Introducing Amazon Detective

Luis Maldonado, Sr. Manager, Product Management, AWS

Gagan Prakash, Sr. Product Manager, AWS

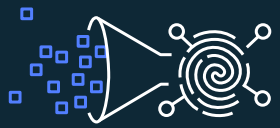
January 29th 2020

aws

Agenda

- Introduction
- How it works
- Demo
- Service details

Investigation challenges



Signal to noise ratio

Complexity

Skills shortage

Costs

Amazon Detective

Preview

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

Built-in data collection

Automated analysis

Visual insights

Amazon Detective example use cases

Amazon Detective example use cases

Finding investigation

How much data was sent?

Is this traffic normal?

What happened just before?

Are these call failures common?

Amazon Detective example use cases

Incident scoping

What API calls were made from that IP?

Do the calls indicate reconnaissance?

What other principal IDs were used?

What other instances communicated with that IP?

Amazon Detective example use cases

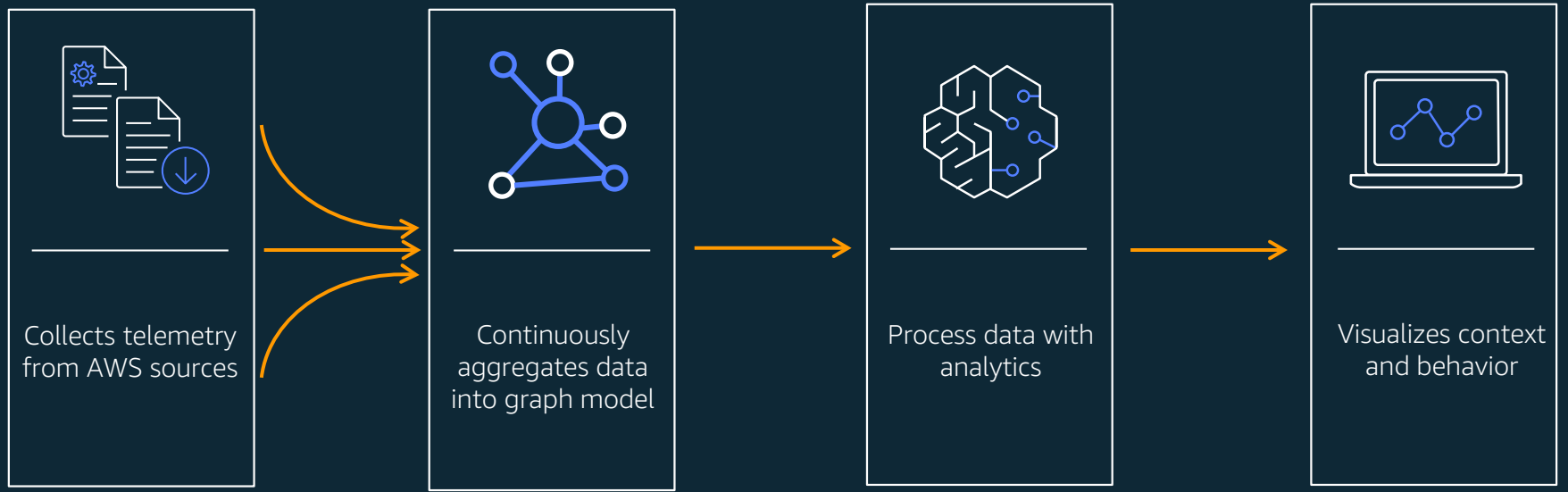
Indicator search

Did this IP address from our threat report communicate with any of EC2 instances over the last year?

