panther | INTERCOM

CASE STUDY

Intercom Builds High-Value Detections That Minimize Alert Fatigue

Intercom is a SaaS company that offers an all-in-one customer communications platform that helps businesses build stronger customer relationships. Intercom was founded in 2011, has grown to over 900 employees, serves over 25,000 paying customers and is a six-time Forbes Cloud 100 honouree. Intercom's threat detection team is geographically dispersed between Chicago, London, and Dublin.

Faster Threat Detection

With detection-as-code, Intercom's team can easily manage detection changes and able to tackle new and emerging threats twice as fast as previously

Reduce noise and alert fatigue

With a well-defined process and valuable context to enable faster investigation, Intercom has been able to reduce noise and alert fatigue.

Effective Use of Time

With features like Panther's Indicator Search, Intercom has reduced time spent investigating suspicious activities by 90%.

The Challenge

Industry
Software

Year Founded
2011

Location
San Francisco, CA

Company Size
1000+

Intercom's threat detection hurdles began with the need to monitor and detect threats in AWS accounts. Initially, they chose StreamAlert because it was engineer friendly and they could write their own detection rules. However, they outgrew StreamAlert soon after. As the business matured, they started processing a substantial amount of log data from numerous data sources, and the operational burden of managing StreamAlert took an unnecessary toll on the team. While evaluating Panther, they reviewed Splunk, Sumologic, and DataDog, but felt none fit their needs. "We found that other vendors couldn't fit our team's profile," said Jacopo Scrinzi, Intercom's Staff Security Engineer. "We like having version control, peer reviews for detections and needed a solution that embraced security as code."

From a security perspective, as Intercom is built on top of AWS, the team wanted to have world-class integration with AWS such as CloudTrail integration is a priority. The vendor they chose had world-class support for AWS logs with pre-built data models, and schemas that would help them onboard AWS quickly. Lastly, they wanted support for log sources such as to consolidate all their threat detection efforts into a single platform.

Choosing Panther

Intercom's security team liked Panther's cloud-native approach, which enabled them to exclusively focus on monitoring infrastructure and write effective detections while minimizing the management overhead. More importantly, Panther offered many of StreamAlert's core features — making the transition smoother.

They loved Panther's approach to creating and managing detections with detection-as-code with this, Intercom's security team was able to set up peer reviews, version controls, and test alerts before pushing detections into production. Further, they could integrate Panther with their CI/CD tool to automate the detection lifecycle.

Overall with detection-as-code, Intercom was able to tackle new and emerging threats twice as fast as previously. Intercom's security team has a motto: Every alert must add value and they live by it. First, they modify Panther's detection rules written in Python and add exceptions or changes to ensure it fits their environment. Second, they test their detections with data replay where applicable.

Third, they ship detections without a destination to monitor alerts and tweak them based on real-world responses. Finally, they use many capabilities available within Panther to prevent alert duplication and ensure these alerts don't cause any fatigue.

Given their high-value alerts, Intercom generally puts emphasis on two kinds of investigations. First, where an action by a user looks suspicious but lacks context; and second, where an actor taking an action is unknown and more data is needed to pinpoint the user. They kickstart their investigation using Panther's Indicator search, which enables them to scan IoCs such as usernames, IPs, and ARNs across log sources within seconds — saving hundreds of hours in investigation and query time and providing timely responses.

Panther's Benefits

FASTER THREAT DETECTION

With detection-as-code, Intercom's team can easily manage detection changes and deploy new ones faster and more automated.

REDUCE NOISE AND ALERT FATIGUE

With a well-defined process and valuable context to enable faster investigation, Intercom has been able to reduce noise and alert fatigue.

GIVE TIME BACK TO THE INVESTIGATION TEAM

With features like Panther's Indicator Search, Intercom has reduced time spent investigating suspicious activities by 90%. By correlating IOCs across data sources, security analysts can detect malicious activity early in the attack sequence to prevent further escalation.

FOSTER A COLLABORATIVE SPIRIT

With Panther's approach to detection building, Intercom's team has been able to bring other teams such as IT onboard to write their own detections for services, empowering them to do more.

Results: Saving time and moving faster

With Panther's ease of use and user-friendly interface, Intercom is already pulling in other teams that weren't as familiar with SIEM tools. With more teams on board, Intercom's threat detection team can remain agile, respond faster and get more accomplished.

*We love Panther. **One of the key reasons we chose Panther is the time saved for our team.** We can focus on what is unique to us; detections that allow us to monitor our environment, and having the infrastructure to do the monitoring.*

Jacopo Scrinzi, Staff Security Engineer for Intercom