

# Integrated IoC Context for Faster, Higher-Confidence Threat Response with Censys and Feedly

## Summary

Security leaders are asked to act on threat intelligence that ages by the hour. A report names an IP address, but adversary infrastructure is torn down, reassigned, or rebuilt faster than reporting can keep pace. A block based on stale data creates false positives and burns analyst time.

Feedly, the AI platform CTI teams use to track threats, contextualize what matters, and deliver tailored intel in minutes, consolidates open web reporting on each indicator of compromise (IoC). Censys, the authority for Internet intelligence, supplies the ground truth: what that host looks like right now. One click from a Feedly IoC Insights Card opens the live Censys host record, with last scan time, open ports and services, certificates, network ownership, and CVEs. The result: faster IoC triage, higher-confidence decisions with fewer false positives, and a direct path from one reported host to the rest of an adversary's infrastructure.

## Customer Challenges

- ✦ **Strategic:** CTI programs are measured on decisions, not report volume. Leaders need intelligence they can act on with confidence, which means validating every indicator against reality before the organization commits to a response.
- ✦ **Security:** Reporting is a snapshot. By the time a team acts on a reported IP, the infrastructure may be gone or reassigned to an unrelated tenant. Blocking it creates false positives. Acting late on live infrastructure leaves exposure open.
- ✦ **Operational:** CTI teams research hundreds of IoCs, and each one needs context before anyone can act. Manually looking up each IP in Censys adds steps, slows research, and pulls analysts away from analysis.

## Key Business Outcomes

-  **Faster IoC triage.** Open in Censys replaces copying and pasting an IoC into Censys. One click from an IoC Insights Card opens the host lookup page. No Censys account is needed to view it.
-  **Higher-confidence response.** Know whether a host is still up before you block it. Prioritize with evidence, not assumption, and avoid false positives.
-  **More context per click.** See where the host is and what it's running, plus the details open web reporting can leave out: ports, TLS certificates, ASN, hosting provider, and CVEs.
-  **Wider view of the adversary.** Pivot from one reported host to related infrastructure using shared certificates, service combinations, and fingerprints.

## Joint Solution Overview

Feedly and Censys each answer half of the question a CTI team asks about every indicator. Feedly consolidates open web reporting in IoC Insights Cards: who reported an IoC, what it has been linked to, and which threat actors and malware families it connects to. Feedly is trusted by 380+ CTI teams, including half of the Fortune 10. On the other side, Censys supplies the ground truth. The Censys Internet Map is first-party observation of hosts, services, and certificates, with known services rescanned daily. Its host record shows when the IP was last scanned, which ports and services answered, who owns the netblock, and which other hosts share its certificates. Governments, over 50% of the Fortune 500, and leading threat intelligence providers rely on Censys for that view.

Together, they put intelligence and ground truth in a single research workflow. Analysts select Open in Censys from any IoC Insights Card, or from the IoC table on Threat Actor and Malware Insights Cards, and move from what the world is saying about an IP address to what is true about that host today. CISOs and CTI Directors get defensible, evidence-backed decisions. SOC Directors get fewer false-positive blocks and faster triage. CTI analysts get Censys host context without leaving their workflow.