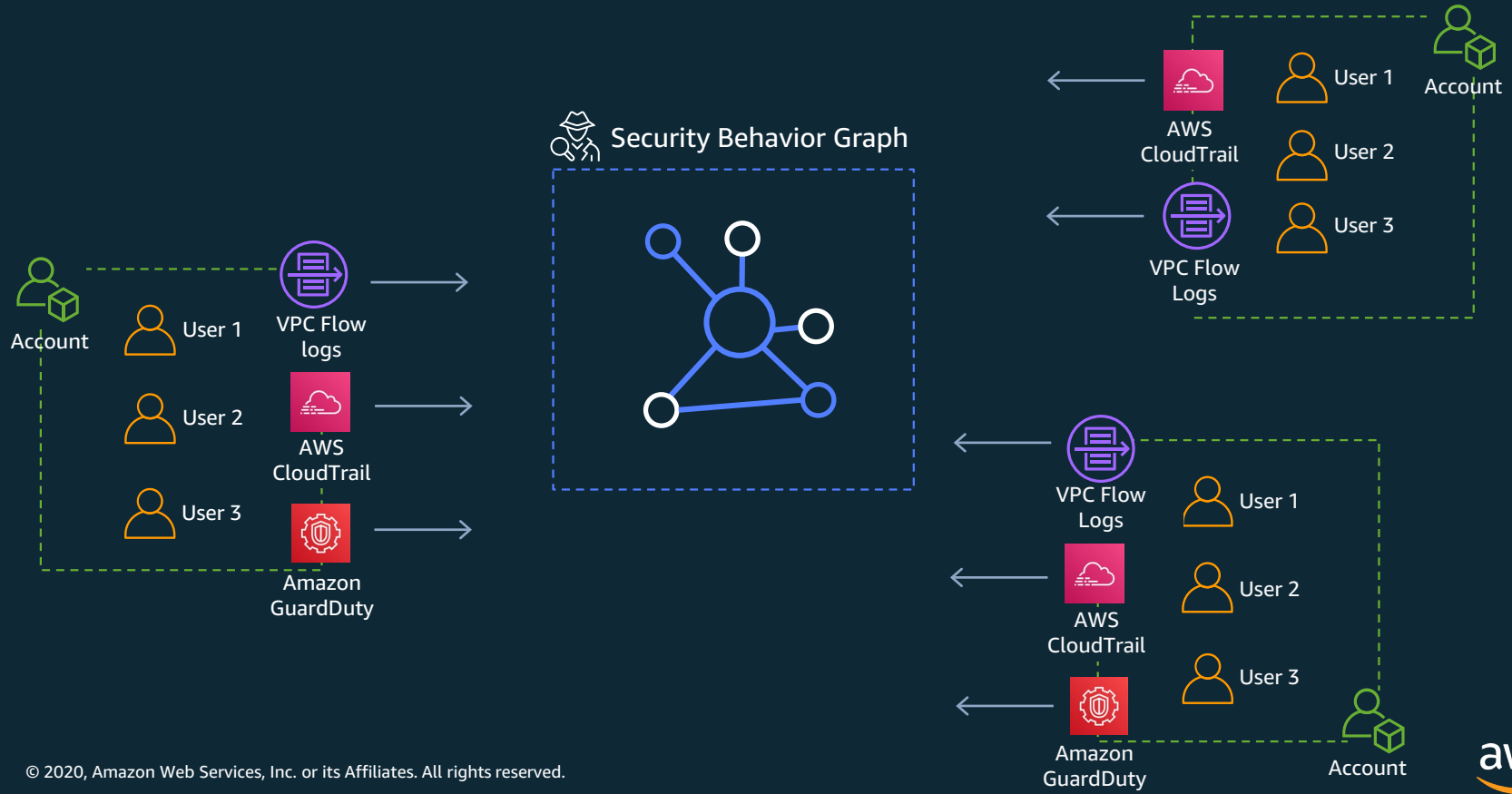
Did this suspicious user agent issue any API calls?

