

# Get a 360-Degree View of Threats with Eclectiq and Group-IB Threat Intelligence & Attribution

Quickly identify external and insider threats with enriched intelligence and accelerated attribution.

## The Challenge

Security teams face increasing challenges in detecting and responding to cyber threats due to fragmented intelligence and delayed attribution. Advanced Persistent Threats (APTs), phishing campaigns, stolen data misuse, and sophisticated malware operations make it difficult for analysts to prioritize and act on threats. Without automated correlation and deep contextual intelligence, security operations teams struggle with slow investigations, unprioritized alerts, and an incomplete understanding of adversary tactics.

## Joint Solution

### Deepen threat tracking

Eclectiq Intelligence Center integrates with Group-IB's industry-leading threat intelligence, sourced from real-world investigations, law enforcement collaborations, and a global technical network. Analysts gain deeper insights into adversaries' tactics, techniques, and procedures (TTPs), enabling proactive defense strategies.

### Better understand advanced tactics

SOC and CTI teams can proactively identify active threats and predict adversary movements. By correlating network sensor sightings with Group-IB's profiling of threat actors, Eclectiq users gain early warning of targeted campaigns and emerging attack trends.

### Accelerate attribution insights

With Eclectiq's Graph, analysts can quickly pivot from indicators of compromise (IOCs) to attribution insights. Group-IB enriches investigations with malware analysis, proprietary sensors, and external threat-hunting intelligence, providing high-confidence attribution.

# Key Use Cases

## Enhance detection of APT threats

Security analysts need real-time intelligence to detect APTs and improve the incident triage triage. By integrating Group-IB's APT Threat Intelligence into Eclectiq Threat Intelligence Platform (TIP), organizations gain high-confidence IOCs and TTPs that are automatically correlated with existing intelligence. This enables faster detection of APT-related activity, reduces false positives, and improves incident response times.

## Block malware command and control (c2) traffic

Disrupting malware C2 traffic is challenging due to encrypted and evolving communication techniques. By integrating Group-IB's Malware C2 intelligence into Eclectiq TIP, analysts gain visibility into active malware operations and can block malicious C2 communications in real time. This disrupts attacker infrastructure and mitigates malware-related damage.

## Prevent compromise from stolen data

Threat actors use compromised credentials and payment card data for unauthorized access and financial fraud. By ingesting Group-IB's Compromised Data Feeds into Eclectiq TIP, organizations can proactively detect and block attempts to use stolen data. This prevents account takeovers, credential-stuffing attacks, and fraud-related breaches.

## Mitigate phishing attacks

Security teams struggle to detect and mitigate phishing attacks that target their brand and employees. Eclectiq TIP integrates Group-IB's Phishing Kits and Brand Abuse intelligence, allowing organizations to monitor, analyze, and block malicious phishing campaigns in real time. This improves brand protection and reduces credential theft incidents.

## Improve incident response with human intelligence threats

Identifying and responding to social engineering, insider threats, and human-driven attacks remains difficult for many security teams. Eclectiq TIP ingests Group-IB's Human Intelligence Threat data, allowing security analysts to correlate insider threats with broader intelligence sources. This improves detection and containment of social engineering tactics and insider risks.

## About Eclectiq

Eclectiq is a global provider of threat intelligence technology and services that empower customers to neutralize critical cyber threats to their business. Guided by our values – being curious, bold, accountable, and collaborative – we help security teams make smarter, faster decisions with dynamic solutions that reduce complexity and streamline threat detection and response.

Visit [www.eclectiq.com](http://www.eclectiq.com) or follow us on [LinkedIn](#) and [X](#) for more information.

## About Group-IB

Group-IB is a Singapore-based provider of solutions for the detection and prevention of cyberattacks and online fraud, and high-tech crime investigations. Group-IB's Threat Intelligence & Attribution system has been named one of the best in class by Gartner, Forrester, and IDC.

Visit [www.group-ib.com](http://www.group-ib.com) for more information.

Connect with our experts and see the solution in action!

[Request a Demo](#)