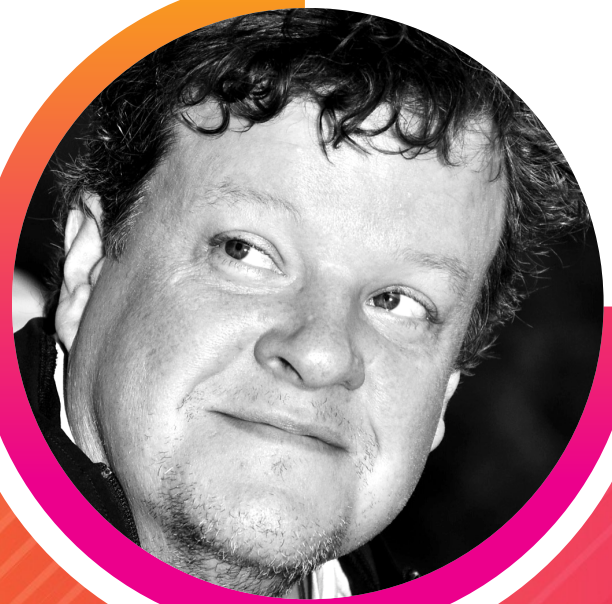
You Have Your ATO, Now What?



Patrick Shumate
Staff Solutions Architect | Splunk

Stephen Alexander
Sr. Solutions Architect | Amazon Web Services

splunk> .conf19

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only, and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Wait … I Have How Many AWS Accounts?

splunk> .conf19

Agenda and Scope:

1. What we are talking about
2. ATO: Authority To Operate
3. SCP: Service Control Policy
4. Who should be in the room
   - One or more Cloud workloads
   - More that 6 months Cloud Admin exp
   - Splunk Admin Skills

The Landscape

Many Organizations have dozens or more AWS Accounts

- How many are managed by Service Integrators (SI)?

Many Organizations have Accounts that have ATO from 2 or 3+ years ago

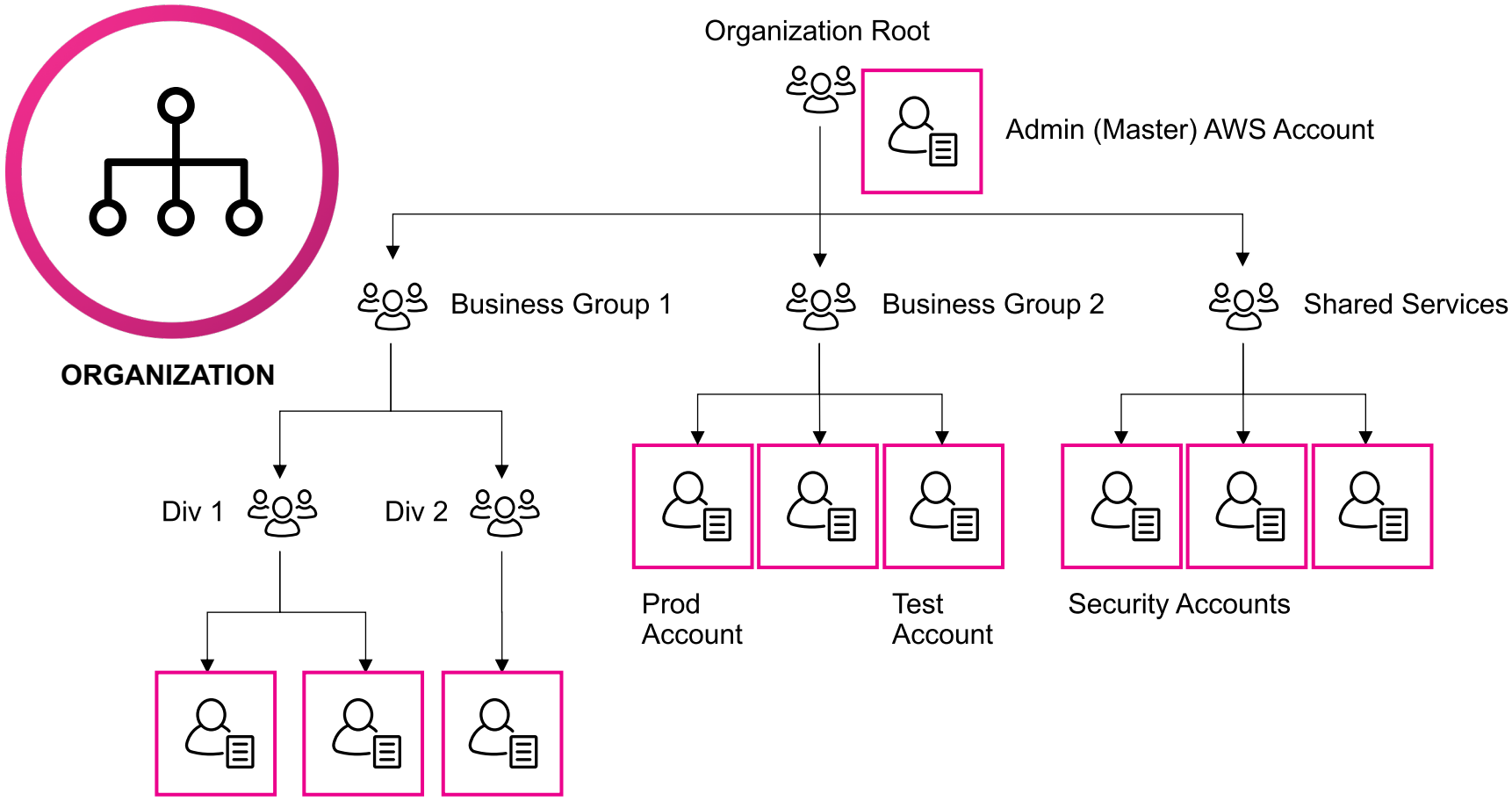
- Have they been updated since then?

Many Organizations have never completed a Well Architected Review

- Over 60+ questions, many focused on AWS specific controls for:
  - Security
  - Operations
  - Fault Tolerance

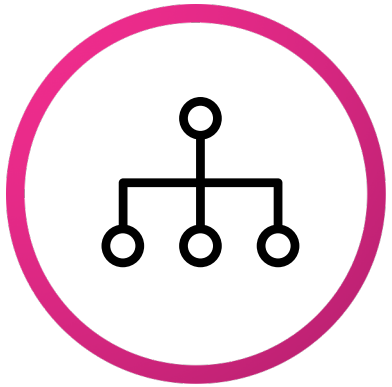
AWS Organizations

Centralize governance across multiple AWS accounts



AWS Organizations

Central governance and management



Govern Account Access

- Enforce Federated Access (Roles vs Users)

