sumo logic

Financial services company cuts fraud losses 50% with Cloud SIEM

Results at a glance

- → 50% reduction in fraud losses after implementing custom insights and detection logic
- → Detects account takeover and abnormal activity within minutes, not days
- → Faster analyst onboarding using Dojo AI to accelerate query building and learning
- → Only took minutes to onboard data sources into Cloud SIEM, getting analysts up to speed faster
- → Faster MTTR and proactive incident mitigation through integrating existing tools with Sumo Logic

PRODUCTS

Cloud SIEM

USE CASES

Threat detection, investigation, and response

ENVIRONMENT

AWS

Challenge

When you're responsible for securing more than $127 billion in assets, your security tools need to work for you, not against you. That was the challenge facing the SOC team at a major financial services firm, whose previous SIEM created more operational burden than security value.

INDUSTRY
Financial services

ABOUT
A large U.S.-based insurance holding company that offers life insurance, annuities, and retirement solutions, managing over $127 billion in assets.

While their prior SIEM was supposed to protect their environment, it was difficult to manage and maintain instead.

- Searches were slow and painful to use, slowing investigation speed.
- Visibility gaps ran rampant as their prior SIEM didn't support log ingestion for many of their critical platforms.
- Limited cloud-to-cloud integration options for data sources in their cloud-centric environment.
- Limited fraud detection capabilities.

Overall, it wasn't scalable and didn't integrate well with their environment. They wanted to find a reliable, cloud-native, easy-to-use security tool that their SOC team could easily manage without experiencing team burnout and fatigue.

Our previous SIEM was difficult to manage and maintain. We did not have good options for cloud-to-cloud integration for many data sources. Searches were slow and painful to use. Our team's response to security events was high, and efficiency was impacted. The lack of support for many of our critical platforms left a gap and increased the risk of missing a potential security event in our environment.

One of the targeted KPIs once we began using Sumo Logic was to provide a visualization into our fraud account takeover activity, which one of our business units is now able to use.

Senior IT Cybersecurity Engineer
Financial Services Company

Solution

Replacing a core security tool isn't a decision made lightly. The team evaluated six SIEM solutions, narrowing the field to two finalists - CrowdStrike and Sumo Logic - for a head-to-head proof-of-concept.

CrowdStrike was out quickly. “It wasn’t even a matter of time. They just weren't able to show us that the tool was able to be easily administered. We had a lot of doubts about their ability to even meet our criteria at all," notes their Cybersecurity Engineer.

Unlike the competition, Sumo Logic checked every box. "Sumo Logic's Insights feature provided us with a ‘MSSP-in-a-box’ feel native to the platform. Its easy-to-navigate interface allowed our security analysts to quickly find value with faster detection and response through correlated events.”

They valued that Sumo Logic’s flexible licensing let them focus on the data that matters most to their SOC. “The Sumo Logic sales team did an excellent job demoing the Platform and showing how Sumo Logic would meet our vendor requirements and use cases,” the Senior IT Cybersecurity Engineer explains. “We quickly understood how easy the Platform was to navigate, our ability to self-service and onboard data, and the pre-built detection logic that would save us time on rule tuning. Sumo Logic was the only solution we evaluated that met every piece of our requirements.”

Easy-to-use security solution

Given the struggles with their prior SIEM, the team wanted their new SIEM to be reliable and simple to manage. Onboarding data sources into Sumo Logic took their SOC minutes, which was dramatically faster than what they were used to.

They wanted analysts to start using the tool instantly rather than sitting through long onboarding delays. “We wanted them to be able to search through the tool with ease and be able to pull back results quickly and correlate data across multiple platforms.” And they got that with Sumo Logic.

CUSTOMER EXPERIENCE

Sumo Logic was the only solution we evaluated that met every piece of our requirements.

Senior IT Cybersecurity Engineer
Financial Services Company

Built-in detection logic and custom insights

A key requirement for their SOC was pre-built detection logic so their analysts could get up to speed more quickly without needing a third party.

During the POC, they threw Sumo Logic a challenge: integrate Fraudshare, their threat intelligence platform that detects IP addresses and email addresses associated with fraudulent activity, into Sumo Logic's Cloud SIEM. To achieve this, the Sumo Logic team built custom scripts to upload all indicators of compromise (IoCs), adding a critical layer of technical authenticity to the solution.

