SOLUTION BRIEF

Modernize SOC Investigation with Censys, Splunk ES, and Splunk SOAR

As digital estates grow and Internet-facing infrastructure evolves quickly, Security Operation Center (SOC) teams are under pressure to modernize investigations and respond despite high alert volumes, tool sprawl, and limited analyst resources. Manual enrichment and gaps in external visibility can slow triage, complicate scoping, and make consistent response more difficult. Censys strengthens Splunk ES and Splunk SOAR with Internet intelligence, exposed asset context, and attack surface change visibility, helping teams validate exposure, investigate with greater confidence, and automate response with more speed and consistency.

Customer Challenges

- High volumes of notable events can slow triage, consume analyst's time, and make it harder to quickly validate exposure and prioritize the alerts that require immediate attention.
- When analysts cannot quickly pivot from a single IOC to related infrastructure, services, or certificates, it becomes harder to assess scope, investigate unfamiliar indicators, and make confident response decisions.
- Limited visibility into changing internet-facing assets, services, and certificates leaves exposures and vulnerabilities open for attackers to exploit. If this visibility is not connected into the broader security ecosystem, MTTD and MTTR are both reduced.

Joint Solution Overview

Censys supports Splunk-based SOC operations in three distinct ways, each designed for a different stage of investigation and response. Together, these integrations allow Splunk users to combine automated enrichment, broader Internet intelligence, and attack surface change visibility to modernize investigation and response workflows.

Censys Platform + Splunk Enterprise Security (ES)
Brings Internet intelligence into the SIEM workflow so analysts can investigate indicators, validate exposure, pivot across related infrastructure, and scope threats faster.

Censys Platform + Splunk SOAR
Automates repeatable enrichment and response actions using Censys context on hosts, services, certificates, and related infrastructure to reduce manual effort and improve consistency.

Censys ASM for Splunk Platform
Connects comprehensive external attack surface visibility into your alerting, correlation, and reporting workflows in Splunk, allowing for automated workflows and a faster, more consistent response.

Key Business Outcomes

Faster, more confident triage in Splunk ES
External context on assets, services, certificates, and infrastructure relationships helps analysts validate exposure, assess severity, and prioritize investigations with greater confidence.

Stronger visibility into evolving external risk
Awareness of newly exposed assets and changes to internet-facing services or certificates helps teams better understand shifting attack surface risk and make more informed prioritization and response decisions.

More efficient and consistent response with SOAR
Automated enrichment and response workflows reduce manual effort, improve consistency, and help SOC teams scale investigations more effectively.

Primary User Personas

Censys + Splunk Enterprise Security
SOC Manager
SIEM Owner
Security Engineer
Detection Engineer
Threat Hunter
Threat Intelligence Analyst

Censys + Splunk SOAR
SOAR Owner
Security Automation Lead
Incident Response Lead
SOC Manager

Censys ASM
Network Security Engineer
Vulnerability Analyst

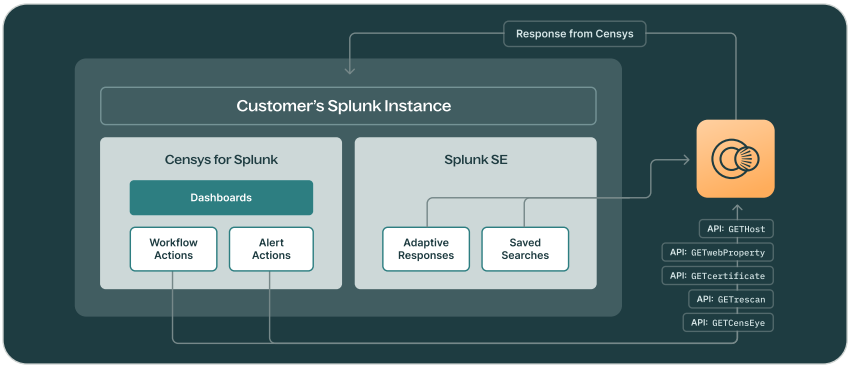

Fig. 1 Censys SOC Workflow Integration for Splunk Platform

Splunkbase Marketplace

- Censys Platform for Splunk SOAR
- Censys Platform for Splunk Enterprise Security (ES)
- Censys ASM Add-on for Splunk Platform
- Censys ASM for Splunk Platform

Use Cases

IOC enrichment and triage in Splunk ES

External context on IPs, domains, certificates, services, and related infrastructure enriches notable events in Splunk ES, helping analysts validate exposure, assess severity, and prioritize investigations faster.

Automated enrichment and response in Splunk SOAR

Automated enrichment and response workflows in Splunk SOAR apply Censys context on hosts, services, certificates, and infrastructure relationships to reduce manual effort, improve consistency, and accelerate investigations.

Attack surface change investigation and response with ASM in Splunk SOAR

Attack surface visibility and change-based context from Censys ASM strengthen automated workflows in Splunk SOAR, helping teams identify newly exposed assets, track external changes over time, and respond more consistently as Internet-facing risk evolves.

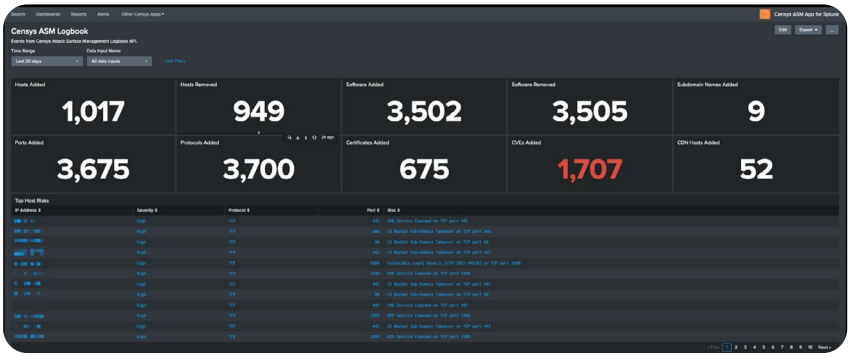

Fig. 2 Censys ASM Logbook dashboard in Splunk, showing 30-day trends in hosts, services, certificates, and CVEs added or removed to help analysts monitor external exposure changes and prioritize risk.

Request a Demo

See how Censys extends Splunk ES and Splunk SOAR with external context that improves triage, reduces manual enrichment, and supports more consistent response.

Contact Censys

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.