Services	Lateral Tool Transfer
Exfiltration	Exfiltration Over C2 Channel		
Impact	Data Encrypted for Impact	Inhibit System Recovery	Service Stop

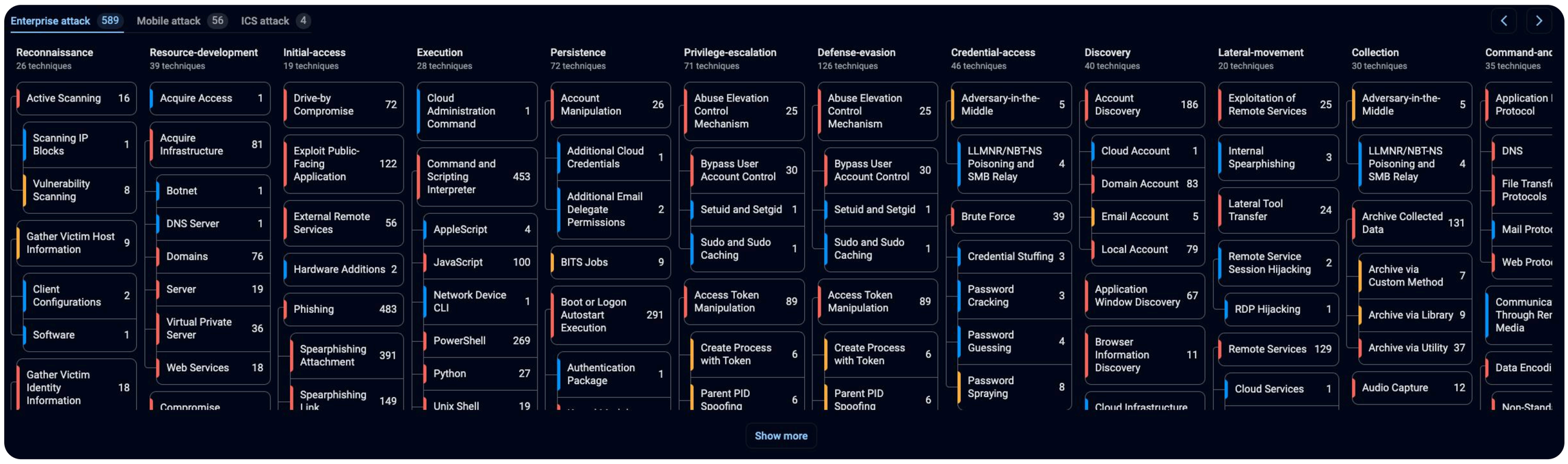


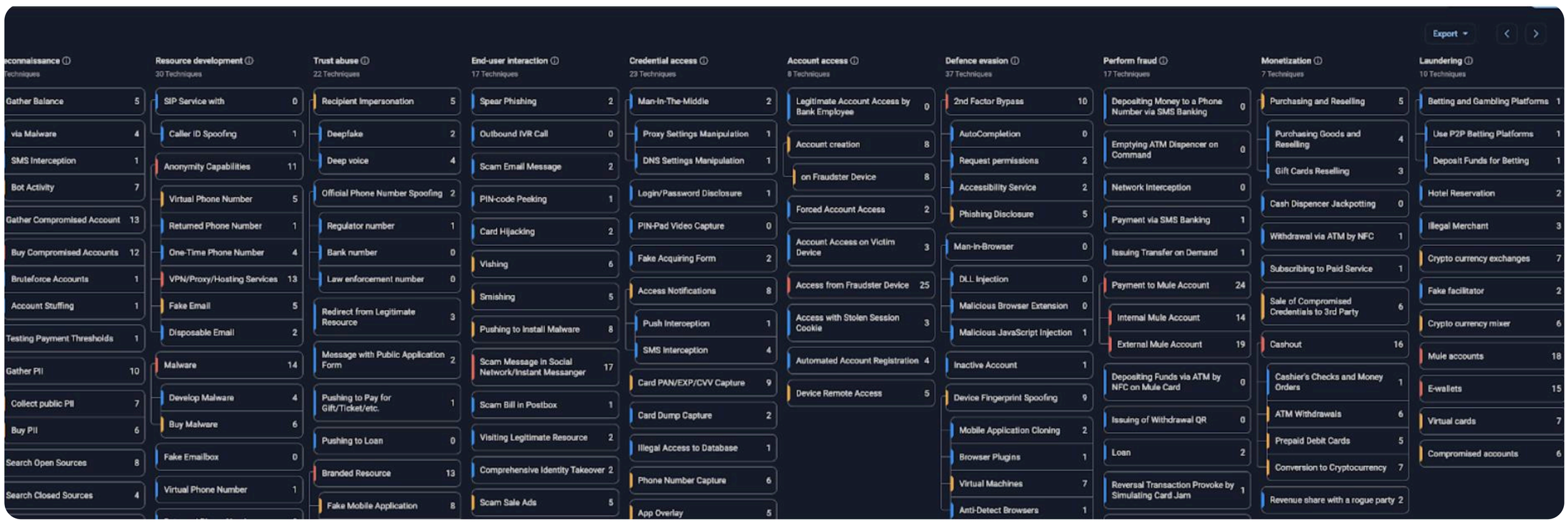
Image:
Group-IB Threat Intelligence
& MITRE ATT&CK® Matrix

Unconventional fraud - Tame it with an evolving fraud framework

By design, frameworks have limitations. And in some areas, those limitations can prove to be business-critical — especially when it comes to missing or misinterpreting fraud indicators and understanding modern fraud schemes. MITRE mainly focuses on conventional threats, APTs, and cybercriminal groups. It does not focus on evolving fraud and its schemes such as deepfake, synthetic media exploits, transaction/payment fraud, social engineering, mule networks, Account Take Over (ATO) which limits the development and understanding of Fraud Intelligence.

To bridge the gap and help you uncover and defend against hyper-scaling digital fraud, last year Group-IB introduced **Fraud Matrix**.

Fraud Matrix is a practical framework that translates this intelligence into actionable insights. It helps teams visualise, categorise, and respond to fraud threats across both cyber and fraud domains.



10 tactics **200+** techniques/ subtechniques **6** platforms/ channels **100+** mitigations and detections. (also need to add the "why" & "how" highlight text just like the current for this new one

The general idea is that **Fraud Matrix can map any fraud scenario** with precision. From the point of view of fraud prevention, just like how MITRE works for cybersecurity, Fraud Matrix helps determine whether fraud scenarios can be detected using existing prevention solutions such as sessional and transaction-based anti-fraud systems.

From the point of view of fraud intelligence, Fraud Matrix provides the foundation for Group-IB's reports on fraud activities, leveraging an **AI-driven matrix** to identify and analyze fraud tactics and techniques.

Image:
Group-IB Fraud Intelligence showcasing fraud tactics and techniques

> To build advanced defense strategies against cyber threats and fraud, Group-IB consistently tracks hundreds of threat actor campaigns. By correlating TTPs, uncovering IOCs, mapping threat actors' dark web movements, and profiling their countries of origin and usernames, we piece together the complete attack lifecycle — from initial infection access all the way to monetization. Let's map some of the campaigns.

Operational Insight for SOC Managers, IR Teams

Visualizing real threat scenarios: Decoding attack sequences

Let’s look at campaigns and tooling with widely-observed attack techniques linked to specific threat actors

01 Ransomware operations – Financially motivated extortion

Threat actor/group: Qilin Ransomware, BlackCat (ALPHV), LockBit

Group-IB’s research identifies their combined tactics and techniques using the MITRE ATT&CK framework (Although operators may use different tactics across the kill chain, these MITRE techniques shown are representative, not exhaustive — a combined blend of overlapping behaviors):

Attack lifecycle:

Initial Access

- **T1566.001 – Phishing: Spearphishing Attachment**

Phishing emails delivering initial payloads or access links.

- **T1133 – External Remote Services**

RDP brute-force attacks on exposed endpoints.

- **T1190 – Exploit Public-Facing Application**

Vulnerabilities in VPNs apps, web app, etc.

- **T1583 – Acquire Infrastructure Leverage of Initial Access Brokers (IABs) for credentials or foothold.**

Execution, Persistence and Defense Evasion

- **T1059.001 – Command and Scripting Interpreter: PowerShell**

Use of PowerShell scripts for covert execution.

- **T1027 – Obfuscated Files or Information**

Fileless malware or RATs with stealth capabilities.

- **T1055 – Process Injection**

RATs injected into legitimate processes for stealth.

Privilege Escalation and Lateral Movement

- **T1003.001 – OS Credential Dumping: LSASS Memory**

Credential theft via Mimikatz and Cobalt Strike.

- **T1078.001 – Valid Accounts: Domain Accounts**

Movement with stolen Active Directory credentials.

- **T1562.001 – Impair Defenses: Disable or Modify Tools**

Disabling EDR/AV or Windows Defender.
ressure.Defense Evasion

Exfiltration

- **T1048.003 – Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted/Obfuscated Protocol**

FTP, cloud storage abuse (e.g., Mega, Dropbox), TOR.

- **T1567.002 – Exfiltration to Cloud Storage**

Use of Dropbox, Google Drive, etc., for covert communication

Impact: Payload Deployment

- **T1491.001 – Defacement: Internal Defacement**

Threatening internal leaks or warning messages as extortion leverage.

- **T1486 – Data Encrypted for Impact**

File encryption rendering business-critical data inaccessible.

- **T1490 – Inhibit System Recovery**

Deletion of backups and shadow copies.

- **T1489 – Service Stop**

Termination of processes or services that might hinder encryption.

- **T1499 – Endpoint Denial of Service**

Lockout or crippling of systems to accelerate ransom pressure.Defense Evasion

02 APT espionage campaigns – State-sponsored cyber operations

Threat actor/group:
APT41, Dark Pink APT

Group-IB's research identifies their combined tactics and techniques using the MITRE ATT&CK framework:

Attack lifecycle:

Reconnaissance

- T1593.001 – Search Open Websites/Domains: Social Media Attackers use job sites, LinkedIn, and social networks for target profiling.
- T1589 – Gather Victim Identity Information Collection of names, roles, and relationships.
- T1584.001 – Compromise Infrastructure: Websites Watering hole attacks compromise high-traffic sites.

Initial Access

- T1566.001 – Phishing: Spearphishing Attachment Trojanized ISO files or weaponized documents in phishing emails.
- T1190 – Exploit Public-Facing Application Zero-day exploitation against exposed services.
- T1195.002 – Supply Chain Compromise: Compromise Software Supply Chain Infiltration via compromised third-party software.

Execution, Persistence and Privilege Escalation

- T1059.003 – Command and Scripting Interpreter: Windows Command Shell Execution of scripts or malware like Ctealer.
- T1055.001 – Process Injection: Dynamic-link Library Injection Custom malware deploying into legitimate processes.
- T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder Persistence through registry keys.
- T1053.005 – Scheduled Task/Job: Scheduled Task Task scheduling for long-term presence.

Command and Control and Exfiltration

- T1567.002 – Exfiltration Over Web Service: Exfiltration to Cloud Storage Use of Dropbox, Google Drive, etc., for covert communication.
- T1095 – Non-Application Layer Protocol DNS tunneling to exfiltrate data.
- T1105 – Ingress Tool Transfer Encrypted Telegram bots used to receive payloads.

Impact

- **T1496 – Resource Hijacking Abuse of system resources for long-term surveillance.**
- **T1565.001 – Data Manipulation: Stored Data Manipulation Espionage and IP theft through targeted data extraction.**

03 Banking malware and financial fraud – Targeting financial institutions

Banking Trojans: Ajina.Banker and Grandoreiro

Threat Actor: Ajina.Banker: Threat Actor/Group (Unknown), Grandoreiro Threat Actor/Group: Grandoreiro Operators

Motive: infiltrate victims' devices, enabling them to harvest credentials, intercept authentication mechanisms, and hijack active sessions.

Group-IB's research identifies their combined tactics and techniques using the MITRE ATT&CK framework (Although operators may use different tactics across the kill chain, these MITRE techniques shown are representative, not exhaustive — a combined blend of overlapping behaviors):

Attack lifecycle:

Initial Access

- Ajina.Banker:
  T1566.001 – Phishing: Spearphishing Attachment: Malicious APK files disguised as legitimate banking or utility apps are distributed via Telegram, luring users into installing them.

- Grandoreiro:
  T1566.002 – Phishing: Spearphishing Link: Phishing emails impersonating government or financial institutions contain links leading to the download of the Grandoreiro trojan.

Execution

- Ajina.Banker:
  T1204.002 – User Execution: Malicious File: Users are tricked into manually installing the malicious APKs, granting extensive permissions that enable the malware's functionality.

- Grandoreiro:
  T1059.005 – Command and Scripting Interpreter: Visual Basic: Utilizes Visual Basic scripts for execution and to establish persistence on infected systems.

Defense Evasion

- Ajina.Banker:
  T1406 – Obfuscated Files or Information: The malware employs obfuscation techniques to evade detection by security solutions.

- Grandoreiro:
  T1027 – Obfuscated Files or Information: Implements multiple anti-analysis techniques, including code obfuscation and the use of Captcha implementations, to hinder detection and analysis.

Credential Access

- Ajina.Banker:
  T1414 – Input Capture: Intercepts SMS messages, including two-factor authentication (2FA) codes, to gain unauthorized access to banking accounts.

- Grandoreiro:
  T1056.001 – Input Capture: Keylogging: Captures keystrokes to harvest credentials and other sensitive information.

Command and Control (C2)

- Ajina.Banker:
  T1071.001 – Application Layer Protocol: Web Protocols: Communicates with C2 servers over HTTP/HTTPS to exfiltrate data and receive commands.

- Grandoreiro:
  T1071.001 – Application Layer Protocol: Web Protocols: Utilizes HTTP for C2 communications, often employing domain generation algorithms (DGAs) to generate dynamic domains.

Exfiltration

- Ajina.Banker:
  T1041 – Exfiltration Over C2 Channel: Exfiltrates stolen data, including credentials and SMS messages, through established C2 channels.

- Grandoreiro:
  T1041 – Exfiltration Over C2 Channel: Sends harvested data to remote servers controlled by the attackers via HTTP requests.

Impact

- Ajina.Banker:
  T1499 – Endpoint Denial of Service: Potentially disrupts device functionality by abusing permissions and interfering with normal operations.

- Grandoreiro:
  T1499 – Endpoint Denial of Service: This may impact system performance and stability, hinder user operations, and facilitate further malicious activities.

