SOLUTION BRIEF

Accelerate SOC Investigation with Censys and Microsoft Sentinel

Modern Security Operations Centers (SOCs) are challenged by two related problems - keeping pace with a constantly shifting external footprint and quickly understanding unfamiliar internet infrastructure during investigations. As cloud services, third-party dependencies, and rapid deployment cycles expand what is exposed, organizations need a reliable way to validate external assets, detect exposure changes, and confirm remediation. At the same time, SOC analysts need faster context on suspicious IPs, domains, and certificates without relying on slow, manual enrichment. Together, Censys and Microsoft Sentinel unify these workflows by bringing authoritative internet intelligence directly into the SOC to improve external exposure governance while enabling faster, higher-confidence triage and investigation.

Customer Challenges

Attack Surface Management (ASM) Challenges

- **Visibility Gaps:** Incomplete inventory of internet-facing IPs/domains/certificates and exposed services.
- **Change & Drift:** Cloud-native change introduces new exposures and misconfigurations.
- **Verification Delays:** Difficulty confirming externally whether vulnerabilities/config changes are truly remediated.

SOC / External Threat Investigation Challenges

- **Unknown External Infrastructure:** Alerts reference external IPs/domains/certs with limited context for triage.
- **Operational Drag:** "Swivel-chair" workflows across multiple tools slow investigations.
- **Time-Variant Evidence:** Infrastructure state changes over time; current view may not match incident-time reality.

Joint Solution Overview

Censys and Microsoft Sentinel combine Censys Internet intelligence with Sentinel's cloud-native SIEM/SOAR workflows to support both attack surface monitoring and SOC investigation. The integration brings Censys ASM risk and logbook events into Sentinel and enriches investigations with Censys Platform context on internet-facing hosts, services, certificates, and historical infrastructure observations.

Key Business Outcomes

- **Improve Visibility into External Asset Changes** with Censys ASM logbook events in Microsoft Sentinel.
- **Faster Investigation and Remediation of Internet-Exposed Risk** with Censys ASM risk events surfaced directly as alerts within Sentinel.
- **Accelerate SOC Triage and Investigation** with external context from the Censys Platform that helps analysts validate risk, investigate unfamiliar infrastructure, and make faster decisions.
- **Improve Incident-Time Investigation Accuracy** with historical context from the Censys Platform that helps analysts understand how infrastructure appeared at the time of compromise.

Buyer Personas

ASM

- CISO
- Security Engineering Director
- Vulnerability Management Lead
- Exposure Management Lead

SOC

- SOC Director
- Incident Response Lead
- Threat Intelligence Lead

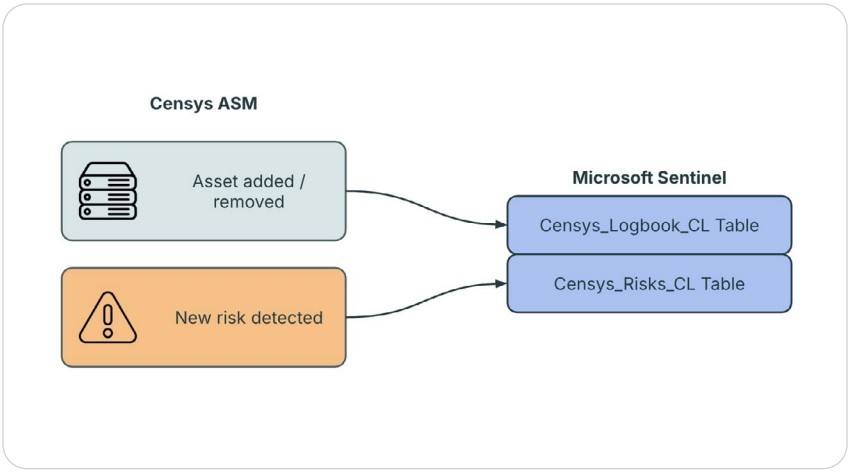

Fig. 1 Depicts the flow of Censys ASM data, including risk and logbook events, into Microsoft Sentinel to provide unified visibility and actionability on external attack surface changes.

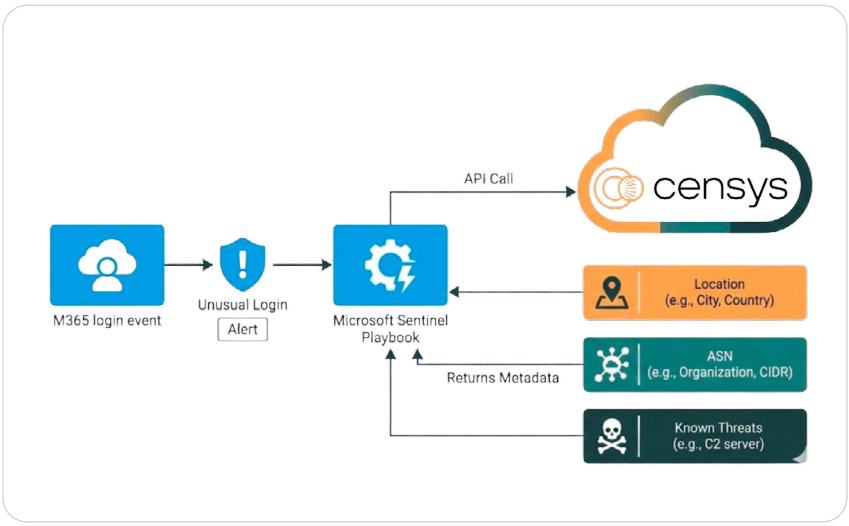

Fig. 2 Depicts the flow of external context from the Censys Platform, including host, service, certificate, and historical data, into Microsoft Sentinel to enrich alerts and accelerate triage and incident response.

Request a Demo

See how Censys and Microsoft Sentinel improves visibility and accelerates SOC investigation.

Contact Censys

ASM Use Cases

Prioritize Internet-Exposed Risk in Sentinel

Ingest Censys ASM risk events into Microsoft Sentinel to alert analysts of meaningful exposure changes, enabling faster identification, triage, and remediation.

Monitor External Asset Changes in Sentinel

Bring Censys ASM logbook events into Microsoft Sentinel to detect when internet-facing assets appear, disappear, or change, strengthening visibility into the external attack surface.

SOC Use Cases

Automated Enrichment for External Infrastructure

Enrich alerts with context on IPs, domains, certificates, ports, and services to speed triage and reduce manual investigation.

Historical Context for Incident Analysis

Review historical observations to understand how infrastructure appeared at the time of compromise and improve investigative accuracy.

Pivoting Across Related Infrastructure

Pivot from a single indicator to related hosts, services, and certificates to expand scope and uncover connected infrastructure faster.

Summary

Censys and Microsoft Sentinel deliver authoritative internet intelligence directly inside Sentinel to support two operational needs: for ASM, it improves visibility and governance of external exposure, detects drift, and validates remediation; for SOC, it accelerates investigations of unknown external infrastructure through automated enrichment, historical context, and rapid pivoting.

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.