panther | cedar

CASE STUDY

Cedar Scales Security and Gains Better Visibility with Panther

A modern approach to security operations leveraging detections-as-code

Challenges

Storing and searching rapidly increasing volumes of data

Mapping alerts to business needs

Centralizing audit logs and security data

Solution

Normalized data to enhance visibility and improve performance

Customized alerting with Python

Centralized security data lake for long-term storage

Benefits

Detected new risks that had previously been obfuscated

Reduced time spent creating new alerts from 2 weeks to 1-2 days

Reduced false positives by 80%

Cedar is revolutionizing healthcare technology & patient experience

Cedar combines healthcare, tech, and design to create a seamless financial experience for every patient. Cedar serves more than 10 million patients per year and works with 33 client partners around the United States. Cedar collects, processes, and stores healthcare and financial information for its customers and partners. The Cedar security team needed to unify data, enhance security monitoring, accelerate business decision-making, and document activities to meet strict compliance mandates.

Too much data from too many places

Cedar's security team relied on a combination of traditional SIEM solutions and open-source software to monitor its services, applications, and security controls. However, these failed to support the volume of log data generated from disparate cloud sources and were unable to map back to Cedar's unique business needs for security, leading to poor performance and incomplete visibility.

Inability to scale with the business

As Cedar rapidly grew and evolved, it adopted many new applications and cloud services. Across the organization Google Workspace (formerly GSuite) became a key collaboration tool, but each team used it differently. The increased IT complexity increased the risk of data breaches and noncompliance.

panther | cedar

CASE STUDY

Detections-as-Code: Helping Cedar Scale Security

Leveraging Infrastructure-as-Code to streamline operations

Cedar deployed Panther as Infrastructure-as-code (IaS) to build its security monitoring infrastructure and reduce the overhead associated with collecting new data from their cloud environment. By leveraging reusable templates and cloud systems like SQS and S3 to move and store data, Cedar's security team can easily ingest and unify data across multiple cloud accounts and regions.

Gaining real-time visibility into security risk changes

Cedar leverages Panther's stream processing detection engine to analyze logs for suspicious activity in real-time. For example, Cedar configured their AWS CloudTrail to send logs to Panther, established an alerting threshold to avoid alert flooding, and sent alerts to Slack for fast review.

Applying CI/CD to security and compliance

Using Panther, Cedar can easily build new rules that allow them to continuously iterate their security program. The Panther platform enables Cedar to easily integrate detection management into its CI/CD pipeline for an automated, hands-off approach to deploying new alerts.

Creating detection pipelines with Python and automation

By using Panther to build alerts with Python, Cedar's team created a repeatable and easy-to-maintain process that enabled consistent, flexibile security monitoring across divergent cloud resources. When the security team creates a new detection, a branch from the repository is pushed to source control, and a pull request is opened. When the merge occurs, Cedar's new detections are automatically pushed and enabled in Panther.

Enhancing controls with detection-as-code

Cedar's team customizes Panther's out-of-the-box alerts, sets baseline behaviors, and utilizes popular Python libraries for enhanced monitoring and detection and response. The team now manages all of their detections as code in a GitHub repository and uses source control to conduct code review and versioning. Because all of their alert logic is written in Python, the Cedar team can quickly understand the alerts generated, providing better visibility into patterns and greater control over alerting.

The Results: A Small but Mighty Security Team

With Panther's ability to create a unified view of people, processes, and technology, Cedar's security team created an automated, systematic, repeatable, predictable, and shareable approach to security that continues to improve their overall security posture.

cedar

"Panther's architecture is perfect for modern technology organizations: easy to roll out, scalable, and with an interface that helps us centralize and expand several of our core security & compliance operations."

Aaron Zollman
CISO, Cedar

Detect Any Breach, Anywhere

Try Panther

panther.com