How it works

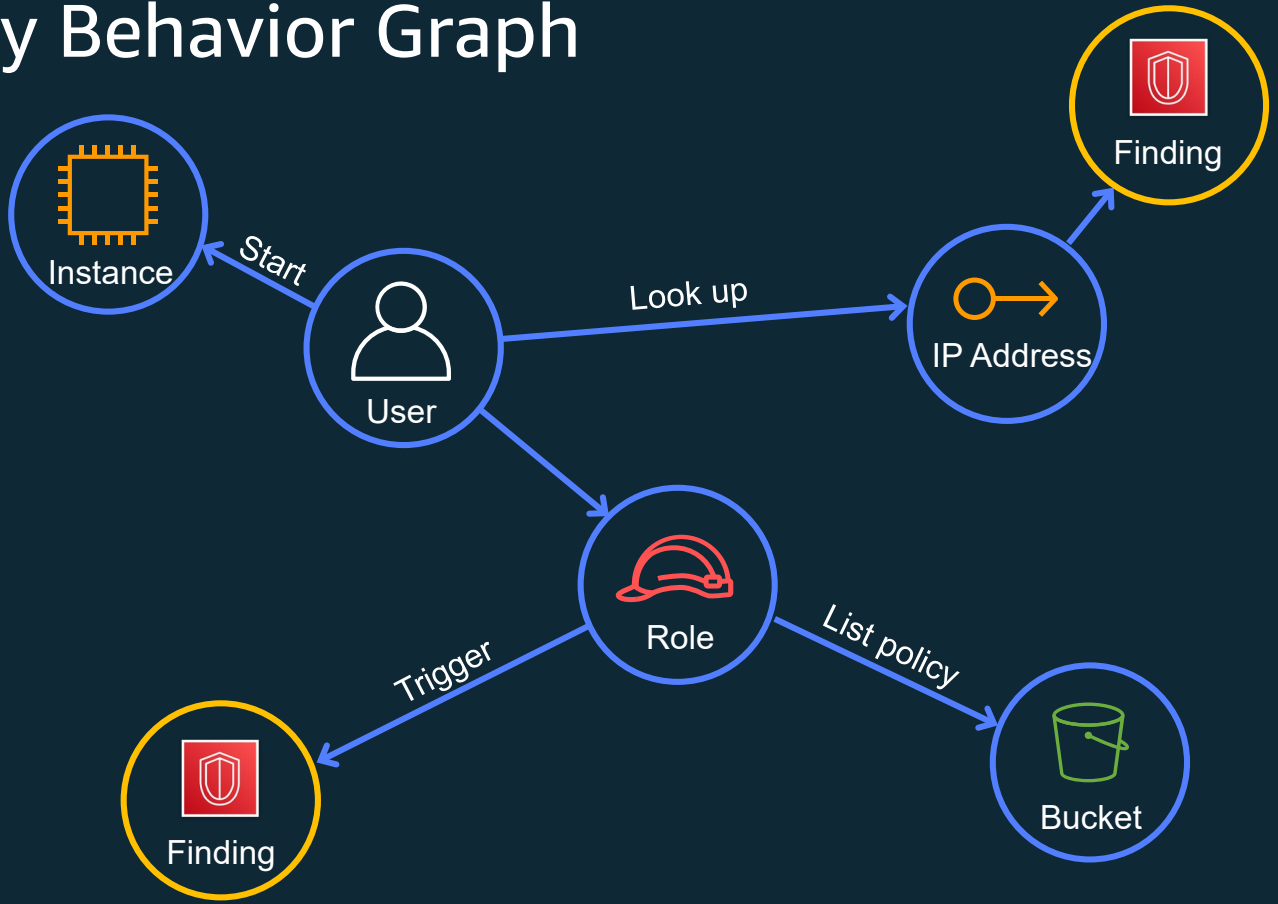
Amazon Detective processing flow



Multi-account telemetry collection



Security Behavior Graph



Can you see the traffic flow between the IP and the instance?

