censys

Censys Platform and Torq: First-Party Internet Context for Your AI SOC

Censys gives Torq's AI SOC a current, first-party view of any host, domain, certificate, or web property on the public Internet, so every alert starts with evidence instead of a manual lookup.

CUSTOMER CHALLENGES

An alert fires on an IP address. Before anyone can act, an analyst has to find out what it is. They check what's running on it, who owns it, whether it's known bad, what it resolved to last week, and whether it's part of something larger. Answering that usually means four or five tools, four or five API keys, and a lot of tab-switching.

Most teams can't afford to enrich every alert, so context arrives late, on a fraction of events, and often after the ticket is already closed. Adversaries rotate infrastructure faster than a manual workflow can follow. An AI SOC is only as good as the context it reasons on. If that context is thin, stale, or metered, automation just moves the guesswork faster.

JOINT SOLUTION OVERVIEW

Censys scans the public Internet itself, continuously and across all ports, and adds active DNS resolution on top. Torq turns that data into automated triage, investigation, and response, so Censys context is in the case before an analyst opens it.

Enrich Every Alert

Every IP in a Torq case can carry ownership, open services, threat labels, and a Reputation Score with the evidence behind it, without rationing lookups.

Detect Adversary Infrastructure

Save any Censys query as a Collection, like a C2 framework, a phishing kit, or your own assets. Torq acts as soon as a new match appears.

Investigate to Full Scope

Pivot from one indicator into an adversary's wider infrastructure. Reconstruct what any host, certificate, or domain looked like on the day of an incident.

VALUE

Context on every alert, not a sample. With credit-free host enrichment, Torq can enrich raw events upstream of detection, not only the alerts that get through.

One call instead of five. Ownership, DNS, services, named threats, reputation, and third-party signals such as GreyNoise, IPinfo, and VPN/proxy/Tor detection all arrive in a single Censys response. That means fewer integrations to maintain in every playbook.

Tickets that close on the whole problem. Pivots expand one confirmed indicator into the rest of the adversary's infrastructure, so analysts can avoid closing a ticket on one IP while others stay live.

Verdicts an agent can defend. Censys Reputation Scores return a label (Benign, Suspicious, Malicious, Honeypot, or Inactive) with a ranked evidence array. Torq's AI can explain every automated decision instead of relying on an opaque score.

Detections you define. Any Censys query can become a Torq trigger, which turns Censys into a bespoke threat feed built around your own threat model.

Fixes that are verified. A live rescan confirms an exposure is closed or a threat is gone before the case is marked resolved.

USE CASES

Triage

Know what you're looking at, quickly.

When an alert fires, Torq enriches every IP in the case through the Censys Enrichment API. The response covers geolocation, ASN and WHOIS ownership, forward and reverse DNS, open ports and protocols, named threats such as C2 frameworks and infostealers, and a Reputation Score with its evidence. Domains and certificates in the case can be looked up through Censys as well. The case then opens with context and a verdict the analyst or the agent can act on.

Threat Hunt and Detection Engineering

Track your adversaries, watch your own assets, and build your own feeds.

Censys Collections turn any query into a continuous detection. A threat intel team can track every host running Cobalt Strike, a specific phishing kit, or a JARM fingerprint tied to an actor. A SOC can monitor its own known infrastructure for new services or certificates. A brand team can track lookalike domains and web properties that copy its pages. Censys returns full HTML bodies, redirect chains, detected technologies, and screenshots, so Torq's AI can assess whether a lookalike is actually a phishing page. Each new match can open a Torq case.

Investigate

Go from one indicator to the whole campaign.

Censys stores time-stamped history for hosts, services, certificates, DNS, and web properties. Torq's AI can answer "what was this on the day of the incident?" directly from structured data. Censys pivots on shared attributes, such as TLS certificates and JARM fingerprints, to surface related infrastructure. Torq then hunts for those related indicators across endpoints and logs.

Respond

Act, verify, and remember.

Torq runs the response across your security tools. Censys then performs a live rescan of the host or web property to confirm the threat is no longer active. Torq writes tags back to the host, certificate, or web property in your Censys organization, so the assessment persists across future investigations.

KEY BUSINESS OUTCOMES

Enrichment at volume.

Credit-free host enrichment sized for automation.

Faster triage.

Cases open with context already attached.

Defensible automation.

Every verdict carries its evidence.

Earlier detection.

New adversary infrastructure triggers Torq workflows as soon as Censys identifies it.

Complete scoping.

Pivots and history reveal the full campaign.

Persistent knowledge.

Assessments are tagged back to the asset in Censys.

LEARN MORE

Contact technologyalliance@censys.com to learn how Censys and Torq together give your AI SOC first-party Internet context at every stage of a case.

censys

VISIT
censys.com

CONTACT
hello@censys.com

Censys is the authority in Internet intelligence and insights. Delivering the most comprehensive, accurate, and up-to-date global map of Internet infrastructure, Censys provides the real-time external visibility organizations need to accelerate security operations, investigate threats, and understand Internet exposure. Global governments, Fortune 500 companies, and security providers trust Censys to uncover risks faster and respond more effectively.