panther | Randori™

CASE STUDY

How Randori uses Panther to write powerful detections & reduce false positive alerts

Randori is a SaaS-based attack surface management company that leverages offensive security principles to proactively provide visibility, actionable insights and validation to prevent breaches. The company continues to experience hyper-growth, having added numerous marquee enterprise customers in the past twelve months. At the end of 2021, Randori's growth accelerated, doubling its annual revenue in a single quarter. Randori's mission is to protect customers by helping them understand the attacker's perspective.

The Challenge

Randori is a security-forward company with extensive cybersecurity expertise. Prior to implementing Panther, the security team had to manually dig through logs to find anomalies. Aaron Fosdick, Chief Information Security Officer (CISO) and his team at Randori had to devote significant time every week reviewing each application's logs and events. While they had some visibility into threats for resources such as Google Workspace, Google Cloud Platform (GCP), Github and other services, they lacked a centralized system to ingest, manage and investigate logs to detect threats.

"We are self-starters with in-depth knowledge of how to take an attacker's perspective, but most legacy SIEMs were not geared to meet our team's specific needs," said Aaron Fosdick, Randori's CISO.

They identified four key requirements for SIEM:

- A modern tool that requires little or no on-premises infrastructure
- Low operational maintenance that would enable them to remain small and efficient
- Offer built-in & custom detections of IaaS events & SaaS applications that could be modified for their environment
- Ensure compliance with SOC 2 and ISO 27001 to meet regulatory and customer requirements in a timely manner

Choosing Panther

Fosdick was familiar with the landscape of the SIEM industry. He knew legacy SIEM tools were a non-starter since they were too slow or bulky and required a team to deploy and manage. With Panther, Fosdick was excited to consolidate and onboard all of the SaaS application log data from Slack, Atlassian and several more. Further, he leveraged out-of-the-box detections to ensure they met regulatory compliance within days while maintaining a small team of security engineers.

With Panther, The Randori security team was thrilled to use Python to customize and write detections. Other SIEM tools use a domain-specific language (DSL) which requires an additional headcount or managed security service provided (MSSP).

With Python, they had endless possibilities. They could easily write and maintain complex detection logic that maps to unique risks in their environment. More importantly, they had access to a large pool of engineers who were familiar with Python and were readily available to develop new detections.

Additionally, Randori used detection-as-code principles to write new detections faster and maintain their detections in a repo that mapped to their CI/CD environment.

Panther's Benefits

With Panther, Fosdick was able to improve security operations within days. Panther enabled Randori to succeed by providing:

Faster triaging with actionable alerts

While most SIEMs cause alert fatigue, Panther allows security teams to create actionable alerts that offer rich context into what happened, when it occurred, and who the actor was. As such, Randori's security team could effectively dismiss or escalate security issues with ease.

Fewer false positives

With an extensive rule repository as well as the flexibility to write custom detections, Randori's security team could fine-tune detections to fit their environment. Additionally, Python helped build complex detections with fewer false positives with better alert context.

Faster time to compliance

In order to comply with PCI requirements, a SIEM is a hard requirement, and many customers were demanding Randori to be compliant. As a result of Panther's out-of-the-box capabilities, Randori was able to meet and exceed numerous risk and compliance regulations such as PCI, SOC 2 and ISO 27001.

Results: Lower cost and higher ROI

With Panther, Randori has saved several hours per week per person, allowing them to focus on detection and response. Alerts can be resolved in minutes instead of hours or even days. All of this enabled Randori to lower their total-cost-of-ownership by approximately 70%.

"We have a solid obligation to protect our customer data, and to say that we trust Panther with our event logs goes a long way for us," Aaron Fosdick, CISO of Randori.

In the future, Randori plans to add more cloud apps and leverage Panther to ingest data from resources like Azure, Syslog and FluentD.

Detect Any Breach, Anywhere

Try Panther

panther.com