### Architecture Diagram

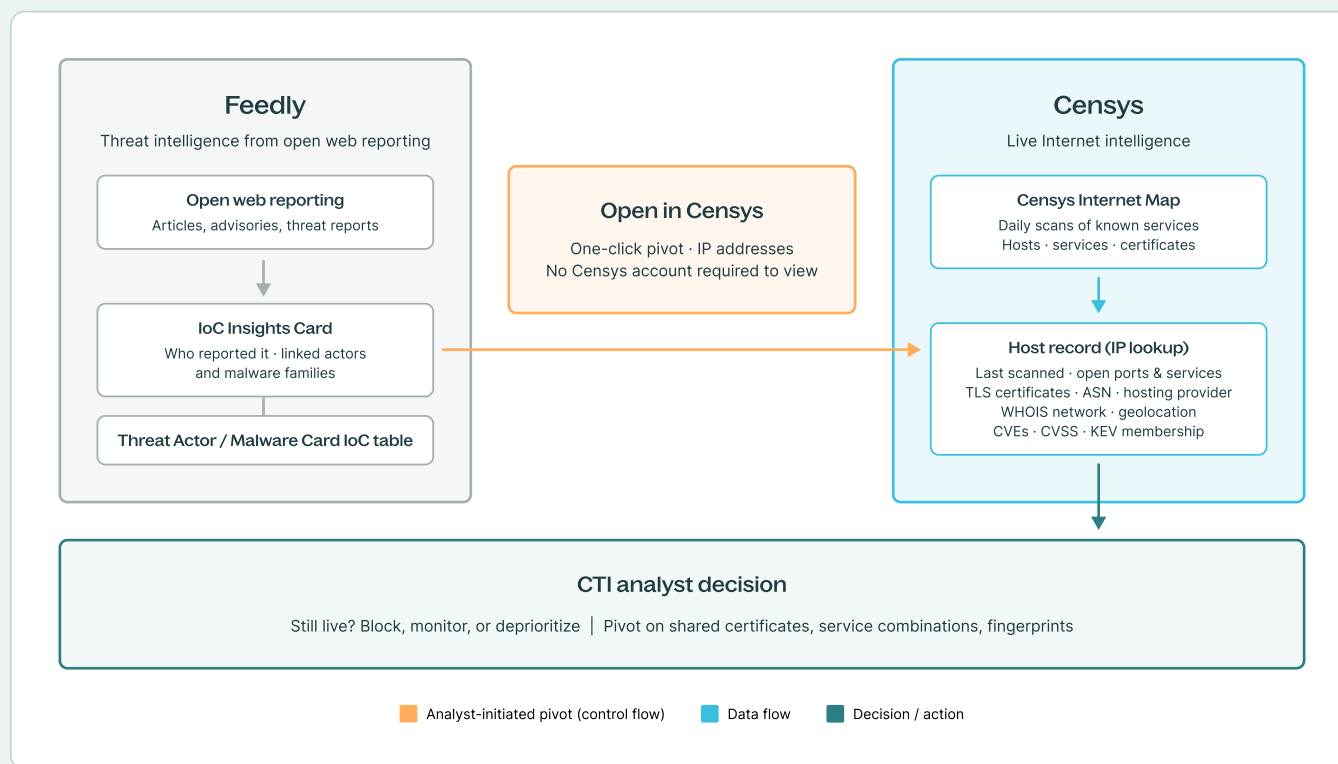


Fig. 1 Open in Censys pivot from Feedly IoC context to live Censys host data.

## Common Use Cases

### Validate and size up a reported IP

A report names an IP, and before anyone acts, the team needs to know whether the host is still up and what kind of host it is. Feedly's IoC Insights Card shows who reported the IP and which threat actors and malware families it connects to. From there, the analyst opens the IP in Censys, which shows the host as it is today: when it was last scanned, which ports and services answered, TLS certificates, ASN, hosting provider, and WHOIS network, with a geolocation map alongside. The CVEs tab adds a count badge, plus CVSS scores and KEV catalog membership when CVEs are present. Teams can then block live infrastructure, skip dead or reassigned IPs, and respond to what the host actually is.

**Workflow:** IoC Insights Card in Feedly → Open in Censys  
→ host record (last scan, ports and services, certificates, hosting, CVEs) → block, monitor, or deprioritize.

### Find the rest of the adversary's infrastructure

A report lists one host, but the adversary may have built more. Feedly shows which threat actor or malware family the IP connects to, giving the analyst the context for the hunt. In Censys, the analyst can then pivot on shared certificates, service combinations, or fingerprints to surface related hosts before the next report does.

**Workflow:** IoC Insights Card (linked actor or malware family)  
→ Open in Censys → pivot on shared certificates, service combinations, or fingerprints → related hosts for your hunt or blocklist workflow.

### Work through a threat actor's or malware family's IoCs

A threat actor or malware family can list many IoCs, and analysts need to decide which hosts to look at first. Feedly sorts the IoC table by the number of articles that mention each IoC, so the higher-volume indicators rise to the top. Analysts open those IPs in Censys first and validate each host one by one, putting their time where reporting is heaviest.

**Workflow:** Threat Actor or Malware Insights Card  
→ sort IoC table by article count → Open in Censys for the top IPs → validate each host one by one.

## Why This Joint Solution Matters

Threat intelligence is only as valuable as the confidence behind the action it drives. Feedly and Censys put both halves of that equation one click apart: what the world is reporting about an indicator, and what is true about that host right now. For security leaders, that means evidence-backed response decisions, fewer false-positive blocks, and CTI teams that spend their time on analysis instead of manual lookups. For practitioners, it means a faster path from a reported IP to a verified answer, plus pivots on shared certificates, service combinations, and fingerprints that expose the rest of an adversary's infrastructure. Feedly consolidates open web reporting, taking you from signals to tailored threat intelligence in minutes. Censys shows the host as it is today.

## Learn More

Contact Censys at [technologyalliance@censys.com](mailto:technologyalliance@censys.com) to learn more about how to integrate IoC context for faster, higher-confidence threat response.



VISIT  
[censys.com](https://censys.com) ➤

CONTACT  
[hello@censys.com](mailto: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.