04

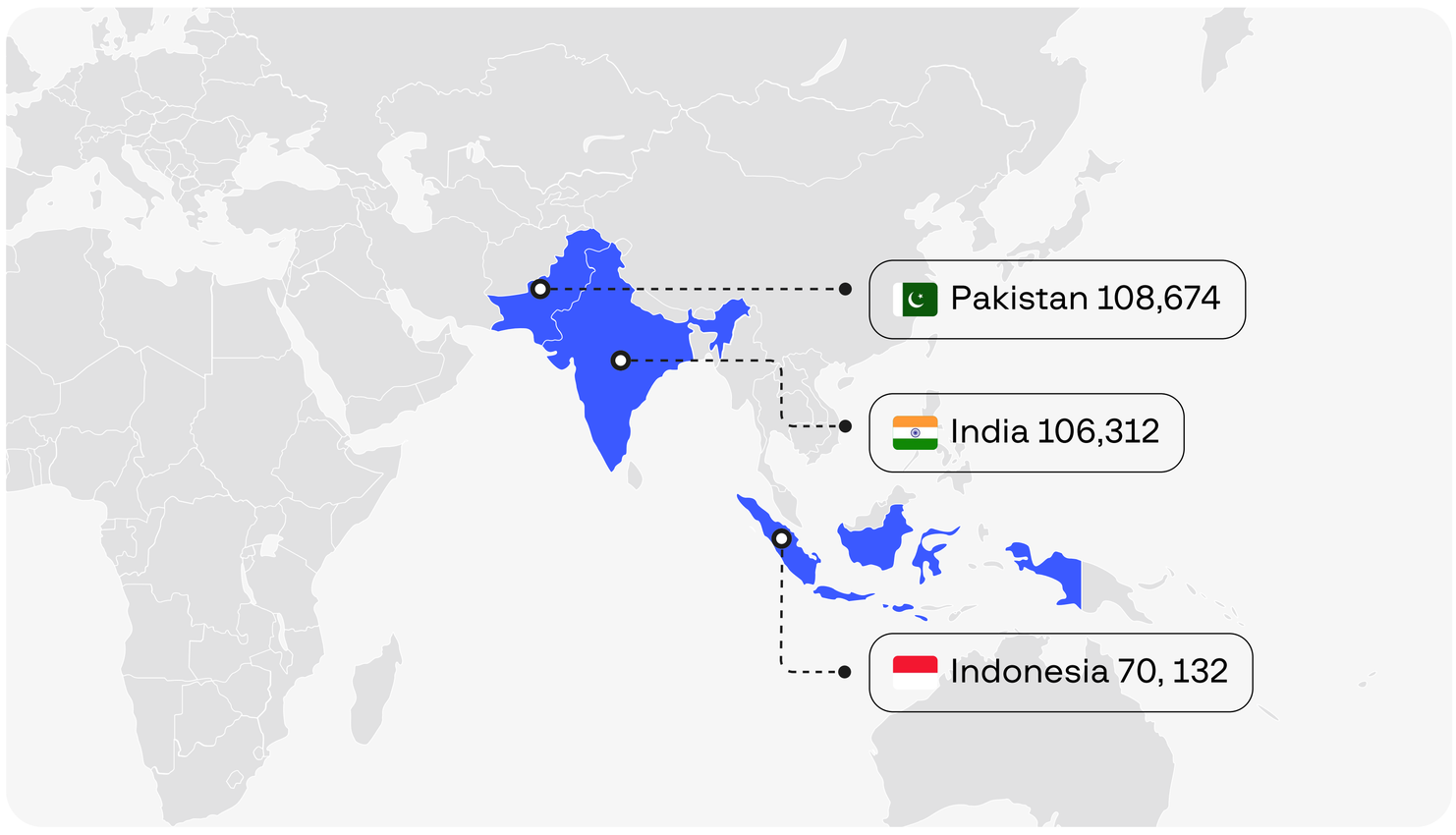
Infostealer malware and identity theft

Infostealers are the silent killers in the digital age—quietly infiltrating systems, extracting sensitive data, and paving the way for secondary attacks. In 2024, their deployment became both more convenient for cybercriminals and more complex for defenders to detect, especially with the use of AI-driven social engineering to craft believable lures; ClickFix techniques to facilitate stealthy installation; Rise in Initial Access Brokers (IABs) who monetize stolen credentials

To grasp the scale of their usage, here's a regional breakdown of compromised hosts and the most prevalent infostealers responsible:

Asia-Pacific

Top Countries



Leading Infostealers

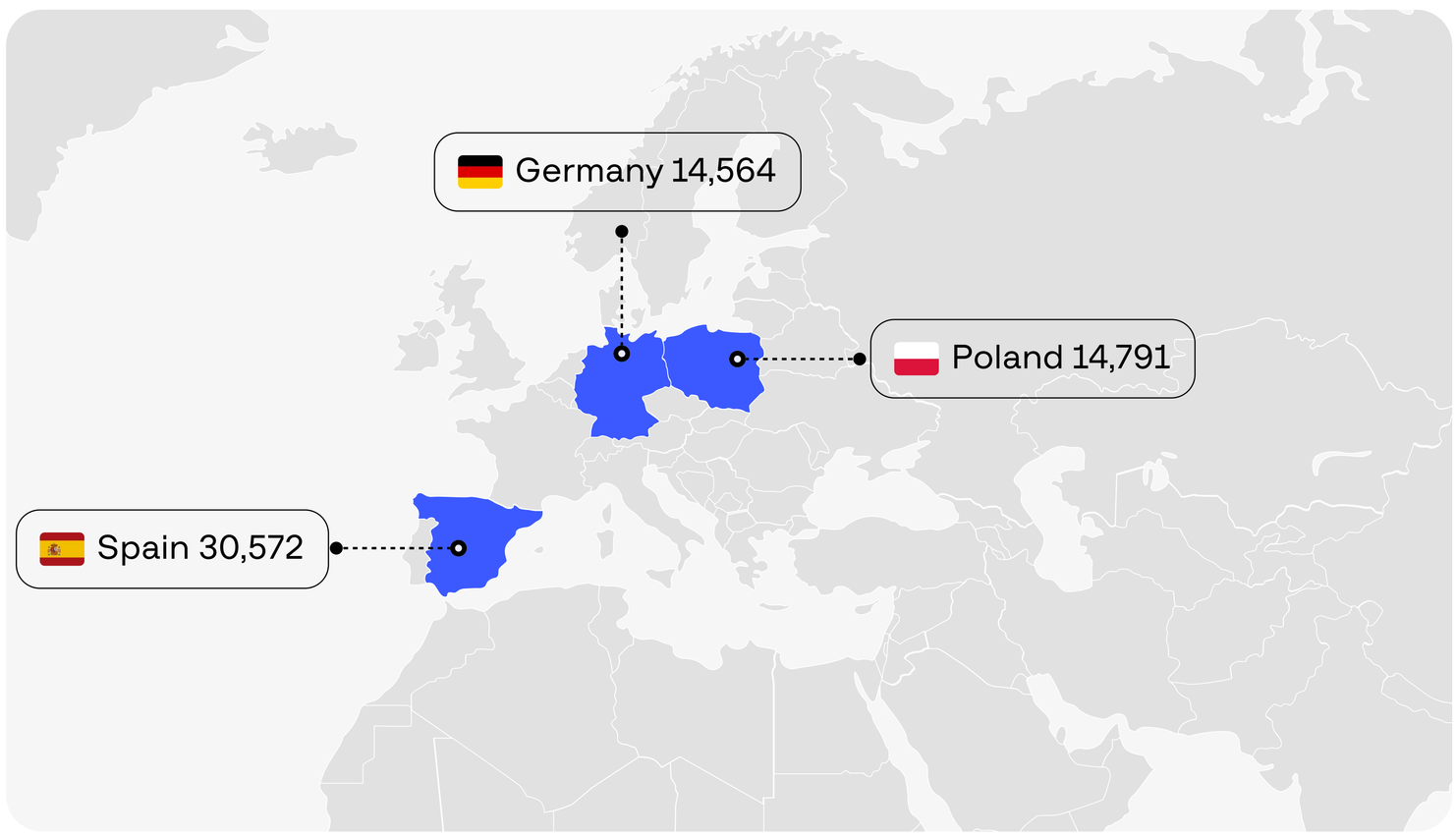
176,965
infections
RisePro

169,116
infections
RedLine Stealer

147,934
infections
Stealc

Europe

Top Countries



Leading Infostealers

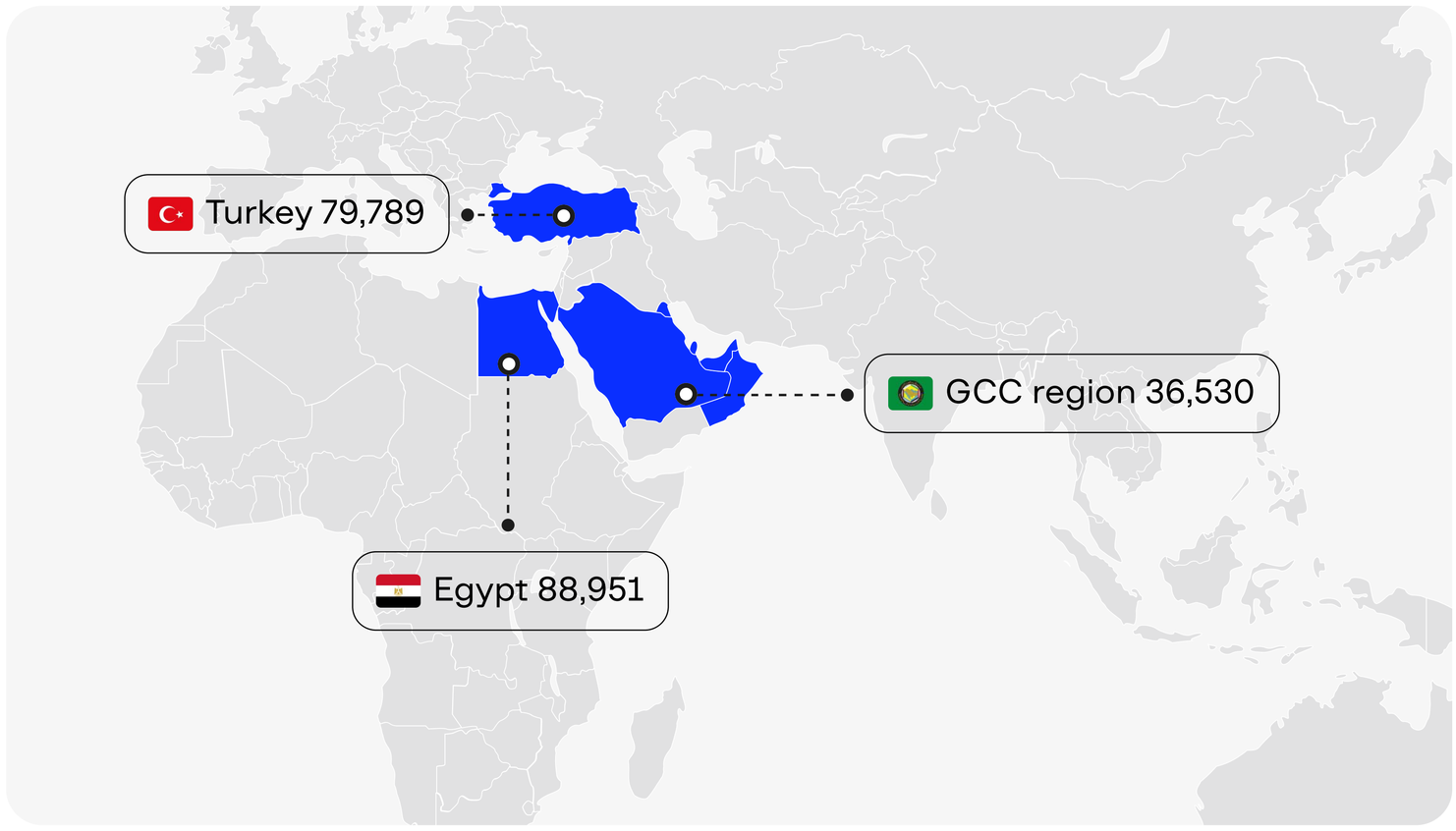
66,121
infections
RedLine Stealer

40,306
infections
RisePro

40,300
infections
Stealc

Middle East & Africa

Top Countries



Leading Infostealers

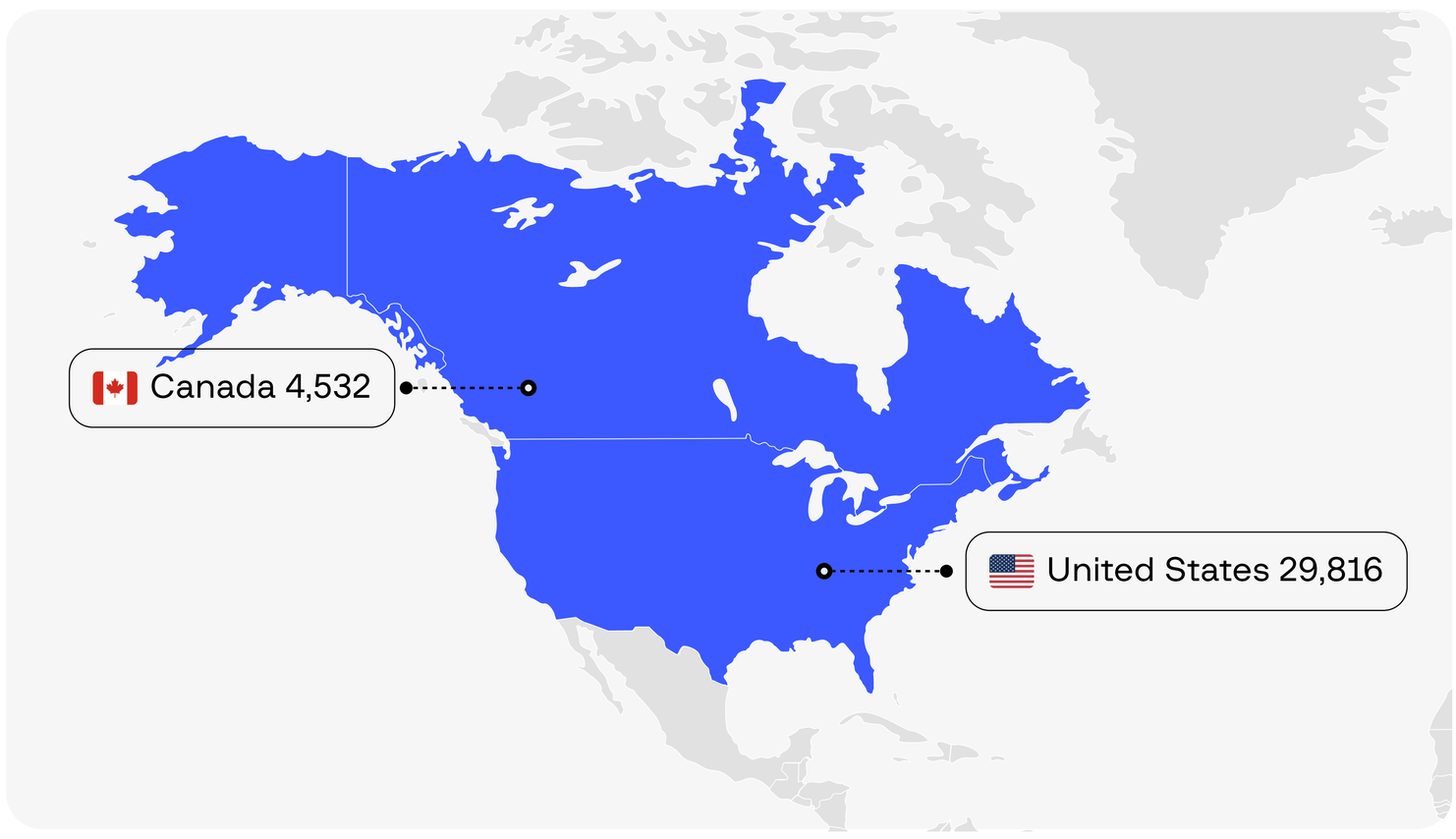
159,067
infections
RisePro

141,724
infections
RedLine Stealer

85,653
infections
Stealc

North America

Top Countries



Leading Infostealers

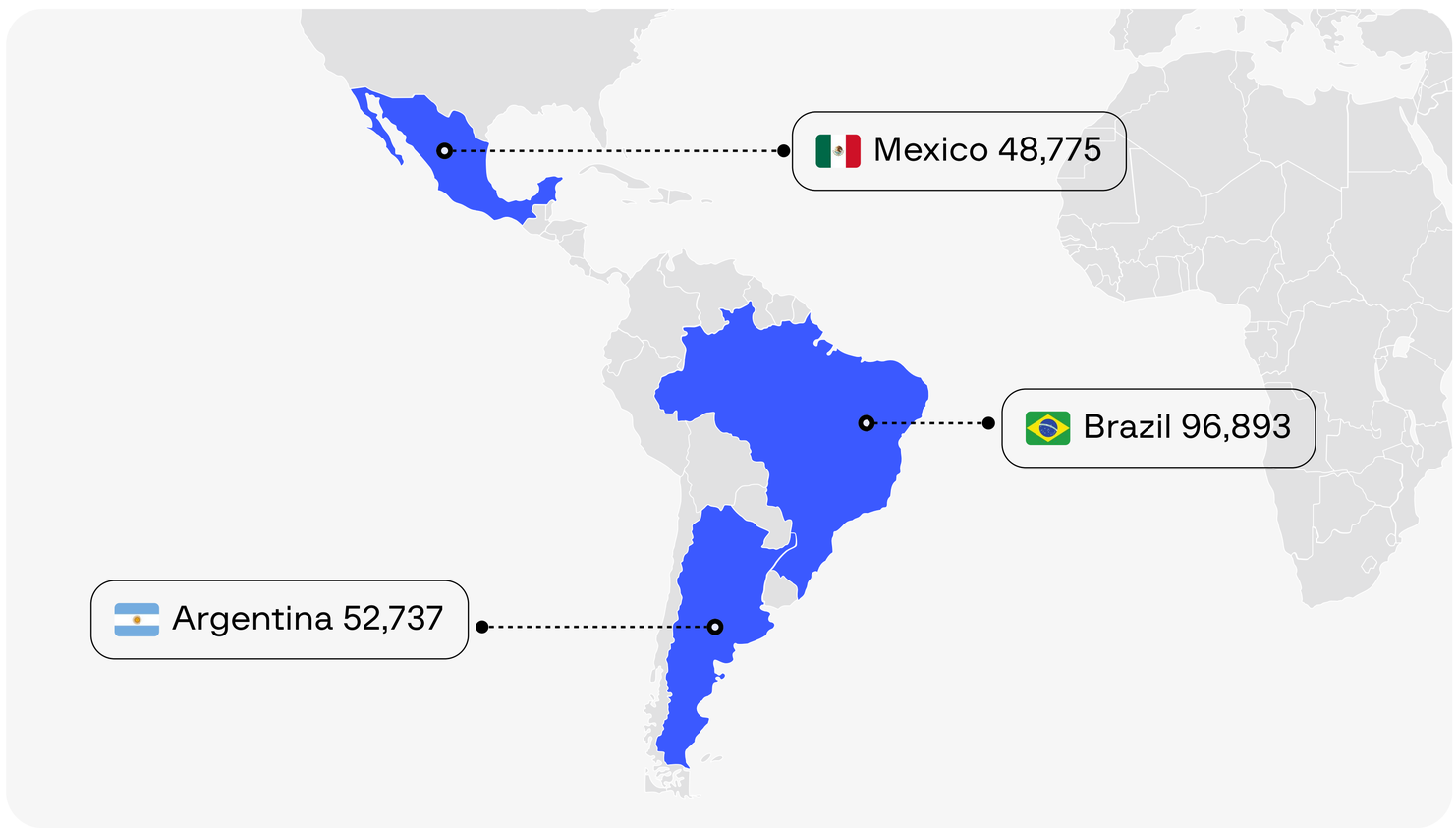
14,537
infections
RedLine Stealer

7,478
infections
META Stealer

5,257
infections
RisePro

Latin America

Top Countries



Leading Infostealers

134,236
infections
RedLine Stealer

121,453
infections
RisePro

85,380
infections
Stealc

A noteworthy incident occurend in 2024, where threat actors deployed the CraxsRAT malware through counterfeit Android applications. These malicious apps were disguised as everyday services, including a dumpling delivery app, to deceive users into downloading them. Once installed, the malware granted attackers remote access to victims' devices, allowing them to harvest sensitive information such as banking credentials and personal data.

