sumo logic

MSSP boosts operational and compliance maturity with Cloud SIEM

Results at a glance

→ Filters 300k daily signals down to 200 prioritized insights, highlighting an average of nine critical alerts per day

→ Helped client organizations close security gaps and improve cybersecurity maturity

→ Maintained an SLA response time for incident detection and response

→ Simplified data management across diverse and unique client environments with automated analysis, enabling each analyst on shift to efficiently handle up to 100 alerts per minute

SECURITY CENTRIC

PRODUCTS

Sumo Logic Platform

Cloud SIEM

Cloud SOAR

USE CASE

Threat detection, investigation, and response

Challenge

Security Centric needed to ensure alignment as its customer base and security operations evolved, leading it to deepen its partnership with Sumo Logic.

As Security Centric's customer base grew and their security operations matured, they saw an opportunity to leverage Sumo Logic's latest platform innovations. The company's security team was using Sumo Logic's Log Analytics Platform, security information and event management (SIEM) and security orchestration, automation, and response (SOAR) solutions.

By further integrating the Platform, Cloud SIEM, and Cloud SOAR into their internal security processes, Security Centric sought to improve efficiency, achieve faster threat detection, and better align with their diverse customer needs.

This collaborative relationship with Sumo Logic allowed Security Centric to provide valuable feedback, influence product development, and ensure that both their security operations and Sumo Logic's product roadmap evolved in tandem.

Solution

Already a partner with Sumo Logic, the MSSP frequently hears from other vendors looking to win their business. Security Centric continues to choose Sumo Logic as their vendor of choice for these top reasons:

SECURITY CENTRIC

INDUSTRY

Managed Security Service Provider (MSSP)

ABOUT

As a managed security service provider (MSSP), Security Centric helps customers achieve cybersecurity maturity through offensive and defensive assessments, Governance, Risk, and Compliance (GRC) consulting, and security engineering services. Security Centric empowers commercial, government, and defense organizations to better understand information security risks and strengthen their security posture.

WEBSITE

securitycentric.com.au

Unified data collection with universal collector and OpenTelemetry

Sumo Logic's universal collector and OpenTelemetry support have streamlined data collection and processing of diverse data sources for Security Centric. With this feature, Security Centric continues to scale its security infrastructure without worrying about compatibility issues, even if they decide to adopt new platforms in the future.

"Sumo Logic handles the heavy lifting by integrating different data sources clients have into one platform and normalizing them, which simplifies what would otherwise be a challenge," Tarek Chaalan, Security Operations Center (SOC) Manager at Security Centric, says.

Advanced SOAR capabilities and custom playbooks

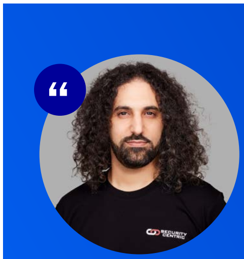
Security Centric developed and deployed custom playbooks which streamlined their security operations, reduced manual intervention, and improved efficiency when mitigating client-side security risks.

Ongoing customer support and collaboration

Any issues or questions they had were quickly addressed, and the MSSP found that they received consistent and effective customer support no matter the situation.

"It's not about the product. It's about the people. It's about the people behind the product and the support they're providing. That's the strength of Sumo Logic," Tarek Chaalan, Security Operations Center (SOC) Manager at Security Centric, notes.

CUSTOMER EXPERIENCE



> Sumo Logic handles the heavy lifting by integrating different data sources clients have into one platform and normalizing them, which simplifies what would otherwise be a challenge.
>
> **Tarek Chaalan**
> SOC Manager
> Security Centric

Seamless ingestion of structured and unstructured data

Sumo Logic's user-friendly interface allowed Security Centric to quickly implement the Platform into their security operations, reducing onboarding time and making it easy for their SOC team to efficiently process and analyze diverse data types.

As Security Centric's customer base expanded, each with its own unique requirements and data sources, the SOC team easily customized the solution for deeper insights into their clients' distinct security environments. Sumo Logic's ability to ingest unstructured and structured log data stood out to Chaalan.

> One of the hardest parts about SIEM is parsing logs. Parsing the logs is one of the toughest things you can have in a product. With Sumo Logic, I didn't have to worry about log parsing and creating custom parsing for unsupported log sources.
>
> **Tarek Chaalan**
> SOC Manager | Security Centric

Results

Improved SLA response times

With Sumo Logic's real-time detection, automated incident analysis, and rapid notification, Security Centric kept incident response times well below its SLA commitment.

"Once Sumo Logic's Cloud SIEM generates an incident, we ensure SLA response times are consistently met. Our team promptly picks up the incident, analyzes it, updates the severity if necessary, provides a conclusive analysis, and takes the appropriate action using Sumo Logic's CSE automation or Cloud SOAR. All of this is done within our SLA commitment."

Expanded incident response capacity and improved compliance maturity

Security Centric's partnership with Sumo Logic helps them manage a high volume of incidents with efficiency. A team of analysts on shift can process up to 100 incident alerts per minute. They achieved this scalability through a custom integration on Sumo Logic's API and automation tools, using Apache Zeppelin.

They also enhanced their clients' compliance maturity and cybersecurity hygiene, which is critical to Security Centric. Sumo Logic helped their team close security gaps, improve compliance, and foster better cybersecurity practices within client organizations. "Our role is not to just stop external threats. It's also to assist the organization to mature and enhance their compliance level," said Chaalan.

Query support with Sumo Logic Mo Copilot

Simplicity and efficiency are vital for Security Centric's SOC team. Sumo Logic Mo Copilot streamlines complex query creation and offers intelligent suggestions for Security Centric.

This support allowed for faster, more accurate data analysis and an improved user experience.

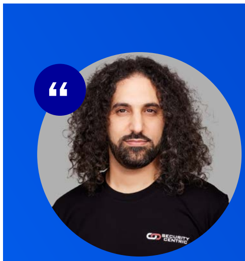
"What I love about Sumo Logic Mo Copilot is how quickly I can write and visualize a log query. Many times, a client will ask me for a query, and I simply search for it on Copilot, and provide it to them instantly. It's a huge value add for partners."

BY THE NUMBERS

100 alerts

processed per minute

CUSTOMER EXPERIENCE



What I love about Sumo Logic Mo Copilot is how quickly I can write and visualize a log query. Many times, a client will ask me for a query, and I simply search for it on Copilot, and provide it to them instantly. It's a huge value add for partners.

Tarek Chaalan
SOC Manager
Security Centric

96% noise reduction

Handling over 300k daily signals and reducing them to 200 actionable insights, Sumo Logic helped Security Centric's SOC team effectively prioritize which alerts needed analysis or investigation, allowing analysts to focus on approximately nine critical issues per day. The security team can handle a high volume of data and focus on what truly matters most — helping clients improve their cybersecurity hygiene.

BY THE NUMBERS

96%

noise reduction

> By filtering out the noise and pinpointing critical insights, Sumo Logic allows us to improve our team's efficacy. We're able to zero in on the most pressing threats and reduce alert fatigue.

Tarek Chaalan
SOC Manager | Security Centric

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