panther | aws

Panther + AWS

Detect AWS misconfigurations and suspicious activity in real-time with detection-as-code and normalized logs in a security data lake

Amazon Web Services (AWS) provides cost-effective and agile cloud services that enable rapid innovation. Purposefully designed as a flexible, secure cloud computing environment, its core infrastructure powers companies across industry verticals and enterprise sizes. However, while the cloud streamlines business operations, expanding environments increase the complexity of enforcing security controls and add to the risk of costly breaches. To operate securely in AWS, data from a variety of services such as CloudTrail, S3, and VPC flow logs need to be collected, analyzed, and retained for threat detection and forensics analysis. But pulling large volumes of data from AWS into a SIEM can be technically challenging and prohibitively costly, and frequently requires dedicated teams to manage ETL pipelines that normalize data at scale.

Security professionals securing AWS environments face a number of key challenges today, including:

Noisy data

Complex environments

Inefficient tools

$ High operational costs

panther | aws

PANTHER FOR AWS

Powered by Detection-as-Code and a Security Data Lake

With a single platform for aggregating, organizing, and prioritizing security-relevant data from AWS accounts, Panther provides the foundation for security teams to monitor activity and enforce controls across rapidly expanding environments.

Panther makes it easy to collect a variety of AWS security logs and provides normalization, real-time analysis, and a scalable data warehouse to store and query data during an investigation. For modern, cloud-focused teams heavily leveraging AWS, Panther provides a fast, scalable, and flexible platform for detection and response. Deployed in a single tenant SaaS environment, Panther removes the operational burden of managing infrastructure and empowers teams to focus on what they know best: security.

With Panther for AWS, security teams can quickly bootstrap a centralized security data lake with all security-relevant logs like CloudTrail,ALB access logs, VPC flow logs, GuardDuty, and more.

Once processed, teams can explore their data with SQL and trigger high-fidelity alerts with Python.

Detection-as-code, real-time alerts, and a scalable security data lake provide the powerful capabilities security teams need to detect increasingly sophisticated threats and answer critical questions during a breach.

KEY FEATURES

Panther Is Designed To Secure Your AWS Environment

Daily Cloud Scans

Continuously monitoring your entire AWS infrastructure for changes and insecure configurations

Complete Resource Visibility

Understand your cloud footprint by modeling AWS resources as JSON

Configuration Change Logs

Enrich CrowdStrike Falcon data and retain historic information so your security team can improve key metrics like Mean Time to Investigate (MTTI) and Mean Time to Respond (MTTD)

Compliance Out-of-the-Box

Map detections to frameworks like MITRE ATT&CK and CIS to ensure regulatory compliance

PANTHER + AWS

Flexible, Scalable, Searchable Cloud Security and Compliance

As cloud environments grow, enforcing security becomes increasingly complicated. A recent report from the Cloud Security Alliance, **"State of Cloud Security Concerns, Challenges, and Incidents"**, found that misconfigurations are one of the leading causes of breaches and outages.

With real time alerts and more than 150 out of the box detections, Panther provides the visibility and alerting infrastructure teams need to monitor configurations across all of their critical AWS services.

Use Case: Enforcing AWS Security Controls

CHALLENGE	SOLUTION
Detecting misconfigurations across complex, sprawling AWS environments.	Detect every configuration change and store a complete history of AWS compliance ina security data lake. Aggregate disparate AWS logs and secure your entire AWS environment with custom and out of the box detection as code. Monitoring of CloudTrail to automatically discover new assets and maintain an accurate inventory and history of all of your AWS cloud assets. Review the state of all of your cloud assets and infrastructure at the time of an incident to effectively investigate it and maintain strong security.

Use Case: Fast Investigations Across Large Volumes of Data

CHALLENGE	SOLUTION
Slow searches, disparate data formats, and limited retention	Quickly create a security data lake, a structured security logs data warehouse without any overhead or data ops. Combine all of your security logs, both AWS and logs from other SaaS applications such as Okta, G Suite and hundreds of other environments. Run fast searches with columnar data and scalable computing power to detect incidents and accelerate security investigations and make it easy to quickly find the malicious needle in your security data haystack that you need.

SEE PANTHER + AWS IN ACTION

Request a Demo