SOLUTION BRIEF

Integrated Internet and Adversary Intelligence for Accelerated SOC Triage and Incident Response

Security Operations Centers (SOCs) are under increasing pressure as internet-facing attack surfaces expand and adversary infrastructure evolves faster than traditional threat feeds can track. Analysts are overwhelmed by alerts that lack external context, rely on stale indicators, and require time-consuming manual investigation. This results in delayed triage, missed correlations, and slower incident response.

Censys and The Vertex Project jointly address this challenge by integrating continuously updated internet intelligence with analyst-driven investigation and correlation workflows. Censys provides continuous and historical visibility into all internet-facing assets and adversary infrastructure, while Vertex operationalizes this intelligence directly within analyst workflows for enrichment, correlation, and action.

Together, the solution enables SOC teams to reduce mean time to triage (MTTT), prioritize high-confidence threats, and accelerate incident response by eliminating manual enrichment steps and delivering actionable context where analysts work.

Customer Challenges

Strategic pressures: Adversaries increasingly rely on distributed, short-lived infrastructure that evades static detection, while SOC and CTI teams are expected to respond faster with fewer resources.

Security challenges: Fragmented data sources and reliance on outdated threat intelligence feeds result in incomplete visibility into internet-facing assets – including external IPs, services, and certificates – leaving teams unable to track how adversary infrastructure evolves over time.

Operational challenges: Alert fatigue caused by high volumes with insufficient context – combined with manual enrichment workflows – slows investigations and increases analyst workload, while a lack of historical internet data and difficulty pivoting across related infrastructure hinder threat hunting and incident response.

Joint Solution Overview

The Censys-Vertex joint solution integrates internet-wide visibility and adversary intelligence with analyst-centric investigation and correlation workflows.

Censys is the leading platform for real-time discovery and monitoring of internet-facing assets, services, certificates, and exposures using the world's largest internet scanning infrastructure.

Vertex provides an analyst-focused investigation platform designed for rapid enrichment, correlation, and visualization.

By embedding Censys intelligence directly into Vertex workflows, SOC teams gain immediate external context for alerts, enabling faster validation, deeper infrastructure correlation, and more confident response decisions.

Business Benefits Include

- Faster alert triage and investigation
- Improved threat validation and prioritization
- Increased SOC efficiency through automated intelligence enrichment

Primary Buyer Personas

- CISO
- SOC Manager
- Threat Intelligence Leads
- Incident Response Teams

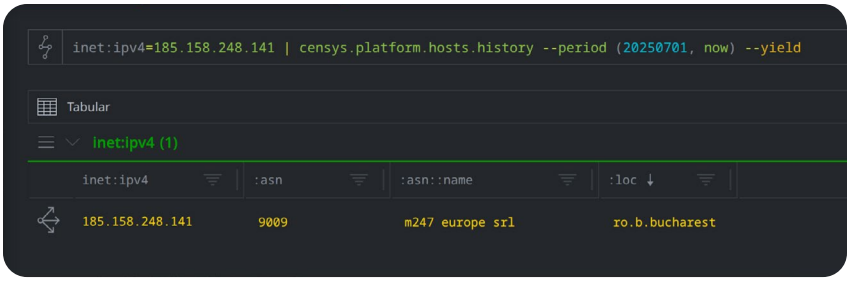

Fig. 1 Querying Censys for Activity Associated with 185.158.248.141 Between July 1, 2025 and the Current Date

Primary Use Cases

Accelerated Alert Triage

What it solves: SOC analysts receive high volumes of alerts that lack external context, forcing manual lookups across disparate tools to determine severity and relevance. This slows triage, increases MTTT, and contributes to alert fatigue.

How it works: When an alert triggers investigation in Vertex's Synapse, Vertex queries Censys APIs for IP, service, and infrastructure content enabling the analyst to review enriched data and prioritize response.

Adversary Infrastructure Correlation

What it solves: Security teams often investigate indicators in isolation and lack visibility into the broader infrastructure supporting an attack. This prevents analysts from identifying related assets, understanding campaign scope, and disrupting adversary operations effectively.

How it works: Vertex queries Censys from an IOC, returning correlated hosts, certificates, and ASNs that Vertex uses to map and visualize adversary infrastructure relationships.

Historical Threat Analysis

What it solves: Without historical Internet visibility, SOC and IR teams cannot trace how attacker infrastructure changes over time, limiting root-cause analysis, retrospective investigations, and proactive threat hunting.

How it works: Vertex queries Censys historical data associated with a given asset or certificate. Censys returns time-based changes in services, ownership, hosting, and exposure. Vertex presents this data to analysts, allowing them to track infrastructure evolution, identify reuse patterns, and correlate current activity with prior campaigns – supporting both incident response and proactive hunting workflows.

Request a demo
Contact Censys or The Vertex Project for a joint solution demonstration

Key Business Outcomes

- Reduced Mean Time to Triage (MTTT)
- Faster Incident Response
- Improved Threat Prioritization
- Expanded Threat Visibility
- Lower Operational Overhead

Technical Integration Highlights

Data Exchange
Threat infrastructure intelligence enriches alerts and entities within Vertex

Investigation Enablement
Analysts can discover, pivot and visualize related adversarial infrastructure

Architecture
Cloud-native, agentless SaaS integration compatible with hybrid environments and cloud SOC environments

Deployment and Integration Model

- Cloud-based SaaS integration
- API-enabled access to Censys intelligence
- Initial integration in days provides immediate enrichment once configured

"At The Vertex Project, we're focused on empowering analysts to move faster and make smarter decisions. Our integration with Censys brings rich Internet intelligence directly into Synapse, enabling analysts to enrich, correlate, and act on data seamlessly within their workflows."

Visi Stark
Co-Founder of The Vertex Project

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.