Group-IB's investigation revealed that this campaign targeted various sectors, including telecommunications and banking, and was part of a broader trend of using fake apps for cyber espionage and fraud in Southeast Asia.

Industries hit:	Finance, Telecom
Threat actor:	EVLF DEV deployed the CraxsRAT malware
Research Origin:	Attributed and tracked by Group-IB's malware intelligence and mobile threat research teams

Attack lifecycle:

Initial Access

- T1476 – Deliver Malicious App via Other Means (Mobile)
  CraxsRAT is distributed through phishing websites that impersonate legitimate brands, enticing users to download malicious Android applications.

Execution

- T1406 – Obfuscated Files or Information (Mobile)
  The malware employs obfuscation techniques, such as base64 encoding of its command and control (C2) server details, to evade detection.

Defense Evasion

- T1407 – Download New Code at Runtime (Mobile)
  CraxsRAT can dynamically load additional code during execution, allowing it to modify its behavior and avoid static analysis.

Credential Access

- T1414 – Input Capture (Mobile)
  The malware captures user inputs, including credentials, by exploiting Android's Accessibility Services.

Discovery

- T1420 – File and Directory Discovery (Mobile)
  CraxsRAT scans the device's file system to identify and access sensitive files and directories.

Command and Control (C2)

- T1437 – Application Layer Protocol (Mobile)
  The malware communicates with its C2 servers using standard application layer protocols, blending in with regular network traffic.

Exfiltration

- T1430 – Data Transfer to External Storage (Mobile)
  CraxsRAT exfiltrates collected data, such as credentials and personal information, to external servers controlled by the attacker.

05 SIM swapping fraud and fraudsters bypassing security layers

Threat actor/group: ScreamedJungle

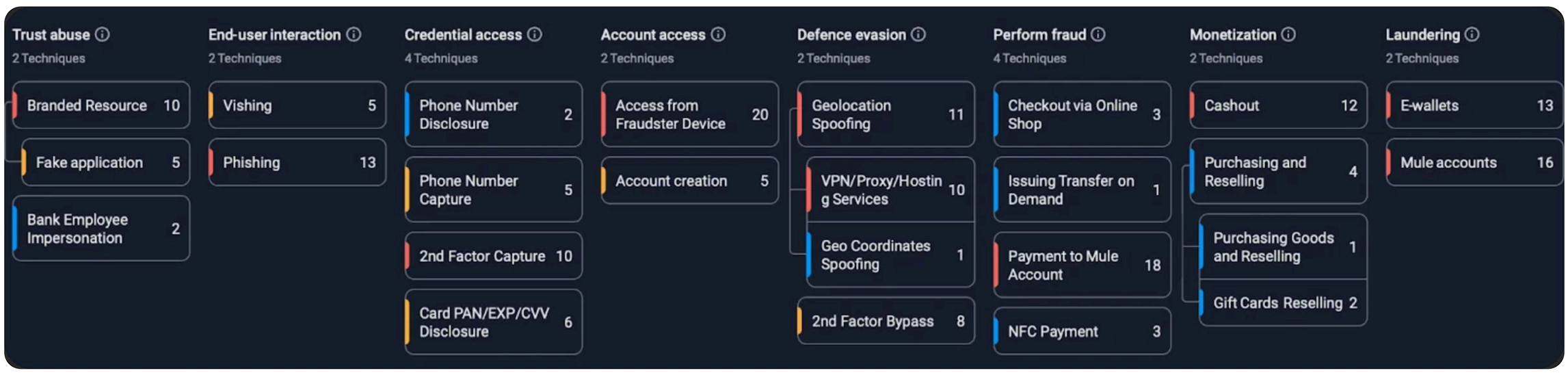


Image:
Deciphering ScreamedJungle fraud techniques using Fraud Matrix

Attack lifecycle (based on Fraud Matrix):

Reconnaissance:

- Over 115 e-commerce websites were compromised by injecting Bablosoft JS script into Magento platforms
- Collection of user fingerprints and detailed visitor information

Resource development and account access:

- Impersonation of legitimate users using stolen fingerprints to gain unauthorized account access

Defense evasion (bypassing fraud protection systems):

- Obfuscation of fraud protection controls that rely on behavioral analysis and device recognition

Monetization:

- Access to online accounts (banking, email), which leads to financial theft and identity fraud

Read about the latest tactics used by adversaries in the forecasts and recommendations section of Group-IB's Hi-Tech Crime Trends Report 2025.

For in-depth insights into the behaviors of different malware, including infostealers, Group-IB provides a free Malware Reports tool. The tool provides access to **over 2 million detailed malware reports featuring comprehensive behavioral analysis, process trees, indicators of compromise, and network activity dumps.**

> We now know what threat data to collect and how it is communicated within processes and teams, the levels of intelligence it produces, and the adversaries it helps to identify and understand. With this foundation in place, the next question is: how do you operationalize all this intelligence? The answer lies in the CTI lifecycle — which we'll discuss next.

For CTI Analysts, Threat Intel Teams

CTI lifecycle: Gather and take action on intelligence to maximize protection

This section offers a high-level framework describing the phases of CTI for strategic direction. You'll find references to this lifecycle throughout the guide. We'll cover CTI technical implementation, integration into systems and automation for day-to-day operational flow in a later section: Operationalizing threat intelligence in security workflows

Security-driven threat intelligence (TI) is like having a well-oiled cogwheel in motion where everything is connected, from collection and ingestion to analysis, enrichment, and dissemination.

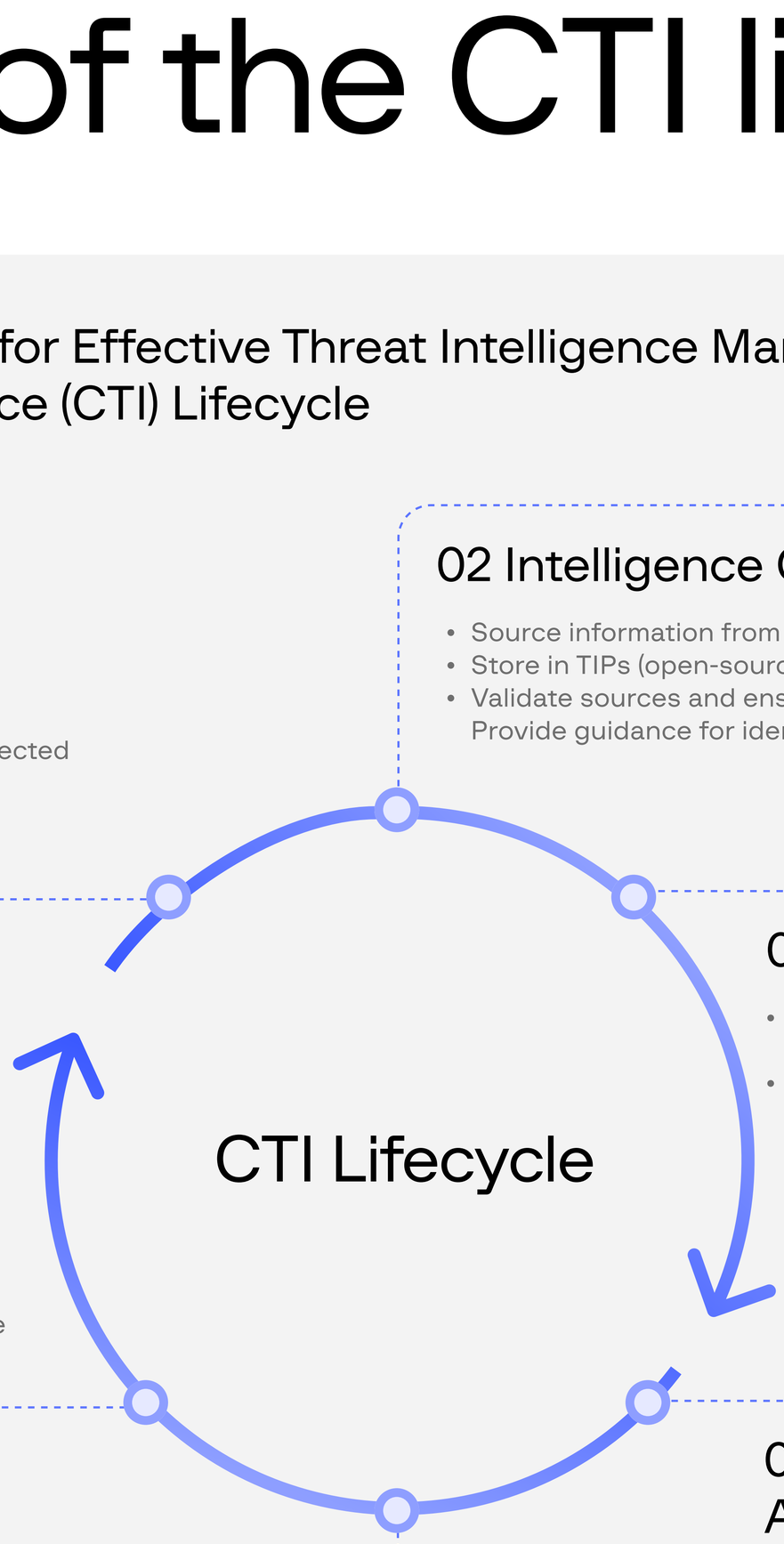
For intelligence to act as your defence, the cogwheel must keep functioning — drawing volumes of data from relevant sources and converting that information into valuable intelligence tailored to your industry, region, and threat landscape.

The days of manually updating SIEM watchlists with malicious IPs are long gone. Attackers today are nimble and persistent. To keep pace, organizations must embrace real-time CTI lifecycles that allow for a combination of many things: (i) continuous, high-fidelity intelligence gathering and enrichment; (ii) a comprehensive understanding of attacker tactics, tools, and global campaigns; (iii) proactive detection and (iv) swift and informed responses to evolving threats.

How do you achieve all that with an efficient CTI lifecycle? Let's find out.

Stages of the CTI lifecycle

A Continuous Process for Effective Threat Intelligence Management
Cyber Threat Intelligence (CTI) Lifecycle



01 Planning

- Understand what needs to be protected
- Align with broader business goals
- Enable informed decision-making
- Support key business functions

02 Intelligence Gathering

- Source information from multiple channels
- Store in TIPs (open-source/commercial)
- Validate sources and ensure relevance
  Provide guidance for identified threats

03 Intelligence Processing

- Normalize formats and languages
  Ensure consistency across sources
- Prepare data for detailed evaluation

04 Intelligence Analysis & Grading

- Put data in action for security decisions
- Analyze threat scope, impact, consequences
- Ascertain reliability and accuracy
- Use Admiralty Code for grading

05 Sharing Intelligence

- Provide timely, accurate intelligence
- Communicate clear action items
- Tailor content to stakeholder needs
- Follow TLP protocol for sharing

06 Feedback & Optimizations

- Review the entire cycle
- Make continuous refinements
- Improve data quality and relevance
- Adapt to emerging threats

1. Planning
Creating an effective CTI program begins with understanding what needs to be protected and why. With this foundation in place, organizations can collect and use the right intelligence. To ensure maximum value, a CTI program should:

- **Identify CTI Stakeholders**

Clearly mention how will CTI needs align with greater business objectives and who will be the rightful stakeholders to consume and base decisions on the intelligence offered

- **Define Priority Intelligence Requirements (PIRs)**

Assess the most critical requirements around CTI, depending on your high-risk or critical assets, threat actor mapping to your landscape, techniques used and where are you most exposed.
Talk to leadership early to understand their priorities and shape your intelligence program around real business needs.

2. Intelligence gathering
Once you define your objectives (e.g., protecting network components, assets, or accounts), the focus shifts to sourcing information. Effective gathering involves:

- Creating a comprehensive view of potential threats using relevant data sources (commercial, government, OSINT, industry groups, dark web, vulnerability databases)
- Storing the information on either open-source or commercial Threat Intelligence Platforms (TIPs)
- Enriching and contextualizing intelligence by:
  - Validating sources
  - Ensuring relevance to your industry and organization
  - Providing clear guidance for addressing any identified threats

3. Intelligence processing
Collating data from various sources requires normalizing formats and languages (commonality) to allow for effective analysis. This step ensures consistency and prepares the data for detailed evaluation.

4. Intelligence gathering and grading
This stage puts data in action, with you deriving intelligence on which you can base your security decisions. Analysing the scope, impact and consequences of threats is a key part of the process and allows you to prioritize actions.

Before that, however, you must ascertain the reliability (how trustworthy is the source?) and accuracy (is the information credible?) of your intelligence. For this we use the Admiralty Code (also known as the **NATO Intelligence Source and Reliability Rating System).**

How does the Admiralty Code work within the Group-IB Threat Intelligence platform?
In our platform, the Admiralty Code consists of two components that come together to form a single code: **reliability and credibility**. Reliability and credibility are essential components in evaluating the overall trustworthiness of the data within our platform.

