
AWS
re:Invent

SEC301

Security investigations with Amazon Detective

Keith Gilbert
Senior Security Engineer
Amazon Detective

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Amazon Detective overview

Investigation enablement

Step-by-step investigation

Review



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon Detective overview



AWS re:Invent

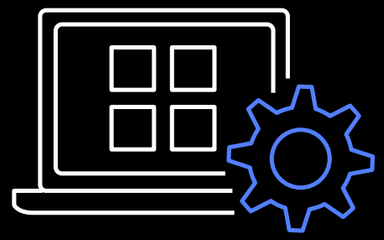
© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon Detective benefits

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



Built-in data collection

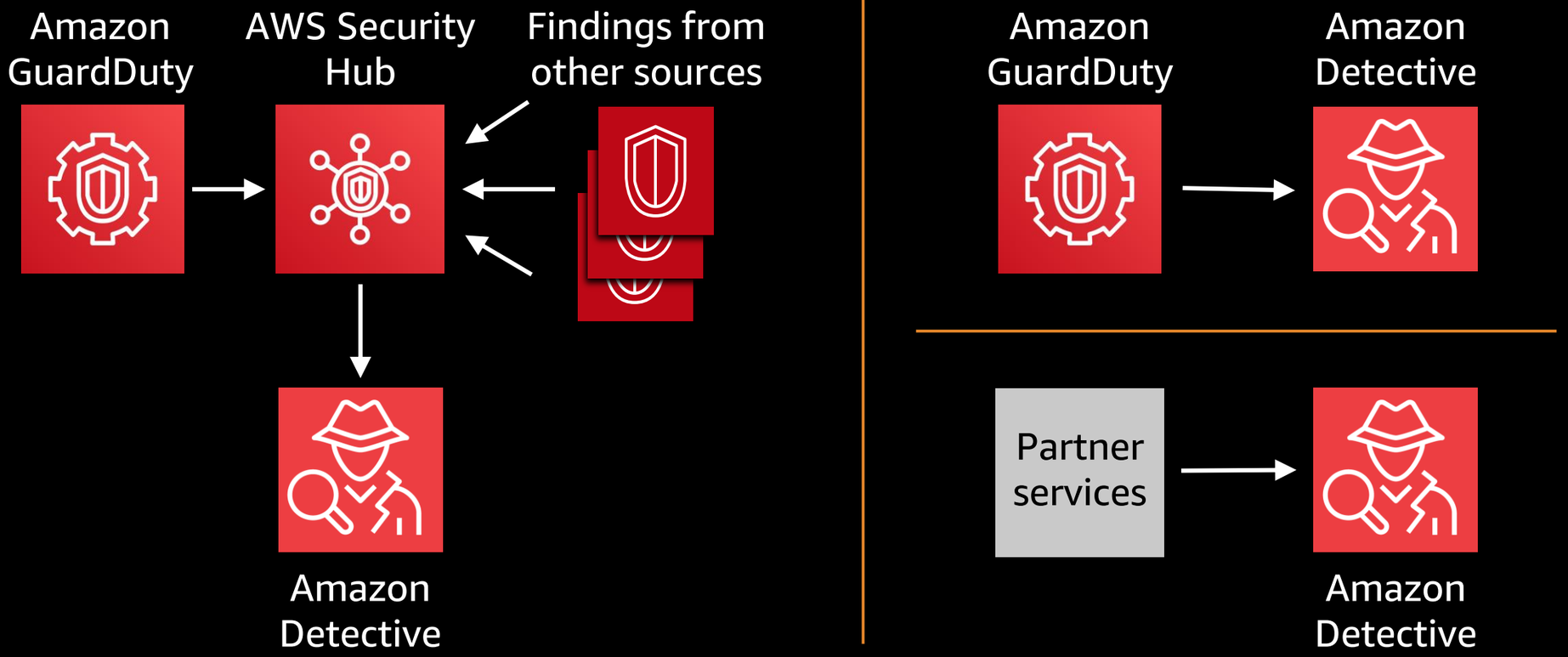


Automated analysis