Automate Account Creation

- Centralize, govern and automate to meet your baseline

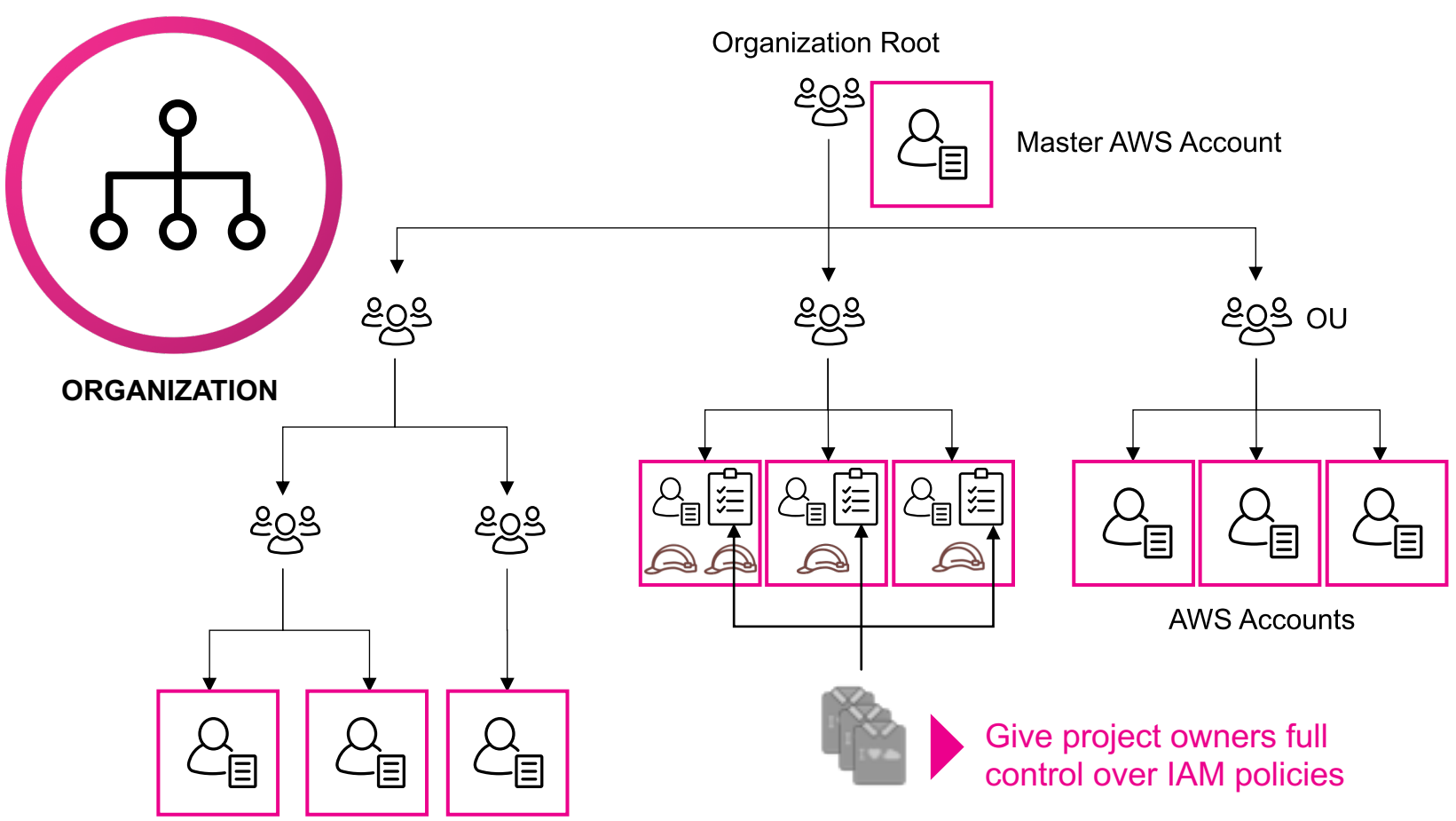
Enforce CloudTrail and Config Logging

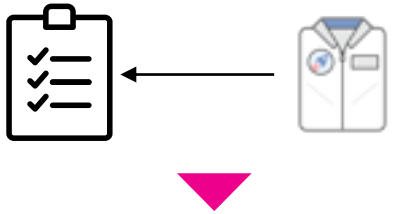
- Enable by default to your specific configuration standards

Service Control Policies

- One of the most amazing things ever!

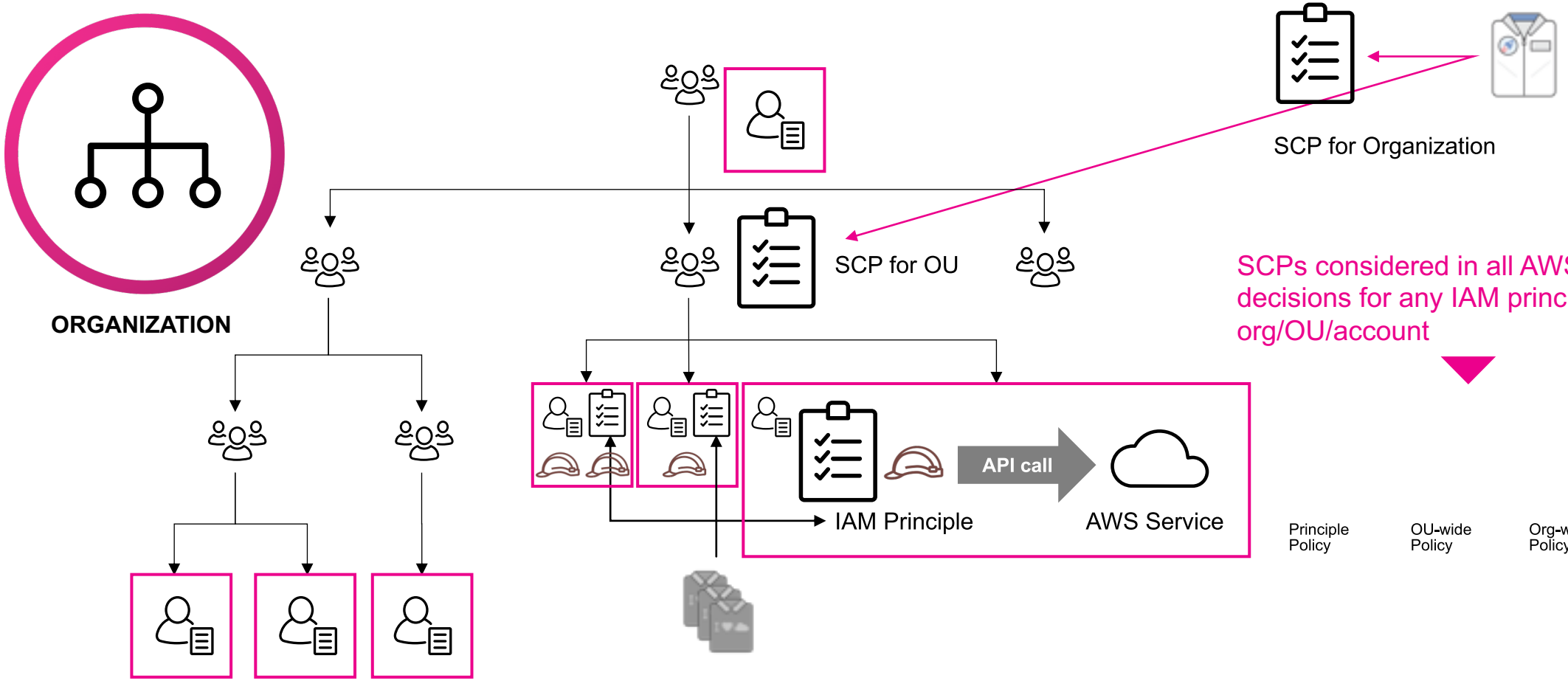
SCPs: IAM Policies Applied to AWS Organizations, OUs, and Accounts





Administrator sets SCP as an organization-level boundary

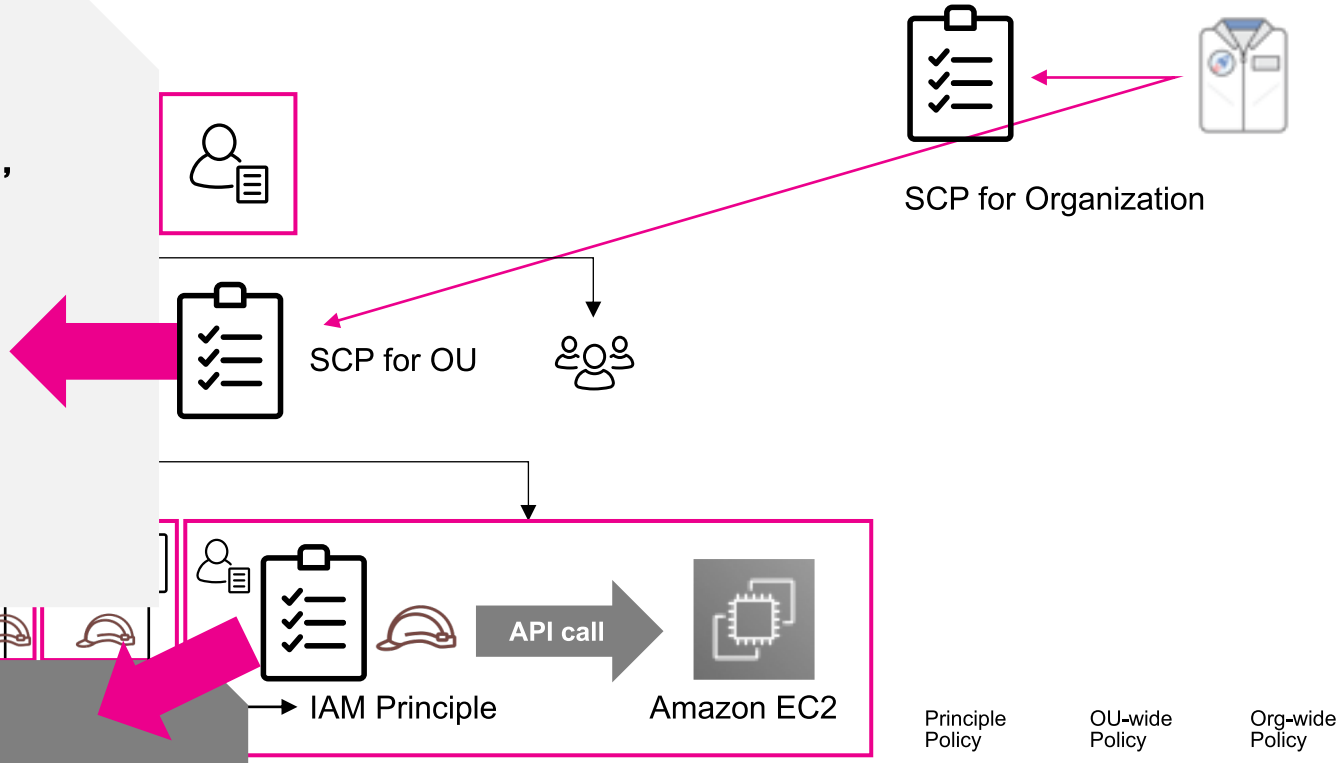
SCP in an AWS Authorization



SCPs considered in all AWS authorization decisions for any IAM principal in the org/OU/account

SCP Example: Amazon EC2 Instance Types

```
{
  "Effect": "Deny",
  "Action": "ec2:RunInstances",
  "Resource": "arn:aws:ec2:*:*:instance/*",
  "Condition": {
    "StringNotLike": {
      "ec2:InstanceType": [
        "*.nano",
        "*.micro",
        "*.small"
      ]
    }
  }
}
```



