SOLUTION BRIEF

Censys Integration for EclecticIQ Intelligence Center™

Operationalize Internet Intelligence for Faster Threat Investigation and Exposure Visibility

Bring Censys Internet Intelligence into EclecticIQ Intelligence Center™ with automated indicator ingestion and IPv4/IPv6 enrichment. Security teams can rapidly validate suspicious infrastructure, correlate attacker activity, and operationalize exposure intelligence directly within intelligence and investigation workflows.

Customer Challenges

Security teams need timely visibility into exposed and attacker-controlled infrastructure associated with emerging threats. However, critical infrastructure intelligence often resides outside core intelligence operations and investigation workflows.

Without automation, analysts must manually search external sources to validate infrastructure, enrich IP observables, and correlate internet-facing assets with active investigations. This results in fragmented analysis, increased investigation time, delayed response, and missed opportunities to identify adversary infrastructure and exposure risks.

Organizations also face challenges continuously ingesting large volumes of infrastructure indicators and internet intelligence while maintaining operational context for threat hunting, SOC investigations, and exposure monitoring.

Joint Solution Overview

The Censys integration for EclecticIQ Intelligence Center™ combines EclecticIQ's threat intelligence operations platform with Censys Internet Intelligence to deliver actionable infrastructure context throughout the intelligence lifecycle.

The integration provides two complementary capabilities:

EclecticIQ - Censys Enricher
EclecticIQ's Censys Enricher enables on-demand enrichment of IPv4 and IPv6 observables using the Censys Global Asset API. Analysts can quickly retrieve infrastructure intelligence, exposed service information, and contextual data associated with internet-facing assets to support investigation and triage workflows.

EclecticIQ - Censys Incoming Feed
EclecticIQ's Censys Incoming Feed continuously ingests indicators and observables from the Censys Advanced Threat Intelligence Indicator Feed using configurable Censys queries aligned with organizational monitoring priorities. Retrieved data is normalized into structured Indicator entities and observables for operational use across threat intelligence, detection engineering, and investigation workflows.

Together, the integration operationalizes internet-scale visibility from Censys within EclecticIQ Intelligence Center™, helping teams investigate suspicious infrastructure faster, identify potential threats earlier, and reduce manual analyst effort.

Key Business Outcomes

- Operationalize Censys Internet Intelligence directly within intelligence workflows
- Accelerate infrastructure investigations and incident response
- Reduce manual enrichment and analyst tool switching
- Improve visibility into exposed and internet-facing infrastructure
- Continuously ingest infrastructure indicators aligned to organizational priorities
- Enhance threat hunting and infrastructure correlation capabilities
- Support exposure management and attack surface monitoring initiatives

Key Personas

Security Operations VP / Director / Lead

Head of Threat Intelligence / CTI Director

Threat Hunting Team Lead

Primary Use Cases

Infrastructure Investigation and Validation

During triage and incident response, analysts enrich IPv4 and IPv6 observables with Censys infrastructure intelligence to validate suspicious assets, identify exposed services, and understand internet-facing infrastructure. This accelerates decision-making when infrastructure serves as a primary investigative signal.

Threat Hunting and Infrastructure Correlation

Threat hunters pivot across Censys Internet Intelligence and existing intelligence holdings in EclecticIQ Intelligence Center™ to uncover relationships between infrastructure, campaigns, and threat actors. Teams can identify overlaps, track infrastructure reuse, and reduce time spent investigating disconnected leads.

Continuous Threat Intelligence Ingestion

Security teams continuously ingest indicators and observables from the Censys Advanced Threat Intelligence Indicator Feed using configurable monitoring queries. This supports intelligence-led investigations, detection engineering, and proactive monitoring with continuously updated infrastructure intelligence.

SOC Triage Acceleration

By bringing Censys context directly into analyst workflows, the integration reduces manual lookups and tool switching. Analysts gain immediate access to infrastructure intelligence, enabling faster validation of suspicious assets and more efficient case progression.

Exposure and Attack Surface Monitoring

Security teams monitor suspicious internet-facing infrastructure relevant to their organization, industry, or threat landscape. Leveraging Censys Internet Intelligence helps improve visibility into exposed assets, emerging attacker infrastructure, and potential risks across the global internet.

Adversary Infrastructure Discovery

Analysts leverage Censys visibility into global internet infrastructure to identify potentially malicious hosts, services, certificates, and related observables associated with threat actor operations. This enables earlier identification of attacker-controlled infrastructure and supports proactive threat hunting efforts.

How Censys Enricher Works

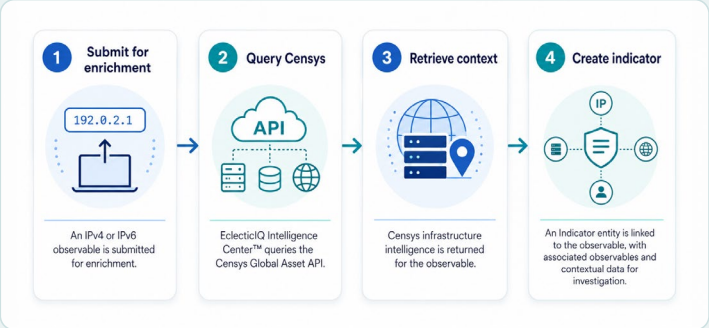

Fig. 1 Use the Enricher to provide investigation-time context for suspicious IPv4 and IPv6 infrastructure.

How Censys Incoming Feed Works

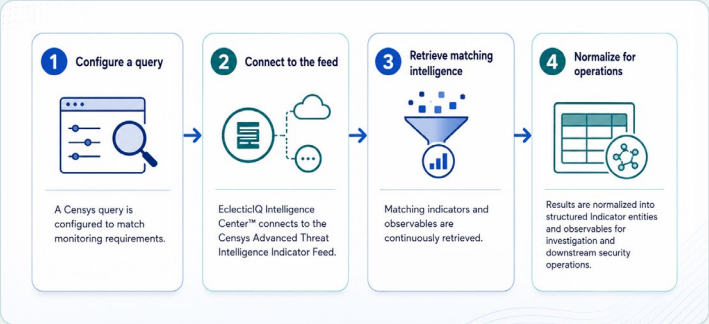

Fig. 2 Use the Incoming Feed for continuous ingestion of Censys threat intelligence and infrastructure indicators.

Why This Joint Solution Matters

Together, Censys and EclecticIQ help organizations operationalize internet intelligence at scale, enabling security teams to move from fragmented infrastructure investigations to intelligence-driven operations. The integration delivers faster threat detection, improved infrastructure visibility, and more efficient use of security resources.e.

Learn More

Learn how Censys and EclecticIQ can help your organization investigate suspicious infrastructure faster, identify potential threats earlier, and reduce manual analyst effort.

Contact Censys Contact Eclectic IQ

censys

VISIT
censys.com

CONTACT
hello@censys.com

Censys is the authority for Internet intelligence and insights. Delivering the most complete, accurate, and up-to-date global map of Internet infrastructure, Censys provides industry leading solutions for attack surface management, threat hunting, and proactive incident response. Global governments, Fortune 500 companies, and security providers around the world trust Censys to uncover risks faster, respond more effectively, and prevent breaches before they happen.