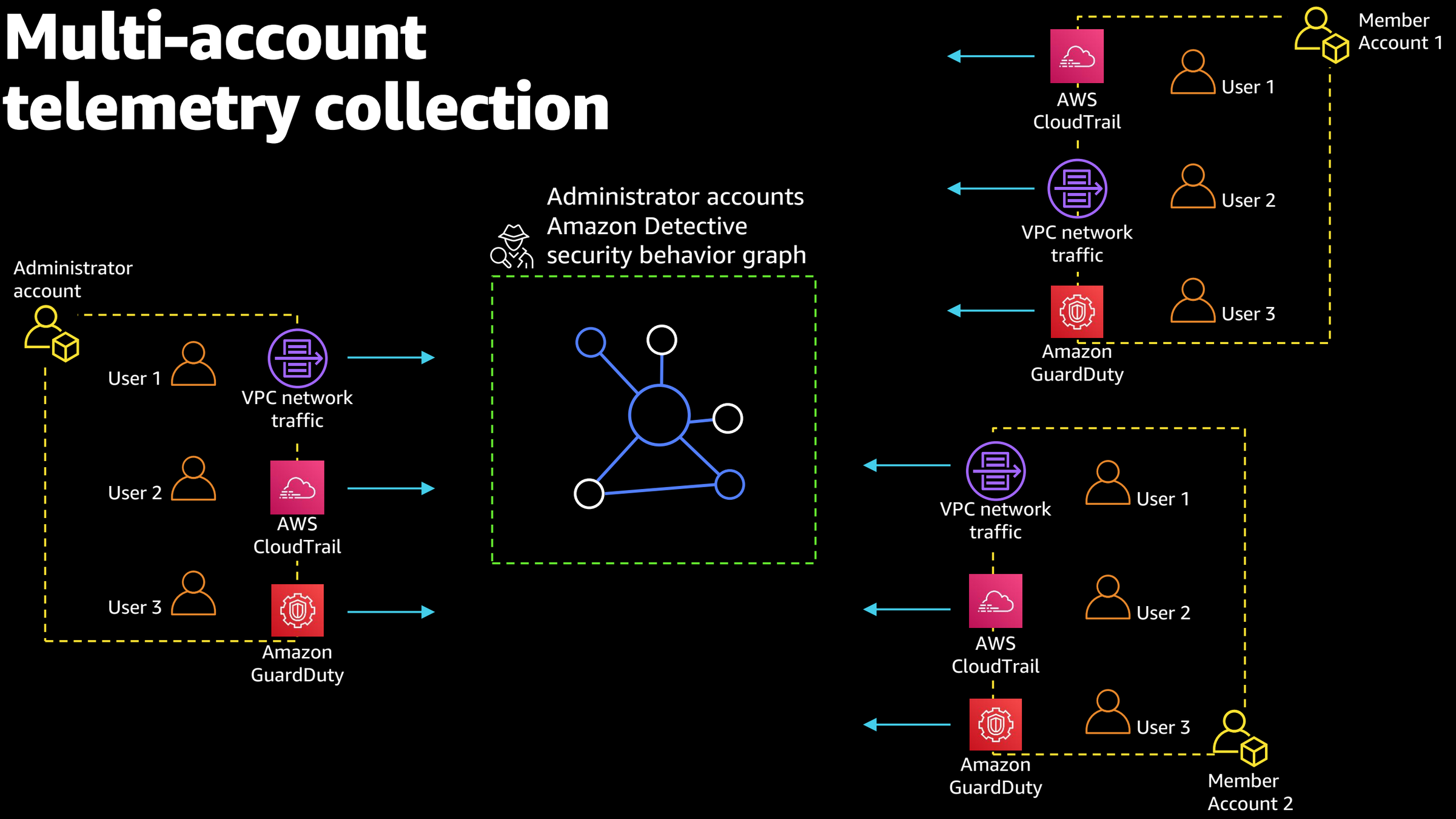


Visual insights

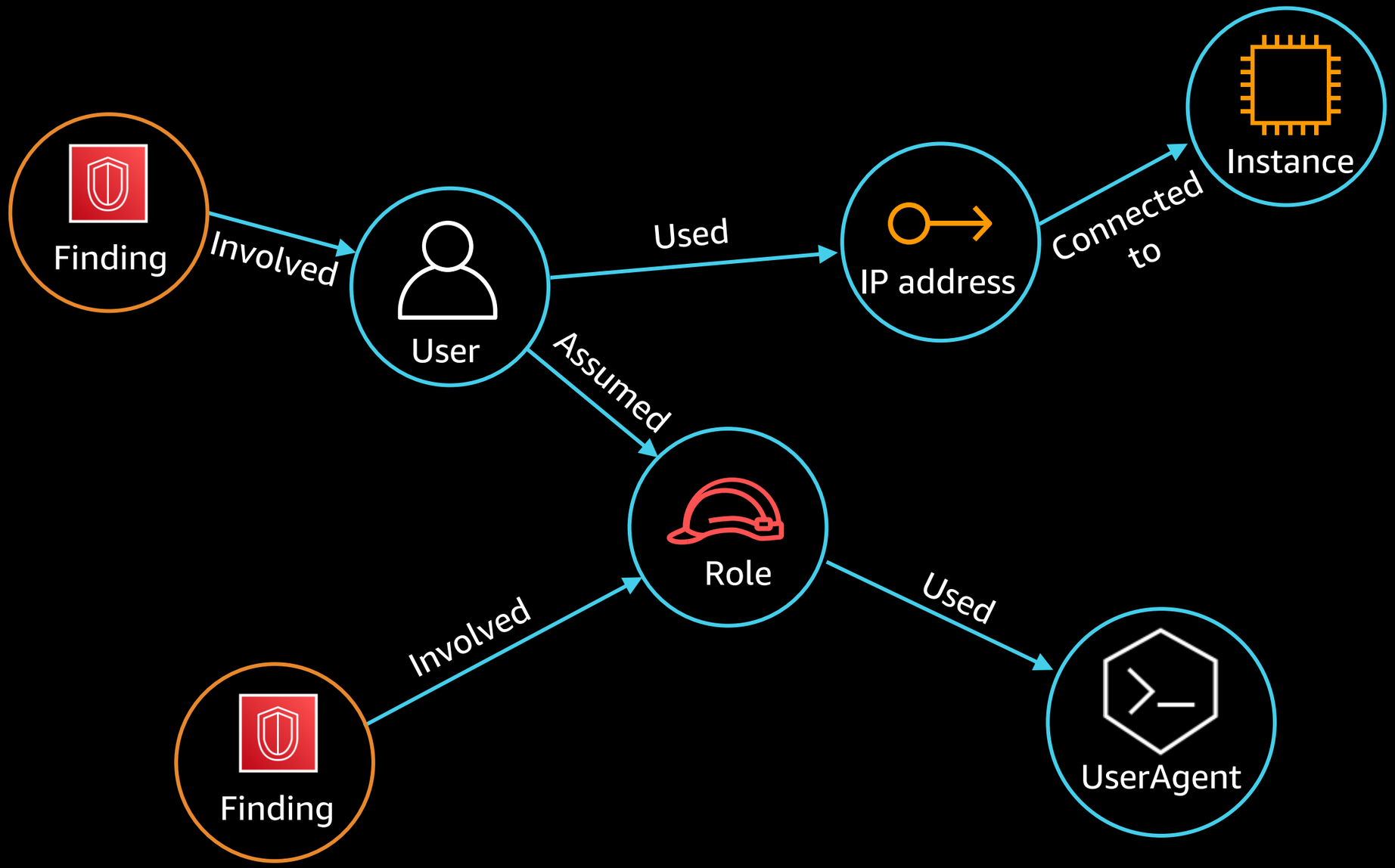
Detective usage flow



Multi-account telemetry collection



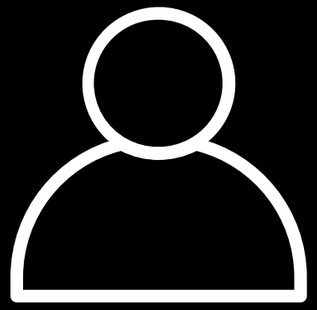
Security behavior graph



Supported entity profiles



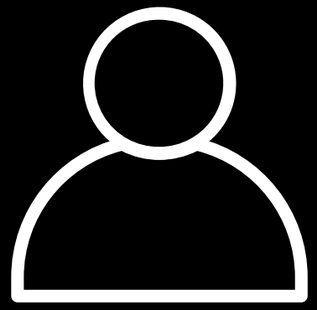
Finding



AWS user



AWS role



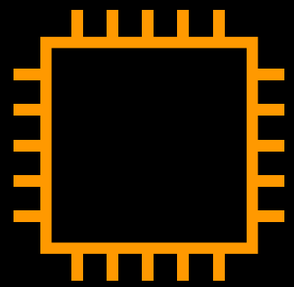
Federated user



Role session



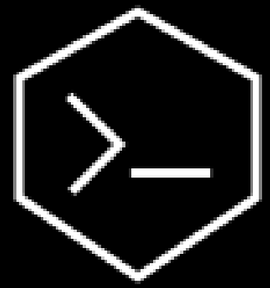
Account



EC2 instance



IP address



User agent

Use cases and personas

Alert analyst

1 Finding / alert triage
Accelerate triage and avoid unnecessary escalations

