AWS Detective

CloudSiksha

AWS Detective

- Amazon Detective makes it easy to analyze, investigate, and quickly identify the cause of a potential security threat or suspicious activity
- Amazon Detective automatically collects historical data from your AWS resources and uses machine learning, statistical analysis, and chart theory to create a linked dataset that enables you to conduct faster and more efficient security audits

Benefits of AWS Detective

- Using Amazon Detective's ready-made data aggregations, summaries, and contexts, you can quickly analyze and determine the nature and scope of potential security problems
- Amazon Detective holds aggregated data for up to a year and makes it available through a series of visualizations that show changes in the type and extent of activity in a selected time window and links these changes to safety findings

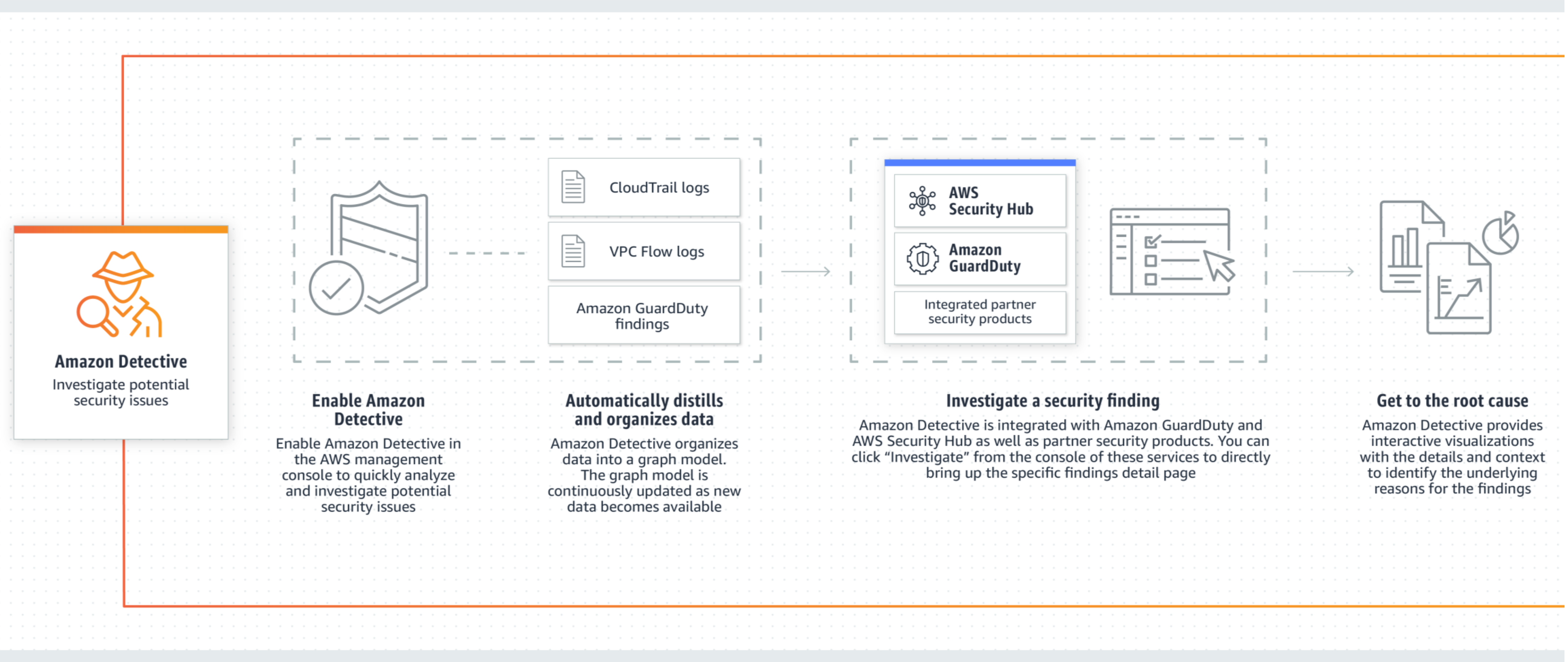
Data Sources

- With Amazon Detective, customers can view summaries and analytics data on AWS CloudTrail events and VPC flow logs. For customers who have Amazon GuardDuty enabled, Detective also processes the findings from Amazon GuardDuty.

