panther | _zapier

Zapier Transforms Their Security Team From Manual Triage to Proactive Detection

Industry: Software Development **HQ:** San Francisco, CA **Founded:** 2011 **Employees:** 501-1000

Zapier's choice to deploy and implement Panther saves them an estimated $400,000 annually through offset tooling and incident response costs. Panther's out-of-the-box data integrations and detection rules, ease of ingestion and affordable pricing model, and customizable Python detections make it an ideal solution for modern security teams seeking streamlined cloud-based solutions with robust detection and response capabilities.

> "That old approach of having the entire team of entry-level people just triaging alerts all day doesn't really scale with the way that cloud environments work. You need to be more deliberate about how you approach detection engineering."
>
> MICHAEL KUCHERA
> SECURITY INCIDENT RESPONSE LEADER

Michael Kuchera, Zapier's Security Incident Response Leader, was brought in and tasked with building a new Detection and Response team. Their leadership team knew that it was time to take their security to the next level and find a solution that consolidated their security events into one system for centralized visibility and delivered flexibility to easily create custom detections to monitor for potential threats in their environment. Michael's search for a modern SIEM led him to Panther, where he found a solution that matched his team's needs. If Panther didn't exist, Michael admits that they likely would have needed to build something similar themselves since they couldn't find another solution offering the same level of customization at a scalable cost.

"Given that the security team in general was pretty small, there were a couple of key things that we needed that were non-negotiable. One was a hosted modern, scalable solution that didn't take somebody's full-time job administering. We also wanted something that made ingesting cloud logs easy. Panther is built as a cloud solution, so it came with that ease of use."

Challenges

Lacking centralized security event logging, monitoring, and correlation

Missing capabilities for advanced detection creation and management

Building out a detection and Response team from the ground up

Solutions

Centralizing security event visibility with out-of-the-box data ingestion and normalization

Embracing Python-based detections-as-code for rule creation and management

Deploying a scalable, cloud-based SIEM with no tool-specific coding knowledge required

Results

Increased security log monitoring from 20% of security data to 70%

Reduced false positive alert rates and improved response times

Enabled and established an effective Detections & Response team

Centralizing Security Event Logging

At the outset, Zapier's security logs were mixed in with a legacy infrastructure logging tool, making it challenging to gain a comprehensive view of the company's security posture. Given a combination of unsupported log sources and high costs to ingest, only about 20% of their security events were being logged into the existing tooling, leading to gaps in visibility and threat coverage. This lack of centralization also resulted in inefficiencies in incident detection and response, as the security team had to manually sift through disparate data sources to identify potential threats. As a result, Zapier recognized the need for a solution that could streamline event management and provide a unified platform for monitoring and responding to security incidents.

With Panther, Zapier was able to easily centralize security event management and correlation. Panther's out of the box data ingestion integrations with commonly used SaaS products especially made onboarding their data simple for Zapier. Their first six critical data sources were onboarded on day two- in about half the time they estimate it would have taken on a legacy SIEM product.

Panther's scalability and budget-friendly pricing ensure that Zapier can adapt to evolving security needs without experiencing performance bottlenecks. As the company expands its infrastructure and adds new services, Panther can seamlessly accommodate the increased workload and data volume without overhead maintenance or skyrocketing costs like legacy SIEMs often require. With Panther's ease of data ingestion and pricing model, they've increased their visibility from 20% of their security logs to 70% with plans to achieve 100% in the near future.

Engineering First Detection & Response

Zapier's existing security program was making use of a legacy infrastructure tool that wasn't suited to their security-specific use cases. They were limited to basic event threshold detections but knew that they needed a tool that supported advanced detection use cases to achieve comprehensive threat coverage across all of their log sources. Their prior tool didn't provide pre-written detection or enable effective custom detections, meaning they couldn't get alerts for known security concerns in their environment.

While there are a number of SIEMs on the market that deliver advanced detection capabilities, Panther stood out for its use of Python-based detections. With Panther, Michael didn't need to limit his Detection & Response hiring to engineers with tool-specific knowledge already in place or invest heavily in education and onboarding with tool-specific training. Adopting Python-based detections allowed the security team to leverage their existing engineering skills to develop sophisticated detection rules.

The Zapier security team creates new detection rules based on gap analyses across their environment. Utilizing a combination of Panther's out-of-the-box rules and their own custom detections, Zapier has achieved comprehensive threat coverage, improved response times, and reduced false positive alerts. The platform's advanced analysis capabilities allowed the security team to identify genuine security threats more accurately, minimizing the occurrence of false alarms.

Establishing a Detection & Response Team

To establish an effective Detection & Response team, Michael needed to find the right solution to centralize their security workflows. When Michael started his search for the right tool for their team, Panther stood out due to its modern, cloud-native architecture, ease of use, and its support for Python-based detection logic, aligning perfectly with the team's existing engineering skills.

The urgency to find a solution was driven especially by the lack of visibility and aggregation of security-related events, especially from critical sources like Okta, Google, Slack, and Zoom. The team was limited by this lack of employee data for their internal security. With the shift away from traditional in-office working environments and on-prem services, employee data like this is critical for security teams to monitor.

> "Your identities and what your people do are how you interface with the world. And so you need to have your security perimeter at the identity level. And if you don't have visibility at your identity level, then you don't have basic security for a cloud setup."

MICHAEL KUCHERA
SECURITY INCIDENT RESPONSE LEADER

Their security team has successfully used Panther in proactive detection and incident response, like in instances where the platform helped catch potential threats like server-side request forgeries in AWS and analyze historical role assumptions from AWS admins.