JOINT SOLUTION BRIEF

See Further, Investigate Faster: Censys Internet Intelligence Delivered Through ServiceNow TISC

Summary

Effective threat investigation requires deep infrastructure intelligence at the point of analysis. The Censys integration for ServiceNow Threat Intelligence Security Center (TISC) delivers exactly that. Censys continuously scans the entire public internet providing rich context on open ports, software versions, certificate relationships, and historical changes. That intelligence is now surfaced directly inside ServiceNow TISC, automatically enriching observables, enabling live rescans, and powering threat actor infrastructure mapping through CensEye, all within the analyst's native ServiceNow workflow.

The result is richer context on every observable enabling faster investigations as analysts pivot from a single indicator to related infrastructure without switching tools, and reduced risk as automated enrichment ensures no observable goes unanalyzed regardless of alert volume or team capacity.

Joint Solution Overview

Censys scans the entire public internet daily, including ports, services, certificates, software versions, and infrastructure history across billions of IPs and domains. CensEye extends that by automatically pivoting from a single indicator to the broader cluster of assets an adversary is running, using shared fingerprints, certificates, and hosting patterns to connect the dots.

ServiceNow TISC is where that intelligence needs to land. It's the investigation platform SOC and CTI teams live in to track indicators, run workflows, and coordinate response. The Censys integration puts enrichment, rescans, host history, and CensEye pivots directly inside TISC, so analysts get the context they need without breaking their workflow to go find it.

Customer Challenges

The threat landscape doesn't stand still. Adversaries reuse infrastructure, the same TLS certificates, hosting providers, and ASN patterns appear across campaigns, but spotting those connections requires internet-scale visibility that most teams don't have at their fingertips. Add cloud sprawl into the mix and the attack surface your team mapped last quarter may look completely different today.

When an indicator lands in your queue, context is everything. An IP address without port data, service banners, or certificate history is just a number. Determining whether it's a known C2, a misconfigured asset, or part of a larger campaign requires the kind of infrastructure detail that typically lives outside the investigation platform which can cause analysts to either skip it or go looking elsewhere.

Volume makes it worse. Alert queues grow faster than teams can manually look things up. Every tool context-switch burns time and attention. And when enrichment depends on an analyst having the bandwidth to run a separate query, it simply doesn't happen consistently which can cause gaps in coverage that adversaries can move through undetected.

Use Cases

Know what you're looking at before you start.

Observables are enriched automatically, or on demand, with real-time Censys data covering ports, services, certificates, and geolocation.

Always work from current data.

Trigger a live rescan on any host or web property to pull current infrastructure state, not whatever was cached last time.

Reconstruct what happened and when.

Pull full host history for any IP - a timestamped record of what services appeared, changed, or went dark to reconstruct timelines and spot infrastructure reuse.

Investigate any indicator, immediately.

Look up any IP, domain, or certificate hash on the spot, even if it isn't in TISC yet. The result lands in the Threat Intel Library automatically.

Turn one indicator into a campaign map.

Run a CensEye pivot to go from one indicator to the full cluster of adversary infrastructure sharing the same fingerprints, certificates, or hosting patterns.

Why This Joint Solution Matters

Most threat intel teams aren't short on data. They are short on time. Analysts juggle alert queues, investigation backlogs, and tool sprawl, and the infrastructure context they need to make good decisions often lives somewhere they have to go looking for it. This integration changes that. Censys internet intelligence surfaces inside ServiceNow TISC automatically, so by the time an analyst opens an observable, the work of figuring out what it is has already happened. That means faster investigations, fewer dead ends, and the ability to connect a single suspicious IP to a broader campaign without leaving the platform or breaking stride.

Get Started

Contact Censys

Key Business Outcomes

Enrichment at scale. Observables are enriched automatically with no manual lookups, no backlog allowing analysts to spend time on analysis, no data gathering.

Faster time to verdict. Ports, services, certificates, and history surface at the point of investigation, not after a trip to another tool.

Infrastructure-level attribution. CensEye connects a single indicator to the broader adversary cluster, surfacing patterns no individual observable would reveal.

Current infrastructure state. On-demand rescans mean analysts are always working from live data, not a cached snapshot from last week.

One workflow, not five. Enrichment, history, and pivot activity all run through TISC. Less context-switching, fewer gaps.

censys

VISIT
censys.com

CONTACT
hello@censys.com