Different between Detective & GuardDuty

- Amazon GuardDuty is a threat detection service that continuously monitors and protects your AWS accounts and workloads for malicious and unauthorized behavior
- Amazon Detective simplifies the process of investigating security outcomes and determining the root cause. Amazon Detective analyzes trillions of events from multiple data sources, such as: B. Findings from PC Flow-Logs, AWS CloudTrail Logs and Amazon GuardDuty, and automatically creates a diagram model that gives you a unified, interactive view of your resources

AWS Detective



Amazon Detective

Investigate potential security issues

CloudTrail logs

VPC Flow logs

Amazon GuardDuty findings

AWS Security Hub

Amazon GuardDuty

Integrated partner security products

Enable Amazon Detective

Enable Amazon Detective in the AWS management console to quickly analyze and investigate potential security issues

Automatically distills and organizes data

Amazon Detective organizes data into a graph model. The graph model is continuously updated as new data becomes available

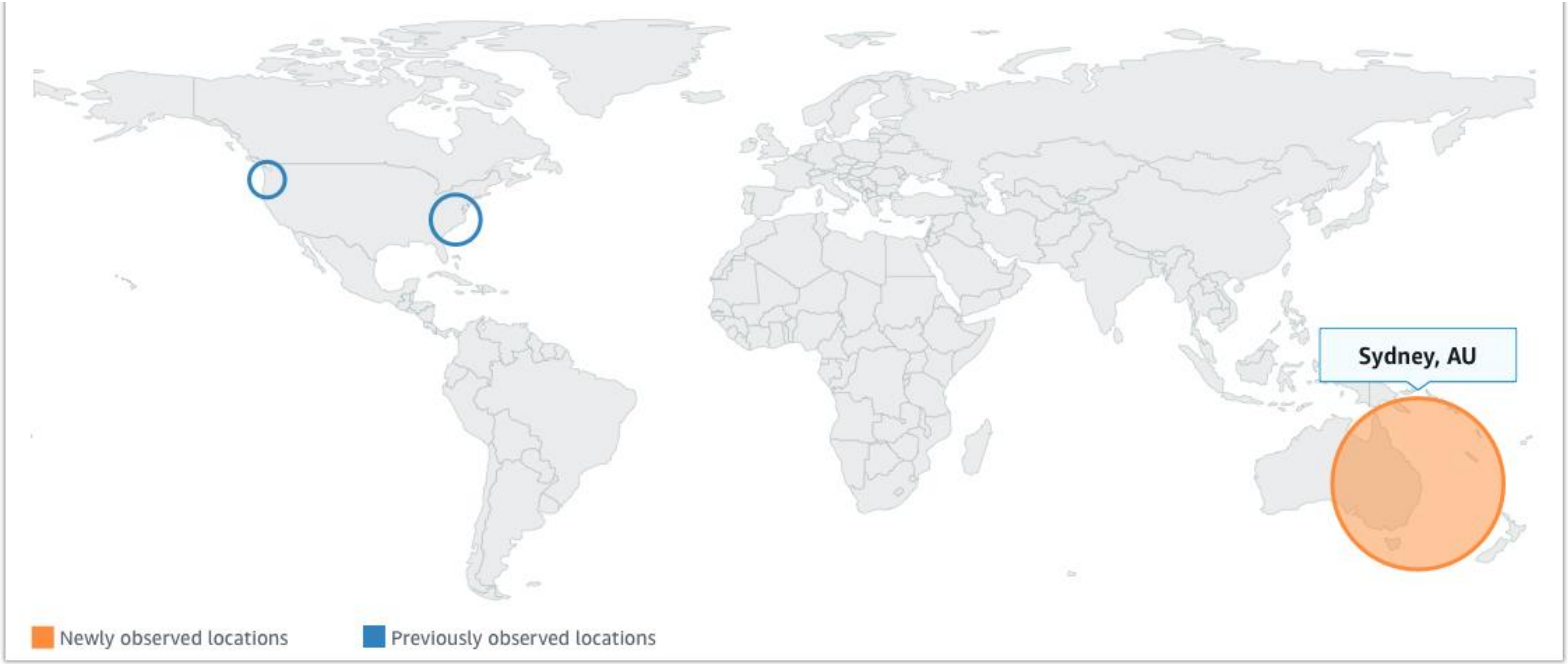
Investigate a security finding

Amazon Detective is integrated with Amazon GuardDuty and AWS Security Hub as well as partner security products. You can click “Investigate” from the console of these services to directly bring up the specific findings detail page

