Financial Services Lean Security Team Offsets Head Count with Panther's Streamlined SecOps

Industry: Financial Services **HQ:** San Francisco, CA

> "As a small team, it's difficult to keep track of all our security logs. But with Panther, we can easily integrate our logs from multiple sources and get a clear picture of our security posture. This has helped us to identify and respond to threats more quickly, and to improve our overall security."

HEAD OF IT

A Leading FinTech Company Needed to Improve their Security Posture

Security is paramount for financial services, and this team is committed to protecting customers personal financial information with industry-leading security technology. They have a team of security experts who are constantly monitoring their systems for potential threats.

The security team needed a SIEM solution that could efficiently ingest and analyze log data from multiple sources without the burden of complex configurations and extensive engineering time. Traditional tools forced them to make tough decisions about which logs to prioritize, leading to concerns about potential visibility gaps. Moreover, the team faced challenges with convoluted detection logic languages, hindering their ability to fine-tune detections for their unique environment.

Frustrated with these challenges, they sought out a more effective SIEM platform. They found Panther, which offered ease of use, out-of-the-box detections, and exceptional customer support. Panther's integrations with tools like AWS, Google Workspace, and Okta empowered the team to proactively detect and respond to security threats, improving their cybersecurity posture and operational efficiency.

Challenges

Difficulties monitoring multiple log sources with limited resources

Redundant security tools and alert integrations

Reactive security threat detection increased burden on their small security team

Solutions

Centralized log storage deployed for efficient threat monitoring

Integrated solution without redundancies for streamlined log source management

Strengthened threat detection with refined rules, reducing strain on security resources

Results

Enhanced the adaptability of their detection and response procedures

Panther's cloud-native architecture allowed them to prioritize security over tool upkeep

Cut security costs by eliminating the need for a managed SOC

Streamlining Log Source Management and Security Monitoring

BOne of the challenges the team faced was effectively managing and monitoring multiple log sources with limited resources. In search of a solution, they turned to Panther for its comprehensive capabilities in log ingestion and customizable detections.

Panther helped consolidate tools and streamline log source management by providing a centralized platform that addressed the complexity of their IT and InfoSec responsibilities. With Panther integrating multiple log sources and reducing complexity from disparate tools, the team could finally focus on actionable security insights.

Leveraging Panther's intuitive user interface, they efficiently onboarded a variety of log sources, including AWS, Google Workspace, Okta, and Salesforce. This seamless deployment significantly alleviated the burden on the small team, sparing them the need for a dedicated security engineer and managed SOC.

> "Panther saved us from the need for a dedicated security engineer. The onboarding process is easy, and we can easily integrate new log sources. I would recommend Panther to any organization looking for an easy-to-use SIEM."

Increasing Threat Coverage with Detections-as-Code

With 500+ out of the box detections provided by Panther, the team found that they rarely needed to write their own detection rules. This proved particularly beneficial given their small team. Panther's out-of-the-box detections and user-friendly approach allowed them to tune and customize rules without a need for extensive coding or engineering resources.

While other SIEMs provide their users with generic and hard to edit detections, Panther's comprehensive out-of-the-box detection packs deliver security value with little to no tuning. Spending less time customizing and creating detections frees up the small security team to work on additional priorities, eliminating the need for additional headcount.

Unparalleled Support and Proactive Engagement

The team benefits from Panther's responsive, proactive and authentically helpful customer support. Panther's team works with them to tailor solutions to their needs, enabling them to easily integrate with their custom security tools. Their feedback has fostered a strong relationship between the two teams and solidified their confidence in Panther's capabilities.

When a third party security vendor had a reported breach, Panther proactively provided threat hunting queries to the team, while their managed SOC at the time took hours to respond. With Panther's proactive support and streamlined security operations, the team was able to end their partnership with the managed SOC, reducing security costs.

> "Panther's support team is incredibly proactive. They listen to customer requirements and promptly implement them in the tool, giving us an extra edge in the cybersecurity field."