sumo logic

Unified SIEM dashboard automates security investigations

Results at a glance

- → Centralized security visibility across cloud and on-premises infrastructure
- → Seamless integration into existing AWS and Azure services
- → Consolidated 20 separate dashboards into a single-pane view
- → Accelerated investigations with automated alert triage and threat correlations

SUMO LOGIC SOLUTION

Cloud SIEM

Cloud Security Analytics

USE CASE

Application security

Threat detection and investigation

Security automation

ENVIRONMENT

AWS

Azure

sumo

Challenge

Keeping pace with the growing and changing business while defending it from cyber threats was challenging.

To manage cybersecurity for its broad infrastructure, SPS Commerce used a hybrid staffing model that included the internal security operations center (SOC) team and a managed services provider aiding with 24/7 coverage for monitoring alerts.

"It's a bit of a truism that the attackers only have to be successful once while our SOC team has to be successful 100 percent of the time. So, we really needed the visibility and the data to detect and respond to those threats," said Nick Kemske, SOC and Incident Response Manager of SPS Commerce.

INDUSTRY

Application software
Technology

ABOUT

As a leading electronic data interchange (EDI) provider, SPS Commerce has an expansive infrastructure to serve more than 70,000 customers worldwide. It consists of on-premises systems, cloud footprints in AWS and Azure, and a wide range of custom applications and toolsets.

Solution

For visibility across the company's attack surface, SPS Commerce wanted central access to all the data sources to give the SOC team accurate security visibility and insights. This required investment in a SIEM solution.

As part of the SOC team's requirements, they wanted a solution that would give them the added value of seeing the same systems, logs and metrics the rest of the company was gathering to monitor the environment. Sumo Logic was the perfect solution because the infrastructure team already used the platform for their observability use cases.

"When selecting a SIEM, we didn't want to get too far afield and separate from what our infrastructure partners were doing. Expanding the company's Sumo Logic usage to include our SIEM needs gives us better opportunity to collaborate and partner with teams to resolve issues when they come up."

Nick Kemske
SOC and Incident Response Manager, SPS Commerce

Results

Fast implementation and ramp-up to support SOC needs

As the infrastructure team had already deployed the Sumo Logic platform and was collecting the company's logs from infrastructure data sources, the SOC team enjoyed a jumpstart in their adoption effort. Using the platform's cloud collectors made it a turnkey process for the team to integrate additional data sources from their security tools, such as the company's CrowdStrike and Tenable solutions.

"Sumo Logic makes it easy to get started by taking advantage of everything that's pre-built in the application like the out-of-the-box security rule sets," said Kemske, adding that "there's lots of really fantastic documentation about how the overall platform works, so it allowed us to really get up to speed quickly."

Single source for security telemetry and insights

With Sumo Logic ingesting all the desired log data, the solution is now the SOC team's authoritative security data source. "Everything goes into Sumo Logic for our security monitoring. I have a saying on my team, that 'all means all' when you think about security and the importance of monitoring everything," said Kemske.

From switches and routers to AWS and Azure logs, all the telemetry comes together in Sumo Logic for triaging alerts and correlating threats across the company's infrastructure. Based on the data source's use case for security analysis, the SOC team leverages Sumo Logic's flexible data tiering to denote which sources Cloud SIEM should continuously process and analyze.

With integrated threat intelligence feeds, the SOC team leverages Cloud SIEM's more than 700 pre-built rules along with the team's custom rules to obtain enriched and actionable insights. "All that is married together in Cloud SIEM, which then kicks off the investigation workflow for my team. It's really a great and seamless journey," noted Kemske.

Faster investigations with automation and a single-pane view

Before adopting Cloud SIEM, the SOC team's investigation workflow relied on 20 separate system dashboards that required a lengthy, manual effort to weave together a view of the company's entire footprint. With Cloud SIEM in place, the team now has visibility into what's happening in the environment — all from a single console that doesn't require the team to pivot across tools.

"Cloud SIEM has underpinned our shift from a very rote, manual process to one that's much more automated, which has been really helpful in giving us visibility and saving time on our investigations," Kemske explained, adding that "because we can also easily kick off JIRA tickets from Cloud SIEM, we can integrate a lot better with our delivery teams and partners in the way that they expect."

By the numbers

20→1

Consolidated 20 separate dashboards into a single-pane view

Learn more

How SPS commerce uses security insights from Sumo Logic to improve cybersecurity

WATCH THE FULL SESSION

855 Main Street, Redwood City, CA 94603

Learn More
Toll-Free: 1.855.LOG.SUMO | Int'l: 1.650.810.8700

sumologic.com