It worked immediately. Within weeks of going live, the SOC team caught an account takeover when someone attempted MFA with a phone number flagged in FraudShare. "We were able to see that insight within minutes and lock that account down," the Cybersecurity Engineer says.

Flexible licensing that adapts to their needs

Sumo Logic's flexible licensing model simplified pricing and changed how the team thinks about data. Instead of making hard tradeoffs, they could prioritize critical logs for continuous monitoring while keeping less urgent data searchable.

The Senior IT Cybersecurity Engineer says, “The licensing model gives us the flexibility to bring in more data through the flex tier and then decide what logs are most important to send to the SIEM for security analysis. Prior to Sumo Logic, cost was a major driver on what and how many logs we could bring in for security analysis and investigations.”

Results

50% reduction in fraud losses

The Special Investigations Unit (SIU) was buried in manual work. Tasked with uncovering fraudulent customer activity, the team had no automated way to detect or respond to threats before Sumo Logic. Now, the SIU team has direct access to Sumo Logic to quickly identify abnormal customer activity.

Within the first 30 days of deploying custom insights, they successfully identified an account takeover on a customer's account and quickly locked it down before it escalated into a security incident.

"Our relationship with our Special Investigations Unit has gotten to the point where we're so quick about responding to these alerts that we're locking these accounts down within minutes instead of days later. The custom dashboards visualize critical fraud metrics for our business units to view on their own and without technical help. Sumo Logic's early impact has shown a reduction in fraud losses of around 40-50%," the Senior IT Cybersecurity Engineer says.

A truly independent SOC

The team achieved their main goal of becoming an independent SOC. Tasks now take them minutes to handle independently. They also have better cross-team collaboration with shared dashboards, standardized searches, and unified context during incidents.

"The ease of administration is pivotal to making us a more independent SOC. Having the capability to add our own data sources is great for us to be more self-sufficient and not need to lean on third parties to help us take care of our own platforms," the Cybersecurity Engineer says.

Faster onboarding and better efficiency with Dojo AI

Their SOC works faster using Dojo AI. New team members can get up to speed in no time. A new hire used Dojo AI to build queries and search through data quickly, helping them learn query syntax faster.

Their Cybersecurity Engineer notes that, "An AI-powered Cloud SIEM was something we were looking for in a security tool. Dojo AI works great for our SOC team, giving them a natural language option to return query syntax faster and get better results for incident investigations."

BY THE NUMBERS

Fraud containment
Days → Minutes

BY THE NUMBERS

50%
reduction in fraud losses

"We're locking these accounts down within minutes instead of days later. The custom dashboards visualize critical fraud metrics for our business units to view on their own and without technical help. Sumo Logic's early impact has shown a reduction in fraud losses of around 40-50%."

Senior IT Cybersecurity Engineer
Financial Services Company

Easy integration into existing platforms

Sumo Logic easily adapted to their existing security stack. Using Sumo Logic's API, they built an automated data pipeline that pulls every insight generated in Sumo Logic directly to their SOAR platform, creating cases and playbooks automatically.

Rather than starting from scratch with each alert, they now follow standardized, repeatable processes. Analysts have a step-by-step playbook for handling an insight. This reduces their time to respond, and they're proactive with incident mitigation.

A true vendor partnership

Not every vendor becomes a partner. For this financial services firm's SOC team, Sumo Logic did by delivering on every must-have from day one: ease of use, simple search, quick onboarding, and built-in detection.

"The Sumo Logic team was outstanding from the first day we engaged with them. The level of effort and personal touch was unlike anything we received from any of the other vendors we considered. We've had an excellent experience throughout the evaluation, procurement, onboarding, and implementation of the Platform. They kept a personal touch throughout the process.

The multiple onsite meetings really showed the entire Sumo Logic team was fully invested in helping us meet our requirements. Overall, Sumo Logic has enhanced our security posture by providing a modern approach to data ingestion, analytics, and visualization," the Senior IT Cybersecurity Engineer says.

CUSTOMER EXPERIENCE

An AI-powered Cloud SIEM was something we were looking for in a security tool. Dojo AI works great for our SOC team, giving them a natural language option to return query syntax faster and get better results for incident investigations.

Cybersecurity Engineer
Financial Services Company

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