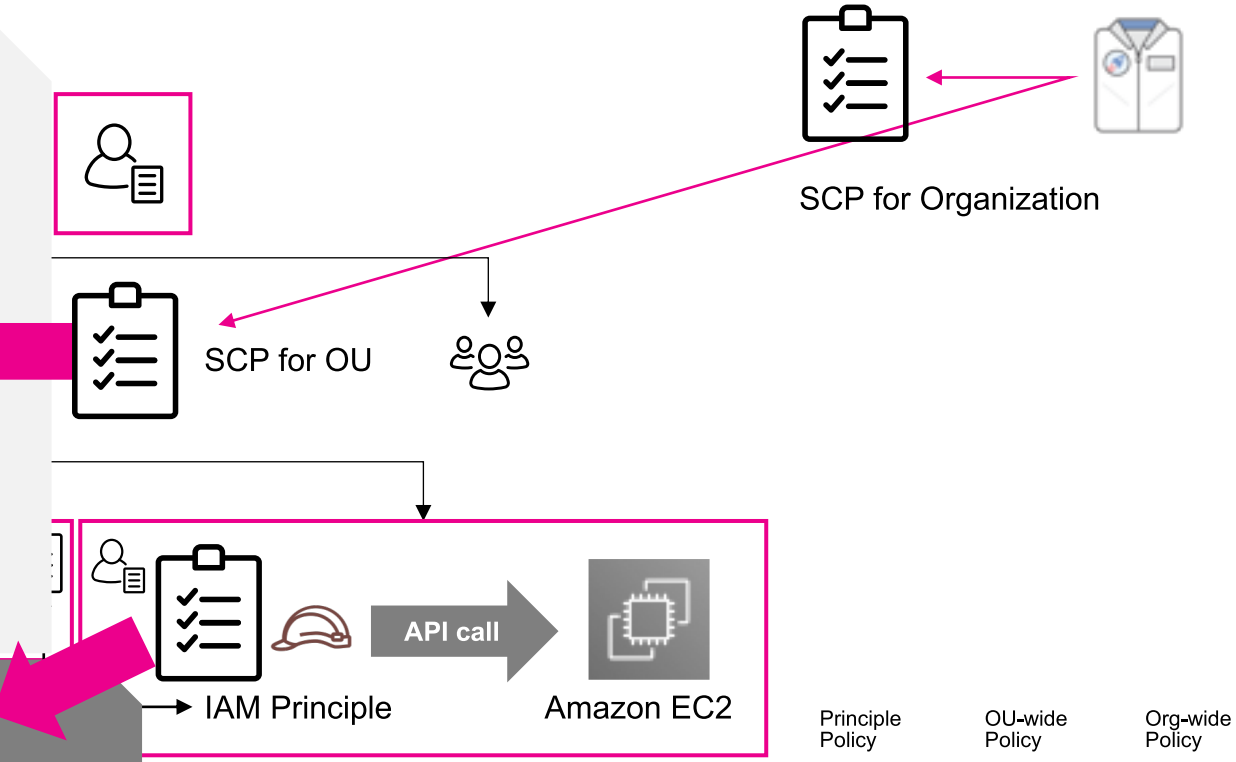

```
{
  "Effect": "Allow",
  "Action": "ec2:RunInstances",
  "Resource": "*"
}
```

SCP Example: Approved AWS Regions

```
{
  "Effect": "Deny",
  "NotAction": [
    "iam:*",
    "organizations:*",
    "route53:*",
    …
  ]
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "aws:RequestedRegion": [
        "us-east-1",
        "us-west-1
      ]
    }
  }
}
```

A few AWS services are global; ensure that you exclude them here

```
{
  "Effect": "Allow",
  "Action": "*",
  "Resource": "*"
}
```



Management Plane vs Data Plane

Management Plane

- What is happening to my AWS Resources
  - Security Group Creation or Modification
  - EC2 Server Reboot or Termination

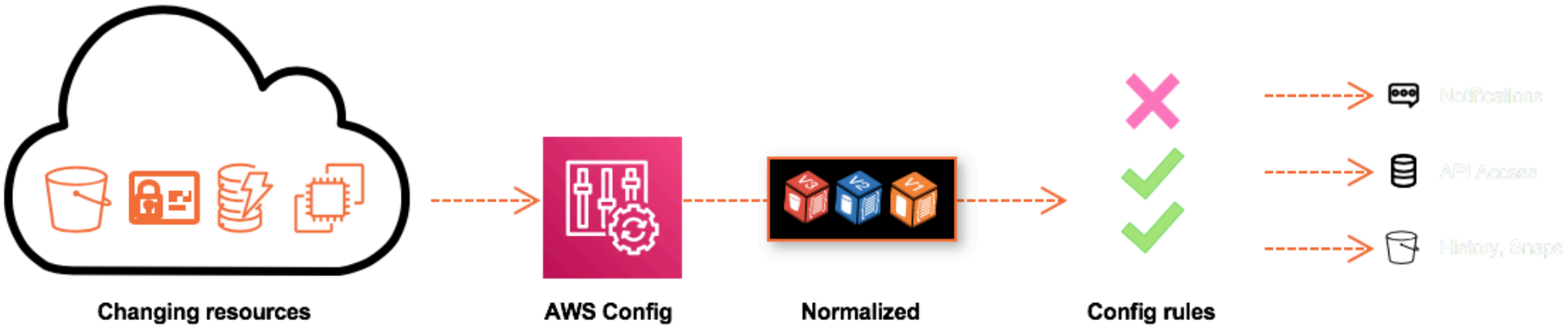
Data Plane

- What is happening to my Applications or Mission Services
  - Ticket creation in ServiceNow
  - Data entry into my Database

AWS Config

Identify resources and detect changes

- Continuous recording and continuous assessment service
- Tracks configuration changes to AWS resources
- Alerts you if the configuration is non-compliant with your policies
- Automated remediation of non-compliant resources



AWS Config Rules

Detect and respond to non compliant changes

Checks the validity of configurations recorded

AWS managed rules

- Defined by AWS
- Requires minimal (or no) configuration
- Rules are maintained by AWS

Customer managed rules

- Authored by you using AWS Lambda
- Rules execute in your account
- You match the rule

AWS Config Dashboard

AWS Config

- **Dashboard**
- Rules
- Resources
- Settings

What's new 2

Learn More

- Documentation
- Partners
- Pricing
- FAQs

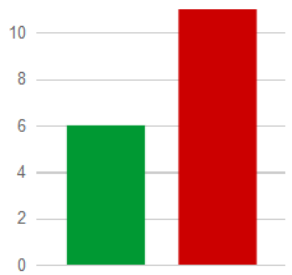
Resources

Total resources	200

Top 10 resource types	Total
CloudWatch Alarm	38
RDS DBSnapshot	26
EC2 SecurityGroup	25
EC2 NetworkInterface	18
S3 Bucket	17
EC2 Subnet	16
EC2 RouteTable	12
EC2 NetworkAcl	8
EC2 Volume	7
EC2 EIP	5

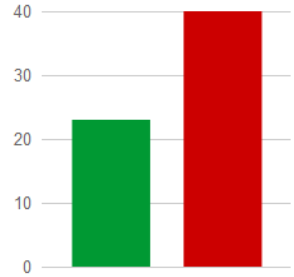
View all 200 resources

Config rule compliance



11
Noncompliant rules

Resource compliance



40
Noncompliant resources

Top 5 noncompliant rules

Rule name	Compliance
s3-bucket-ssl-requests-only	14 noncompliant resource(s)
s3-bucket-logging-enabled	13 noncompliant resource(s)
restricted-ssh	12 noncompliant resource(s)
s3-bucket-versioning-enabled	9 noncompliant resource(s)
encrypted-volumes	4 noncompliant resource(s)