Source reliability (A to F): This letter grade reflects how historically accurate and trustworthy the source is. Each grade reflects a different level of reliability:
A: Completely reliable
B: Usually reliable
C: Fairly reliable
D: Not usually reliable
E: Unreliable
F: Reliability cannot be judged (unknown or untested source)

Information credibility (1 to 6): This number evaluates how credible the information provided is, independent of the source. Each number indicates a different level of credibility:
1: Confirmed information
2: Probably true
3: Possibly true
4: Doubtful information
5: Improbable information
6: Cannot be judged (unverified or highly questionable information)

Information credibility (1 to 6): This number evaluates how credible the information provided is, independent of the source. Each number indicates a different level of credibility:
1: Confirmed information
2: Probably true
3: Possibly true
4: Doubtful information
5: Improbable information
6: Cannot be judged (unverified or highly questionable information)

Rating logic:

- Letter ratings:

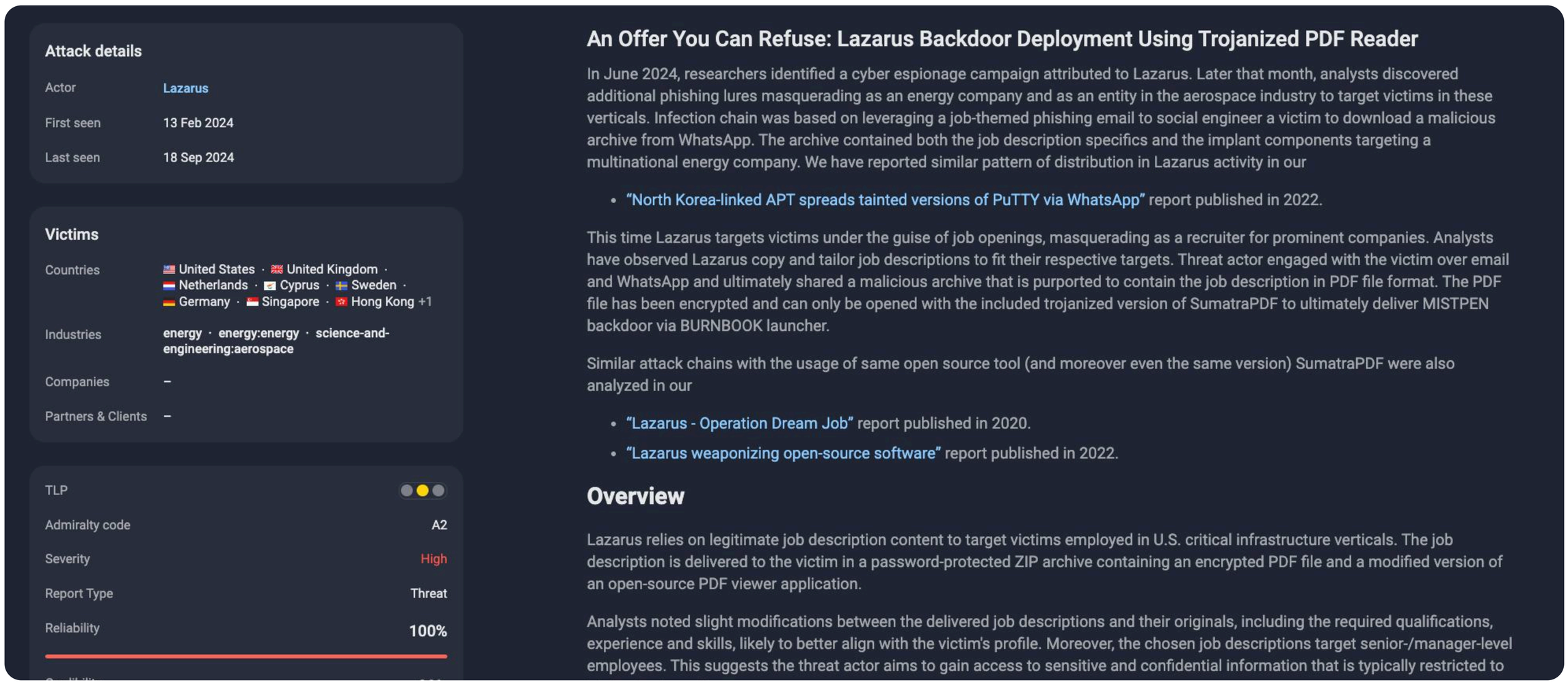
A	B	C	D	E	F
100%	80%	60%	40%	20%	0%

- Numeric ratings:

1	2	3	4	5	6
100%	80%	60%	40%	20%	0%

- **Example codes:**
  - **A1:** This means that the information comes from a completely reliable source (A) and is confirmed as highly credible (1). This combination is the most trustworthy.
  - **B2:** This suggests that the information is probably true and comes from a usually reliable source. It's generally trustworthy but may need further verification.
  - **C3:** This indicates that the information is possibly true and comes from a fairly reliable source. There's some uncertainty, so further investigation might be needed.
  - **D4:** This reflects doubtful information from a source that is not usually reliable. This combination should be treated with caution.
  - **E5:** This represents improbable information from an unreliable source. This is highly questionable and likely to be inaccurate.
  - **F6:** This combines an unknown or untested source (F) with unverified information (6). This is the least trustworthy combination and should be viewed skeptically.

Example:
Admiralty Code: A2



The threat in question is classified as **A2** because it involves a **targeted attack** by the group Lazarus using a Trojanized PDF reader. Although it's considered **high-risk** (with 80% credibility), it mainly affects specific sectors like **energy** and specific countries such as the **US, UK, and the Netherlands**. The use of **social engineering tactics** (like fake job offers) shows that it's a calculated attack rather than a widespread threat. That's why it's considered serious but not marked with the **highest urgency(5)**.

Image:
Group-IB Threat Intelligence showcasing Lazarus group's espionage campaign

5. Intelligence analysis
Once intelligence is graded, analysts use various techniques to extract insights. These include link analysis (graph-based mapping of connections between threat actors, infrastructure, and victims), trend analysis, temporal analysis, mapping to known taxonomies (such as MITRE ATT&CK), and other methods to improve structure and support automation.

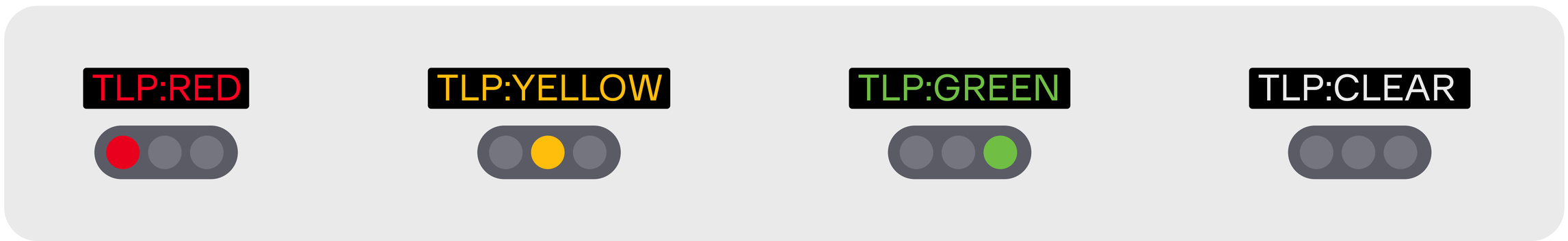
6. Sharing intelligence
The end goal of an effective CTI program is to have timely and accurate intelligence that can shield and pre-empt threats for your business. Communicating these insights into clear action items for stakeholders and tailoring the content and format to their strategic, operational, and tactical needs is a make-or-break factor for success.

When sharing information it is crucial to follow best practices, specifically Traffic Light Protocol (TLP).

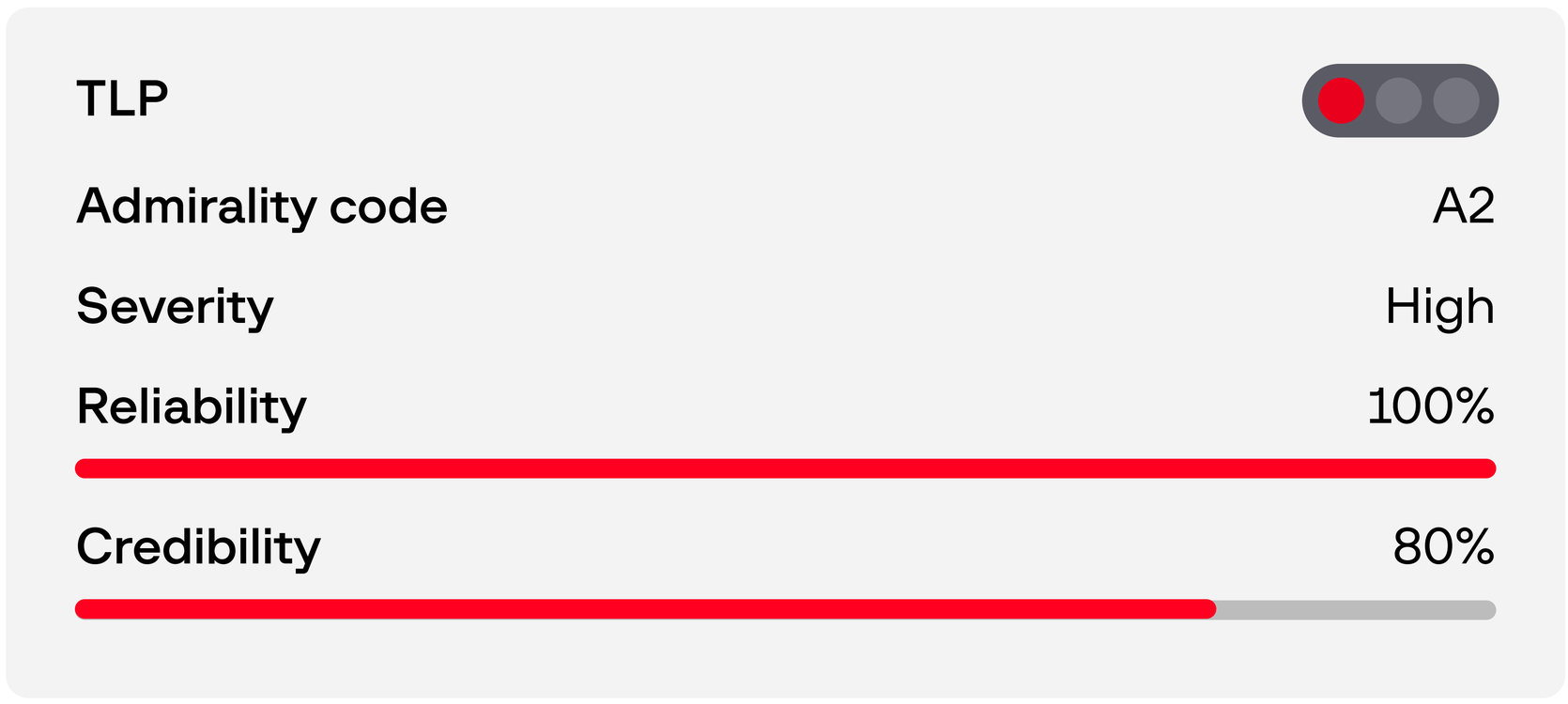
Overview: The Traffic Light Protocol (TLP) was created by the UK's National Infrastructure Security Coordination Centre (NISCC) in 1999. Its purpose is to facilitate the sharing of sensitive information in a controlled manner. TLP is a system of color-coded labels that indicate the sensitivity of information and the corresponding level of distribution control. The TLP system is widely used across various government, military sectors, including cybersecurity, to prevent unintended disclosure of sensitive data and to ensure that information is only shared with authorized parties.

Our platform used **TLP 2.0**, the latest version, which includes refined definitions and clearer guidelines to enhance information sharing while maintaining security.

How TLP Works in Group-IB Threat Intelligence Platform:
We implement the TLP framework using four distinct colors:



TLP:RED
Such information is highly sensitive and cannot be shared with anyone except the intended recipient. If the recipient is a company, all relevant members of the company should receive access to the report. Otherwise, it should not be shared. The red label is normally used for information that could have severe consequences if disclosed to anyone except the intended recipients.



TLP:AMBER

An amber label means that the information should be shared on a need-to-know basis within your organization. Broader dissemination is restricted to ensure controlled and limited sharing.

TLP	
Admiralty code	A1
Severity	Medium
Reliability	50%
Credibility	50%

TLP:GREEN

A green label means that the information can be shared with a broader, although still limited, audience. The information can be shared within your community but not beyond it.

TLP	
Admiralty code	C2
Severity	Medium
Reliability	60%
Credibility	70%

A clear label means that the information is not sensitive and can be shared freely with anyone.

For more information about TLP, visit the FIRST TLP official website

7. Feedback and optimization

This is the phase where the entire cycle is reviewed and continuous refinements are made to optimize the cycle. The goal is to improve the quality and relevance of the data, to maximize results, and to adapt to emerging threats and shifting priorities.

Feedback should be an agile model — continuous, actionable, and operationally integrated, influencing detection rules, intelligence sources, and the overall intelligence strategy.

Let's expand on specific methods for gathering feedback from stakeholders and using it to improve the CTI program.

Post-incident analysis: From the pre-incident phase to post-response, review the threat intelligence program and how effective it is in detecting, responding to, and eliminating threats.

Cyber intelligence simulations: Use real-life case scenarios (such as attack simulations and tabletop exercises) to test and analyze whether the artifact met the criteria defined by expert opinion.
Feedback communication channels: Use communication channels, forums, or internal threat intelligence interfaces to facilitate real-time feedback sharing between CTI teams and intelligence consumers.

Passive threat hunting: Perform retrospective threat-hunting exercises based on CTI inputs to determine whether intelligence has improved proactive detection capabilities.

Source effectiveness and metrics analysis: Rate the effectiveness of your current sources of information and whether they’re relevant, reliable, actionable, and timely (R-R-A-T). In addition, look at your CTI performance across three levels : foundational (directly impacting the prices) advanced, and leading (direct company impact such as cost vs. CTI vs. revenue saved).

> While orchestrating a CTI lifecycle program requires you to answer questions relating to the what and the why of defense building, another key question is who should be part of the process? Building the program requires a skilled, cross-functional team that can work together across various domains and drive the program forward. But who should be in the team, what should their role be, and where should they sit in the security and business architecture? Let’s have a look.

Strategic Insight for CISOs, Heads of Security

Forming a CTI cross-functional team and positioning it in the security stack

CTI is a collaborative effort, not a siloed one. It is therefore essential to structure and position your team in a way that makes them as effective as possible. Each team member owns a part of the CTI function, including people from departments such as SOC, Incident Response, Risk Management, and even Legal and Compliance.

The CTI team provides critical input to risk management and business processes — arguably its highest-value function at this stage. By integrating with the risk management (RM) framework, the team accomplishes the program's strategic, operational, and tactical goals, drives security decision-making, enhances corporate security, and channels intelligence into effective detection, prevention, and response workflows.

Such an alignment ensures that threat intelligence is not just a technical function but a key contributor to the company's growth, maturity, and long-term resilience.

To support the company's evolution, the CTI team must establish **clear internal structures**, including:

- **Documented analytical processes** to ensure consistency and efficiency
- **Defined request channels** for teams seeking support with intelligence
- **Centralized access to reports and findings** to streamline information sharing

The CTI team strengthens its organizational role by formalizing the above processes, ensuring that intelligence-driven decision-making is embedded at all levels.

To begin with, the Cyber Threat Intelligence (CTI) team usually includes two core roles:

- **CTI Team Lead (Manager):** Responsible for CTI Program development, establishing business requirements, PIR (Priority Intelligence Requirements), metrics and maturity, compliance, creating intelligence briefs for stakeholders

- **CTI Analyst:** Responsible for identifying cyber threats, data collection, in-depth research, managing feeds and tuning the TIP (Threat Intelligence Platform)

Depending on their budget, size, and cybersecurity maturity, many organizations may not have a dedicated CTI team. Instead, these responsibilities are often distributed across functions such as the SOC team, the Information Security department, or the Red Team.

As the CTI function matures, organizations may hire skilled experts for specialized roles such as:

- Malware Reverse Engineers
- Vulnerability Researchers
- Dark Web Analysts
- Threat Hunters
- Intelligence Correlation Specialists

The above roles allow for deeper analysis and a more focused intelligence aligned to specific threat domains or business priorities.

Operational Insight for SOC Managers, CTI Program Owners

Key functions of the CTI Team supported by Group-IB Threat Intelligence

Function	Description	Group-IB TI solutions
Data Collection	The CTI team collects data from various sources, including internal logs, external threat feeds, enterprise and open-source intelligence, and the dark web.	+ Databases of threats and malware + Collections of compromises + Feed of suspicious indicators
Analysis	Analysts interpret the collected data to identify potential threats, vulnerabilities, and patterns of malicious activity. Doing so helps to understand the threat landscape and generate new TI	+ Graph pivoting tool for investigation and research + Filtered feeds with detections based on Hunting Rules + Analyst reports (monthly, quarterly and yearly reports) + Malware detonation tool
Vulnerability intelligence	The team assesses software and system vulnerabilities to understand their potential impact on the organization's security	+ Vulnerabilities intelligence, including relationships on the dark web, X and GitHub and related attribution to threat actors
Reporting	The CTI team creates intelligence reports, often in a standardized format, and disseminates them to relevant stakeholders within the organization	+ Dashboard functionality + Reports and notifications

Security awareness	The CTI team may contribute to security awareness programs, educating employees about current threats and safe cybersecurity practices	+ Explanation guides in Help center
Threat feed management	For organizations that use threat intelligence feeds, the CTI team manages the acquisition, monitoring, and integration of such feeds	+ Native integrations + REST API + STIX/TAXII 2.0/2.1 + Custom tools, Postman collections, library and console export utility
Data Collection	The CTI team collects data from various sources, including internal logs, external threat feeds, enterprise and open-source intelligence, and the dark web.	+ Databases of threats and malware + Collections of compromises + Feed of suspicious indicators
Analysis	Analysts interpret the collected data to identify potential threats, vulnerabilities, and patterns of malicious activity. Doing so helps to understand the threat landscape and generate new TI	+ Graph pivoting tool for investigation and research + Filtered feeds with detections based on Hunting Rules + Analyst reports (monthly, quarterly and yearly reports) + Malware detonation tool

> Once you have a team in place that supports your CTI requirements, what about cross-functional communication and external/internal intelligence sharing? This section will help you get to grips with structuring your CTI team, enabling collaboration, and delivering actionable intelligence across the entire organization.