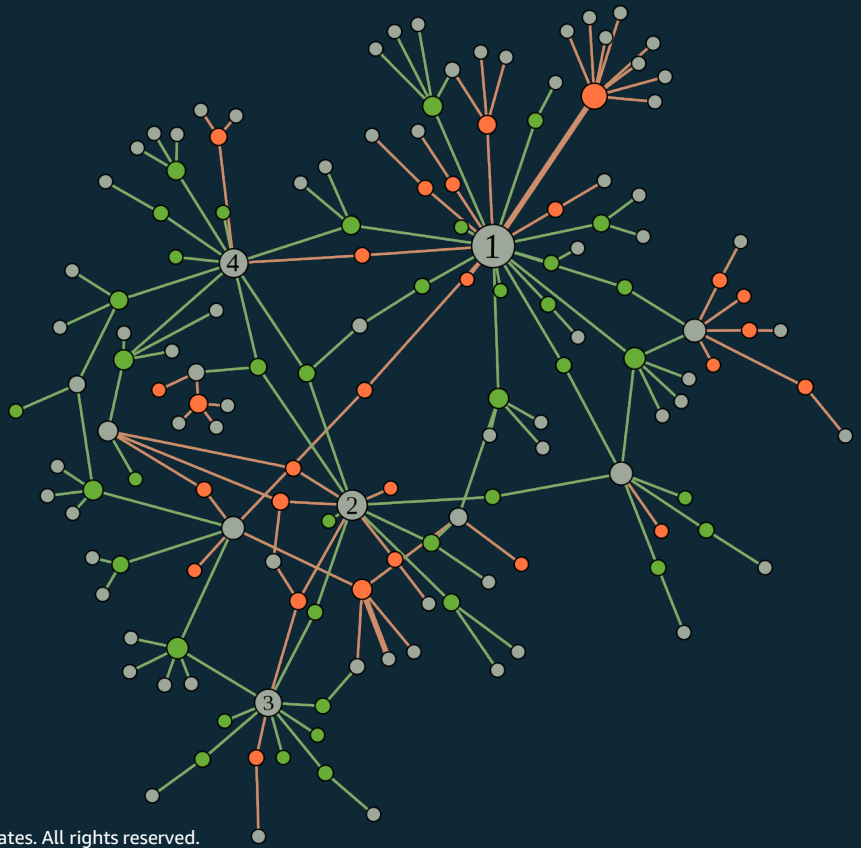
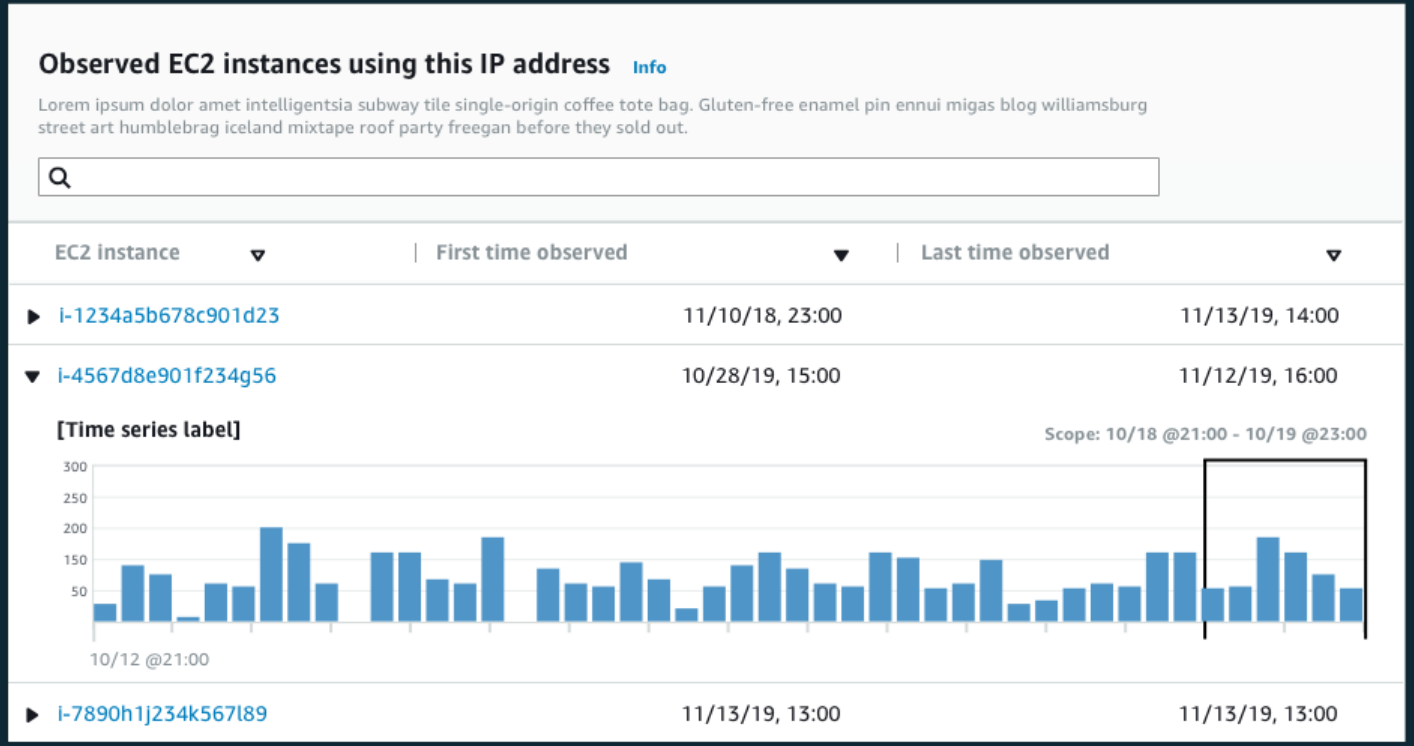
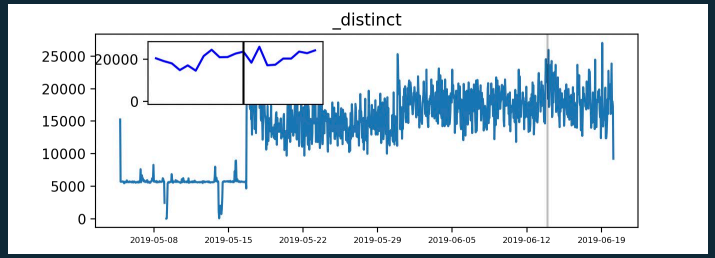


