sumo logic

Boosting customer experience & profits with Cloud SIEM

Results at a glance

- → Improved alert triaging by consolidating from two SIEMs to one
- → Four-month payback with profitability within six months
- → Able to onboard customers in minutes instead of days
- → Doubled customer growth without having to increase security analyst headcount

KOBALT.IO

PRODUCTS

Cloud SIEM

Sumo Logic Platform

USE CASES

Threat detection, investigation and response

SecOps

ENVIRONMENT

Salesforce

Heroku

AWS

KOBALT.IO

INDUSTRY

Managed Security Service Provider (MSSP)

ABOUT

Founded in 2019 on the premise that everybody deserves good security, Kobalt.io develops and manages cybersecurity programs for small and mid-sized businesses worldwide. Headquartered in Vancouver, British Columbia, the company provides virtual CISOs, data privacy officers, security monitoring, and compliance services.

WEBSITE

kobalt.io

Challenge

Kobalt.io needed to modernize its SIEM and consolidate security tools.

Beset with two SIEMs, Kobalt.io suffered from common SOC challenges—tool sprawl, alert fatigue, poor scalability, and high maintenance costs. With the renewal of their contracts with Splunk and Sentinel fast approaching, it was time to reevaluate how to improve their operations.

Kobalt.io SOC manager Chris Spindler noted, “We had to look after the care and feeding of two last-generation SIEMs, with our expenses higher than they should have been for what we were delivering.”

Spindler’s 14-member team had become so overwhelmed by alert volumes and maintaining two SIEMs that he was considering hiring two additional analysts. “Our systems were draining resources, and we weren’t able to scale well,” adds Spindler.

Solution

Seeking higher alert fidelity, cloud-native functionality and transparent pricing, Kobalt.io evaluated half a dozen SIEM solutions, including IBM® QRadar®, LogRhythm, AlienVault, and Sumo Logic.

After a two-week trialing, Kobalt.io unequivocally chose Sumo Logic for the following reasons:

Ease of use

Sumo Logic’s intuitive design meant that within just a couple of hours of tinkering in the trial version of the Sumo Logic platform, Kobalt.io could onboard sources and process alerts.

International data residency

Sumo Logic also allows Kobalt.io to serve its international clients subject to data residency requirements, hosting data in their respective regions.

Extensive integrations

Sumo Logic integrates with hundreds of data sources, including Azure, Google Cloud Platform, AWS, Kubernetes, and Docker, for optimal workflows and ease of customer adoption.

Multi-tenant SIEM instances

Sumo Logic's multi-tenant SIEM software enables Kobalt.io customers to configure and customize their accounts. Customer data is tagged per organization, keeping it separate and secure, which persists throughout the data lifecycle and is enforced at every system layer.

Actionable insights

Sumo Logic's Cloud SIEM combines event management with automated enrichment and contextual awareness, available via an interactive heads-up display, to help reduce false positives and filter out noise from actual indicators of compromise.

Transparent pricing

Sumo Logic's pricing model means Kobalt.io doesn't have to pick and choose which data sources are analyzed, which gives the SOC team the necessary information when they need it to perform prompt and effective security investigations and launch the appropriate response.

Results

From 6,000 monthly alerts to 600

Sumo Logic's Cloud SIEM solution provides cloud-scale correlation based on rules for known threats and subquery-based correlation for emerging new threats. With enhanced alert fidelity from Sumo Logic, the Kobalt.io team can focus on actual potential security threats instead of being bogged down by a flurry of inconsequential user activity alerts.

Spindler explains, "With Sumo Logic, we start with investigation tools integrated into the primary SIEM console, which means instead of opening up 15 different browser tabs so that you could go to places like WHOIS and VirusTotal and all the rest of it, you could do that in one click right out of the interface."

Going from 6,000 monthly alerts to 600, Kobalt.io has reduced alert fatigue and ensured analysts are focusing on what matters.

"Our analysts are our most valuable resource. Simple alarms don't tell you a story, and they don't give you a focus for the investigation. Sumo Logic ensures we spend our analysts' time where it matters most," Spindler explains.

Better alerting has also allowed Kobalt.io to do more with less. Before implementing Sumo Logic, Kobalt.io would have been forced to hire two more security analysts to handle its overwhelming alert volume. Since deploying Sumo Logic, Spindler has been able to keep his team to a dozen people. He adds, "Partnering with Sumo Logic was a no-brainer. Having a system of signals, insights and behavioral algorithms ensures our small team is focused on the right things."

BY THE NUMBERS

6000
→ 600
monthly alerts

CUSTOMER EXPERIENCE

Partnering with Sumo Logic was a no-brainer. Having a system of signals, insights and behavioral algorithms ensures our small team is focused on the right things.

Chris Spindler
SOC manager
Kobalt.io

Days-long customer onboarding to 15 minutes

Kobalt.io's main concern was migrating its customers to a new solution. With Sumo Logic, they migrated 25 customers in 20 days without direct access to the environments that they were monitoring. Migration to Sumo Logic was easy enough for Spindler to delegate tier-two analysts to help customers, spreading the workload. Since migrating, Kobalt.io can spin up new customers in just 15 minutes.

Spindler describes, "Sumo Logic is compatible with the predominant products that are out there on the market, so there's good support for what our customers are running. Migrating customers was easy for us because instead of having one person dedicated to onboarding, we were able to spread the tasks out across the entire team."

The ease of deployment and support for hundreds of third-party technologies has allowed Kobalt.io to grow faster than ever. We have doubled our customer base since we first deployed Sumo Logic.

Chris Spindler
SOC manager
Kobalt.io

100% ROI in four months

There were hidden costs to Kobalt.io's original SIEM solutions that exceeded the cost of the tools and licensing.

Spindler describes, "Splunk, for example, relies on heavy forwarders, a server or a virtual server instance, and those come with a monthly cost. With Microsoft Sentinel, logic apps and functions and data volume charges need to be paid and accounted for, and you need the infrastructure to manage all of that." In contrast, Sumo Logic doesn't come with any of those extra charges.

BY THE NUMBERS

20 days
to migrate
25 customers

2x
customer base

CUSTOMER EXPERIENCE

Splunk, for example, relies on heavy forwarders, a server or a virtual server instance, and those come with a monthly cost. With Microsoft Sentinel, logic apps and functions and data volume charges need to be paid and accounted for, and you need the infrastructure to manage all of that.

Chris Spindler
SOC manager
Kobalt.io

Sumo Logic's flexible pricing model also means serious cost savings for Kobalt.io.

> The advantage of Sumo Logic for us is that if a customer comes to us with a small data volume or a single source they want us to monitor, we can do that. We don't have to say, "No, I'm sorry, you've got to give us half a terabyte a day, otherwise, we can't offer you a data ingestion rate that you can afford.

Chris Spindler
SOC manager
Kobalt.io

BY THE NUMBERS

4 months
payback period

6 months
profitability

According to Spindler, Sumo Logic's pricing model means Kobalt.io can offer a full monitoring service for less than the cost of hiring an entry-level security specialist.

Within four months, Sumo Logic Cloud SIEM had paid for itself. Once Kobalt.io sunset Splunk and Microsoft Sentinel, the organization was profitable within six months of rolling out Sumo Logic.

Read more about other customer successes — from retail to healthcare to fintech here.

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

sumologic.com

855 Main Street, Redwood City, CA 94603