

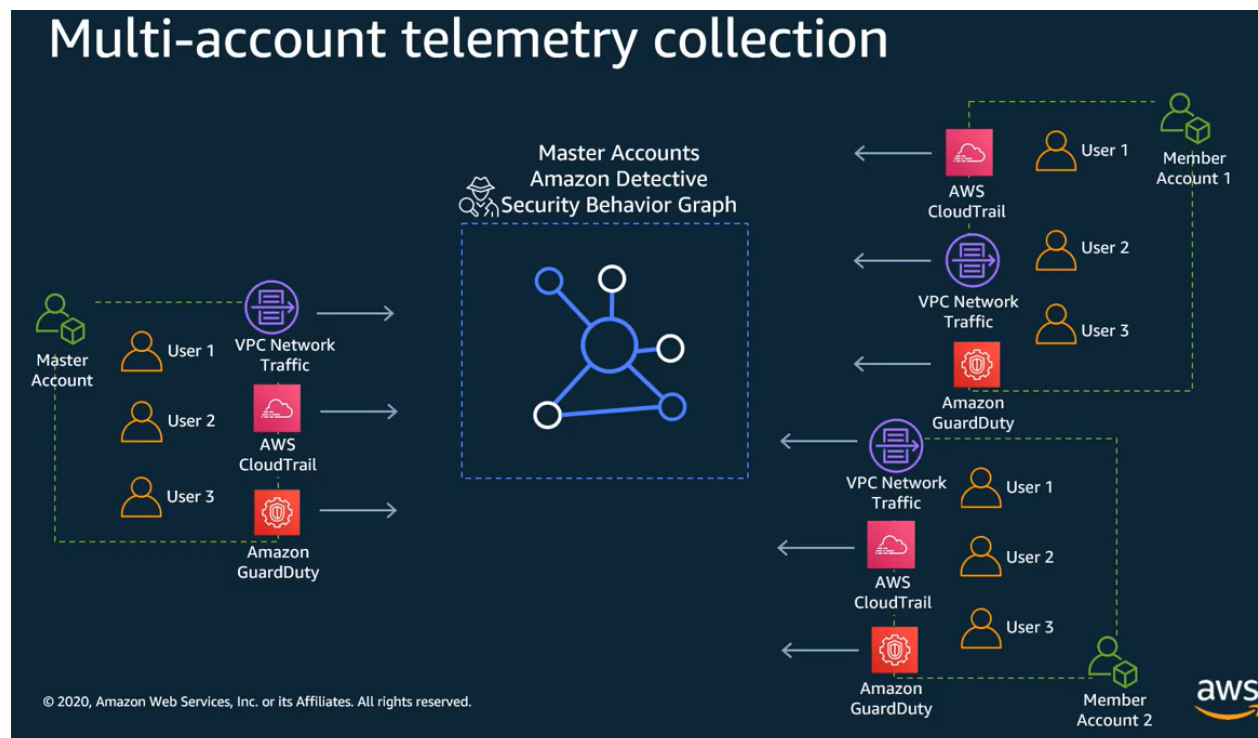
Overview

Analyze and visualize security data to rapidly get to the root cause of potential security issues.

Amazon Detective makes it easy to investigate, analyze, and quickly identify the root cause of potential security issues or suspicious activities.

Amazon Detective automatically collects log data from your AWS resources and uses machine learning, statistical analysis, and graph theory to help you visualize and conduct faster and more efficient security investigations.

Amazon Detective is integrated with AWS security services such as Amazon GuardDuty and AWS Security Hub as well as AWS partner security products.




Workflow

We currently bring the logs without any setup and automatically analyze them and store the logs for a year. The following data will be brought in for the analysis:


- CloudTrail management event
- VPC flow logs Events
- Guard Duty Findings

You don't need to have CloudTrail or VPC Flow logs enabled on your account in order to analyze these data.


Quickly analyze, investigate, and identify the root cause of security issues



Built-in data collection



Automated analysis



Visual insights

Use cases

1. Findings / Alert triage
Accelerate triage and avoid unnecessary escalations. Let's say you have Guard Duty findings and wanted to see whether you need to escalate it or not, Amazon Detective can help you decide that.
2. Incident Investigation
Now that you know there is an issue, Amazon detective helps you find out how long this issue is happening based on the history data. Or How many resources are affected
3. Threat Hunting
You may have an indicator like an IP address and you want to find out how your environment and resources are interacted with it. Then this is useful