Incident responder

2 Incident investigation
Improve context and surface correlated behavior

Hunter

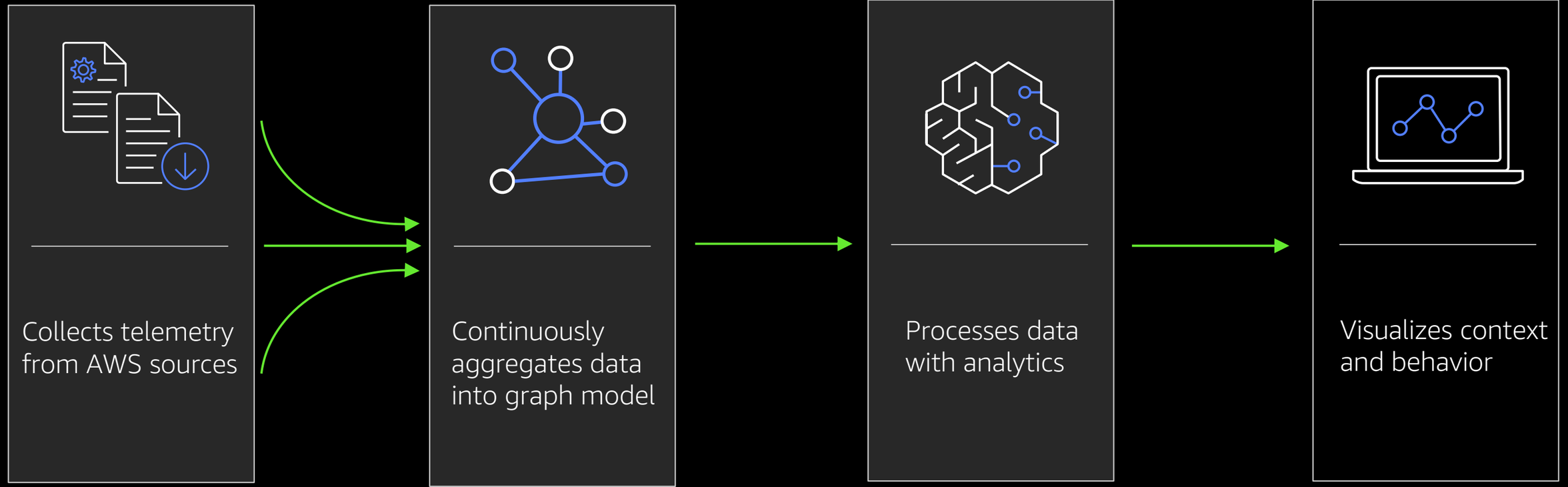
3 Threat verification
Simplify data collection, aggregation, and pivoting

Investigation enablement



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Data flow


Collects telemetry from AWS sources
Continuously aggregates data into graph model
Processes data with analytics
Visualizes context and behavior

IAM entity analysis

Common questions

- What roles did this user assume?
- What users assumed this role?
- What did User X do while using Role Y?
- Was there anything unusual about User X’s use of Role Y?

IAM entity analysis


```
"userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAVA7A5SDPGOJHKCNFJ",
    "arn": "arn:aws:iam::345679696094:user/marymajor",
    "accountId": "345679696094",
    "accessKeyId": "AKIAVA7A5SDPKDQZ7V6P",
    "userName": "marymajor"
},
"eventTime": "2020-09-30T14:35:29Z",
"eventSource": "sts.amazonaws.com",
"eventName": "AssumeRole",
"awsRegion": "us-east-1",
```


. . . record content . . .


```
"assumedRoleUser": {
    "assumedRoleId": "AROAWFTX4ACSETXX4IN5R:marymajor",
    "arn": "arn:aws:sts::424379416740:assumed-role/SecurityAdmin/marymajor"
}
```

