Solution brief

Dig Deep to Detect and Prevent Cyber Underground Threats

Master your threat landscape by integrating Intel 471's cybercrime intelligence with EclecticIQ Threat Intelligence Platform (TIP).

The Challenge

Security teams struggle to track cybercriminal activity hidden in underground forums, marketplaces, and private channels. Without access to closed-source intelligence, organizations lack visibility into adversary tactics, making it difficult to detect threats before they escalate. Additionally, low-confidence indicators contribute to event fatigue, making it harder to focus on real threats. To stay ahead, security teams need high-confidence, structured intelligence that enriches investigations and enables automated threat response.

Joint Solution

Automated integration

Intel 471's closed-source cybercrime intelligence automatically flows into EclecticIQ Threat Intelligence Platform, providing timely and relevant insights on underground threats. This eliminates manual data collection, ensuring that high-confidence intelligence reaches analysts in real time.

Threat pattern visualization

EclecticIQ Threat Intelligence Platform structures and enriches Intel 471's data, including Threat Actor Footprints and Malicious Infrastructure intelligence. Analysts can quickly visualize attack patterns, improving threat detection and streamlining investigations.

Single pane of glass

EclecticIQ Threat Intelligence Platform combines Intel 471's underground threat feeds with third-party intelligence sources, offering analysts a unified view of the cyber threat landscape. This enables efficient intelligence management, deeper correlation, and improved response times—all from a single interface.

Key Use Cases

Track cybercriminal underground

Tracking cybercriminal underground activities is difficult without access to closed sources where adversaries collaborate and plan attacks. By integrating Intel 471's closed-source intelligence into EclecticIQ Threat Intelligence Platform, analysts gain structured data on adversary tactics, including domains, IPs, and URLs. With direct visibility into underground communities, analysts can track threat actor behavior, map their infrastructure, and proactively hunt for new attack campaigns. This enables faster identification of emerging threats, enriched threat intelligence, and a stronger security posture.

Reduce event fatigue from low-confidence indicators

Low-confidence indicators generate alert fatigue, making it challenging for analysts to distinguish real threats from noise. By integrating Intel 471's high-confidence indicators—such as domains, IPs, hashes, and URLs—into EclecticIQ Threat Intelligence Platform, security teams receive enriched intelligence mapped to MITRE ATT&CK, malware intelligence, and YARA rules. This filters out irrelevant data and enhances the accuracy of threat detection, allowing analysts to focus on genuine risks rather than chasing false positives. As a result, SOC teams can improve detection rates, reduce investigation time, and automate responses with greater confidence.

Enrich threat intelligence with context

Threat intelligence often lacks the context needed to assess its relevance and impact. EclecticIQ TIP integrates Intel 471's adversary intelligence, adding key metadata such as expiry time, confidence level, and MITRE ATT&CK techniques. With this enriched intelligence, analysts can better understand the scope of a threat, identify patterns across multiple sources, and take proactive security measures. This contextualized intelligence also helps organizations anticipate threat actor movements and prioritize security efforts more effectively.

Accelerate threat response with actionable intelligence

Without actionable intelligence, security teams struggle to respond quickly to threats. By integrating Intel 471's real-time underground intelligence into EclecticIQ Threat Intelligence Platform, security teams can populate SIEMs with high-confidence indicators and automate response actions. With this integration, threat detection and mitigation are no longer reactive but proactive, reducing dwell time and preventing attackers from gaining a foothold. The ability to automate workflows and trigger rapid responses ensures that SOC teams can neutralize threats before they escalate into full-scale attacks.

About EclecticIQ

EclecticIQ 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.eclecticiq.com or follow us on LinkedIn and X for more information.

About Intel 471

Intel 471 is a leading provider of cybercrime intelligence, offering deep visibility into cybercriminal underground activities. By collecting intelligence from closed sources, malware campaigns, and criminal communities, Intel 471 enables organizations to track adversary behavior, prevent cyber threats, and strengthen security operations. Its intelligence supports threat hunting, fraud prevention, and incident response, helping security teams make data-driven decisions.

Visit www.intel471.com for more information.

Connect with our experts and see the solution in action!

Request a Demo