

Bugcrowd achieves four-minute SLA and cuts costs with unified security platform

Results at a glance

- Maintained four-minute SLA detection and response times, surpassing industry standards
- Improved cost management by optimizing data storage to stay within budget
- Unified and centralized logging platform for faster threat detection
- Accelerated investigation process

bugcrowd

PRODUCTS

Cloud SIEM

Sumo Logic Platform

USE CASES

Platform

SIEM



Challenge

Bugcrowd needed a centralized, efficient, and scalable SIEM solution to streamline its fragmented log infrastructure and improve visibility.

Before implementing Sumo Logic, Bugcrowd found it challenging to manage security data and maintain operational efficiency due to multiple log sources and disparate tools. Engineers often had to navigate between different systems to gather context during investigations, leading to delays and insufficiencies. Junior engineers, in particular, were consistently confused about which tools to use, adding further complexity and more cycles to their process.

As Bugcrowd scaled, they needed a unified platform to manage their complex log data. Tool sprawl made it difficult for Bugcrowd to achieve the consistent visibility, speed, and integration necessary for effective security operations. It was time for Bugcrowd to find a SIEM solution capable of consolidating its logging infrastructure, streamlining processes, and improving overall security operations.

Solution

After evaluating several logging platforms, including Datadog and Splunk, Bugcrowd ultimately chose Sumo Logic for its ability to meet their key requirements: seamless data ingestion/collection, Terraform integration, and API management capabilities.

Sajeeb Lohani, Bugcrowd's Global Technical Information Security Officer (TISO) & Senior Director of Cybersecurity, explains his reasons for selecting Sumo Logic: "We needed appropriate SaaS visibility and logging, and Sumo Logic was one of the few solutions offering a great Terraform provider and hosted collector. Sumo Logic's innovative approach suits our structure well and has proven useful for us."

INDUSTRY

Information technology

ABOUT

Founded in 2012, Bugcrowd provides crowdsourced security services. In addition to managing client crowd engagement, they maintain and update bugs within a client's software. Bugcrowd is headquartered in San Francisco, California, with additional offices in Boston, London and Australia.

WEBSITE

www.bugcrowd.com

Bugcrowd chose Sumo Logic over competitors for these main reasons:

- **Competitive pricing:** Beyond offering a cost-effective solution that fits Bugcrowd's budget, Sumo Logic's solution delivered better value compared to the competitors they evaluated.
- **Unified platform:** Sumo Logic offered a "one-stop-shop" for all Bugcrowd's logging needs. "It's everything you need in one place, done intelligently, with good people backing it. It doesn't take very long to get used to it and to get moving with it," notes Lohani.
- **Free, comprehensive training:** Built into their 30/60/90 day onboarding process, Bugcrowd used Sumo Logic's free training program to ensure engineers became efficient in the tool quickly without added costs.
- **Granular access controls:** By restricting sensitive data access to only people with the right permissions, Bugcrowd maintained regulatory compliance and secure operations.
- **Enhanced API integration:** Sumo Logic's API integrations helped Bugcrowd build a connected ecosystem to monitor anomalous behavior and events.

Results

Four-minute SLA for incident detection and response

Sumo Logic's advanced search and contextual indexing capabilities help Bugcrowd quickly identify and respond to threats. With all their logging needs in one unified solution, their security team can streamline access management instead of dispersing access rights across different systems.

Bugcrowd consistently adheres to its four-minute SLA detection and response time, beating the industry gold standard. Engineers can access actionable data quickly. According to Lohani, "All an engineer has to do is click a link, and they have everything they need in one place. That level of integration and simplicity helps us respond faster and more effectively."

BY THE NUMBERS

4-min SLA

for incident detection
and response

CUSTOMER EXPERIENCE



All an engineer has to do is click a link, and they have everything they need in one place. That level of integration and simplicity helps us respond faster and more effectively.

Sajeed Lohani
Global Technical
Information Security
Officer (TISO) &
Senior Director of
Cybersecurity
Bugcrowd

Quicker and fewer investigations with consolidation

Using Sumo Logic's alert aggregation and custom insights capabilities, Bugcrowd significantly reduces noise within its system. By implementing suppression rules, engineers can focus on high-priority investigations without being overwhelmed by various alerts.

Sumo Logic's Cloud SIEM serves as Bugcrowd's "investigation workbench" for engineers to manage and correlate events. It helps them consolidate multiple signals into a single insight, decreasing the number of investigations they have to do. For example, what might have previously required Bugcrowd five separate Jira tickets is now captured in one insight.

This process, known as signal clustering, helps Bugcrowd save time and create an efficient investigation process. With Cloud SIEM Entities, engineers, especially junior ones, could search by a specific asset identifier and have clear, contextual data for investigations. Lohani explains, "It fits into our environment quite well. We can adapt the Platform to our needs and integrate it into our processes. These capabilities streamline our workflows and align with compliance requirements."

Improved costs and reduced tool sprawl

Sumo Logic helps Bugcrowd optimize its logging infrastructure to ensure they have the operational data they need without incurring additional costs or overages. Sumo Logic's customer support team offers strategies for an optimal setup to keep costs under control.



One thing I really appreciate about Sumo Logic is that they're not money-hungry, unlike many other vendors. Customer support helped us re-architect our data to make it more cost-efficient. Sumo Logic is one of the few vendors that genuinely help us save money rather than upsell us.

Sajeeb Lohani

Global Technical Information Security Officer (TISO) & Senior Director
of Cybersecurity | Bugcrowd

Customizable detections

With Sumo Logic's Cloud SIEM, Bugcrowd creates custom detections that surpass those of competing tools, which allows their security team to protect their organization more effectively.

"We're very proud of the detections that we've written. Some of them are things that even companies who have built the tools themselves don't have. One of the reasons we can do that is because Sumo Logic gives us that interface and provides query support. After we use their feedback, we can innovate and push it further," Lohani said.

Improved engineers' efficiency with free training

Bugcrowd made Sumo Logic training a mandatory part of their onboarding process, requiring engineers to complete certifications within their first 30 days. This approach ensures all team members can quickly leverage the Platform's full capabilities.

"Within just 30 days, our team was not only onboarded but proficient enough to customize the solution to fit our specific needs. Given this and everything else the Platform offers, I would 100% recommend Sumo Logic to other security leaders. It's simple, intuitive, and user-friendly. It's one of the few tools where even a junior engineer can just type in a keyword and get results instantly," notes Lohani.

CUSTOMER EXPERIENCE



I would 100% recommend Sumo Logic to other security leaders. It's simple, intuitive, and user-friendly. It's one of the few tools where even a junior engineer can just type in a keyword and get results instantly.

Sajeeb Lohani
Global Technical
Information Security
Officer (TISO) &
Senior Director of
Cybersecurity
Bugcrowd

Read more about other customer successes — from retail to healthcare to fintech [here](#).

s u m o

Learn More

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

sumologic.com

© Copyright 2025 Sumo Logic, Inc. Sumo Logic is a trademark or registered trademark of Sumo Logic in the United States and in foreign countries. All other company and product names may be trademarks or registered trademarks of their respective owners. Updated 05/2024

855 Main Street, Redwood City, CA 94603