IAM entity analysis



Role session

`sessionID = CloudTrail.responseElements.assumedRoleUser.assumedRoleId`

Involved

Involved

Assumed



AWS user

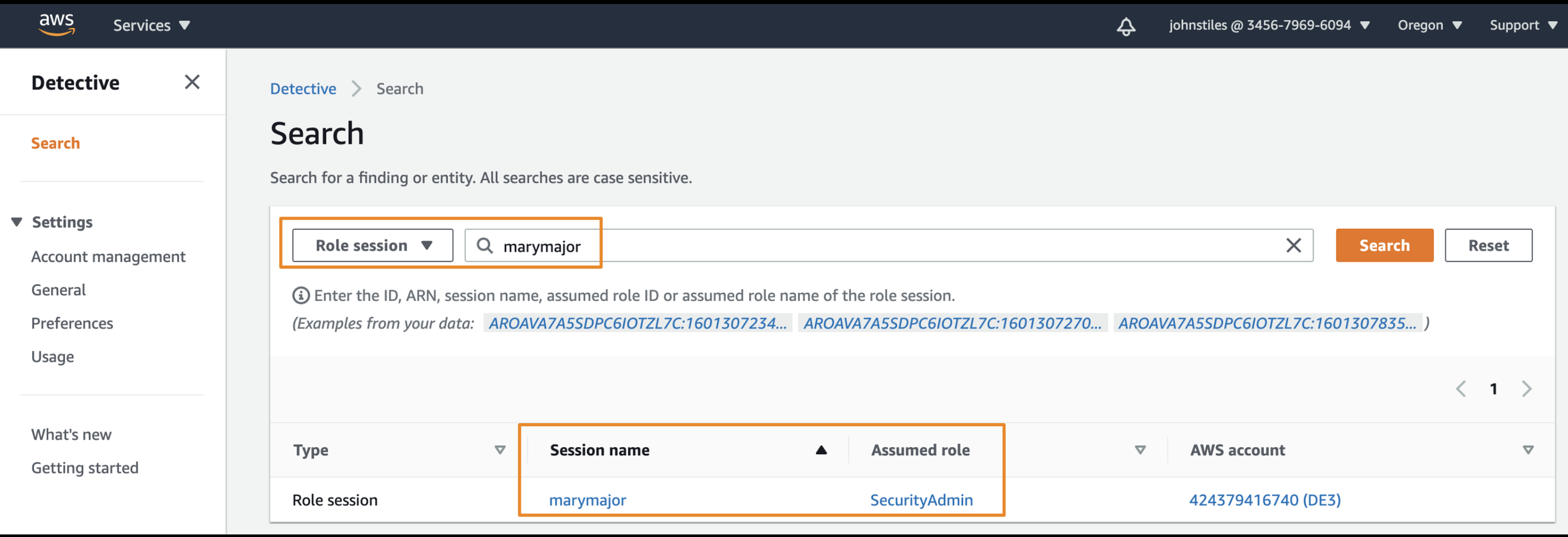


AWS role

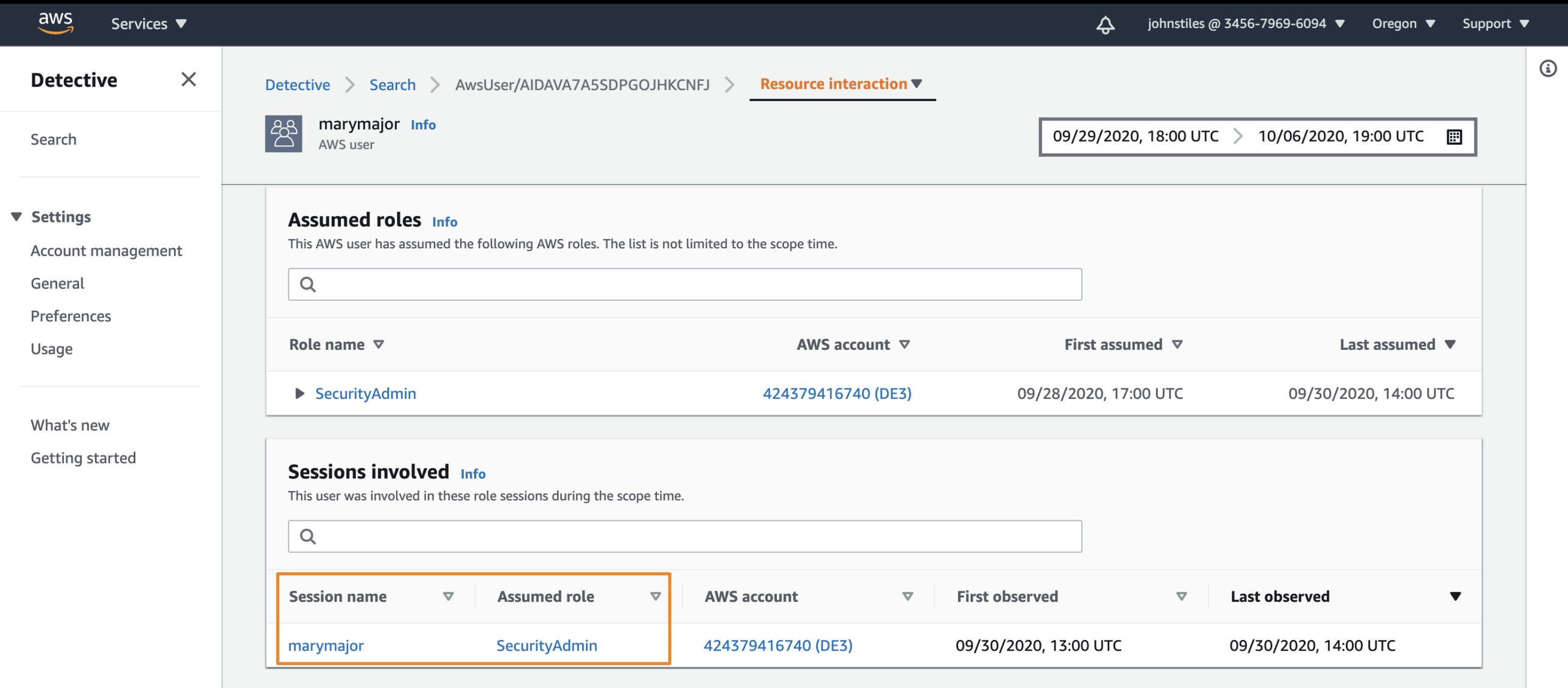
```
principalID = CloudTrail.userIdentity.PrincipalId
name = CloudTrail.userIdentity.username
userType = CloudTrail.userIdentity.type
```

```
principalID =
CloudTrail.responseElements.assumedRoleUser.assume
dRoleId[0:21]
Name =
CloudTrail.requestParameters.roleArn.split(‘/’)[1]
```

