

Rule every threat with Cloud SIEM

Results at a glance

- Reduced alert fatigue and false positives
- Ramped up quickly and learned the ins and outs of the platform
- Gained speed and efficiency in responding to critical issues
- Optimized cyber situational awareness

Roku

SUMO LOGIC SOLUTION

Cloud SIEM

USE CASE

Modernizing Security Ops

Challenge

When adopting a SIEM solution, Roku needed to avoid alert fatigue and stay agile to quickly address true issues.

Maintaining a strong security posture is essential for Roku. “Our security team works day and night to protect the infrastructure and provide a reliable service for our customers. Our customers and their trust are important for us,” shared Huseyin Karaarslan, Sr. Security Engineer at Roku.

As an important part of this strategy, Roku wanted to adopt a SIEM solution to gain cyber situational awareness and an ongoing picture of the company’s environment.

Solution

For its cyber situational awareness, Roku wanted rapid and accurate insights into their domain to understand what’s happening and to ensure active responders could make quick, accurate decisions. This requires an investment in data collection and analysis to maintain a continuous picture of Roku’s infrastructure, and for that, Roku chose Sumo Logic Cloud SIEM.

Results

Optimized situational awareness with rule tuning

Built natively in the cloud, Cloud SIEM makes it fast and easy to gain deep security insights with pre-built applications including out-of-the-box dashboards, queries and rules. With 700+ rules that each map to a tactic and technique related to the MITRE ATT&CK framework, Roku’s security team had a strong starting point for obtaining security insights.

Roku

INDUSTRY

Broadcast media
Consumer electronics

ABOUT

At its start in 2000, Roku pioneered streaming to the TV with its platform that connects viewers, publishers, and advertisers to the vast ecosystem of media content. With its product portfolio of streaming players, TV models, and a channel store, Roku serves millions of customers across North America, Latin America and Europe.

By the numbers

700+

rules out of the box

As a first step, the team embarked on tuning Cloud SIEM rules. “Cloud SIEM’s rules are powerful, and we wanted to tailor them specifically to our organization and infrastructure. Tuning was important for us to familiarize ourselves with the tool, prove value in our investment, and optimize the platform so we could focus on true alarms that require our attention,” commented Karaarslan.

The security team’s tuning process was highly efficient, beginning with using the Sumo Logic platform to write queries to identify the rules that created the highest volume of alerts. From there, Karaarslan created dashboards for the rules to better evaluate the query results. “Because we were working with a thousand or more alerts, the rules analysis dashboards gave us details to see what was going on within our environment and uncover patterns for our tuning exercise,” said Karaarslan.

Through this tuning phase, the security team quickly determined if a rule was working, needed further tuning, or if it no longer applied to the organization. As a result, Roku is experiencing optimized cyber situational awareness with Cloud SIEM that empowers the security team to rapidly identify and act on critical alerts.

[Learn more](#)

SIEM rule tuning to develop cyber situational awareness



[WATCH THE FULL SESSION](#)



“Cloud SIEM’s out-of-the-box rules are powerful. Tuning them for our organization and infrastructure helped familiarize ourselves with the tool, prove value in our investment and optimize the platform so we could focus on true alarms that require our attention.”



Huseyin Karaarslan
Sr. Security Engineer, Roku