For CTI Analysts, Intel Analysts

Writing intelligence reports and sharing intelligence

[Free template download]

Effective reporting is crucial if you want to demonstrate the successful outcome of your CTI program and that it meets the pre-defined objectives. Intelligence reports contain key information and context for employees so that they are informed about the latest threats targeting their industry and understand active security gaps all the while helping stakeholders make better security investments and decisions.

Threat intelligence reports may vary depending on stakeholders' requirements — namely whether to share intelligence internally (within the organization) or externally (within the broader community). For consistency and ease, reporting should be standardized by frequency, format, and key metrics eral layers of data enrichment, correlation, and automation — such as threat intelligence platforms (TIPs), SIEMs, and SOAR systems — to ensure that the information is filtered and validated. We'll expand on this in the sections below.

A typical intelligence report includes:

- **Source and information reliability:** Admiralty Scale score [A–F or 1–6]
- **Sensitivity label:** TLP designation (TLP:RED, AMBER, GREEN, or CLEAR)

Report structure:

- **Executive summary:** A high-level overview of key findings and implications
- **Key threat indicators:** Indicators of Compromise (IOCs), behaviors, and anomalies
- **Threat actor analysis:** Profiles, motivations, and tactics of threat actors
- **Vulnerability insights:** Relevant CVEs and exploitable weaknesses
- **Incident analysis:** Context or case studies involving the threat in action
- **Recommendations:** Actionable steps to mitigate and prevent similar incidents

Supporting materials:

- IOC details (file hashes, URLs, IPs)
- References (reports, advisories, articles)
- Visuals (charts, graphs, diagrams)

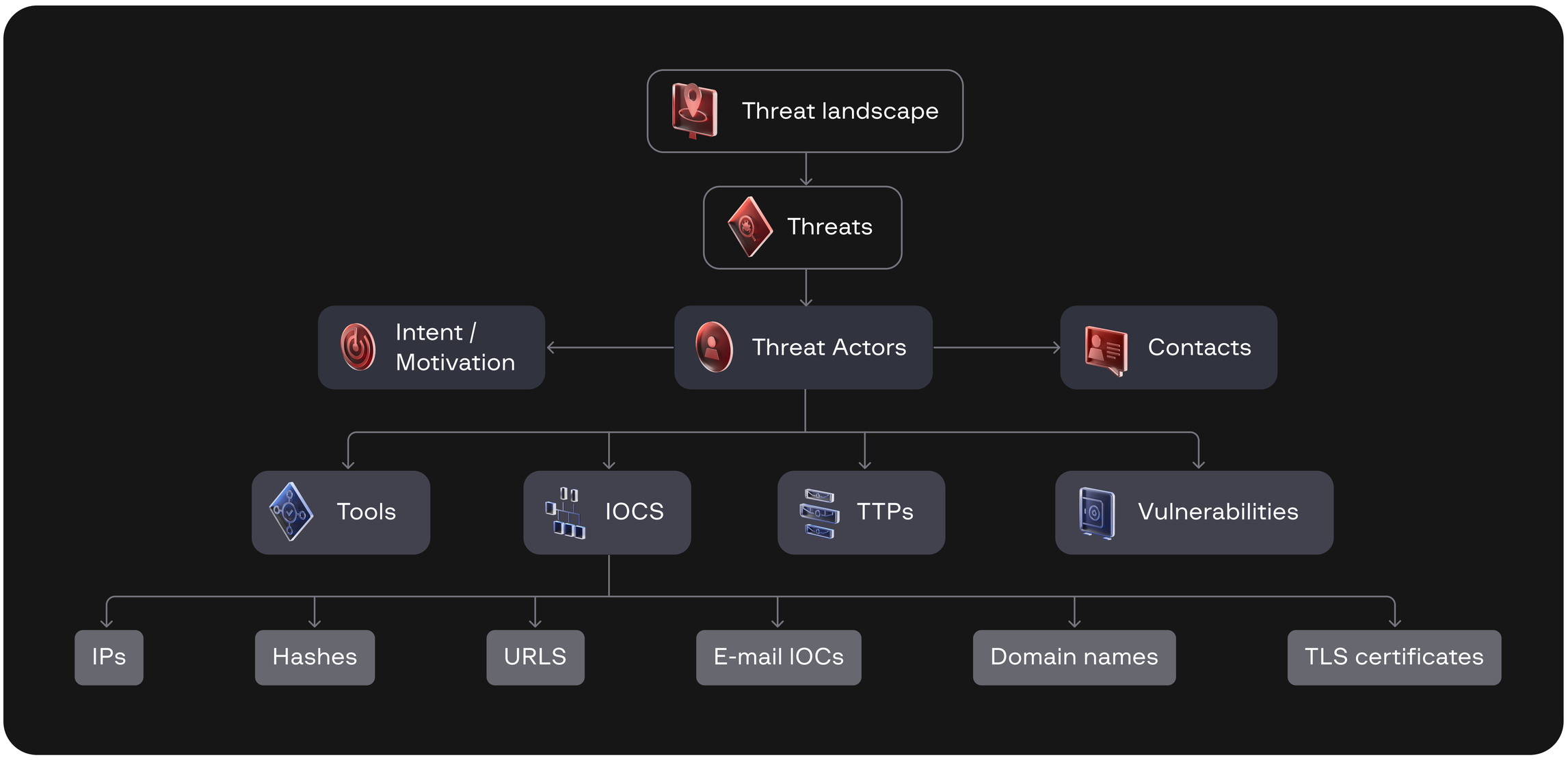
You can download the basic template to manage your reporting needs and pivot it based on stakeholders, organizational information requirements, current program maturity, etc.

> Now that the lifecycle is in place, your team roles are defined, and reporting workflows are established, the next step is translating intelligence into real-world defensive strategies. This means shaping threat profiles, building MITRE heatmaps, identifying vulnerabilities relevant to your business environment, and prioritizing what matters most to your infrastructure and region.

For CTI Analysts, Intel Analysts

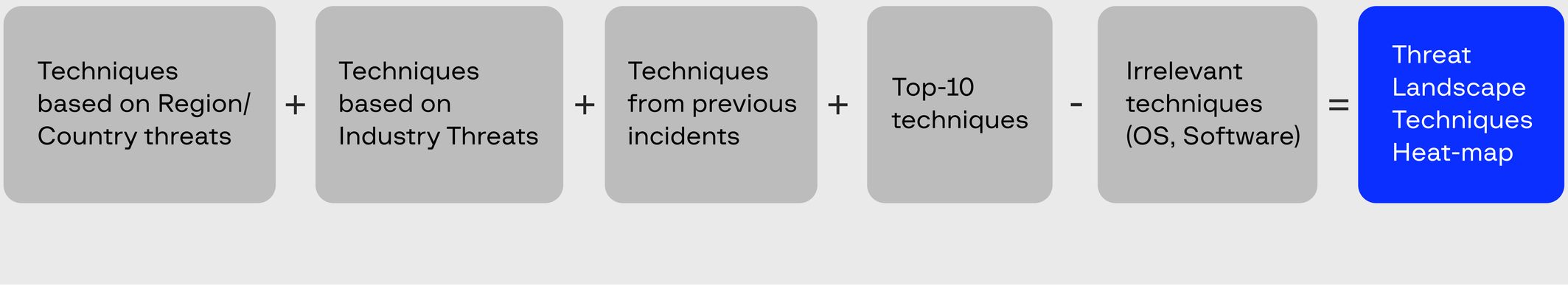
CTI tailored application: Threat landscape heat mapping

The threat landscape is a combination of relevant threats and threat actors (based on industry, region, and partners) divided into TTPs (Tactics, Techniques, and Procedures) used by threat actors (such as malware and living-off-the-land tools), IOCs, intent, motivation, contact details (such as crypto wallet addresses, usernames on forums, and email addresses), as well as the vulnerabilities involved in their intrusions.



The threat landscape is specific to the platform (Windows, Linux, Android, etc.) and infrastructure type (Enterprise/ICS/Mobile, in line with the terminology of MITRE ATT&CK).

You can build a heat map of threat landscape techniques by combining all the tactics, techniques, and procedures relevant to your company. Doing so helps teams to prioritize detection and mitigation decisions.



You should ensure that your investigation covers **techniques, CVEs, and threat actors relevant to your industry**, mapping them across **MITRE ATT&CK** to strengthen your **prevention and detection capabilities**. With many new techniques and sub-techniques evolving all the time and heat maps continuously updating, it is critical to stay aligned with the latest intelligence.

For CTI Analysts, Intel Analysts

Build threat profiles for your business (attached template)

Once intelligence is collected, analyzed, and contextualized, threat profiling refines the information further by identifying key threat actors, motivations, and attack scenarios relevant to your organization. As discussed in previous sections, the attack kill chain expands on the profile to provide the framework for integrating assets (proper categorization, attribute mentions), threat actors, and actions.

Attribute	Details
Threat Actor ID	[TA.ID] — [Threat Actor Name]
Description	[Summary of the actor’s background and typical activities]
Relationship	[Internal/External]
Region of Operation	[Geographic focus]
Motive	[Espionage, Financial Gain, Sabotage, etc.]
Intent	[Deliberate, Opportunistic, Competitive]
Capability	[Skill level, funding, persistence, stealth, and intensity]
Objective	[Credentials, Trade Secrets, System Data, etc.]

Thread Campain: [TC.ID] — [Thread Campain Name]

Thread Scenario: [TS.ID] — [Thread Scenario Name]

Attribute	Details
Asset ID	[CA.ID] — [Asset Name]
Thread Actor ID	[TA.ID] — [Threat Actor Name]
Region of Operation	[Geographic focus of the threat actor]
Motivation	[Espionage, Financial Gain, Sabotage, etc.]
Objective	[Define the main attack goal]

Attack Phases and Techniques

Phase	Description	Mitre Tactic & Technique
Reconnaissance	Describe information gathering methods	Tactic: Reconnaissance Technique: Example
Weaponization	Describe how the attack is prepared	Tactic: Resource Development Technique: Example
Delivery	Describe how the malicious payload reaches the target	Tactic: Initial Access Technique: Example
Exploitation	Describe how the vulnerability is exploited	Tactic: Execution Technique: Example
Persistence	Describe how attackers maintain access	Tactic: Persistence Technique: Example
Privilege Escalation	Describe how attackers gain higher-level access	Tactic: Privilege Escalation Technique: Example
Defense Evasion	Describe methods used to bypass security controls	Tactic: Defense Evasion Technique: Example
Credential Access	Describe how credentials are stolen	Tactic: Credential Access Technique: Example
Discovery	Describe how attackers explore the network	Tactic: Discovery Technique: Example
Lateral Movement	Describe how attackers spread across systems	Tactic: Lateral Movement Technique: Example
Exfiltration	Describe how data is stolen	Tactic: Exfiltration Technique: Example

IOCs

- Mention any related IOCs

Recommendations on detection and response

- Specific guidance for security teams

Historical references

- Past campaigns: [If the attack is linked to previous incidents]
- Similar threat actors: [Other groups using similar techniques]

Based on threat profiles, which clearly show how attacks are launched and what defense strategies should be implemented to mitigate the risk, incident response teams can analyze and contextualize related threats and also assess the proclivity of facing similar attacks in the future — helping prioritize defenses. Automating the collection and correlation of threat data (supported by Group-IB Threat Intelligence) to detect suspicious patterns in network activity leads to prompt and real-time detection. Automation also helps predefine response actions based on threat profiles to enable swift containment and mitigation.

> Now that you have a clear view of how intelligence is collected, enriched, shared, and utilized across teams and security components, let’s see how we can put it all into action.

02
Section

Practical application of CTI and Group-IB Threat Intelligence Platform

Strategic Insight for CISOs, Heads of Security

Forming a CTI cross-functional team and positioning it in the security stack

Real-time monitoring and visibility: Constantly monitoring the attack surface and network-wide visibility into the risks emerging in an organization's environment (or multiple environments) helps businesses act ahead and uncover potential threats before they can cause harm.

Data from various sources (such as dark web marketplaces, underground forums, and communities) can give companies an exclusive view of how vulnerabilities are exploited, if at all. Illegal mentions, such as personally identifiable information (PII) and intellectual property (IP), digital assets, and credentials, are often traded, which makes that visibility crucial.

01 A typical use case:

A financial services provider has been experiencing account takeover (ATO) attempts and fraudulent transactions. Upon investigation, it is discovered that several phishing websites are impersonating the bank's online portal and stealing customer credentials.

- CTI monitors dark web marketplaces, social media channels, and underground forums for leaked credentials linked to the company's users.
- On the dark web, CTI analysts track discussions related to stolen credentials, domain spoofing, and phishing kits.
- CTI tools continuously scan for newly registered illicit domains mimicking the bank's official websites.
- IP addresses used by phishing sites are cross-checked against known attacker infrastructure.
- Phishing domains distributed via emails, social media, and SMS are detected, reported, and included in the takedown workflow.
- To prevent ATO fraud, accounts accessed from unusual geographical locations, used for frequent high-value withdrawals, or showing mismatched device fingerprinting are reviewed or closed.

Situational awareness and context:	The region, geopolitics, and industries relevant to the business in question must be analyzed to understand its threat landscape. Threat intelligence derived from such an analysis helps create threat profiles by identifying trends, patterns, and potential IoCs or TTPs. The enhanced situational awareness is crucial for anticipating potential attack vectors and allows for proactive defense.

02 A typical use case:

A financial institution wants to expand its portfolio and enter an emerging but high-risk market.

With the help of specific intelligence, the business builds an industry-specific threat landscape that focuses on threats specifically targeting financial institutions, including previously observed attack vectors in the banking sector (e.g., phishing and stolen credentials, supply chain risks, card skimming and ATM threats).

The CTI team identifies past attack patterns, regional TTPs, and leaked credentials, helping to create a risk profile of threats most likely to impact the business.

This helps the financial institution to pivot its expansion and penetration strategy by making strategic decisions to:

- Map the attack surface to assess exposure
- Limit high-risk services where necessary
- Build TI feeds into their XDR and SIEM to block and detect tactics used in the region

Direct impact:	A more risk-informed, targeted and intelligence-driven approach to secure business expansion while staying ahead of emerging threats.
Proactive defenses:	Understanding the most relevant threat actors and threats to your business and industry allows for active, proactive defense. By giving context to security events, showing how they fit into the tactics, techniques, and procedures used by threat actors, examining the timeline of a threat actor's different campaigns, the TTPs they use, and changes in their capabilities — then mapping all this information against the MITRE ATT&CK framework — organizations can create threat profiles that they can defend against. Such insights can then be provided to the Blue and Red teams for simulation, emulation, and further security testing.

03

A typical use case:

A manufacturing firm notices unusual administrative account activity and file encryption attempts within its operational technology (OT) network.

Initial investigations and forensics suggest behavior aligned with the Qilin ransomware group, a financially motivated threat actor recently uncovered by Group-IB.

To move beyond reactive response, the company's Cyber Threat Intelligence (CTI) team analyzes Qilin's tactics, techniques, and procedures (TTPs).

With the help of red teaming, the firm simulates a ransomware deployment in a controlled environment to identify and patch vulnerabilities that could be exploited.

The company then proactively strengthens its defenses by enhancing detection rules to identify Qilin ransomware payload indicators, blocking threat actor-linked IPs, domains, and hashes, finding critical risks within the network before adversaries can exploit them, triggering the incident response playbook, and more.

Improved security posture:

By regularly collecting and analyzing data on potential threats, businesses can improve their security posture and better protect themselves from cyberattacks. Doing so may involve identifying and mitigating vulnerabilities, improving incident response processes, and implementing stronger security controls.

Simulation, emulation, and other offensive operations:

CTI can build your defenses and improve how you detect, respond, and recover from cyber threats by helping you replicate attackers' behavior and their methods. Copying the exact TTPs with an extra layer of visibility into the lower level of data required for emulation activities creates a realistic interpretation and an extra layer of evaluation of your own defenses. Both these endeavors are essential for red teaming, vulnerability assessment, and other intrusive activities and they will help you understand how resilient you are in the face of cyber threats.

Full-scale cyberattack simulations help answer the following questions: **How effectively do the organization's existing security measures protect important data? Is the organization's alert and monitoring system configured correctly? To what extent is the company's security team prepared to counter attacks conducted by highly skilled hackers? What possibilities become available to attackers within the infrastructure if users or their devices are compromised?**

04

A typical use case:

Group-IB performed a red team engagement for a group of companies (in the manufacturing industry). The goal was to gain administrative access to the Active Directory domain controller at the company's headquarters.

