Solution brief

EclecticIQ

Microsoft Sentinel

Powering Intelligent Security with EclecticIQ Intelligence Center and Microsoft Sentinel

Turn high-confidence threat intelligence into action with smarter detection, faster response, and enhanced threat visibility.

The Challenge

Security teams are inundated with a high volume of alerts and lack the contextual intelligence needed to distinguish true threats from false positives. As a result, SOC and CTI analysts often struggle to prioritize incidents, leading to delayed investigations and ineffective responses. Threat hunting is also hindered by fragmented, outdated, or low-confidence threat data. Without accurate and timely intelligence, analysts waste valuable time chasing irrelevant alerts instead of focusing on high-impact threats that demand immediate attention.

Joint Solution

Comprehensive threat intelligence for deeper insights

EclecticIQ Intelligence Center enriches Microsoft Sentinel's telemetry—spanning users, devices, applications, and infrastructure—with high-confidence threat actor data, TTPs, and observables. This integration delivers broader visibility and sharper threat context to strengthen detection and response.

Real-time situational awareness & incident investigation

Through bi-directional integration, sightings from Microsoft Sentinel are fed into EclecticIQ Intelligence Center. This integration enables analysts to track, visualize, and correlate security incidents at scale, leading to faster threat attribution, improved attack pattern recognition, and proactive defense.

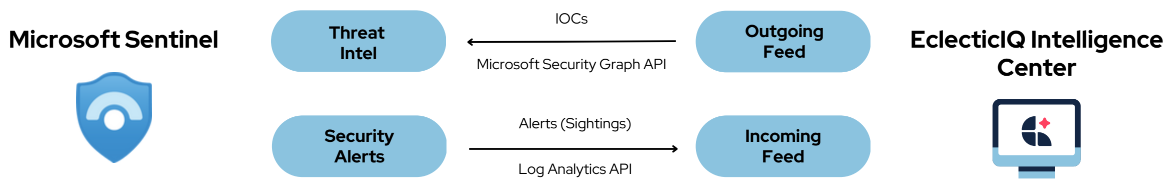
Advanced threat detection & reduced alert fatigue

Sentinel's AI-driven analytics and machine learning combine with EclecticIQ's high-confidence IOCs and observables helps reduce false positives and sharpen detection. Analysts can quickly identify high-fidelity threats and cut through alert noise.

Accelerated incident response with AI & automation

Microsoft Sentinel's orchestration capabilities work in tandem with EclecticIQ's enriched intelligence to automate threat containment. Analysts can prioritize actions based on severity and context—cutting down investigation time and improving SOC performance.

EclecticIQ Intelligence Center and Microsoft Sentinel



Key Use Cases

Enrich microsoft sentinel alerts with high-confidence threat intelligence

Microsoft Sentinel generates numerous security alerts daily, but without proper context, analysts struggle to prioritize them effectively. By integrating EclecticIQ Intelligence Center, security teams can automatically enrich Sentinel alerts with relevant threat intelligence, including known threat actors, TTPs, and malicious indicators. Analysts gain immediate insights into the nature and severity of threats, allowing them to triage incidents faster and reduce false positives.

Leverage Microsoft Sentinel sightings for threat correlation

Microsoft Sentinel continuously collects sightings of malicious activity from across an organization's environment. However, these detections need correlation with external threat intelligence to be truly effective. By feeding Sentinel sightings into EclecticIQ Intelligence Center, analysts can automatically match them against known threat campaigns, adversary tactics, and emerging attack patterns. This enables CTI and SOC teams to quickly assess if activity ties to a broader campaign and respond with precision.

Filter and prioritize iocs for more effective threat hunting

Not all IOCs are equally relevant to an organization. Some may be outdated, low-confidence, or unrelated to an active threat campaign. By using EclecticIQ Intelligence Center, SOC analysts can filter IOCs based on attributes such as threat severity, expiration dates, and intelligence confidence levels before importing them into Sentinel. This helps eliminate unnecessary noise and ensures that threat hunters focus only on high-priority, actionable intelligence, improving efficiency and detection accuracy.

Automate incident response and threat mitigation

Manual incident response processes slow down containment efforts and increase the risk of damage from cyberattacks. With this integration, Microsoft Sentinel's automated playbooks can leverage EclecticIQ's high-confidence intelligence to trigger automated responses, such as: Blocking malicious IOCs, Isolating compromised endpoints, notifying security teams with enriched intelligence, improve response times, minimize attack impact, and streamline SOC operations.

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 Microsoft Sentinel

Microsoft Sentinel is a modern, cloud-native SIEM and SOAR solution that helps security teams detect, investigate, and respond to threats with speed and precision. Leveraging Microsoft's decades of cybersecurity expertise, Sentinel uses AI and built-in automation to provide enterprise-wide visibility, reduce complexity, and lower operational costs.

Visit www.microsoft.com/security to learn more.

Connect with our experts and see the solution in action!

Request a Demo