sumo logic

New standard set for managed security services

Results at a glance

→ Accelerated customer onboarding from 60 days to two hours to realize a 95% time savings

→ Reduced time-to-detect by 75% to meet 15-minute response SLA

→ Streamlined investigation decisions from one hour to three minutes, capturing 98% time savings

→ Offered differentiated service with security and log analytics

→ Enabled scalable data analysis that ingests 2 TB per day

→ Reduced tooling costs by $2.5M by consolidating on Sumo Logic

SRG

SUMO LOGIC SOLUTION

Cloud Security Analytics

Cloud SIEM

Log Analytics

USE CASE

Audit and Compliance

Threat Detection and Investigation

Challenge

Security Resource Group Inc. (SRG) needed a SIEM solution that provided faster customer onboarding and better scalability for its 24/7 security monitoring services.

As a top-tier managed security services provider (MSSP), SRG's International customer base was consistently expanding; however, the company's legacy managed security information and event management (SIEM) solution wasn't keeping pace with the growth. The solution ran on-premises and demanded mass amounts of compute and storage resources, making it exponentially costly and time-consuming to maintain. In addition, the SIEM was exceedingly complex for onboarding new customers. The lengthy process often required up to 60 days or more to complete.

Ultimately, SRG wanted to move to a modern SIEM solution that would support the MSSP's growth, agility and goal of delivering fast time-to-value.

Solution

SRG created a list of 21 requirements for their desired replacement, expecting they might need to adopt multiple solutions to equip the security team with the full set of capabilities.

SRG

INDUSTRY

MSSP

ABOUT

With headquarters in Regina, Saskatchewan, SRG was formed in 1996 and has since grown into a large-scale provider of world-class cybersecurity services and physical protective security services to organizations across Canada and specific to their MSSP business, expansion internationally.

SRG's marquee managed security service offering provides clients with 24/7 real-time security monitoring that's delivered via a bundle of industry-leading security tools, proven practices based on industry-recognized methodologies and a skilled cybersecurity team.

WEBSITE

securityresourcegroup.com

James Morris, Vice President Cyber Service and Technology at SRG, describes, “After an exhaustive review of many industry SIEM’s, we did a full integration testing of three solutions, and at the end of the day, we decided to partner with Sumo Logic. I’ll tell you right now, it’s the best decision we ever made. Sumo Logic ticked all the boxes for our requirements in a single solution. It provided flexibility in the platform for our security team to do non-traditional things for security monitoring.”

Results

Delivering fast time-to-value with onboarding in two hours

Sumo Logic’s MSSP platform features a multi-tenant, cloud-native architecture that simplifies customer management with a single, unified console and ingests 2TB a day across SRG’s customer base. In addition, with the platform’s built-in scalability, SRG can spin up a new customer environment without having to spend any cycles in the onboarding process worrying about performance issues.

With the solution’s ease of use and native API integrations, SRG experienced a big win with accelerated customer onboarding.

“With Sumo Logic, it only takes us two hours from the point that we sign a new contract to the point our customer has their SIEM up and running and can see value from it. We needed 60 days before, depending on the size and scope of the opportunity, so that’s a massive 95% reduction in onboarding time,” Morris shared.

BY THE NUMBERS

2TB
daily across SRG’s customer base

60 days →2 hrs
time to value

Providing customers with a differentiated MSSP service

Sumo Logic provides SRG with a single, integrated log management platform that supports many use cases — from the MSSP's native cloud SIEM needs to log analytics, infrastructure monitoring and more. This breadth in log telemetry empowers SRG's security team to not only collect the data they need for managing a customer's security operations center (SOC) but also to offer log analytics for a customer's operational intelligence.

SRG's unique approach to leveraging the breadth of Sumo Logic's data insights creates a differentiated MSSP offering in the market and provides a win-win for SRG and its customers.

> **“A portion of the data that comes in is valuable for security analytics, and a typical MSSP will drop the rest. At SRG, we bring in all the data with Sumo Logic and let our customers leverage the log analytics for their business intelligence at no charge.”**
>
> **James Morris**
> Vice President, Cyber Services and Technology
> SRG

Explaining further how this is a win-win for SRG and its customers, Morris shared, “Sumo Logic gives us a one-stop-ingestion-shop that helps us identify things like brute force attacks and other risks stemming from misconfigurations. We can then advise customers on where they need to fix their configurations, which improves the quality of the security analytics. As a result, our team can focus on real detections to meet our 15-minute service level agreement for the time between detection and response.”

Freeing up time to focus on threat hunting and customer value

SRG's previous SIEM solution was plagued with false positives, which created a lot of stress for the security team and limited the number of tickets they could complete daily. Sumo Logic alleviated these challenges.

The platform's advanced analytics parses, maps and creates normalized records from data and correlates detected threats, which reduced SRG's alert noise by 75% and decreased the team's event management decision time from one hour to three minutes. As a result, SRG's security analysts are less stressed, can focus on the threats that matter most and have greater time efficiency.

"Running a SOC for our customers means we have to do the right thing every time, the first time and in very little time. Sumo Logic allows us to do that," said Morris

BY THE NUMBERS

75%
less alert noise

1 hr → 3 mins
event management decision time

> **We now have more time to spend on threat hunting, providing value and advisory services for our customers. Our threat hunting time-to-detect reduced by over 200% and our accuracy increased three fold."**

James Morris
Vice President, Cyber Services and Technology
SRG

Fostering customer collaboration with unified visibility

With Sumo Logic, the SRG analysts have the go-to dashboards they need to gain an overarching view across the customer base and easy drill-downs to obtain deeper insights into a specific client's security posture. The platform's role-based access control (RBAC) also enables SRG to let customers view their data, so they can see exactly the same data and insights that SRG does.

"Providing customers access to Sumo Logic fosters collaboration where we can work hand-in-hand from the same data. Our customers have an in-depth knowledge of their environment, so it makes the process significantly faster and cleaner when we need to go through a log entry together to understand it," said Morris.

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

su
mo

Learn More

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

sumologic.com

855 Main Street, Redwood City, CA 94603