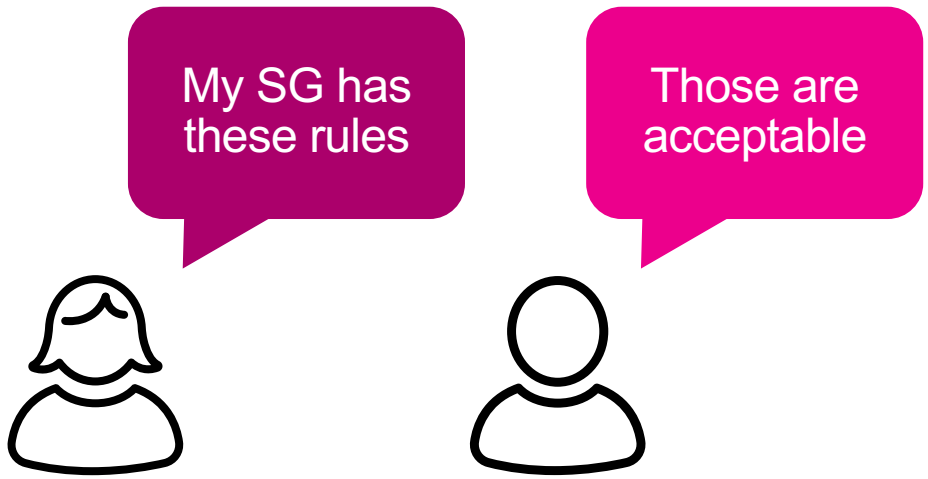
View all 11 noncompliant rules

splunk> .conf19

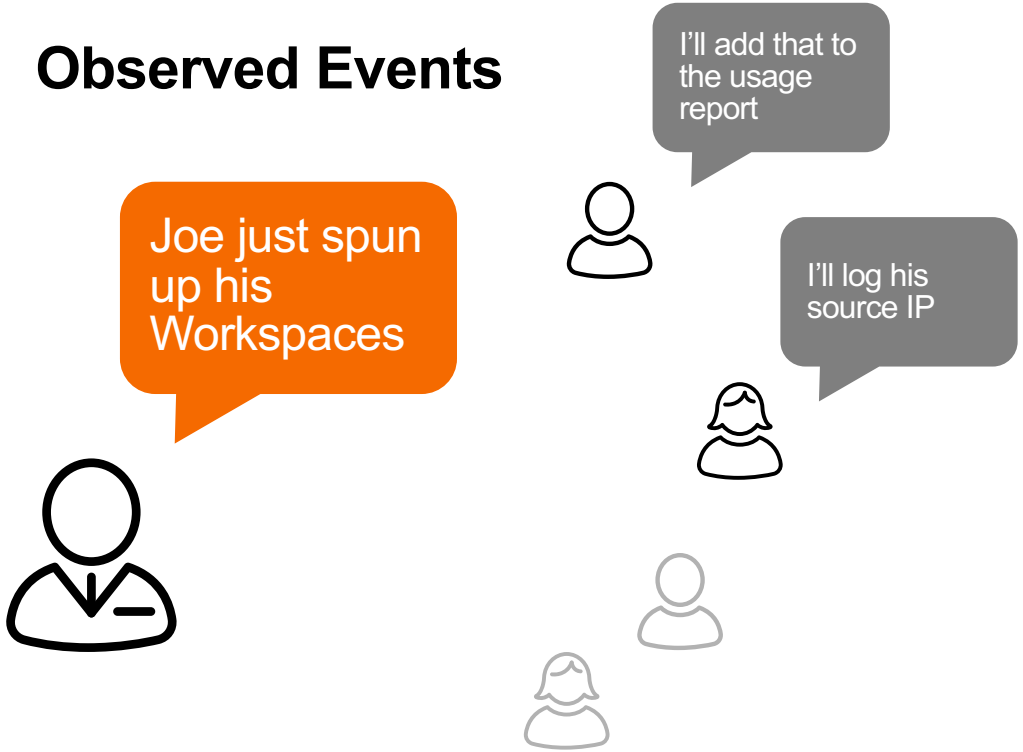
Compliance vs Events

Not all actions are compliance related concerns

Compliance Verification



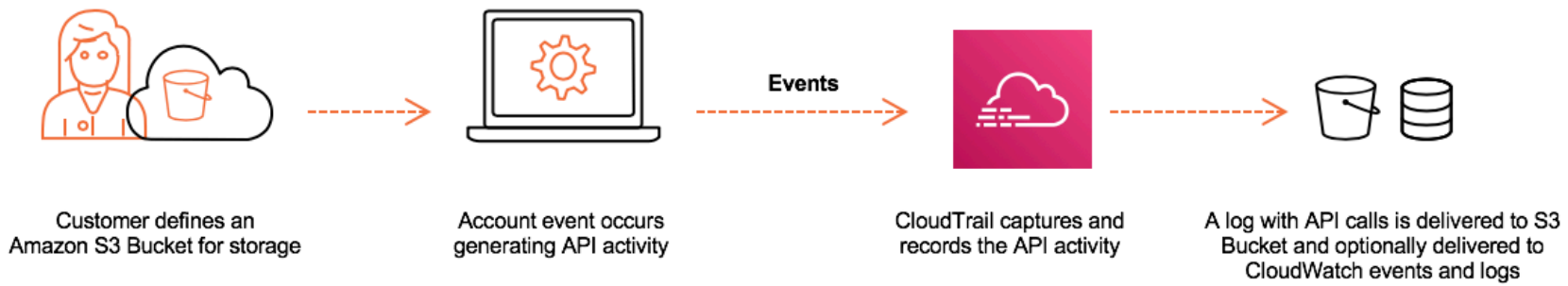
Observed Events



CloudTrail

Detect and investigate activity

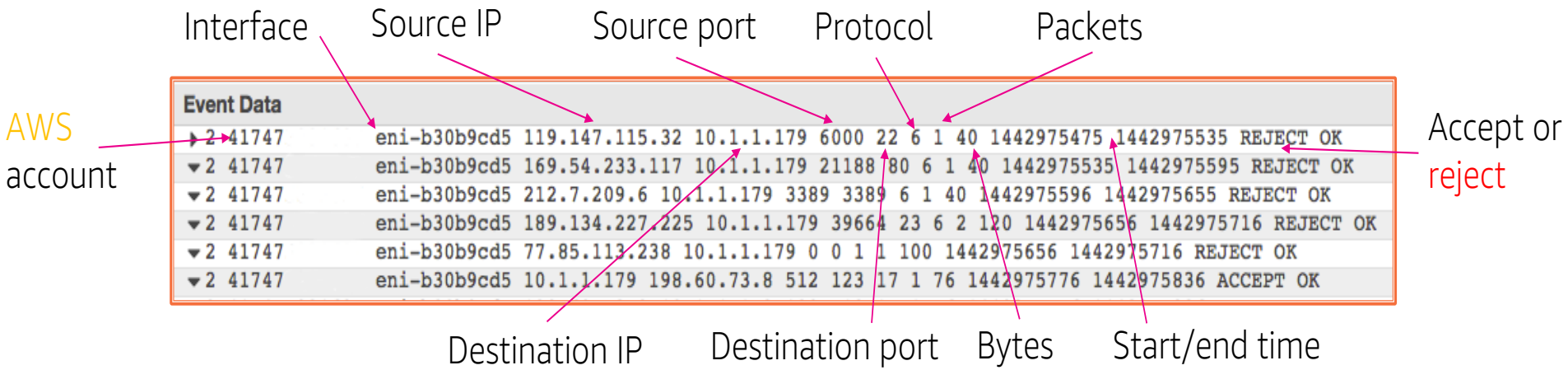
- Compliance audits of account activity using automatically recorded and centrally stored event logs
- Perform security audits and operational troubleshooting using API usage events
- Apply governance automatically in response to API events using custom workflows
- Raise alarms in response to Account Activity



Network Layer Logging

VPC flow logs

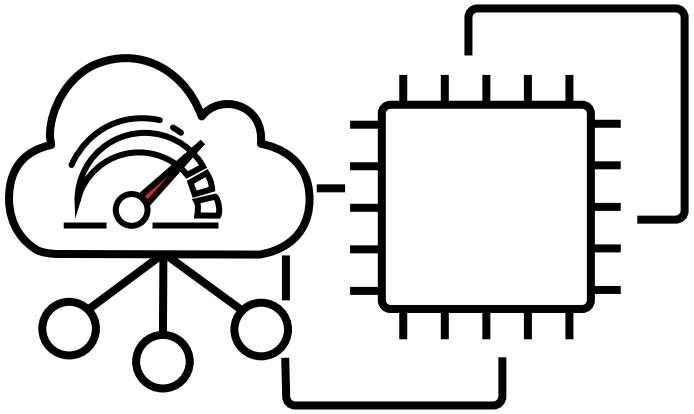
- Agentless
- Enable per elastic network interface, per subnet, or per VPC
- Logged to CloudWatch Logs or S3
- Create metrics from logged data
- Alarm based on those metrics (ex. Number of Rejected packets on Port 22)



splunk> .conf19

Network Layer Logging

Traffic mirroring, ELB logs and DNS logs



VPC Traffic Mirroring (New!)

- Capture and Inspect
- Not yet in GovCloud, only with Nitro-based Instances

AWS Elastic Load Balancing Access Logs

- Requests sent to the ELB
  - Type (http/s, ws, wss), client:port, target:port, response processing time, user agent, ssl protocol…

DNS Logs

- Public Hosted zones only

S3 Object Level Logging

Some property differences

Log Property	AWS CloudTrail	Amazon S3 Server Logs
Deliver logs to more than one destination (for example, send the same logs to two different buckets)	YES	
Turn on logs for a subset of objects (prefix)	YES	
Object operations (using Amazon S3 APIs)	YES	YES
Bucket operations (using Amazon S3 APIs)	YES	YES
Fields for object lock parameters, Amazon S3 select properties for log records	YES	
Fields for Object Size, Total Time, Turn-Around Time, and HTTP Referrer for log records		YES
Lifecycle transitions, expirations, restores		YES
Authentication failures[1]		YES

1. CloudTrail does not deliver logs for requests that fail authentication (in which the provided credentials are not valid). However, it does include logs for requests in which authorization fails (AccessDenied) and requests that are made by anonymous users.

More LOGS!!

