Solution brief

Achieve and Accelerate Proactive Threat Management with EclecticIQ and Kaspersky

Leverage Kaspersky's rich threat intelligence within EclecticIQ Intelligence Center to enhance threat visibility, accelerate response, and strengthen proactive defense.

The Challenge

Security teams struggle to detect and respond to sophisticated cyber threats due to fragmented intelligence and manual analysis. The increasing complexity of cyberattacks—ransomware, APT campaigns, and mobile botnets—demands real-time threat enrichment, automated correlation, and a unified intelligence-driven approach. Without these capabilities, security teams risk slow detection, limited visibility, and ineffective responses to evolving cyber threats.

Joint Solution

Comprehensive threat intelligence integration

EclecticIQ offers deep integrations with Kaspersky threat intelligence, including Threat Data Feeds, Threat Lookups, and APT Intelligence Reporting. These integrations provide real-time insights into global threat activity, enabling security teams to proactively detect and mitigate emerging cyber threats before they impact business operations.

Single pane of glass for enhanced threat intelligence

EclecticIQ consolidates multiple intelligence sources, including Kaspersky's IP, URL, and hash-based threat intelligence, into a single pane of glass. This unified view allows security teams to gain an extended threat picture, improving investigations and accelerating incident response with enriched context.

Accelerated threat correlation and visualization

By combining EclecticIQ's advanced workspaces, datasets, and automation features with Kaspersky's intelligence feeds, analysts can quickly correlate and visualize threats in real time. This seamless integration enhances situational awareness, ensuring that security teams focus on the most relevant and actionable threats.

Stronger defences against advanced threats

As cyber threats grow more sophisticated, adversaries deploy orchestrated campaigns, tailored TTPs, and advanced intrusion techniques to evade detection. Kaspersky's threat intelligence—integrated into EclecticIQ Threat Intelligence Platform (TIP) - enables organizations to track emerging threats, identify malicious indicators, and mitigate advanced cyberattacks proactively.

Key Use Cases

IP reputation monitoring

Malicious IP addresses are often leveraged in cyberattacks, yet security teams struggle to detect and block them in real time. By integrating Kaspersky's IP Reputation Data Feed with EclecticIQ's TIP, organizations gain real-time intelligence on suspicious IPs, allowing security teams to enrich investigations, prioritize threats, and implement proactive blocking measures. This results in faster threat detection and reduced exposure to malicious network activity.

Mobile threat detection

Mobile botnets pose a significant risk, yet many organizations lack visibility into mobile malware activity. By integrating Kaspersky's Mobile Botnet Data Feed with EclecticIQ's TIP, security teams can detect and investigate mobile-based threats targeting Android and iOS devices. This enhanced visibility enables early detection and proactive mitigation of mobile threats.

Protection against targeted system attacks

Sophisticated cyber threats increasingly target critical infrastructure, yet organizations lack visibility into these attacks. Kaspersky's threat intelligence feeds provide real-time insights into malicious activity in specialized environments, helping security teams detect and mitigate threats. Integrating this intelligence into EclecticIQ enhances visibility and control, reducing overall risk.

Ransomware threat intelligence

Ransomware attacks continue to evolve, using malicious URLs to distribute payloads and execute attacks. Security teams require intelligence that enables them to identify and block ransomware-related domains before infections occur. By ingesting Kaspersky's Ransomware URL Data Feed into EclecticIQ's TIP, analysts can correlate, track, and block ransomware-related domains before an attack. This reduces ransomware risk and strengthens incident response.

Malware hash intelligence

The sheer volume of new and evolving malware makes it difficult for security teams to detect and correlate threats effectively. By integrating Kaspersky's Malicious Hash Data Feed into EclecticIQ's TIP, organizations benefit from automated hash enrichment and correlation, improving malware detection accuracy and response times.

Advanced persistent threat (APT) detection

APT campaigns leverage advanced TTPs to remain undetected, making early identification a significant challenge for security teams. With Kaspersky's APT Hash, APT IP, and APT URL Data Feeds, EclecticIQ enables analysts to track APT actors, correlate intelligence, and enhance attribution efforts. This helps security teams detect and defend against sophisticated cyber espionage campaigns.

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 Kaspersky

Kaspersky is a global cybersecurity and digital privacy company founded in 1997. With deep threat intelligence and security expertise, we provide innovative security solutions and services to protect businesses, critical infrastructure, governments, and consumers worldwide. The company's comprehensive security portfolio includes leading endpoint protection and specialized security solutions and services to fight sophisticated and evolving digital threats

Visit www.kaspersky.co.in for more information.

Connect with our experts and see the solution in action! **Request a Demo**