Image courtesy of Wikimedia

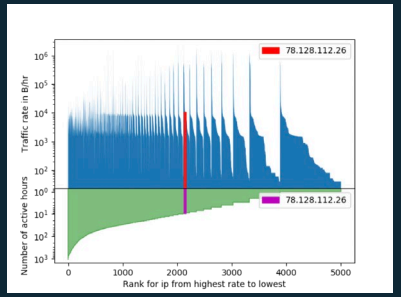
How about now?



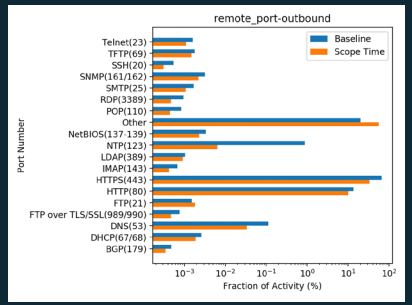
Powered by data scientists



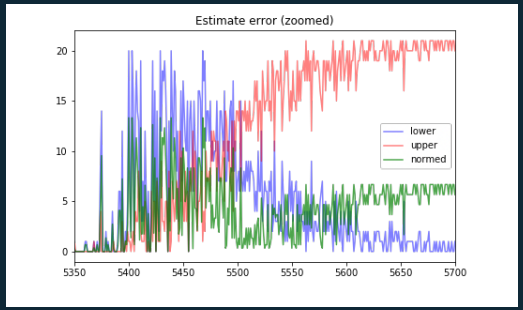
Behavioral baselines



Distributions



Time series analysis



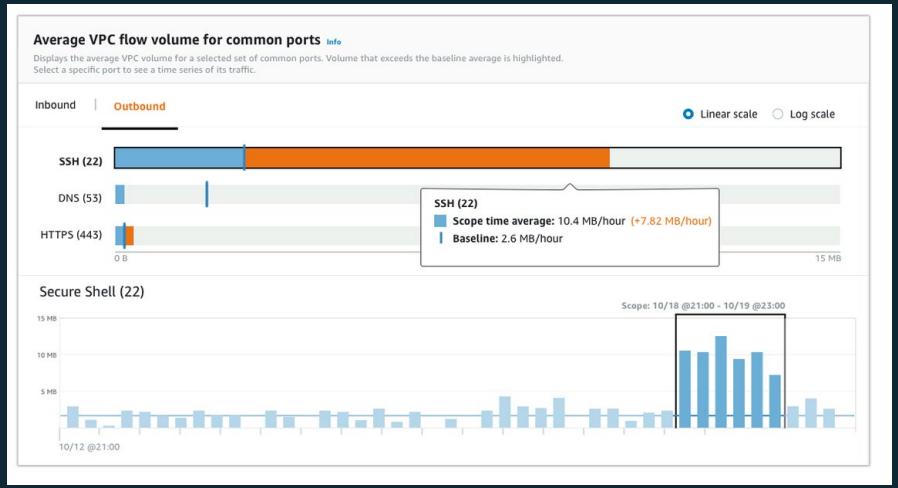
Data stream analytics

aws

Visualized for security analysts

How much data was sent?

Is this traffic normal?



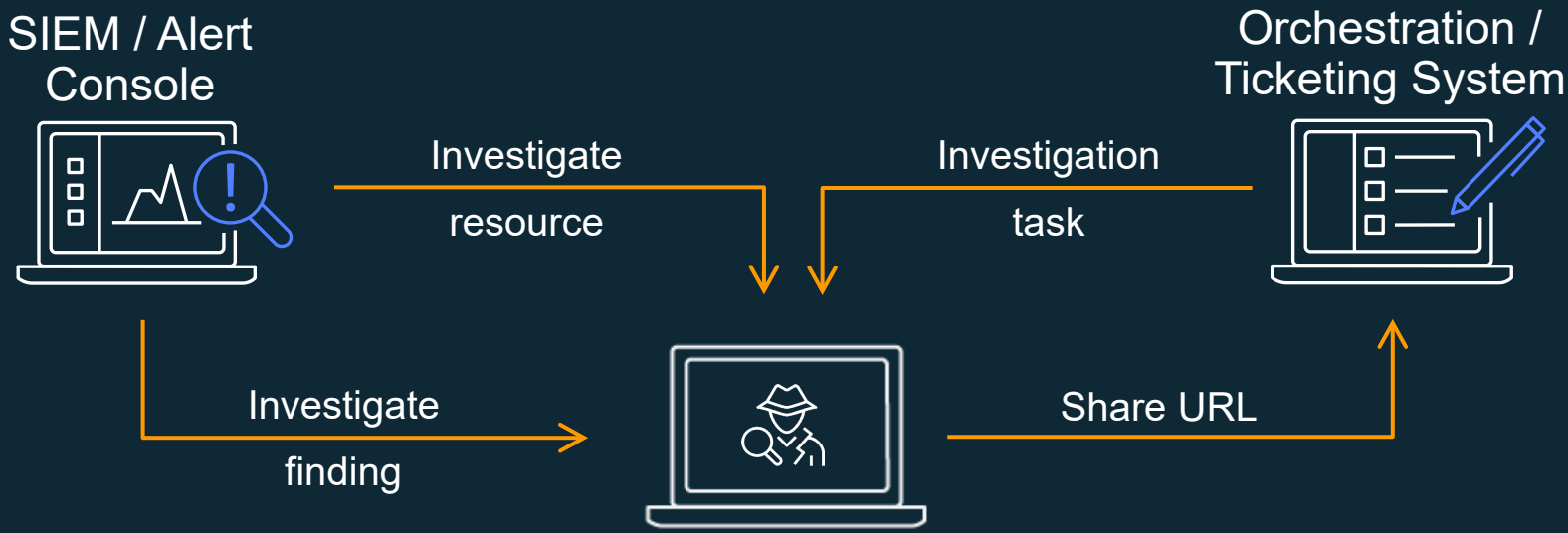
What happened just before?