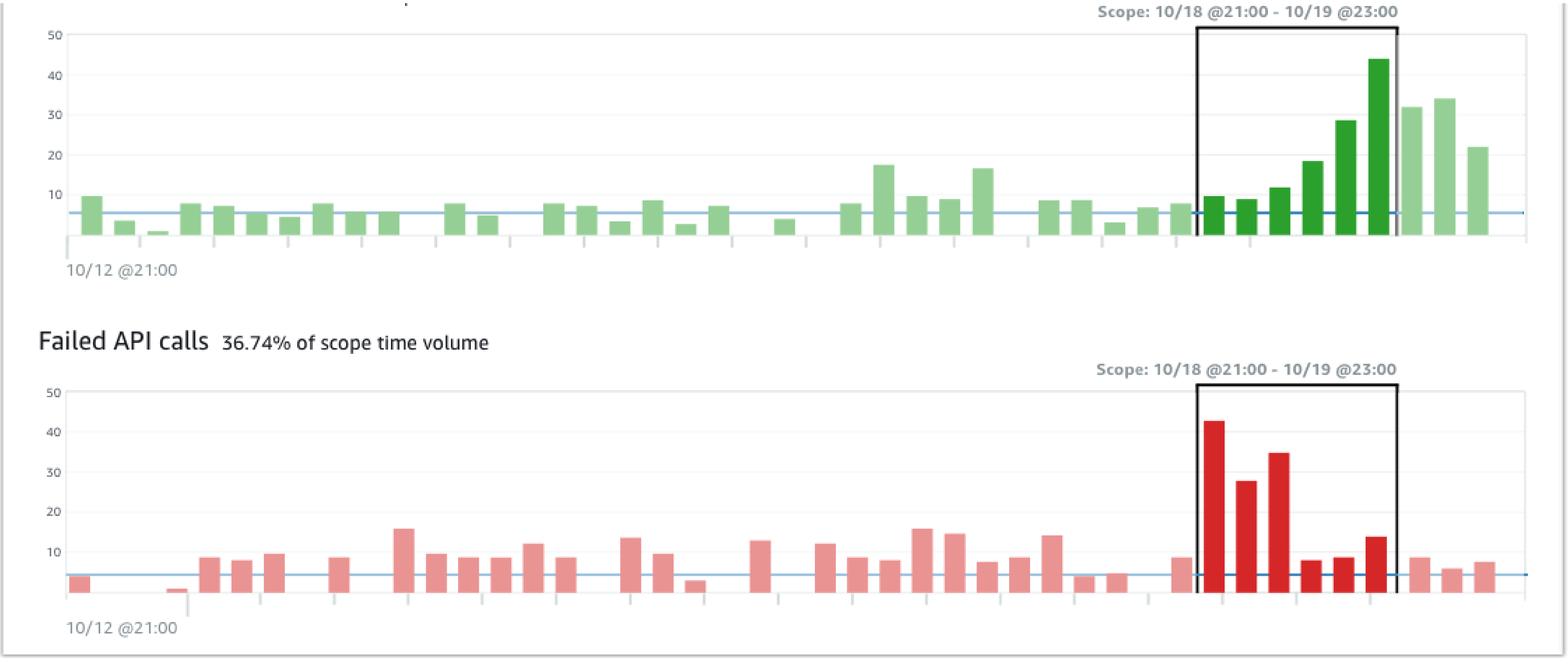
Get to the root cause

Amazon Detective provides interactive visualizations with the details and context to identify the underlying reasons for the findings

Some Findings



Some Findings



Failed API calls 36.74% of scope time volume

Scope: 10/18 @21:00 - 10/19 @23:00
50
40
30
20
10
10/12 @21:00
Scope: 10/18 @21:00 - 10/19 @23:00
50
40
30
20
10
10/12 @21:00

CloudSiksha

Thanks