For context, the customer uses multi-factor authentication (smart cards) for all types of access at the headquarters, including remote and external services.

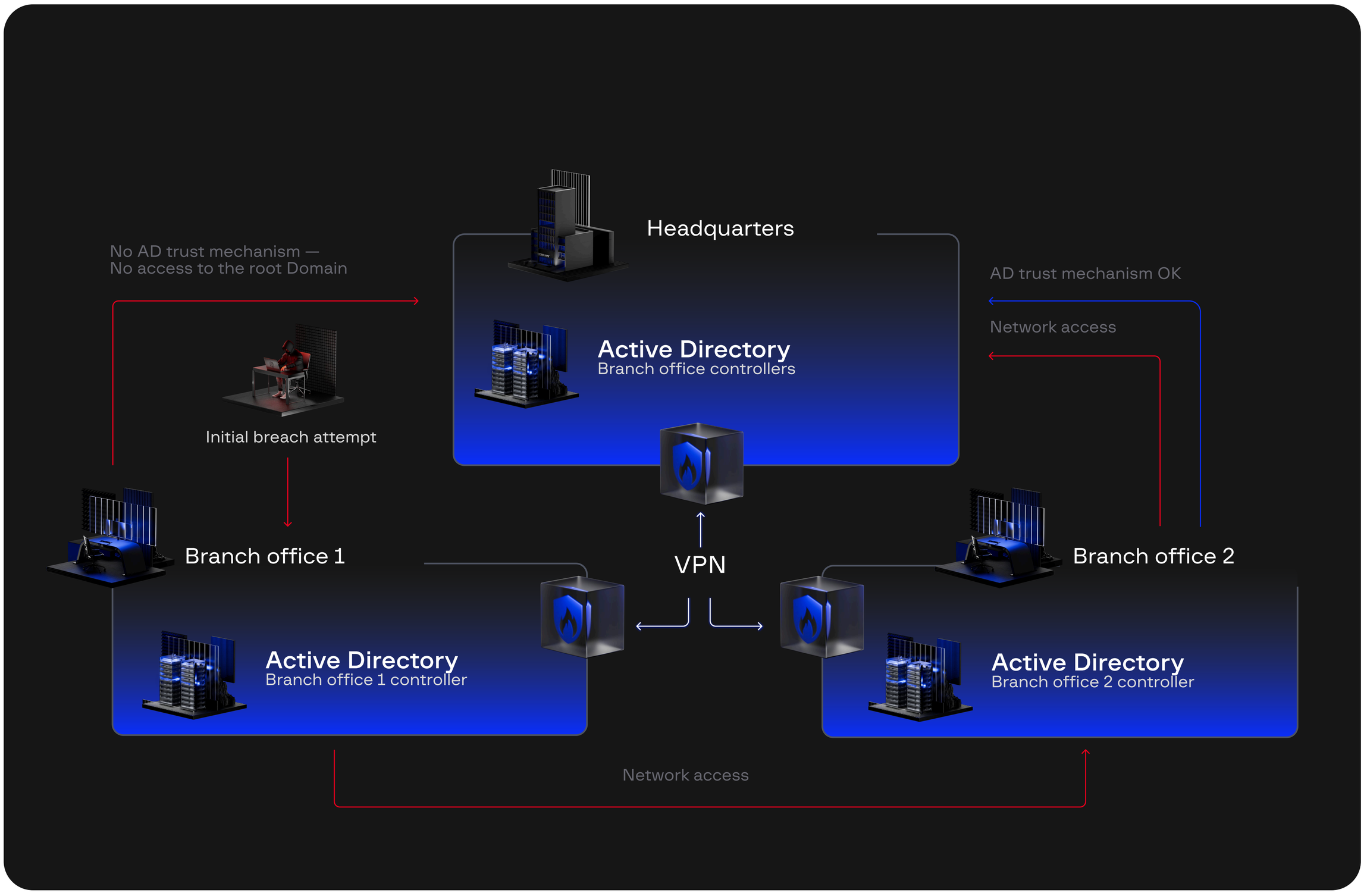
Group-IB's reconnaissance revealed a poorly protected subsidiary with weak security controls. The Red Team compromised branch1.domain.com, discovering a site-to-site full-mesh VPN linking multiple branches.

They extended the "attack" to branch2.domain.com, where domain admin privileges were obtained due to weak trust mechanisms.

Using a Golden Ticket Kerberos attack, the Red team bypassed smart card protection and escalated privileges to headquarters' Active Directory.

The operation helped the company identify its cybersecurity strengths and weaknesses and create a plan for improvement.

Gaining access to ActiveDirectory



Threat response and its three stages:

When integrated early into an intelligence program, CTI helps teams detect and prevent threats before a breach can occur.

Doing so enables:

1. Prevention: Identifying and mitigating threats before they materialize.
2. Early detection and response: Detecting and responding before a threat can cause material impact requires CTI visibility and swift action to combat the threat actor.
3. Incident response: During active incidents, Cyber Threat Intelligence (CTI) helps teams understand the scope and nature of the attack, including the TTPs (Tactics, Techniques, and Procedures) used. It also aids response efforts to effectively contain and neutralize the threat.

Threat hunting:

Threat intelligence serves as a foundation for threat hunting by providing context on known threats all the while enabling proactive discovery of unknown threats. CTI helps react to incidents and address “known known” (well-understood and documented) threats in the wild, but what about the “unknown unknowns” (completely new and undiscovered threats)? This is where threat hunting proves indispensable.

Analysts actively search for undocumented threats by looking for anomalies such as misused permissions, configuration errors, data leaks, or emerging attack patterns that evade traditional alerts. Their expertise in adversary tactics and in-depth understanding of the environment allows them to spot subtle signs of compromise that automated tools are likely to overlook.

Threat hunters don’t just search for risks on the surface of internal infrastructure — they go deeper to uncover hidden attacker infrastructure, map out the kill chain, and connect the dots for effective attack correlation and attribution.

---

05 A typical use case:

CTI analysts scrutinize underground forums, marketplaces, and social media community groups, using targeted search queries and keywords to uncover discussions about a high-impact exploit.

Their findings indicate a potential threat to vulnerable web servers, malware deployment, and unauthorized access to critical infrastructure.

The threat hunting process begins by defining the hunting hypothesis, focusing on the potential exploit and identifying the tactics, techniques, and procedures (TTPs) linked to it.

Threat intelligence validation and dark web monitoring:

- Correlate findings across dark web sources, social media, and security research reports
- Determine whether the exploit is a work in progress (WIP), in testing, or already being used in the wild
- Assess the scope of compromise and its exploitability

Doing the above will help analysts take mitigation actions such as analyzing the exploit, applying patches and security updates, developing custom detection rules (YARA, Sigma) for SOC teams, sharing intelligence with industry partners, and issuing a collaborative takedown for listings related to exploits.

Risk assessment:

Each organization has an asset inventory, the security priority of which should be scored based on how critical the information or asset is. Every organization continually assesses its network (data and communication devices) for risks in order to ensure that threats are averted proactively.

By identifying and evaluating risks to each asset (software, hardware, data, digital assets), we can prioritize security measures and assess the impact caused by a security property being violated. Doing so helps organizations avoid making scanty or uninformed security decisions. TI enhances risk assessment by providing real-time insights into threats, helping organizations make data-driven decisions instead of relying on universal risk models.

Post-incident analysis:

Cyber Threat Intelligence (CTI) enhances defense by learning from past incidents. The process improves detection and response strategies, prevents similar attacks, and strengthens the overall security posture of a business.
Intelligence gathered after an incident becomes a critical layer of defense against potential future attack vectors. It also helps determine whether the threat has fully subsided or is lingering. Insights gathered during incident response are integrated into security systems, including new Indicators of Compromise (IOCs), target information, and TTPs. The integration bolsters defenses by securing systems against similar or evolving threats.

06 A typical use case:

In January 2022, Group-IB supported an INTERPOL-led operation against TMT (also known as SilverTerrier), a prolific BEC cybercrime network tracked since 2019.
Group-IB's Cyber Investigations Team analyzed past BEC incidents and examined malware samples, phishing tactics, and financial patterns to build a detailed threat profile.
The team identified malicious IPs, email domains, and key TTPs, including spear-phishing and remote access Trojans.
Security systems were strengthened with newly identified IOCs, which led to faster threat detection, improved response strategies, and enhanced intelligence-sharing across the cybersecurity community.

Prioritization of resources:

The sheer volume of available information when ingesting CTI can lead to analysis paralysis. Aggregating data helps teams identify the most relevant TTPs. With intelligence-informed security decisions, businesses can focus their resources on the threats that are most relevant to them rather than investing in a one-size-fits-all approach to threat intelligence.
CTI reduces the cost and impact of cyber risks by pre-empting attacks or providing a complete understanding of an attack's scope. This enables organizations to minimize negative consequences and promptly implement defensive measures.

07

A typical use case:

To help with making informed decisions, a tech company expanding to LATAM integrates Cyber Threat Intelligence (CTI) into its risk management, expansion, and investment strategy.

CTI reveals regulatory risks and compliance gaps that could lead to penalties as well as high threat actor activity and ongoing cyber campaigns targeting companies in the region.

To mitigate risks, the company takes the following steps:

- Adopts all relevant regional regulations to ensure compliance
- Establishes fraud prevention and digital risk protection after CTI reports indicate an increase in banking malware attacks and brand impersonation for phishing purposes
- Proactively detects and mitigates fraud and impersonation attempts before they can impact business operations
- Builds a dynamic risk profile based on current and emerging threats specific to its industry
- Maps vulnerability intelligence (CVEs, zero-days) to regional APT activity to close security gaps before they can be exploited

CTI operational execution: Domains, functions and requirements

Irrespective of your CTI capability and maturity stage, whether building one or refining a pre-established program, the framework must align intelligence outputs with genuine business needs. This means focusing on everything from strategic executive buy-in to tactical threat detection and operational use cases across your SOC, IR, MSSPs, vulnerability management, and C-suite.

The infographic below outlines the components of an effective CTI framework. It maps different functions as well as their domain, purpose, and security goals and it explains how to collect, process, analyze, and act on threat intelligence across each function.

Mapping out cybersecurity functions, purpose

Cybersecurity Function: Third-party Risk Management
Domain Purpose: To Assess, Monitor and Contain Risks From Third-Party Risks (Suppliers, Vendors, etc)

Identify Third-party risks
OSINT lookup, Breach Intelligence for Vendor Compromises
Track supply chain threats
Vendor Mentions on Underground Forums, or For Breaches
Attack Vectors and Vulnerabilities in Vendor Tech Stack
Assign Risk Level For Each Vendor

Incident Response In Third-party Risks
IOC feeds into SIEM/XDR indicating third-party compromises
Playbook for Containment and Response
Adversary TTP-Based Hunting for Vendor Compromises

Cybersecurity Function: Workforce & Resource Management
Domain Purpose: Train and account cybersecurity team for evolving threats

Resource and Team Management
Skills & Competencies Tracking
Intelligence-Led Training
Technology & Tooling (SIEM, SOAR, TIPs)
Collection, Processing & Analysis Capabilities
Collaboration, Knowledge-Sharing & Coordination Across Teams

Threat Feed Management
Documented analytical processes for consistency and efficiency
Defined request channels for intelligence support
Centralized access to reports and findings

Cybersecurity Function: Vulnerability Management
Domain Purpose: Identify and Contain Existing & Emerging Vulnerabilities That Are High-Risk

Identification & Patch Management
Total Vulnerabilities Detected / Total Assets Scanned
% Vulnerability Assessed Criticality and Patched
Prioritize high-risk vulnerabilities Based on Exploitability and Business Impact

Active Monitoring & Remediation
Attack Surface Mapping for Exposed Assets, Internet-Facing Services, and Misconfigurations
Recommended Actions, Workflows for Remediation on Actively Exploited Vulnerabilities

Cybersecurity Function: Risk Profile Building
Domain Purpose: Keeping Pace with Security Risks Relevant to An Organization's Environment

Risk Identification
Historical Attack Data
Industry/Region-specific Risks
Tracking Adversaries and TTPs (MITRE ATT&CK mapping), Infrastructure

Risk Scoring & Prioritization
Based on critical asset targeted, impact, frequency, and actor sophistication
Attack Surface Monitoring for Exposed/Leaked Data, Vulnerable Endpoints, Assets

Proactive Containment
Attack simulations and Red Teaming relevant with risk profile
Custom Detection Rules
Automated Responses Based on Risk Profile

Cybersecurity Function: Threat Validation
Domain Purpose: Confirm the Severity, and Impact of Threats Through Contextual Intelligence

Threat Filtering & Confirmation
Check indicators (IPs, domains, hashes, signatures) are active, malicious, and relevant before blocking
Check Adversary TTPs being actively used in attacks
Distinguish False Negatives & False Positives

Update Detection Logic & Risk Models
Based On New Validation Insights

Cybersecurity Function: Feedback & Intelligence Management
Domain Purpose: Analyze & Optimize CTI performance through continuous feedback

PIRs Requested vs Effectiveness
Standard Metrics
Feedback completed for standard PIRs
Number of internal, new incidents discovered and worked on
Number of IOCs observed
Number of IOCs added to SOC
Mean Time to Detect (MTTD) & Mean Time to Respond (MTTR)

Adaptive Models & ML-based Threat Pattern Recognition
Threat Intelligence Efficacy Metrics (False Positives, False Negatives)
Maturity-based progression metrics
Detection Rule Refinement (SOC Feedback Loops)
TTPs emulated vs. ATT&CK

Iterative Intelligence Optimization
Risk-Based Prioritization Updates
Evolving Threat Landscape Adaptation
Feedback from Incident Response Teams, SOC analysts, and threat hunters

Cybersecurity Function: Intelligence Analysis
Domain Purpose: Contextualize, and Standardize Raw Data Into Actionable Intelligence For Risk Management

Ingestion, Standardization & Correlation
IOC Normalization (JSON, STIX, CSV)
Duplicate Removal, Contextualization
Threat Correlation & Attribution

Threat Intelligence Enrichment
Risk Scoring
Context to raw IOCs to improve detection accuracy
WHOIS, Passive DNS, VirusTotal, OSINT Lookups
MITRE ATT&CK mapping
Identifying TTPs & Behavioral Indicators

Cybersecurity Function: Intelligence-Sharing
Domain Purpose: Constantly Sharing Adversary Knowledge Within Community For Collective Retaliation

Internal Intelligence Sharing
Integration with security tools for automated intelligence sharing
Updates across SOC, IR, Risk, and Compliance teams
Structured intelligence reporting for decision-makers

External Intelligence Sharing
Information-sharing with vendors and community partners
Public-private partnerships
Automated intelligence exchange (STIX/TAXII, TLP-tagging)
Collaboration with industry and law enforcement for investigations and defense

Formats
Reports, Dashboards, Alerts, API Feeds
Open-Source Contributions
Threat Intelligence Platforms (TIPs) for Storing, Managing, and Distributing CTI

Cybersecurity Function: Risk Management
Domain Purpose: Identify, Assess and Eliminate Cyber Risks Effectively

Updated intelligence on emerging threats
Adversary tactics, defined vulnerabilities for risk-based decisions

Cybersecurity Function: Integrations
Domain Purpose: Secure, Scalable Integrations For CTI Flow Across Tools, Continuous Optimization and Easy Intelligence-Sharing

Seamless Intelligence-Sharing and Actioning
APIs & Standardized Formats → CTI feeds integrate with SIEM, XDR, EDR, SOAR for automated action.
YARA & Sigma Rules → Enable scalable malware & TTP detection.
STIX/TAXII & API-Supported Intelligence Sharing → Ensures structured threat exchange across platforms.
Contextualized Feeds & Enriched Threat Alerts → Based on adversarial TTPs & real-time IOCs.
IOCs in Detection Workflows → Used for threat validation & automated response.

Cyber Threat Intelligence (CTI) Framework

Cybersecurity Function: Intelligence Requirements & Direction
Domain Purpose: Defining Stakeholder Involvement, Priorities & Objectives

Intelligence Program Management
Governance & Oversight
Strategic Alignment with Business & Risk Objectives
Continuous Improvement & Evolution of CTI Capabilities
Development of security policies, procedures, and long-term cybersecurity strategies based on threat intelligence.