Are these call failures common?

aws

Demo

Amazon Detective workflow integration



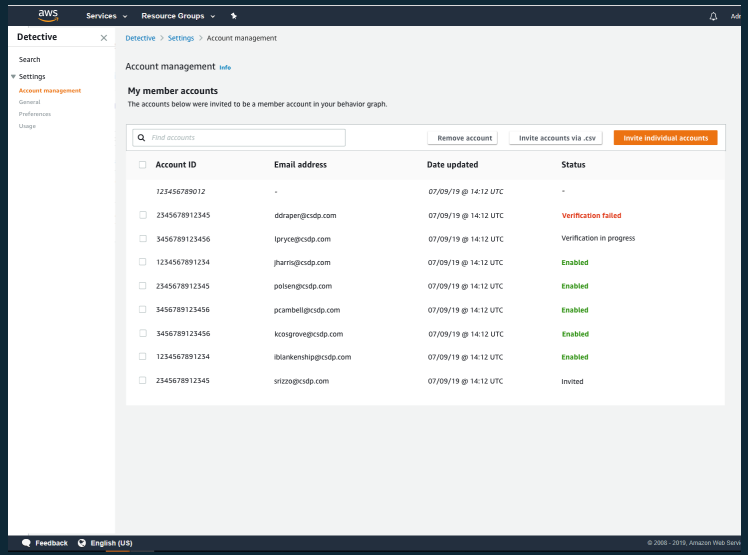
Amazon Detective integrations and managed services

Technology partners

Services partners

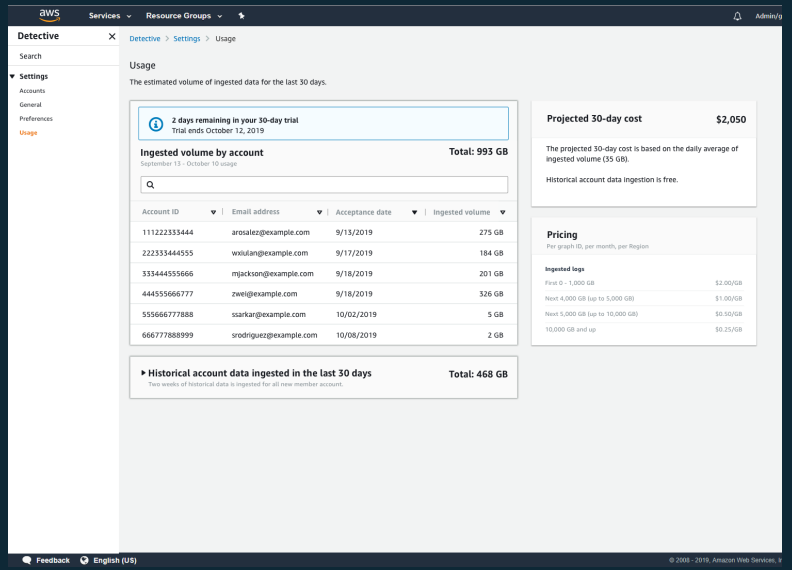
aws

Getting started



Simple multi-account management

30 day free trial and cost estimator



2 weeks of preloaded data

US-East Pricing

	Price
First 1000 GB/month	$2.00 / GB
Next 4000 GB/month	$1.00 / GB
Next 5000 GB/month	$0.50 / GB
Above 10000 GB/month	$0.25 / GB

What's included

- Data sources
  - Amazon Virtual Private Cloud (Amazon VPC) Flow Logs
  - CloudTrail management events
  - GuardDuty findings
- 1 year of Security Graph data

aws

Preview available in 5 regions

General Availability (GA) in all commercial regions Q1 2020

aws

Learn more and sign up

aws.amazon.com/detective

Q&A