panther | #FloQast

CASE STUDY

Floqast Accelerates Detection Testing and Deployment With Panther

FloQast is an accounting software company based in Los Angeles, California. The business streamlines accounting workflows so their customers can complete critical accounting processes faster and more efficiently.

Technically, FloQast is a cloud-native organization with no on-premise hardware. The organization's infrastructure footprint in Amazon Web Services (AWS) was rapidly expanding - leading to a drastic increase in security-relevant logs. Its security team needed a modern Security Information and Event Management (SIEM) that was easy to manage and could scale alongside AWS. However, the team found that traditional SIEM solutions relied on proprietary coding languages and inefficient data ingestion - making progress difficult.

Powerful Detection-as-Code

FloQast could not only use the out-of-the-box detections but also easily translate pre-written detections from other platforms.

Ingest Ten Times More Data

Types of logs that could be ingested expanded dramatically, as the team no longer needed to create custom ingestions for applications with no native integration.

Flexibility and Scalability

Colleagues from other teams (such as application security) now have the toolset to investigate independently without engaging the Detection & Response team.

The Challenge

Unreliable Data Ingestion: FloQast's threat detection solution lacked centralized logging, and the team relied on disparate systems, each individually integrated with Slack, to do alerting for them. FloQast lacked a central solution to allow them to make changes that would benefit their entire security stack.

Limited Detection Capabilities: Using a proprietary language to code detections hindered FloQast's security team. Adapting to vendor-specific code and tooling was not as applicable across other functions and security teams. They were seeking a solution to allow them to easily hire people who could write detections in a widely accessible language.

Adversity With Detection Testing: Writing detections without a practical way to test them was becoming a significant frustration for the FloQast security team. Whenever a detection was tweaked, they were forced to wait until that event reoccurred to determine its accuracy.

Industry
Fintech

Year Founded
2013

Location
Los Angeles, CA

Company Size
500+

The Solution

Increased Data Ingestion and Retention

After deploying Panther, FloQast was able to ingest approximately ten times the amount of data compared to their legacy platform. Plus, types of logs that could be ingested expanded dramatically, as the team no longer needed to create custom ingestions for applications with no native integration.

With Okta logs, for example, Panther provides a built-in integration to ingest and normalize key "indicator of compromise" fields, along with built-in detections to enable effective alerting on specific behaviors. Finally, the team was able to remove restrictions on data retention significantly after deploying Panther.

Robust Out-of-the-Box Detection for AWS and Modern Technology Stack

When getting started, FloQast was able to turn on a variety of detections immediately. The pre-built logic for AWS environments and other common SaaS tools made it easier to hit the ground running with Panther.

Ability To Grow The Team and Train Staff Quickly

Panther opened the door for FloQast to access a broader talent pool given how widely SQL and Python are used across security and other functions. Even FloQast colleagues from other teams (such as application security) now have the toolset to investigate independently without engaging the Detection & Response team.

Powerful and Flexible Detection-as-Code

By leveraging the universal coding power of Python, FloQast grew confident that as their detection requirements increased in complexity, Panther would be up to the task. With Panther, FloQast could not only use the out-of-the-box detections but also easily translate pre-written detections from other platforms.

The Results

With Panther, FloQast is well-positioned to continue optimizing its detection and response process. With easy-to-learn detection writing (Python) and query functionality (SQL) for everyone on the security team, the Detection & Response team has more time to focus on their role in maintaining the company's security posture.

Panther has enabled FloQast to:

- Ingest ten times more data from a wider list of data sources
- Significantly reduce restrictions on data retention
- Craft powerful and flexible detections with Python
- Analyze logs as they are ingested and leverage more context for alerts
- Improve the flexibility and scalability of their detection and response processes