panther | Benchling

Benchling's Code Driven SecOps Program is Enabled by Panther

Industry: Software Development **HQ:** San Francisco, CA **Founded:** 2012 **Employees:** 501-1000

Benchling develops software that powers the biotechnology industry. The company has experienced rapid growth in the last several years. Given the critical nature of their industry, security is a top focus. During their search for a Detection Platform they needed to remain compliant and meet their customers' high security standards in addition to finding a tool that enables them to apply standard software engineering practices to their detection writing processes.

Embracing Code-Driven SecOps

Given their tech stack and customer requirements, Benchling was looking for a Detection Platform that would grant them total ownership of their data in their own environment and keep costs linear and predictable despite rapidly growing cloud infrastructure log volumes.

Benchling needed a robust Detection program that would scale alongside their growth. Benchling wanted to have a program in place, and found alignment with Panther's platform for code-driven security operations.

In order to meet these goals, Benchling built a security team responsible for writing reliable detections, minimizing alert volumes, and ensuring the detection engine's consistency through unit testing. Panther's support for writing detections-as-code with CI/CD proved crucial for Benchling. The ability to use Python, write unit tests, and automate processes enhanced detection performance and reliability. Benchling's engineering first approach to security pairs perfectly with Panther's Code-Driven detection engine. Using CI/CD to deploy detections, the Benchling team is confident in both the efficacy of their rules to catch true positives while tuning out noisy false positives.

> "Our detection and response team cannot be responding to hundreds of alerts a day. For that reason, we needed a detection engine that's reliable and unit-testable."

BRIAN MALONEY
ENGINEERING MANAGER

Challenges

Integrating with Benchling's tech stack and existing data processing and infrastructure needs

Scalable programmatic approach to Security Detection development that allows detections to be change-managed via GitOps

Delivering extensible detections (using external APIs and data sources) is a challenge with many products on the market

Maintaining control over Benchling generated security telemetry

Solutions

Leveraging a code-driven detection engine enabled the security team to write reliable, tested detections

Using a general programming language like Python allows detection logic to access anything with an API, such as their own cloud infrastructure and partner SaaS

Deploying Panther Cloud Connected - Built with serverless architecture, Panther's Cloud Connected deployment option fit Benchling's unique infrastructure and data needs perfectly

Results

Timely and effective detection deployment with true CI/CD resulted in high fidelity detections

Simple Detection maintainability as program grew to meet the needs of the business

Quickly iterated and deployed critical detections as part of response actions

Detections are written inside a Benchling controlled environment and with predictable Panther data ingest costs

Crafting Complex Detection Logic in Python

Benchling takes advantage of Panther to write powerful, environment-specific detections. Detections in Panther are written in Python – a highly expressable and widely adopted language. The combination of Python and the security data lake makes it easy to craft robust detections that call on efficiently stored and organized data. At Benchling, there was nuanced malicious behavior the team wanted to detect. The behavior had multiple indicators and required calculation and correlation across disparate variables to alert correctly. Using a combination of batch-styled SQL queries to build dynamic baselines for certain behaviors and Python to process results, Benchling was able to correlate data from multiple heterogeneous datasets to create a custom detection tailored for Benchling's specific use case.

> "With Panther Cloud Connected, not only do we run Panther on our own AWS infrastructure, but we also run it on our own Snowflake, which allows us to continue to uphold the highest standards for our customers."

BRIAN MALONEY
ENGINEERING MANAGER

Meeting Unique Data Needs

Given their industry, it is important to Benchling that they own all of their data on their own infrastructure. Built with serverless architecture, Panther's Cloud Connected deployment option fits both Benchling's budget and infrastructure needs perfectly. Leveraging Panther Cloud Connected, Benchling was able to double their data ingest without breaking their budget, ensuring every single security-relevant event can be monitored. Benchling needed a SIEM that would work with their custom data processing workflows and support their unique processes. Panther seamlessly integrated with Benchling's data workflow. Their Panther deployment and data workflows ensure they maintain ownership of their data at all times, strengthening Benchling's security posture while making use of Panther's powerful detection engine.

Additionally, using a world-class data warehouse like Snowflake unlocks analytics capabilities that are simply not present in other SIEM software. Benchling's highly-skilled detection engineers can easily use Snowflake in conjunction with other data analysis tools using the same tools for querying and analysis that data scientists use. By bringing extensibility to both detection logic and analysis capabilities, Panther provides a truly open platform for deriving actionable Security intelligence from raw log data.

At the end of the day, Panther is enabling a highly technical team to maximize their time spent on writing and optimizing detections for their unique environment.

> "Panther is freeing up our engineers' time to do what they do well, which is writing detections and responding to novel threats. Without the ease of use combined with scalability we get from Panther, the Benchling Security Operations program would not be as mature as we are today."

WILLIAM PHILLIPS
HEAD OF SECURITY OPERATIONS