IAM entity analysis



IAM entity analysis

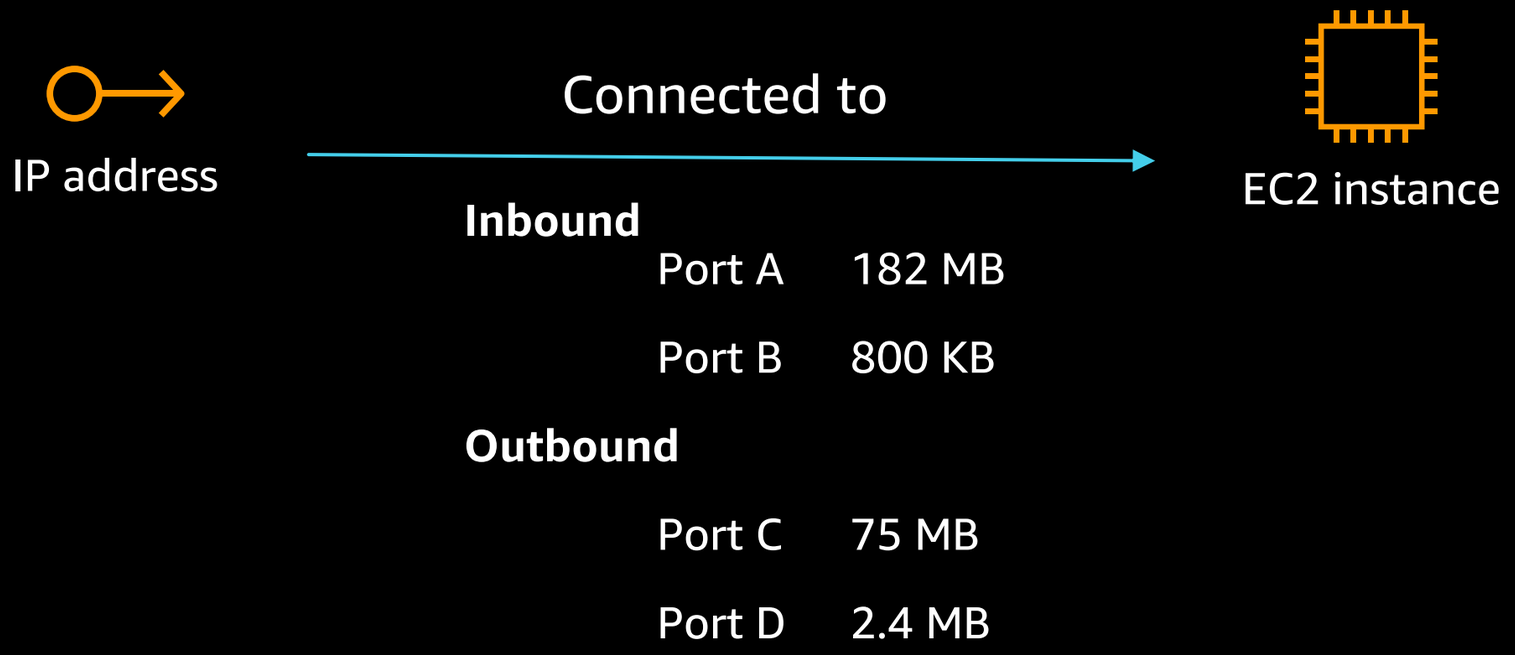


IP address resource interaction

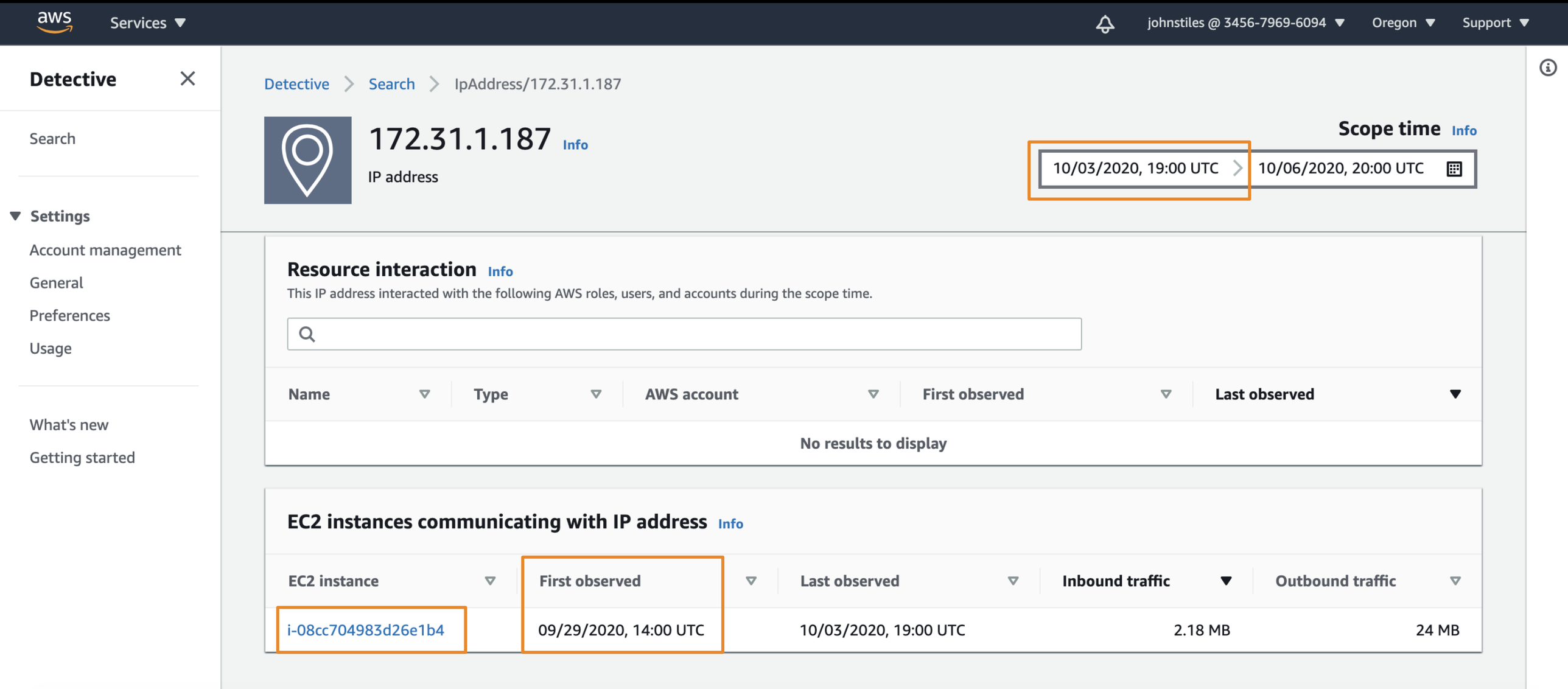
Common questions

- Has this IP address ever communicated with any of my infrastructure?
  - When?
  - How much?
- What ports did the IP address communicate with?
- Has there been any AWS CloudTrail activity from this IP address?
  - Which IAM users or roles?
  - When?
- Which EC2 instances have I seen use this IP address?