AWS services you may use …

Amazon Relational Database Service (RDS)

- Error Logs
- Slow Query and General Logs

Amazon Lambda

AWS Step Functions

Amazon EMR

Amazon SageMaker

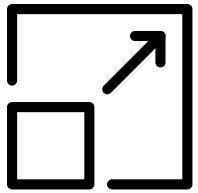
Etc …

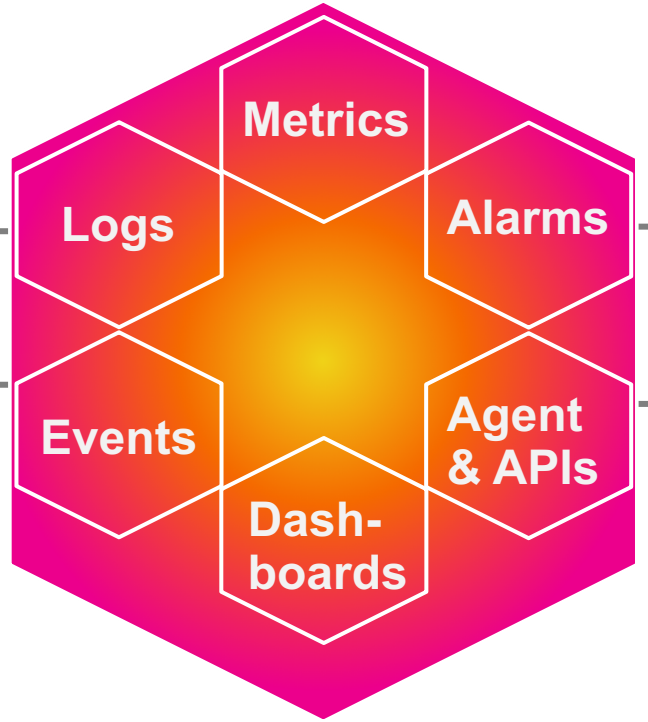
Ensure you enable logging for each service you use

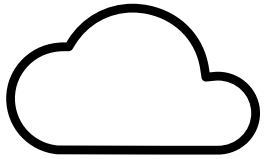
Amazon CloudWatch

Complete visibility of cloud resources and applications

Highly scalable

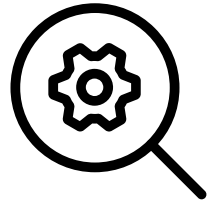






Cloud native defaults

Single solution for metrics and logs



Monitor with automation

Amazon CloudWatch Events

Amazon CloudWatch

- Near real-time stream of system events depicting changes in AWS resources
- Integration with multiple AWS services as sources and targets

Vulnerabilities and Patching

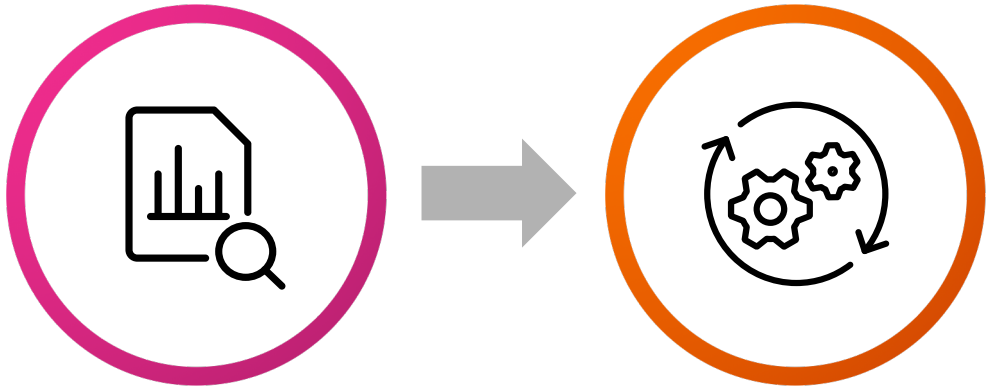
Detect and respond

Amazon Inspector

- Vulnerability Scanning
- Port reachability scanning

AWS Systems Manager

- Patch management
- Interactive shell without using SSH!
- Inventory and State Management

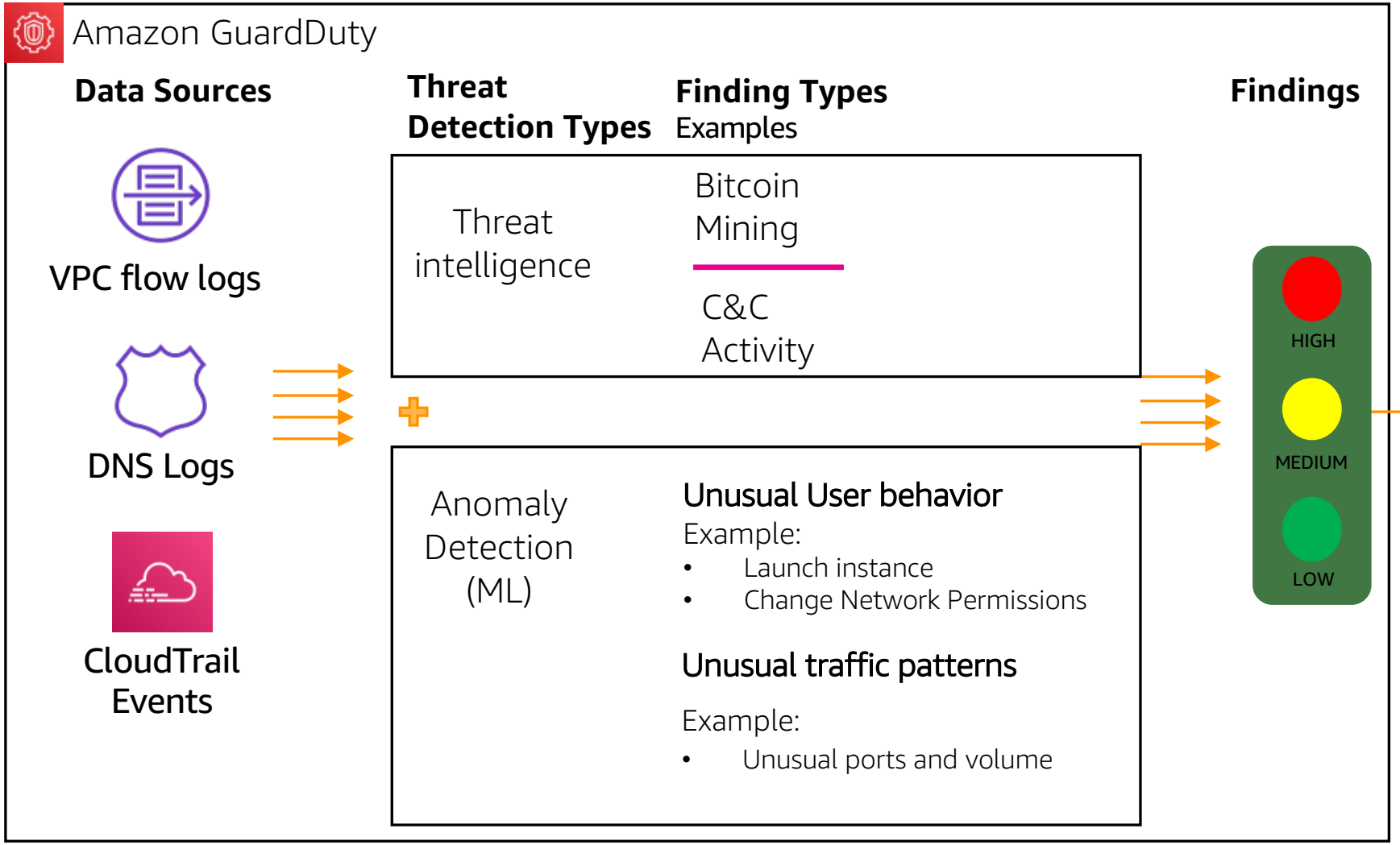


Discover Findings

Automate Mitigations

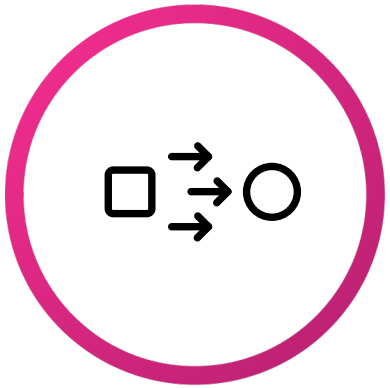
Amazon GuardDuty

Intelligent threat detection



WOW!!

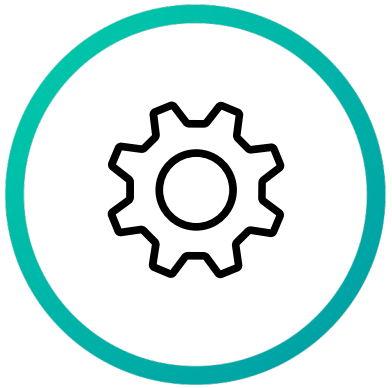
Is All of That Consolidated?



Across Accounts?

Is There a SIEM?

Does it SOAR?



Good Intentions are Bad

Mechanisms and good processes are required

Guardrails, Auditability

- If a log fall in your environment, and no one audits it…

Consolidation to Splunk

- Multi- Account, Multi-Organization automated getting data in (GDI)

Near Real-time: If a qualified event is received, does someone re-act.

