

Threat Hunting with Censys

Track Adversary Infrastructure + Uncover Hidden Threats

Intelligence That Moves Security Teams from Reactive to Proactive

The Censys Threat Hunting Module empowers security teams to shift from reacting to alerts to actively uncovering and mitigating threats before they can cause harm. By combining live scanning and enriched historical context, it enables faster, more precise investigations. Security teams can reduce investigation times from hours to minutes, gain deeper insights into adversary tactics, and take proactive steps to eliminate threats before they impact their organization. Threat Hunters no longer have to rely on fragmented visibility or reactive security measures. Instead, they can hunt with confidence, armed with the most comprehensive view of adversary infrastructure across the global Internet.



Censys for Threat Hunting Differentiators

The Feature	Why It Matters
Censys Threats Dataset	Censys threat dataset provides a real-time view of adversarial infrastructure, providing detections for known red team tools (including custom scanners for cobalt strike), fingerprints based on management techniques and patterns used by threat actors, and detections based on URL endpoints associated with generic malware operations. The threat dataset also offers extended context on threats such as descriptions, alternative names, actors, campaigns, and reference links.
CensEye	CensEye helps threat hunters to quickly identify and correlate malicious infrastructure by detecting hosts and web properties with similar characteristics. This advanced pivoting capability accelerates investigations, allowing analysts to uncover high-value adversary assets and track evolving threats faster and with better precision.
Live Discovery and Live Rescan	Achieve real-time threat detection and validation with on-demand scanning capabilities. Live Discovery exposes previously unknown configurations, while Live Rescan systematically analyzes existing services and endpoints to confirm potential threats and track configuration drift. This ensures continuous monitoring and empowers rapid response to emerging security anomalies.
Exploration Dashboards	Interactive dashboards offer visibility into threat infrastructure, allowing hunters to explore data and trends, uncover anomalies, and jump start investigations effectively.
Certificate and Host History Visualization	Explore historical relationships between hosts and certificates to build weaponization timelines, uncover TTPs, and unlock historical attributes to use in detections.
Advanced Pivoting and Contextual Hashes	Streamline threat investigations by enabling seamless pivoting across hosts, certificates, and historical data. Threat Hunters can quickly expand their search, surface related indicators and helpful configuration-based hashes such as TLSH, JARM, JA3, JA4+ to build a comprehensive view of an adversary's operations.

Key Outcomes

Proactively Identify Adversary Infrastructure

The Censys Threat Hunting Module proactively identifies and tracks adversary infrastructure, including C2 servers, using proprietary scanning and behavioral analytics. This enriched intelligence empowers threat hunters to uncover evolving threats, expand IOCs, and enhance incident response efficiency.

Accelerated Investigations + Threat Correlation

By streamlining investigations with powerful pivoting, rare term detection, and real-time scanning, Censys reduces the time needed to identify and analyze malicious infrastructure. This efficiency allows security teams to prioritize high-risk threats and act faster to mitigate adversary activity.

Build More Accurate Detections

Powered by the Censys Internet Map, the Threat Hunting module automates manual processes and surfaces critical threat context from parsed fields and contextual hashes like JARM, JA3, JA4+, and more. These enhancements provide stronger insights into our data and help threat hunters to build more accurate detections to better track specific APTs and improve their overall operational efficiency.



VISIT
censys.com ➤

CONTACT
hello@censys.com ➤

Censys' mission is to be the one place to understand everything on the internet. Frustrated by the lack of trustworthy Internet intelligence, we set out to create the industry's most comprehensive, accurate, and up-to-date map of the Internet. Today, Censys delivers real-time Internet intelligence and actionable threat insights to global governments, over 50% of the Fortune 500, and leading threat intelligence providers worldwide.