People, Process and Technology
Intelligence Collection, Processing & Tools
Source Reference and Viability
People Skills, competency and Availability
Intelligence Collection, Analysis, Automation, Orchestration, Dissemination, Feedback & Optimization Processes

Stakeholder Engagement
Identify stakeholders and involvement (SOC, IR teams, CISO, MSSPs)
Enlist intelligence priorities and objectives
Build communication & feedback mechanisms

Intelligence Requirement Development
Prioritized Intelligence Requirements (PIRs)
Gap Analysis & decision support alignment

Cybersecurity Function: Intelligence Collection
Domain Purpose: Comprehensive Coverage & Analysis of Sources To Derive CTI for Security Decision-Making

Threat Data Sources
OSINT, Dark Web, Commercial Feeds, Web Scraping
API Integrations (STIX/TAXII), Vendor CTI feeds
Log Collection & Sensor Data (EDR, XDR, SIEM)

Collection Management
Source Validation & Prioritization
Automated Data Ingestion
Internal vs External Data Collation

Cybersecurity Function: Automation, Incident Response & Operationalization
Domain Purpose: Enhance Threat Detection, Streamline CTI Workflows, And Operationalize Intelligence

Detection & Threat Correlation
Analyzed intelligence into rules for security tools (YARA, Sigma rules, custom detection logic)
Threat Hunting Queries (e.g., Splunk, Elastic, Microsoft Sentinel)
Anomaly Detection (ML-based)
IOC to TTP Mapping for Threat Actor Profiling

Incident Response Integration
Intelligence-driven incident prioritization
Live enrichment of incidents using CTI feeds (IOC/TTP context)
Root cause analysis & post-incident review

SOC & Integration
SIEM, SOAR, XDR Automations
Incident Response Playbooks (Containment, Remediation)
Ticketing & Escalation Mechanisms

Automated Threat Response
Playbook Execution & Response Triggers
Automated Threat Containment & Remediation
AI-driven Adaptive Defenses

Cybersecurity Function: Fraud Detection and Prevention
Domain Purpose: Identification of Fraud Indicators to Enable Proactive Protection & Deconstructions Of Fraud Schemes and Tactics

Fraud Monitoring
Leaked payment data, PII, and financial credentials being sold
Track Fraud networks for Account TakeOvers (ATO), identity fraud, and Mule Networks
Identify Fraudsters TTs, scam schemes
Threat Actor TTP Mapping to MITRE ATT&CK for Emerging Fraud Prediction
Identify Fraud Patterns Using ML + CTI for Pre-Fraud Indicators to Stop Attacks

Fraud Analysis
Enrich anti-fraud systems with real-time indicators
(IP addresses, device fingerprints, and compromised identities)
Geolocation and Behavioural Indicators for Anomaly Detection
Based on Location, Account Activity, Login Behaviour, Device Usage.

Cybersecurity Function: Threat Hunting
Domain Purpose: Actively Hunting For Risks Within Perimeter For Improved Security System Defenses

IOC-Based Hunting for Threats in the Wild Using Predefined Rules, Signatures, and Correlation of Log Data Across Network
Network and Endpoint Anomaly Detection For New Threats
TTP-Based Hunting (MITRE ATT&CK) for Attack Maneuvers, and Not Static Indicators
Hypothesis-Based Hunting for Adversary Tactics, and Potential Infiltration

Threat Hunting Automation
Automating Hunting Queries and IOC Enrichment.
YARA & Sigma Rules for Malware and Attacker Behaviors at Scale.
Enriching Hunt Results with Real-time CTI to Validate Potential Threats.

Active Monitoring
Mentions of your organization, credentials, or breached data.

Operational Insight for Detection Engineers, IR Leads

Integrating threat intelligence in security workflows

The success of a CTI program depends on continuously gathering up-to-date technical and non-technical insights relating to detecting and preventing attacks. While defensive infrastructure regularly ingests base-level indicators such as IP addresses, domains, and hash values, the volume at which this needs to be constantly ingested and updated means that manual processing is impossible. Moreover, such raw threat data lacks context unless it is enriched with details about threat profiles.

Without context, security teams may struggle to prioritize threats effectively. Automation therefore plays an important role in creating a constant stream of tactical and operational intelligence (about baseline-level indicators that can be automated), leaving security teams to focus on what really matters: instead of manually looking at threats and managing them, they can concentrate on strategic intelligence (based on TTP-level and above indicators), geopolitical and situational awareness, and threat-hunting and pivoting activities — all to inform corporate security decisions and ensure better knowledge and risk management.

Cyber threat intelligence (CTI) ingestion, operation, and optimization workflow

Technical execution of intelligence integration into security operations: This workflow is a direct application of the [Group-IB CTI Framework Support (Page 58].
Each phase aligns with tools like SIEM, SOAR, EDR, and TIP — enabling real-time enrichment, response, and feedback loops.

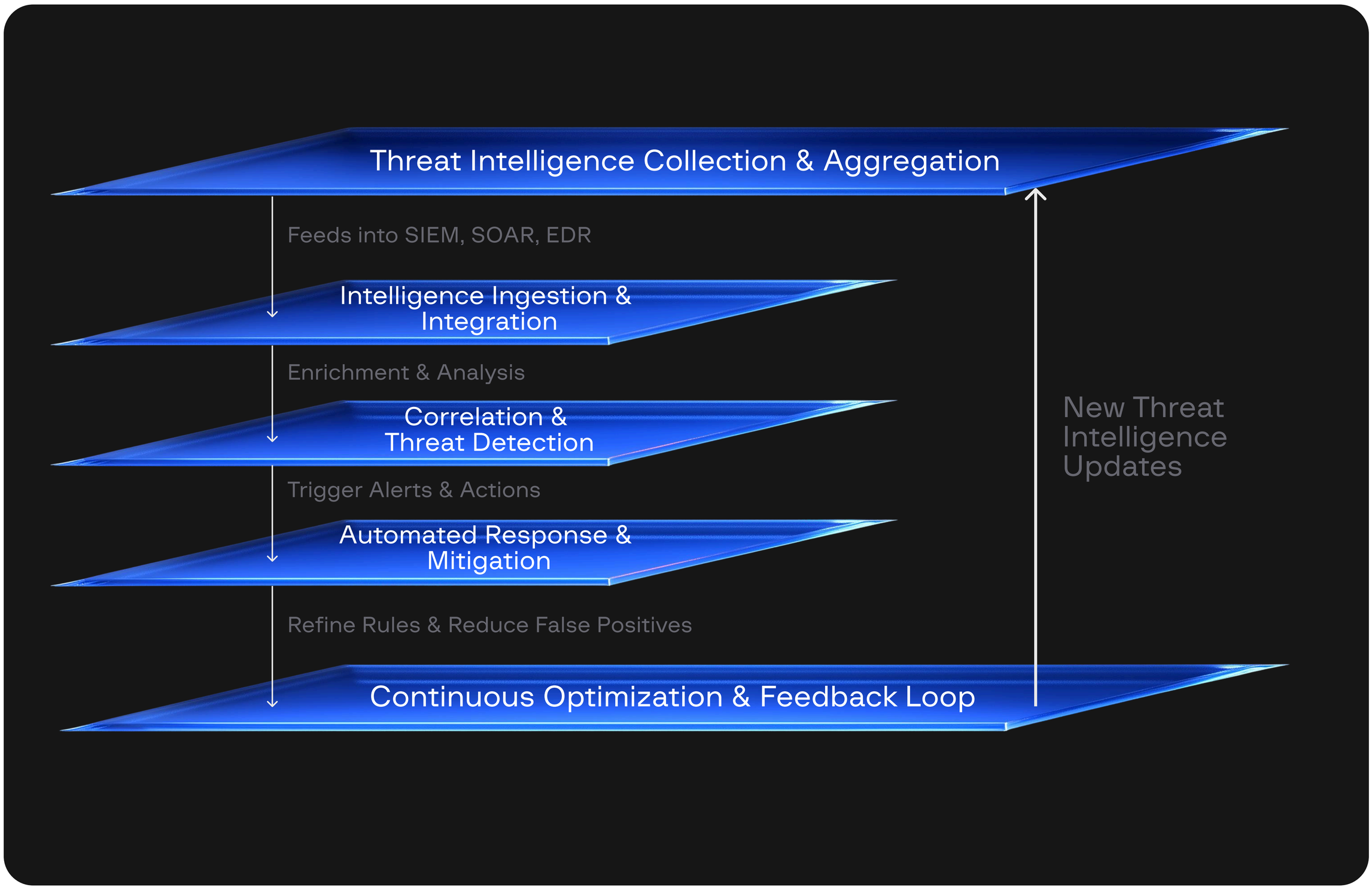


Image:
CTI ingestion, operation, optimization workflow.

1. Collection of threat intelligence

- Sources: OSINT feeds, HUMINT, SIGINT, mainstream sources, dark web, customer alerts, commercial CTI providers, malware sandboxes
- Automation: API ingestion, STIX/TAXII connectors, web scraping

2. Processing and enrichment of threat intelligence

Providing enriched data with normalized outputs, allowing for contextualization.

- Logs are ingested and normalized into structured formats (JSON, STIX, CSV)
- Duplicates are removed, feeds are correlated, and alerts are created for suspicious events
- Enrichment: Enriching IOCs, risk scoring, WHOIS data lookups, MITRE ATT&CK mapping

How a misconfigured workflow opens up a cybersecurity gap

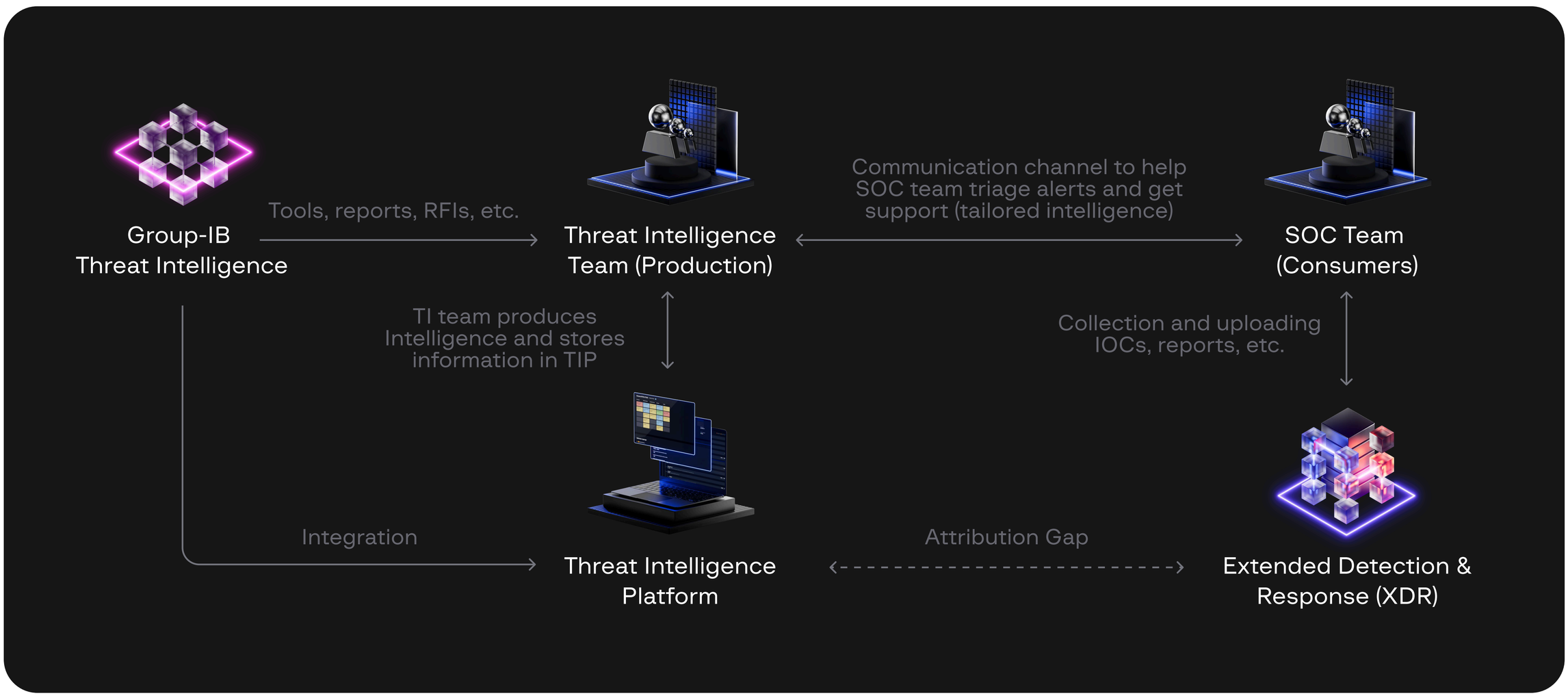


Image:
Cybersecurity gap scenerio due to misconfiguration

3. Data routing to security tools

SIEM (Security Information and Event Management):

- Ingest IOCs for log correlation and real-time alerting
- Generate detection rules based on intelligence

SOAR (Security Orchestration, Automation, and Response):

- Automate incident response workflows
- Create security tickets for review by analysts

XDR (Extended Detection and Response):

- Correlate IOCs with endpoint/network telemetry
- Automate blocking of malicious entities (IPs, domains, hashes)

---

4. Automated threat response

The library of remedial actions is growing and includes steps such as escalating an incident, disabling actions, quarantining systems, and marking an incident as non-malicious.

SOAR (Security Orchestration, Automation, and Response):

- Trigger playbooks for automated containment (firewall rules, EDR quarantines)
- Integrate with ticketing systems for incident tracking and oversight by analysts

EDR (Endpoint Detection and Response):

- Push threat intelligence updates to firewalls, EDR, and email security tools
- Automate remediation actions such as isolating infected hosts and disabling access

Threat hunting and incident analysis:

- Automate threat hunts based on newly acquired intelligence
- Use behavioral analytics to detect lateral movement and persistence

5. Management of feedback and intelligence

- Keep your community, customers, partners, MSSPs, and internal teams updated with the latest threat intelligence to strengthen collective defense.
- Use threat intelligence insights to enhance detection rules and signatures:
- Build a feedback loop to periodically review which detection rules are working in identifying attacks.

Optimizing CTI and integrating it effectively into your cyber defense program is essential. The next step is validation — that is, testing your EDR systems to assess whether your prevention controls effectively mitigate and obfuscate the defined threats.

- Update threat profiles as TTPs evolve
- Track new vulnerabilities (CVEs), techniques, and adversary behavior and adapt detection controls accordingly
- Regularly review and adjust intelligence requirements to align with the changing business and threat landscape

> Once you have a team in place that supports your CTI requirements, what about cross-functional communication and external/internal intelligence sharing? This section will help you get to grips with structuring your CTI team, enabling collaboration, and delivering actionable intelligence across the entire organization.

Strategic Insight for CISOs, Procurement, Security Leads

Making the right choice for your business in terms of CTI capability

When it comes choosing the right Cyber Threat Intelligence (CTI) source, one size doesn't fit all. The right choice depends on your organization's maturity, goals, and internal capabilities.

So, how do you choose from:

01 Platform or Vendor

02 Only TI Vendor

03 Only TIP

04 Both

Threat Intelligence Platforms (TIPs) combine external threat data with internal data to contextualize and prioritize alerts for security teams. Such platforms help with threat identification and response while offering various features, integrations, and flexible deployment options such as on-premise or cloud-based infrastructure.

When it comes to choosing a platform, some of the key considerations should be: **diverse (but relevant) sources, flexible deployment, scalability options, compatibility and integration options with your existing security stack, and real-time and contextual intelligence that you can translate into security outcomes. If the platform comes with assistance and support expertise for its implementation and enablement, that's a great bonus.**

On the other hand, **threat intelligence vendors** provide contextualized or processed intelligence that helps organizations prioritize and respond to threats. **Similarly as when evaluating a platform, when choosing a vendor, be wary of claims such as "intelligence from all sources." Instead, focus on threat attribution capabilities, industry credibility, a proven track record, strong analyst support, relevance, and the delivery of constantly updated intelligence.**

To simplify, when you are acquiring TIP you are getting an empty (or almost empty) box with a lot of potential in future integrations with public feeds or enterprise CTI vendors. When you are getting only a Threat Intelligence provider (SaaS in most cases), you have a range of different data, including feeds of course and tailored intelligence, with some (usually) limited integration options (compared to TIP) and no (or limited) option to feed into this tool your own data (for example, IOCs from your infrastructure or publicly available community feed). It is also clear that the best case scenario is to get both - TIP and TI provider (or even several TI providers).