- Push driven event buses

Less Sensitive Stuffs

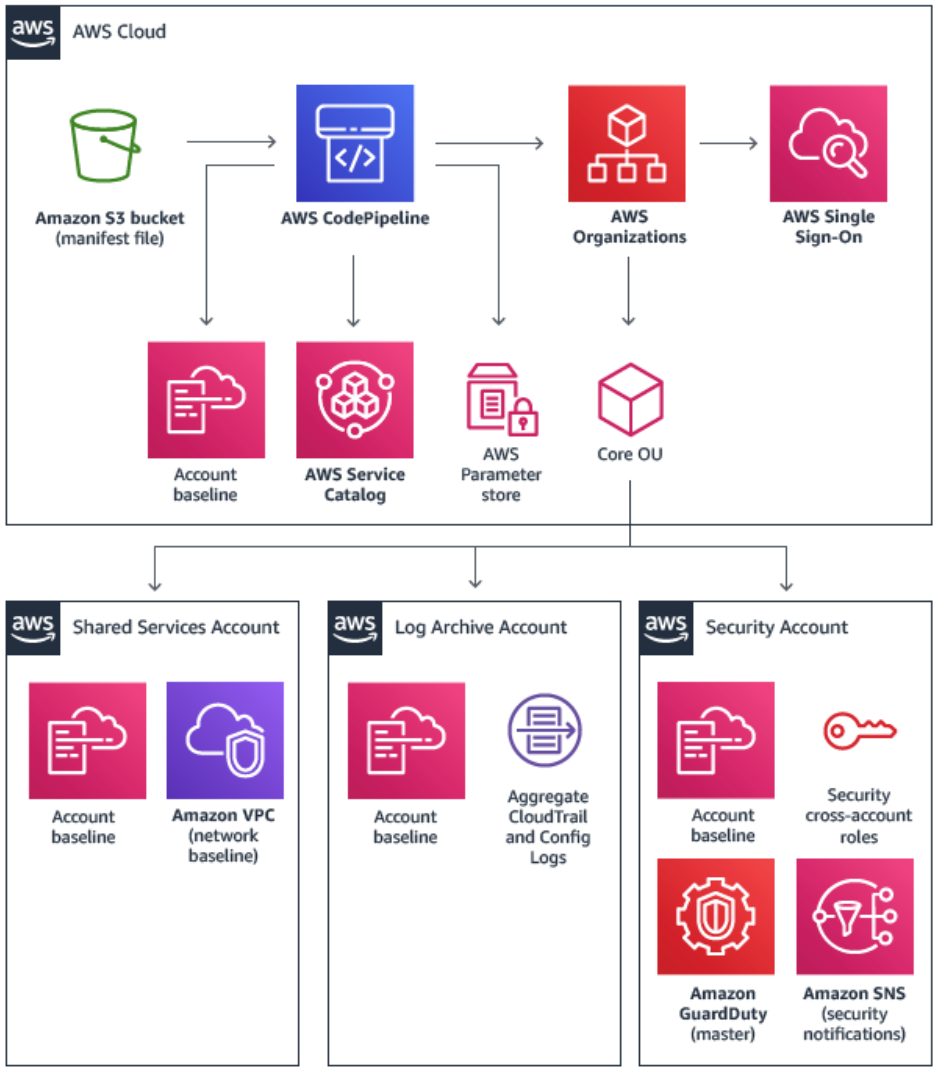
- Poller based, or slower batch push events

"All of your assumed **constraints** are **debatable**."

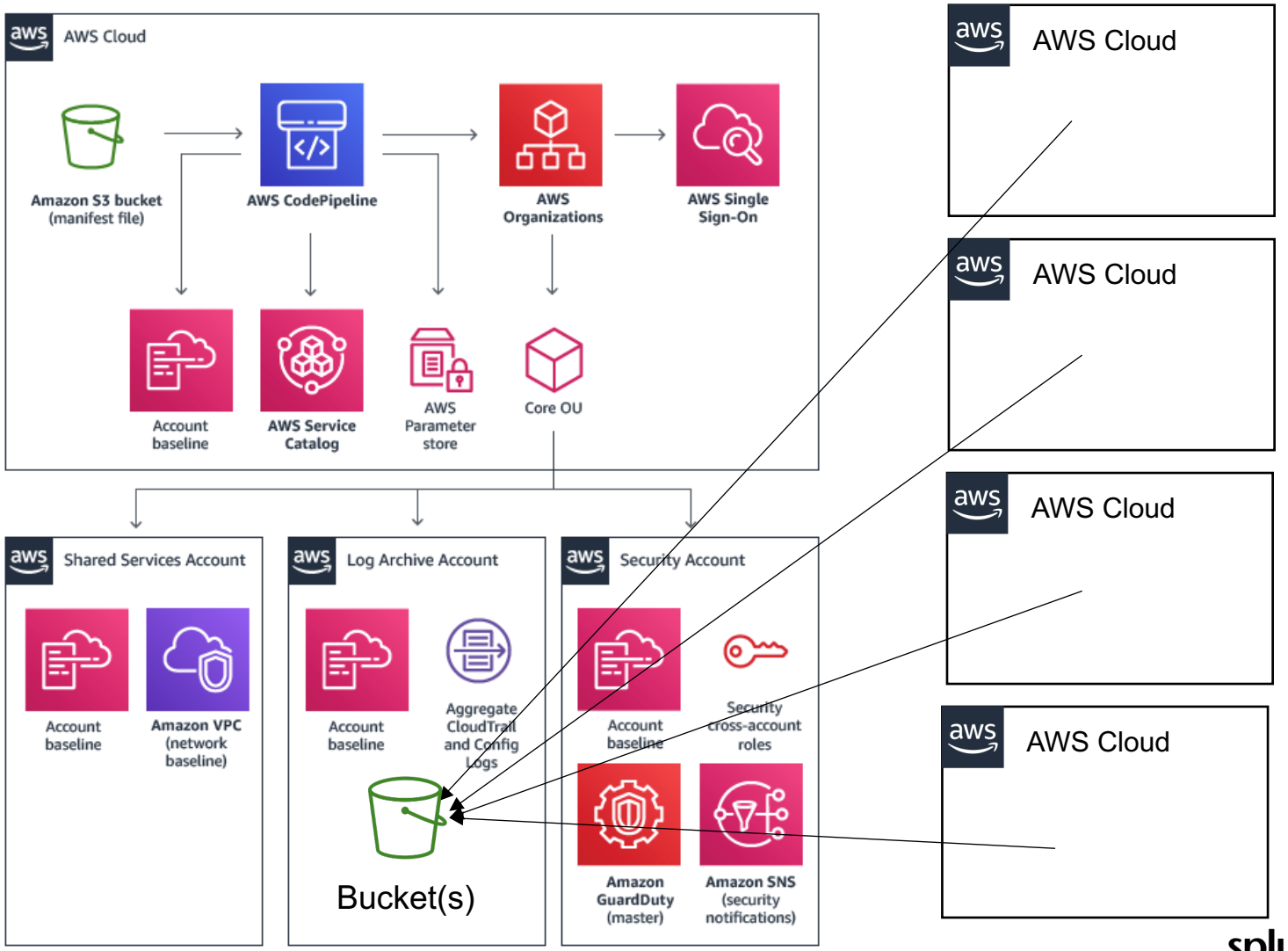
— **Jonathan Allen**, EMEA Enterprise Strategist and Evangelist, AWS

Data Collection Theory

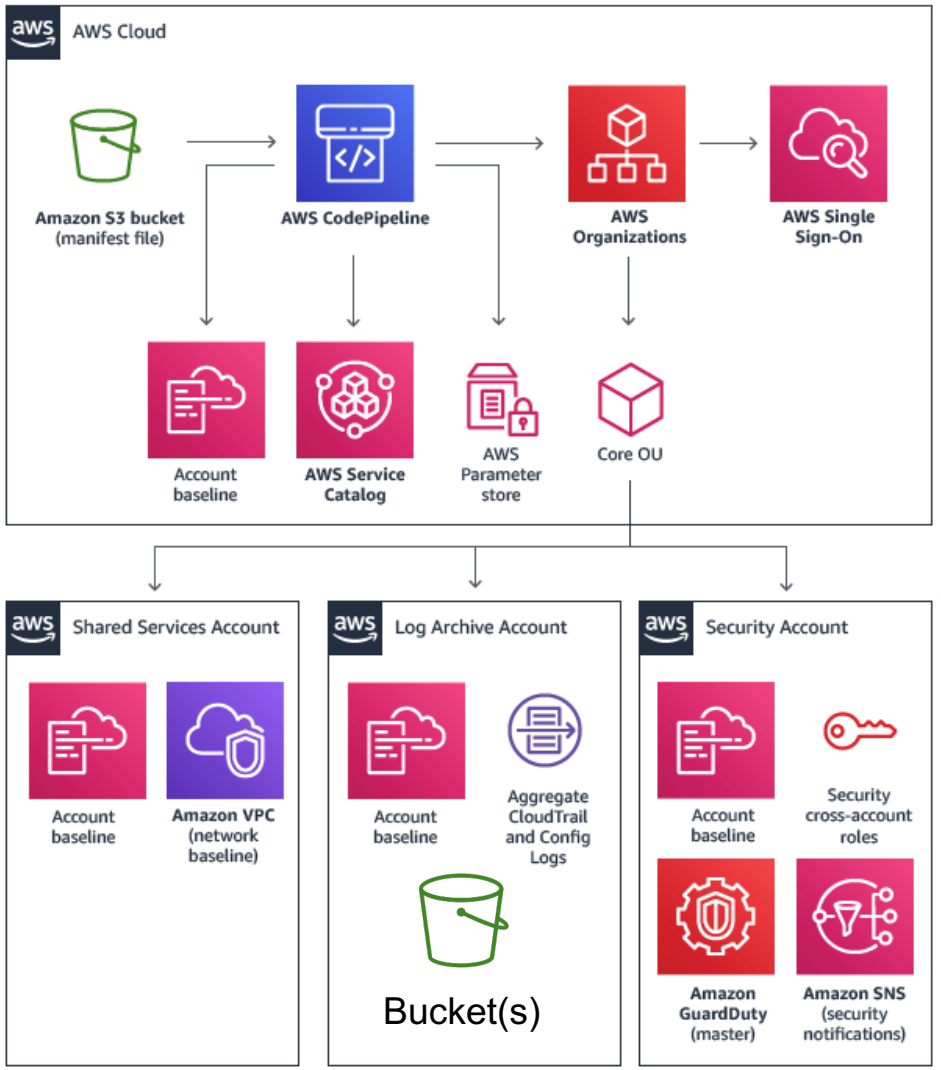
Where does the collection happen?