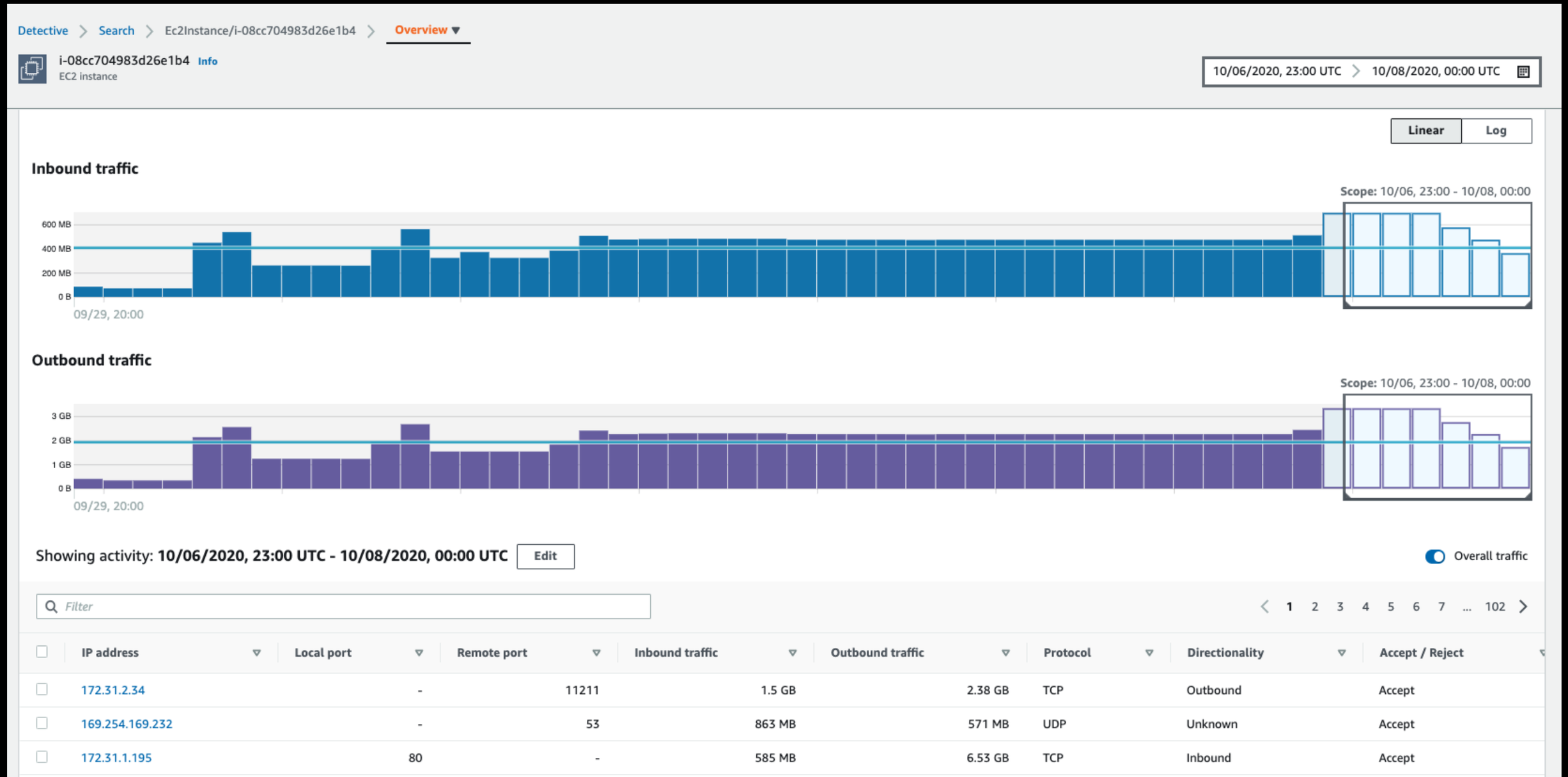
IP address resource interaction



IP address resource interaction



IP address resource interaction



[Case 7486114711] New correspondence added

AW

Amazon Web Services <no-reply-aws@amazon.com>

[redacted]

Tuesday, October 13, 2020 at 3:46 PM

Show Details

Action Items

Manage Add-ins...

A new correspondence was added to case 7486114711

To view this correspondence, please visit the AWS Support Center using the following URL:

https://console.aws.amazon.com/support/home?#/case/?caseId=7486114711&displayId=7486114711&language=en

(If you will connect by federation, log in before following the link.)

*Please note: this e-mail was sent from an address that cannot accept incoming e-mail. Please use the link above if you need to contact us again about this same issue.

Amazon Web Services, Inc. is an affiliate of Amazon.com, Inc.

Some of the content and links in this email may have been generated by an Amazon customer. Amazon is not responsible for the contents or links within.

Review



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon Detective

- Allows multi-account enablement with no data sources to configure
- Decreases complexity and increases efficiency of your AWS security investigations
- Is graph-based with purpose-built model
- Enables multiple personas on your security team to look back up to 1 year
- Records analytic baselines for common types of activity

Amazon Detective

- How Amazon Detective uses finding time to initiate scope
- Surfaces specific details to help evaluate resources
- Enables contextual evaluation of resource activity to investigate
- Provides easy pivots across profiles to iteratively evaluate scope

Visit https://aws.amazon.com/detective

Thank you!



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Please complete the session survey

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.