EclecticIQ Silobreaker

Solution brief

Enhancing Threat Intelligence with EclecticIQ Intelligence Center and Silobreaker

Quickly enrich and analyze malware, threat actors, attack types and vulnerabilities with intelligence from Silobreaker, directly within the EclecticIQ Intelligence Center.

The Challenge

Cyber threats are becoming more sophisticated, with threat actors weaponizing vulnerabilities within an average of seven days. Security teams struggle with an overload of CTI alerts, making it difficult to differentiate critical threats from noise. Traditional investigative methods lack efficient ways to extract insights from massive amounts of unstructured threat intelligence across open, closed, and dark web sources. SOC and CTI teams need a seamless way to enrich and contextualize threat data for faster and more effective decision-making.

Joint Solution

Automated integration for comprehensive threat intelligence

Silobreaker seamlessly integrates with EclecticIQ Intelligence Center, providing direct access to real-time threat intelligence from millions of open, closed, and dark web sources. Analysts can instantly enrich observables—including IPs, domains, malware hashes, and CVEs—with deep context on threat actors, attack campaigns, and geopolitical risks without switching platforms

Observable enrichment for enhanced investigations

Observables such as IPs, domains, and file hashes can be enriched with context from Silobreaker's vast data ecosystem, providing deeper insight into cyber threats. Silobreaker's "In Focus" tool extracts key players, attack patterns, and relevant insights, helping analysts quickly connect emerging threats to broader campaigns. EclecticIQ Intelligence Center then processes and correlates this enriched intelligence, allowing security teams to prioritize risks and make informed decisions faster.

Watchlist monitoring for proactive threat detection

Security teams can track and monitor vulnerabilities, threat actors, malware families, and third-party risks using Silobreaker's automated watchlists inside EclecticIQ Intelligence Center. This allows continuous monitoring of high-risk entities, providing early warnings on emerging threats that may impact the organization's assets or supply chain.

Optimized incident response and threat prioritization

By correlating threat intelligence from Silobreaker with EclecticIQ's advanced analytics and workflows, SOC teams can prioritize critical threats more effectively. The integration reduces false positives and enhances incident triage by providing historical and real-time context on malicious activity. Security teams gain actionable intelligence that improves response times and mitigates potential breaches before they escalate.

Key Use Cases

Prioritized vulnerability and patch management

Security teams need to determine which vulnerabilities pose the highest risk based on real-world exploitation. Silobreaker continuously tracks CVEs that are actively discussed or exploited across open, closed, and dark web sources. EclecticIQ Intelligence Center correlates this intelligence with internal data, helping analysts prioritize patching efforts and reduce the likelihood of exploit-based attacks. By leveraging real-time intelligence, security teams can proactively address vulnerabilities before they are weaponized by adversaries, minimizing exposure to critical threats.

Third-party and supply chain risk monitoring

Organizations need visibility into cyber risks affecting their suppliers and business partners. Silobreaker continuously monitors third parties for mentions in data breaches, underground forums, and security incidents. EclecticIQ Intelligence Center integrates this intelligence, enabling security teams to assess and mitigate risks before they impact business operations. With a unified view of supplier security, organizations can proactively address vulnerabilities in their supply chain, strengthening resilience against cascading cyber risks.

Threat actor and campaign monitoring

Tracking adversaries and their evolving tactics is critical to staying ahead of emerging threats. Silobreaker collects and analyzes threat actor activity across underground forums, security blogs, and intelligence reports. EclecticIQ Intelligence Center enriches this data with historical intelligence, allowing analysts to track attack patterns, predict future threats, and strengthen defenses. With continuous monitoring of attack campaigns, security teams gain early warnings about potential targeting and can implement preemptive security measures to disrupt adversary actions.

SOC incident response acceleration

SOC analysts need immediate access to contextualized threat intelligence to speed up investigations. Silobreaker provides real-time enrichment for security alerts with relevant intelligence on malware, threat actors, and attack techniques. EclecticIQ Intelligence Center correlates alerts with known campaigns, reducing investigation time and improving triage efficiency. By automating intelligence correlation and providing deeper context, analysts can quickly validate threats, prioritize response efforts, and reduce dwell time for active incidents.

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 Silobreaker

Silobreaker helps business, security and intelligence professionals address of the overwhelming amount of unstructured data on the web. By providing powerful tools and visualizations that cut through noise and analyze data from over a million open sources, Silobreaker simplifies monitoring and researching companies and industries, threats, compromises, actors, instabilities, geopolitical developments or any other topic, incident or event.

Visit www.silobreaker.com for more information.

Connect with our experts and see the solution in action!

Request a Demo