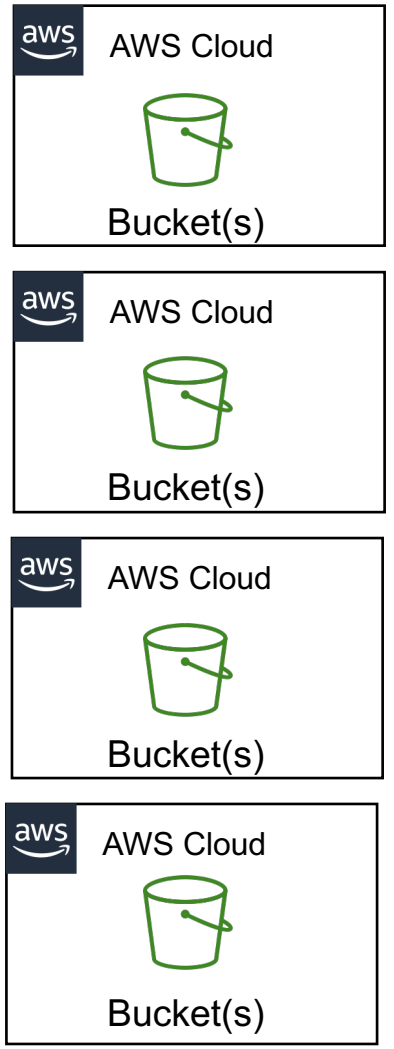


All in One



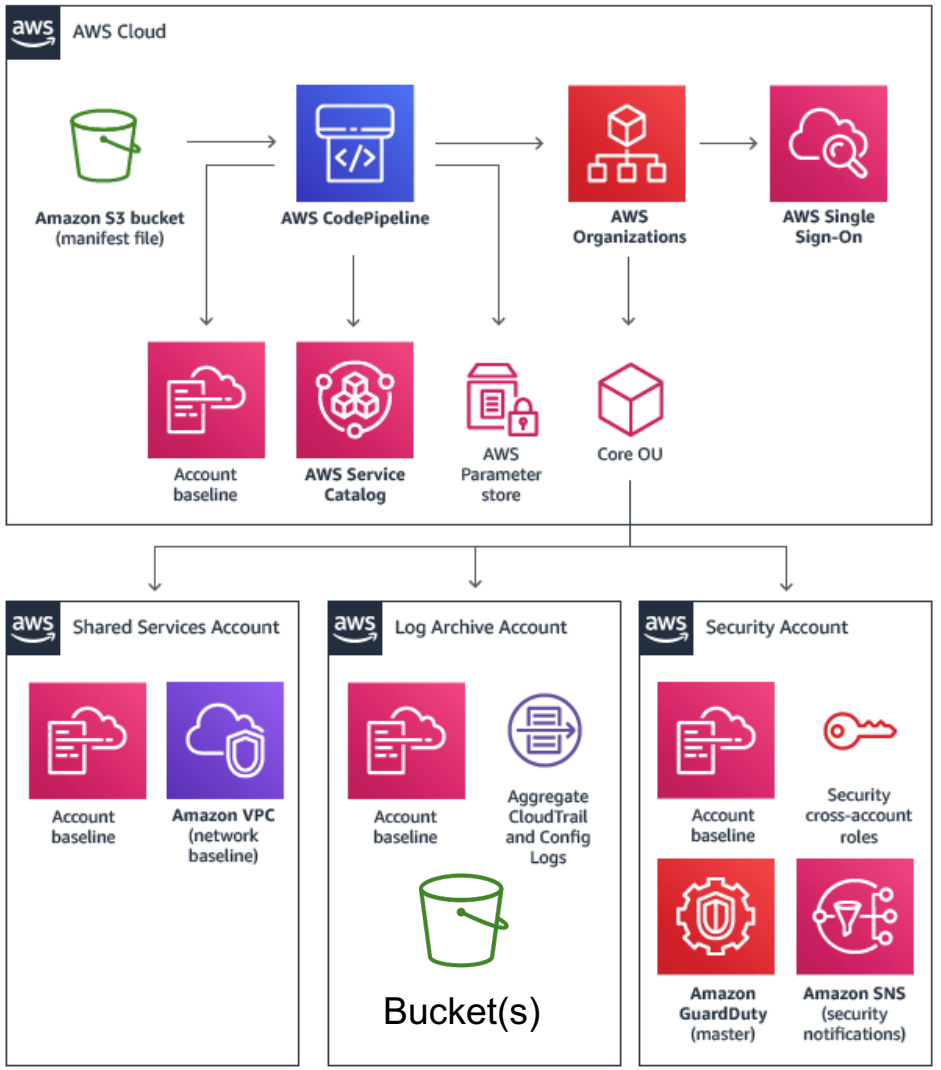
Many to One

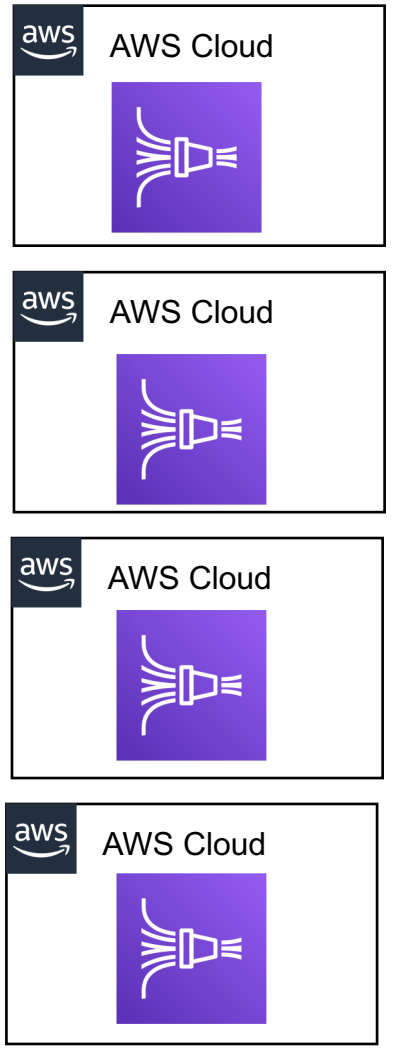




splunk> .conf19

Hybrid to One





splunk> .conf19

Spunk Automation for AWS

- Guided selection of Sources
- CloudFormation Template for CI/CD
- Push the data from each account
- Keep centralized storage

Spunk Automation for AWS

Bucket chain

Bucket Chain automates the S3 > Event > SNS > SQS> Splunk TA

Deploys a tag watcher lambda

- Reads changes from AWS Config/ CloudTrail
- Builds the S3 notifications pipeline to monitored SQS queue