Of course, even the most well-defined CTI function falls short without the right technology and intelligence partners. Here's what to consider when evaluating vendors and platforms:

Select the right threat intelligence sources: Any threat intelligence vendor you choose should have access to many or all of the following sources:

- Forums, threat feeds, and paste sites
- Dark web and Telegram
- News plus both mainstream and alternative social media
- Blogs and code repositories
- Technical data – network telemetry, passive DNS, netflow, endpoint data, etc.
- Foreign-language sources
- Vendor-created finished intelligence

Define your goals and objectives: The first step in setting up a CTI function is to define its overall objectives and identify the benefits it will provide to the department. The objectives should include both technical and non-technical goals and they should address the following issues:

- Key deliverables – What outputs will the CTI function produce?
- Intelligence collection – What types of information will be gathered?
- Threat actor focus – Which adversary groups will be prioritized?
- Integration with MSPs – How will intelligence fit within managed security services?

Such objectives help the department prioritize threats effectively, track CTI maturity, and measure success.

- **Understand the impact of threats on your business:** While departmental assets are often assessed broadly regarding business impact, a mature CTI function should be structured around key business units. This ensures that critical assets are evaluated individually, with consideration given to specific threat actors and attack scenarios.
- **Understand key considerations regarding tools:** A well-equipped CTI function requires tools with the following capabilities:
  - **IOC Ingestion** – Seamless integration of Indicators of Compromise (IOCs) to enhance detection and response
  - **Visualized intelligence** – Uncovering hidden links between criminal activities and infrastructure

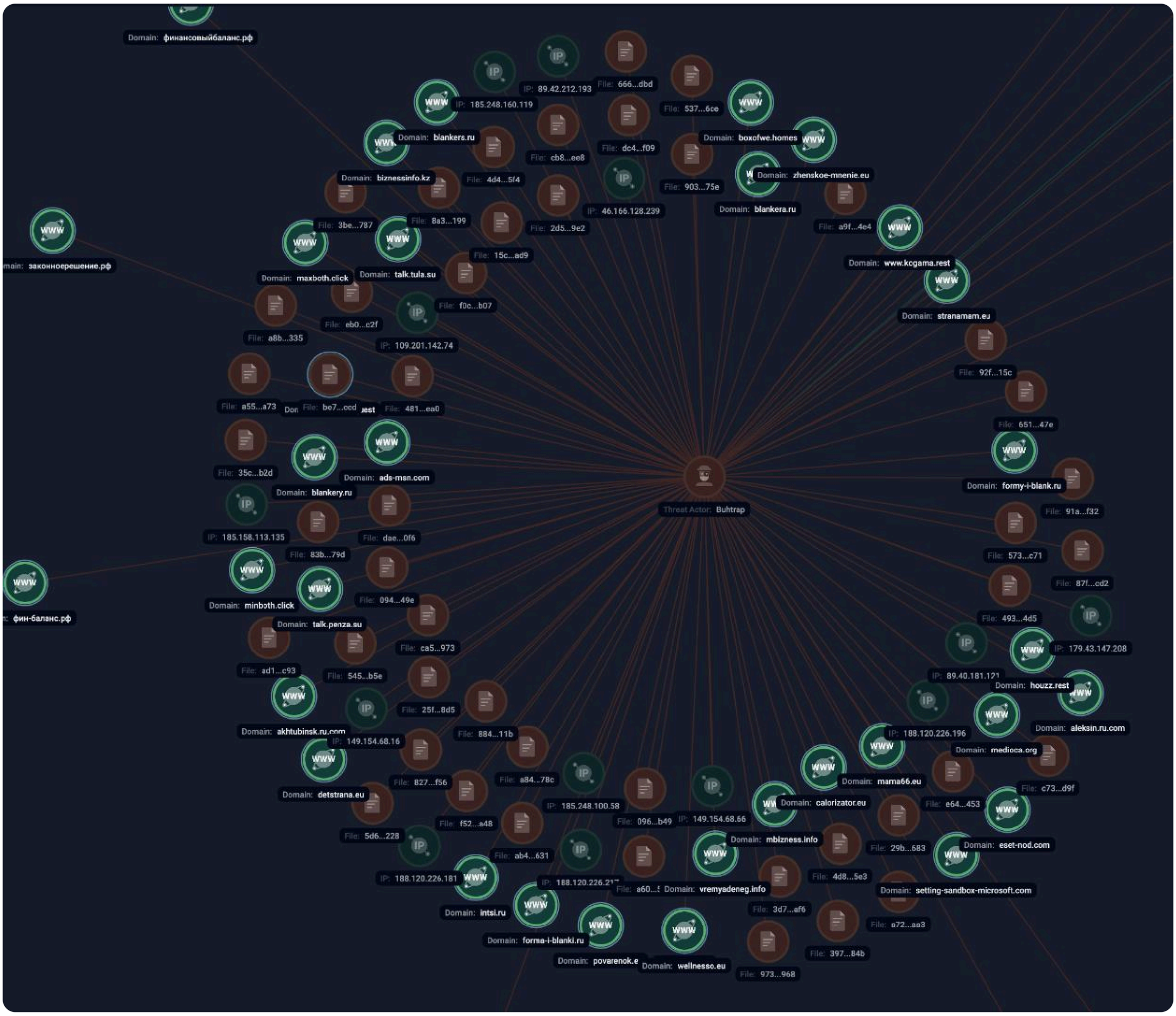


Figure 2:
Group-IB Threat Intelligence's proprietary Network Graph

- **Actionable, relevant, and timely intelligence** – Enabling faster threat identification and mitigation
- **Scalability** – Intelligence that adapts to changing network architectures and emerging threats
- **Defined scope and intelligence focus** – Tailored insights that align with your organization's risk profile
- **Automated analysis and real-time insights** – Supporting intelligence-driven security decisions
- **Integration with existing security infrastructure** – Ensuring smooth interoperability across your cybersecurity ecosystem
- **Threat actor profiling** – Mapped to MITRE ATT&CK, cyber kill chain models, and attacker TTPs for a more in-depth analysis and security improvements
- **Clear communication of threat intelligence** – Ensuring efficient collaboration and response across internal and external teams

By incorporating the above elements, organizations can develop a proactive, intelligence-driven cybersecurity strategy that mitigates threats effectively.

Operational Insight for All Roles — Technology Decision-Makers

How Group-IB threat intelligence supports your CTI framework

Group-IB Threat Intelligence: Solution brief

Group-IB acts as both a vendor and platform provider, delivering the most adversary-centric threat intelligence on the market to help businesses build and mature their CTI programs.

- **Collection of the most diverse intelligence**
  Real-time, high-fidelity insights from the clear, deep, and dark web, all supported by proprietary research and source monitoring.

- **Next-level context and visibility**
  The cohesion between data, analyst expertise, and integration development helps us gain persistent coverage and enable retaliation against cyber threats.

- **Built-in contextualization**
  The intelligence is delivered as alerts, feeds of Indicators of Compromise (IOCs), or detailed reports and it is supported by expert analysis to help evaluate threats in their proper context.
  Indicators are tied to threat actor profiles, TTPs, attribution data, MITRE ATT&CK mapping, and the Fraud Matrix (built-in fraud protection).
  The Group-IB Threat Intelligence Platform includes features such as:

  - **IOC prioritization**
  - **Threat scoring**
  - **Integrations with open-source intelligence**
  - **Dark web feeds**
  - **TTP-based threat analysis**
  - **Attribution and threat actor profiling**
  - **Real-time visibility**
  - **Automated threat feeds**

Future-leaning, advanced tools and features (for source intelligence, threat analysis, virtual assistance and support, faster detection and response):

[Open-Source Tool] Free Malware Report Tool (2M+ reports available for free): Group-IB offers a comprehensive repository of over 2 million malware reports through its Malware Detonation Platform, providing detailed insights into malware behaviors and evolutions. For anyone who would like to integrate these malware reports with the Malware Information Sharing Platform (MISP), Group-IB provides a dedicated integration tool.

[In-Built In TI Platform] AI Assistant: By combining natural language input, real-time correlation, and context-aware ranking, the tool empowers analysts of all skill levels to identify and prioritize high-impact threats. It supports vector searches, extracts critical elements like IOCs, timelines, and geographic focus, thereby reducing the manual workload on analysts. It is also great for threat hunting and building intelligence reports and summaries.

[In-Built In TI Platform] Group-IB Network Graph: A part of its threat intelligence platform, this tool is designed to visualize and analyze cybercriminal activities and identify hidden links in malicious infrastructures. Network Graph is a gamechanger for cybersecurity investigations because it separates and filters relevant data from the clutter, automates adversary intelligence, and uncovers hidden malicious connections (IPs, hosting artifacts, phishing campaigns, emails, etc.) at scale — insights that would take weeks to uncover manually.

[In-built Fraud Intelligence in Fraud Protection Platform] Fraud Matrix (Group-IB's framework to combat fraud): Decipher and intercept fraudsters TTPs and identify pre-fraud indicators to protect your organizations from illicit mentions, laundering and associated activities, invasion attempts, and anything else that could result in financial, integrity and reputational losses.

Easy platform integration: Modern cybersecurity operations rely on a steady flow of consistent, high-quality data across tools. Group-IB Threat Intelligence is continuously optimized to be API-friendly and integration-ready, helping to harmonize data across environments and thereby enabling seamless intelligence automation and real-time threat detection and response.

Operational support at each CTI layer: CTI enables each layer of your security framework with the widest collection of intelligence sources, automated data ingestion methods, expert-driven analysis, and proactive threat tracking mechanisms, helping you not only maintain but continuously enhance your security posture.

Group-IB CTI Framework Support

Collection

Open-source Intelligence (OSINT)
Publicly available data aggregated from multiple sources to identify risks and vulnerabilities
- Code repositories
- Paste sites
- Exploit repositories
- Social media discussions
- URL sharing services

Malware intelligence
Active monitoring and analysis of malware threats using a combination of public and proprietary platforms
- Detonation platform
- Malware emulators
- Malware configuration files extraction
- Public sandboxes

Human intelligence (HUMINT)
Includes seasoned cybersecurity experts with privileged access to critical data, providing unique insights into cybercriminal tactics and strategies
- Malware reverse engineers
- Undercover dark web agents
- DFIR and audit services
- Law enforcement operations
- Regional specialists

Sensor intelligence
(Critical insights into network activity and threat patterns by deploying a variety of advanced tools)
- ISP-level sensors
- Honeypot network
- IP scanners
- Web crawlers

Vulnerability intelligence (VULINT)
(Tracking and assessing vulnerabilities across multiple channels, helping you patch weaknesses before they are exploited)
- CVE list
- Exploit repositories
- Dark web discussions
- Threat campaigns mapping

Data intelligence
(Continuous scanning and analysis of data across multiple channels to detect compromise and exfiltration)
- C&C server analysis
- Dark web markets
- Dark web forums
- Instant messengers data (Telegram, Discord)
- Phishing and malware kits
- Compromised data-checkers

Automated & Expert Analysis

Group-IB Research + Incident Response Data for Threat Actor Profiling
APTs, cybercriminals, and fraudsters

Attribution Insights
Links actor aliases, geolinguistic behavior, and past campaigns to attribute threats

Tracking Evolving Cybercriminal Tactics
Adaptability to evolving attack methods

Incident Reports

Dark web chatter
(ransomware negotiations, underground marketplaces surveillance, affiliate programs and recruitments, threat actor attribution

Enrichment

MITRE Mapping
Correlation of threat actor TTPs into a multi-step sequence

Data Aggregation & Normalization

IOC Enrichment
e.g., file hashes, IPs, URLs with context

Threat Feed Fusion
malware trend analysis, IOCs context

Risk Analysis

Campaign-Level Threat Tracking
linking actor TTPs over time

ML-Based Impact Ranking
Analysis of attack patterns, historical data, and threat actor behaviors to predict emerging risks

AI-Driven Threat Prioritizations
Forecasts and ranks threats by risk level

Group-IB Threat Intelligence

Integration & Delivery (Direct API integrations)

SOAR Integration
Automates workflows, sandbox detonation, IP blacklisting, malicious resource takedown

Attack Surface Management
Continuously maps exposed digital assets to reduce attack risks

MXDR [Smart Alerting for Real-Time Incident Containment]
Automated Alerts and First-Level Threat Response

Risk Assesment and Threat Prioritization

Real-Time Risk Scoring & Severity Analysis of IOCs

Business Impact Ranking
prioritization based on organisational impact

Linking IOCs, TTPs, Threat Actors
components from different sources

Outcomes

Faster threat detection

Proactive threat protection and risk management

Higher fidelity alerts

Improved SOC efficiency

Digital Risk &Brand Protection

Fraud Protection

Group-IB Threat Intelligence at a glance

Growth of cybercrime

Underground Clouds of Logs (UCL) keep growing for initial access

56.8%

of access acquired by Ransomware-as-a-Service groups

25%

by Advanced Persistent Threat groups

AI-driven Threat Intelligence

Data Sources & Intelligence Outputs

Open-source Intelligence (OSINT)

Human Intelligence (HUMINT)

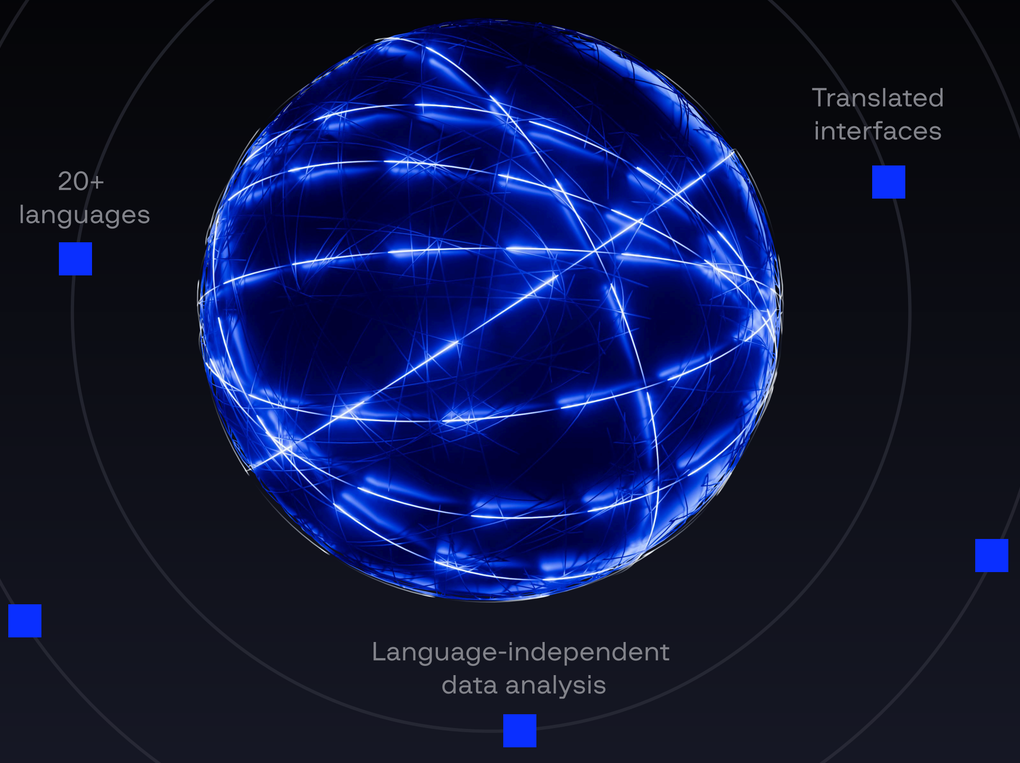
Vulnerability Intelligence (VULINT)

Sensor Intelligence

Data Intelligence

Threat Operations & Expertise

Powered by Localized Intelligence



Localized Presence and Intelligence Infrastructure

Singapore, Vietnam, Thailand, Malaysia, Egypt, Netherlands, Italy, Chile, Uzbekistan, UAE, KSA.

Powered by Unique Digital Crime Resistance Centers

eBook shaped by:

Authors

Pavel Shepetina:
Head of Integration Architecture
& Technical Communication

Jasmine Kharbanda:
Global Content Marketing Manager

Contributors

Dmitry Volkov:
CEO and Founder, Group-IB

Dmitry Shestakov:
Technical Director (ASM, TI, DRP)

Alexander Asmolov:
Head of Cyber Defence Consulting Practice

Anastasia Tikhonova:
Technical Head, APAC

Anastasia Barinova:
Head of Education Practice

GROUP-IB

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

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

500+
Employees

60
Countries

$1 bln+
Saved by our client companies through our technologies

#1*
Incident Response Retainer vendor

*According to Cybersecurity Excellence Awards

11
Unique Digital Crime Resistance Centers

Global partnerships

- INTERPOL
- EUROPOL
- AFRIPOL

Recognized by top industry experts

- Forrester®
- Aité Novarica
- kuppingercole ANALYSTS
- Gartner®
- IDC
- Frost & Sullivan

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