SOLUTION BRIEF

Integrated External Exposure Monitoring, Enrichment, and Response with Censys and Google SecOps

Joint Solution Overview

Internet-facing infrastructure changes faster than most security teams can manually track, yet SOC analysts are still expected to validate exposures, prioritize risk, and confirm remediation before attackers can exploit new openings. The challenge is that exposure monitoring, enrichment, and response validation are often split across separate consoles and teams. Censys and Google SecOps address that gap through two complementary integrations.

Censys ASM tracks internet-facing assets, associated risks, and change activity across the external attack surface. Censys Platform adds deep intelligence on hosts, web properties, certificates, services, protocols, historical changes, and targeted rescanning. Google SecOps SIEM centralizes ingestion, search, detection, and operational monitoring, while Google SecOps SOAR coordinates cases, analyst actions, and playbook-driven response. Together, the integrations create a unified operating model: Censys ASM feeds exposure signals into Google SecOps SIEM, and Censys Platform enables analysts to enrich entities, review host history, and validate remediation in Google SecOps SOAR.

Censys ASM + Censys Platform integrate with Google SecOps SIEM and SOAR

Monitor in SIEM
Censys ASM feeds risk and asset events into Google SecOps SIEM.

Investigate in SOAR
Censys Platform enriches IPs, web properties, certificates, and host history in Google SecOps SOAR.

Validate Response
Targeted rescans help teams confirm current state and remediation closure.

Customer Challenges

- Digital transformation, cloud growth, and hybrid infrastructure create a constantly shifting inventory of internet-facing assets.
- Exposure-related risk changes may not reach the SOC quickly enough, while alerts tied to IPs, hosts, or certificates often lack actionable context.
- Separate attack surface, SIEM, and response tools force manual pivots, inconsistent investigations, and slower remediation validation.
- Security teams need a scalable way to operationalize attack surface change events and standardize enrichment and response workflows.

Key Business Outcomes

Continuous external visibility
Risk and asset events from Censys ASM become visible in Google SecOps alongside broader detections and monitoring workflows.

Faster triage and prioritization
Analysts can search and filter high-severity exposure events, then enrich IPs, web properties, and certificates without leaving Google SecOps.

Higher response confidence
Targeted rescans and host history help teams determine current state, understand change over time, and verify that remediation actually succeeded.

Lower operational overhead
Supported event pipelines and prebuilt playbooks reduce manual exports, swivel-chair investigations, and bespoke integration work.

Better alignment across teams
Exposure management and SOC teams share a common operating model that links monitoring, investigation, and response validation.

User and Buyer Personas

- CISOs
- SOC Leaders
- Incident Responders
- Exposure Management Teams
- Cloud Security Leaders
- Network Security Engineers
- Vulnerability Analysts
- Security Architects

Use Cases

Continuous monitoring of external exposure in Google SecOps

When SOC teams need to continuously monitor external exposure without relying on a separate exposure management queue, Censys ASM risk and logbook events can be ingested directly into Google SecOps SIEM, allowing analysts to track attack surface asset and risk events within their existing workflows using familiar searches, dashboards, and hunt workflows, and to quickly isolate high-priority issues such as policy violations or newly associated assets by querying fields like product name, category, and severity.

Alert enrichment for internet-facing assets

When a security alert arrives with only an IP, hostname, or certificate identifier and little infrastructure context for triage, Google SecOps SOAR can automatically call Censys Platform enrichment actions such as Enrich IPs, Enrich Web Properties, or Enrich Certificates and record the results directly in the case workflow, allowing analysts to quickly determine whether the entity is internet-facing, identify associated services and certificates, and prioritize response with greater speed and confidence.

Remediation validation and current-state confirmation

When a team needs to verify that an exposed service or misconfiguration was truly remediated rather than simply closed in a ticket, Google SecOps SOAR allows responders to validate the current exposure state on demand by initiating a rescan for a host, service, or web property, polling for rescan status, and using the result to confirm remediation closure or continue the investigation if the fix did not persist.

Time-aware investigation of infrastructure change

When teams need to determine whether an exposure is new, recurring, or linked to a recent infrastructure change, Google SecOps SIEM and SOAR work together to provide both real-time change monitoring and deeper historical context. Analysts can review ASM logbook events in Google SecOps SIEM, then use Censys Platform Host History in Google SecOps SOAR to investigate service appearance, certificate changes, and infrastructure drift over time, helping them assess urgency more accurately.

Standardized exposure-to-response workflows

When exposure management and SOC operations rely on separate tools, handoffs often become ad hoc and inconsistent. By connecting Google SecOps SIEM and SOAR with Censys Platform, organizations can create repeatable, auditable workflows that move from monitoring to enrichment, validation, and escalation, with SIEM detections or analyst review triggering a SOAR case, prebuilt playbooks enriching entities, retrieving host history, and initiating rescans, and all outputs captured on the case wall for shared visibility.

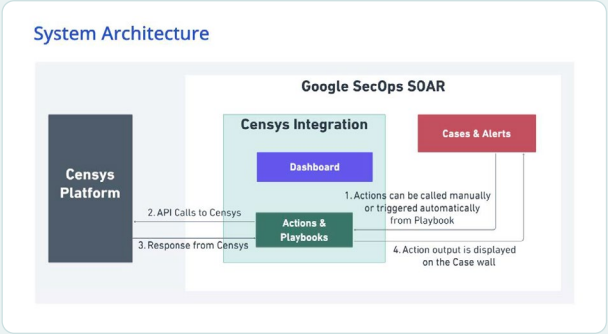

Fig. 1 Censys SOC Workflow Integration for Google SecOps

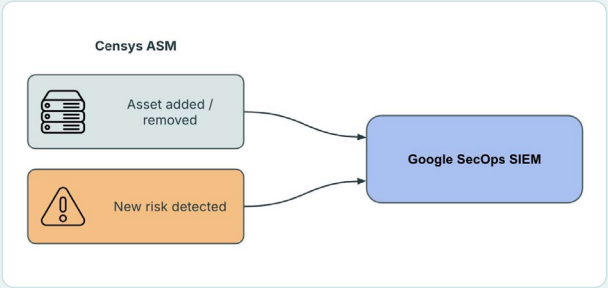

Fig. 2 Censys ASM sends asset and risk events into Google SecOps SIEM for faster response.

Why This Joint Solution Matters

This joint solution is valuable because it unifies external exposure monitoring and analyst response within a single Google SecOps operating model, helping teams move faster from detection to action with greater consistency and less operational friction. Censys ASM makes attack surface changes and risk events visible in Google SecOps SIEM, while Censys Platform equips Google SecOps SOAR with the enrichment, history, and validation actions needed to investigate and respond quickly. Together, the integrations support SOC transformation, attack surface reduction, and cloud security governance while differentiating the joint offer from point solutions that stop at reporting or require manual pivots between monitoring and response.

Request a Demo

Contact Censys for a joint solution demonstration

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.