Asana Uses Engineering Principles to Automate Detection and Response Workflows with Panther

Industry: Software Development **HQ:** San Francisco, CA **Founded:** 2008 **Employees:** 1,001-5,000

Since 2008, Asana, a leading work management platform for organizations, has embraced a mission of enabling teams to work together effortlessly. With millions of users across industries collaborating on its platform, Asana must protect a large, diverse collection of data for its customers, including those within highly regulated sectors such as healthcare. To meet these challenges as quickly and cost-effectively as possible, Asana chose to embrace scalability and automation through engineering-based approaches.

Jackie Bow, Head of Detection and Response at Asana, recognized that traditional detection workflows using a traditional SIEM wouldn't scale for Asana's complex needs. "I have been in security analysis roles before, and I knew that trying to solve detection and response challenges in the traditional ways of black-box SIEM detection and heavy use of manual analyst labor would not match Asana's engineering-first culture or lead to a scalable, sustainable team," Bow said.

> "We're an engineering-driven company, and I wanted to solve the challenges we were facing in an automated way using code and engineering principles."

This approach led Bow and Asana to explore Panther.

Building a Team Focused on DaC

For most detection and response teams using legacy SIEMs, security analysts get a barrage of alerts without the context needed to investigate threats effectively. The root cause of this stems from tools that have preset detections that aren't tailored to the environments they're used in, and alerts that lack context necessary for those triaging them.

> "The reality in many SOCs is that there are just too many alerts to work through, and it results in poor return on investment on actual threats being detected."

Challenges

Scaling a detection and response program that has full visibility and control over detections and tooling

Maintaining the ability to process large amounts of security data

Onboarding a variety of stakeholders and use cases

Solutions

Automating detection and response workflows to support industry compliance

Delivering detection infrastructure-as-a-service to product engineering teams

Dynamically scaling with rapidly growing log volume for cloud workloads

Results

Eliminated introduction of manual tasks through use of intelligent log analysis

Increased threat map coverage using Detection-as-Code

Reduced projected SIEM total cost of ownership (TCO)

Bow's team sought a solution that would facilitate engineering-centric detection workflows that aligned with her team's philosophy. "We used to have a lot of siloes that made detection and response workflows challenging. It was hard to collaborate. With a dedicated Detection and Response function and the tooling that supports it, we've improved our ability to detect and respond to incidents faster," Jackie said.

> "Panther allows us to offer detection-as-a-service to other stakeholder teams. We can work with them to create custom detections that suit their specific needs, and we have the ability to manage 100% of them as code."

Accelerating Detection and Response at Scale with Panther

Asana had been using the open-source log analysis project, StreamAlert, for several years, and Bow's team found it increasingly difficult to maintain the software as they scaled. "Despite the fact that we love open source, we were using StreamAlert for detections, and as we grew, and the StreamAlert open source project became unmaintained, it was harder to manage," said Bow. "We liked how StreamAlert fit into our CI/CD pipelines and overall architecture, but the maintenance costs and the operational overhead became untenable. We were hitting a performance ceiling and needed a more powerful system that could handle the scale of our infrastructure."

With the adoption of Panther, Asana no longer needed to worry about performance or scale. Panther's cloud-native SaaS architecture allowed Asana to leverage the full power of the cloud to seamlessly scale up and down as needed, ensuring that their detection infrastructure could handle the demands of its growing platform. "Our customers expect the best from us, and that's what we built our team and system to deliver. Our cloud surface is large, so Panther's ability to process and analyze all of that data seamlessly has cut down the time it takes us to detect suspicious activity."

Asana Looks Forward to 100% Threat Map Coverage

The Asana Detection and Response team set its compass towards the ambitious goal of 100% threat map coverage. To achieve this, the team must rely on automation and dynamic systems to deal with constantly changing and growing log sources and data volumes.

With other SIEMs, Asana would be forced to choose between incurring exorbitant costs or not analyzing its most critical data. Fortunately, Panther solves both challenges through its ability to manage detection-as-code and limit cost at scale. "Our entire approach was based on avoiding hiring an army of analysts and contractors because we believe we can do better less expensively with well-designed systems," Bow said. "For this to make sense, we also needed a SIEM that we could scale up to our level of demand in a more cost-effective way than the legacy players. We could see a world of getting to our 100% threat surface coverage goal with Panther that would have cost considerably more with a collection of off-the-shelf tools from other vendors."

As the Asana Detection and Response team continues to grow, Bow is excited for the future of building even more automation across the organization and using detections to deliver additional workflow value to teams. "As other security teams, including product security and internal tooling, understand our capabilities better, we're starting to see them ask for things outside of what you'd expect detections to be limited to," Bow said. "It's really cool to see the applications of what we're doing help to make people's jobs easier. It makes it exciting to keep building together."