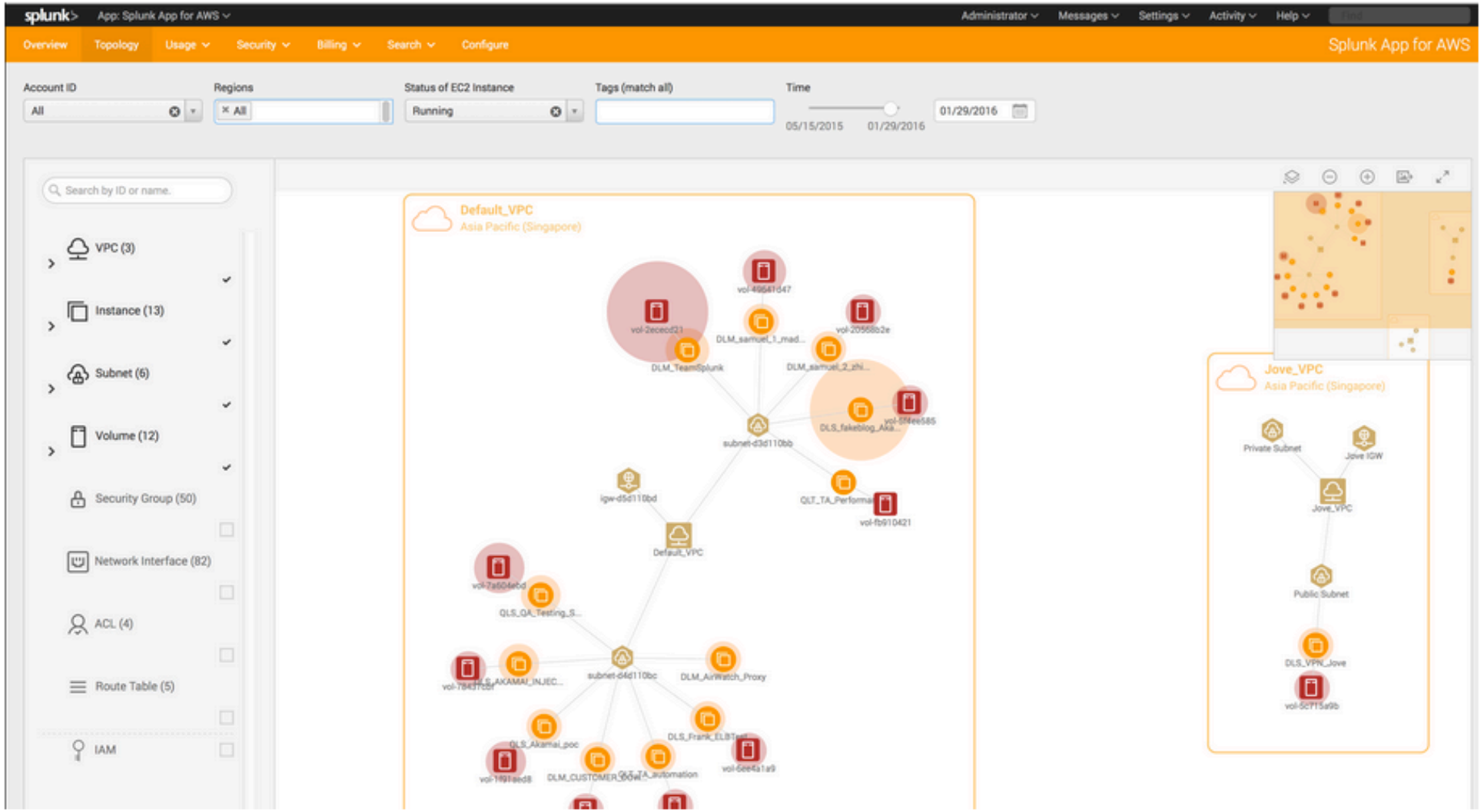
.conf19

splunk>

Building Scalable AWS based Splunk Architectures using Cloud Formation in 30 Minutes or Less

Spunk App for AWS (and TA)

Foundation app to see what is going on in your accounts



splunk> .conf19

Grand Central

Getting Cloud Data into Splunk

splunk> turn data into doing™

Problem Statement

How to enable (cloud) Data-to-Everything?

Customers are struggling to **configure** and **collect data** from cloud providers. They are unable to gain visibility from their cloud deployments and are being exposed to **operational**, **security** and **business** vulnerabilities.

Traditionally Splunk has **not been the easiest** product to get data in, especially from **third party providers**.

The problem is only getting **worse** since “Cloud First” is creating a **scale** issue that customers cannot keep up with.

AWS GDI by the numbers

Manually setting up AWS Services and collecting the data with Splunk

1 account

1 region

3 AWS Service

(CloudTrail, Config, GuardDuty)

~150 clicks

~45 minutes per account, per region

50 accounts

4 regions

3 AWS Services

~150 hours or 1 week

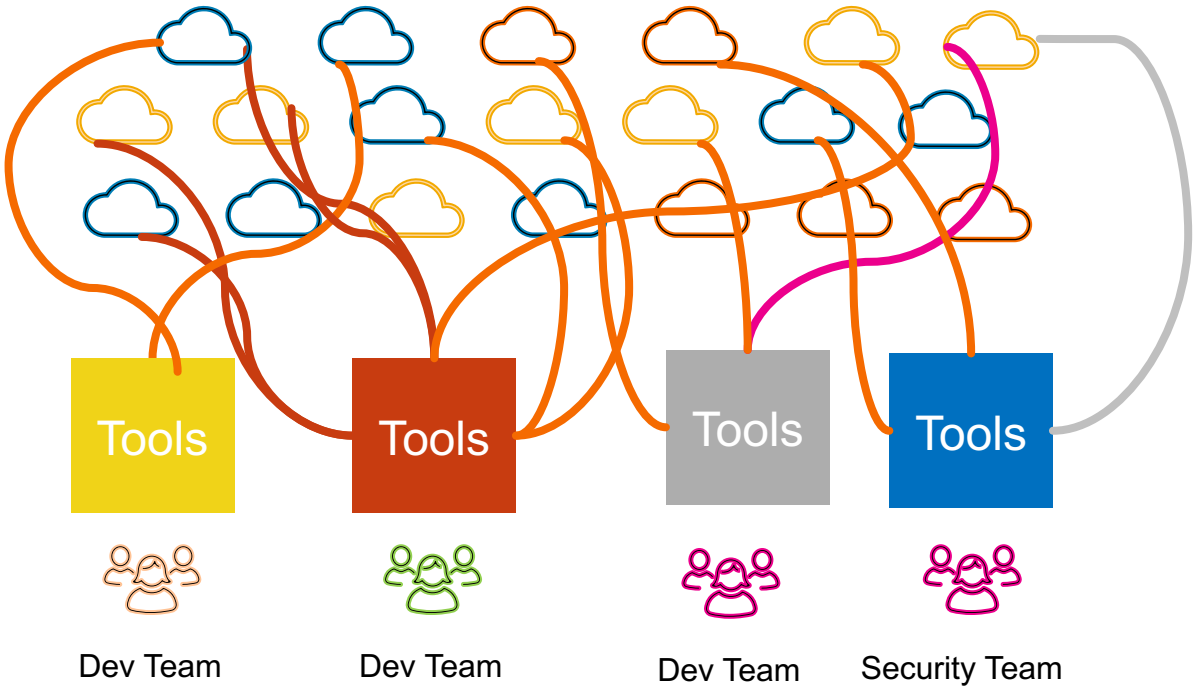
500 accounts

4 regions

3 AWS Services

~1500 hours or 2 months

Problem for Cloud GDI



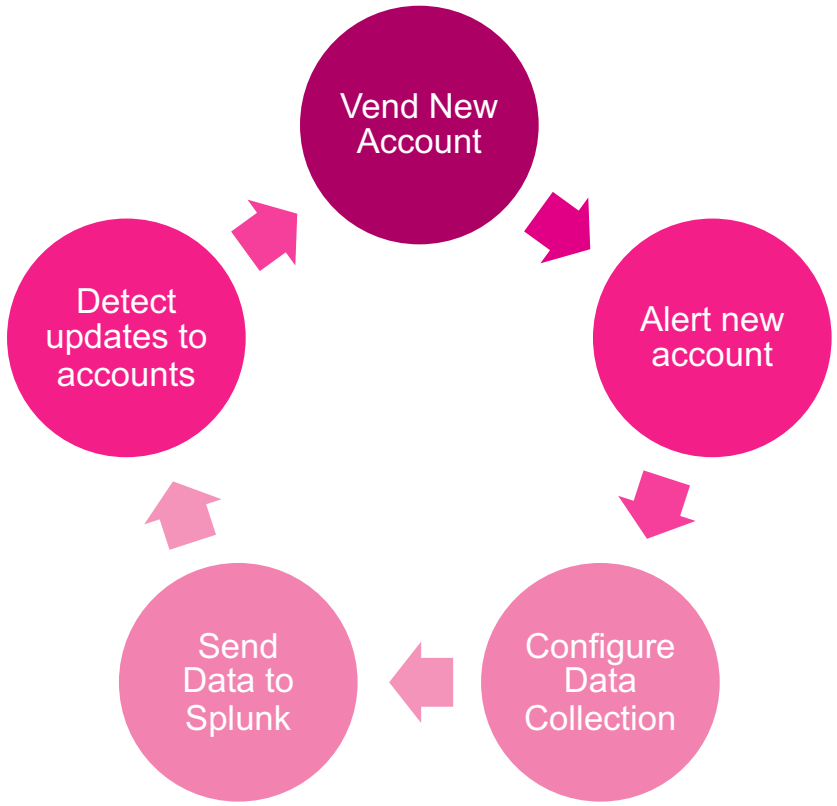
- Setting up data collection per **cloud**, **account**, and **region** takes a great deal of time.
- Different teams setup collection in a different way
- Can’t see or discover accounts being added to Organization

Grand Central

splunk> turn data into doing™

Cloud Data Lifecycle

Managed and monitored by Grand Central



- Central deployment mechanism **across clouds**, **accounts** and **regions**
- **Uniform** data collection methodology
- **Alert** new, updated or deleted accounts
- Critical to the **full lifecycle** of the customer cloud data

How does it work?

splunk> turn data into doing™

Credential Smusher

Take all credentials.csv files and smush them into one file for upload

Step 1 – Download Credentials

Credentials

Credentials.csv
Credentials-1.csv
Credentials-2.csv
Credentials-3.csv
….
Credentials-n.csv

Step 2 – Run credentials_smusher.py

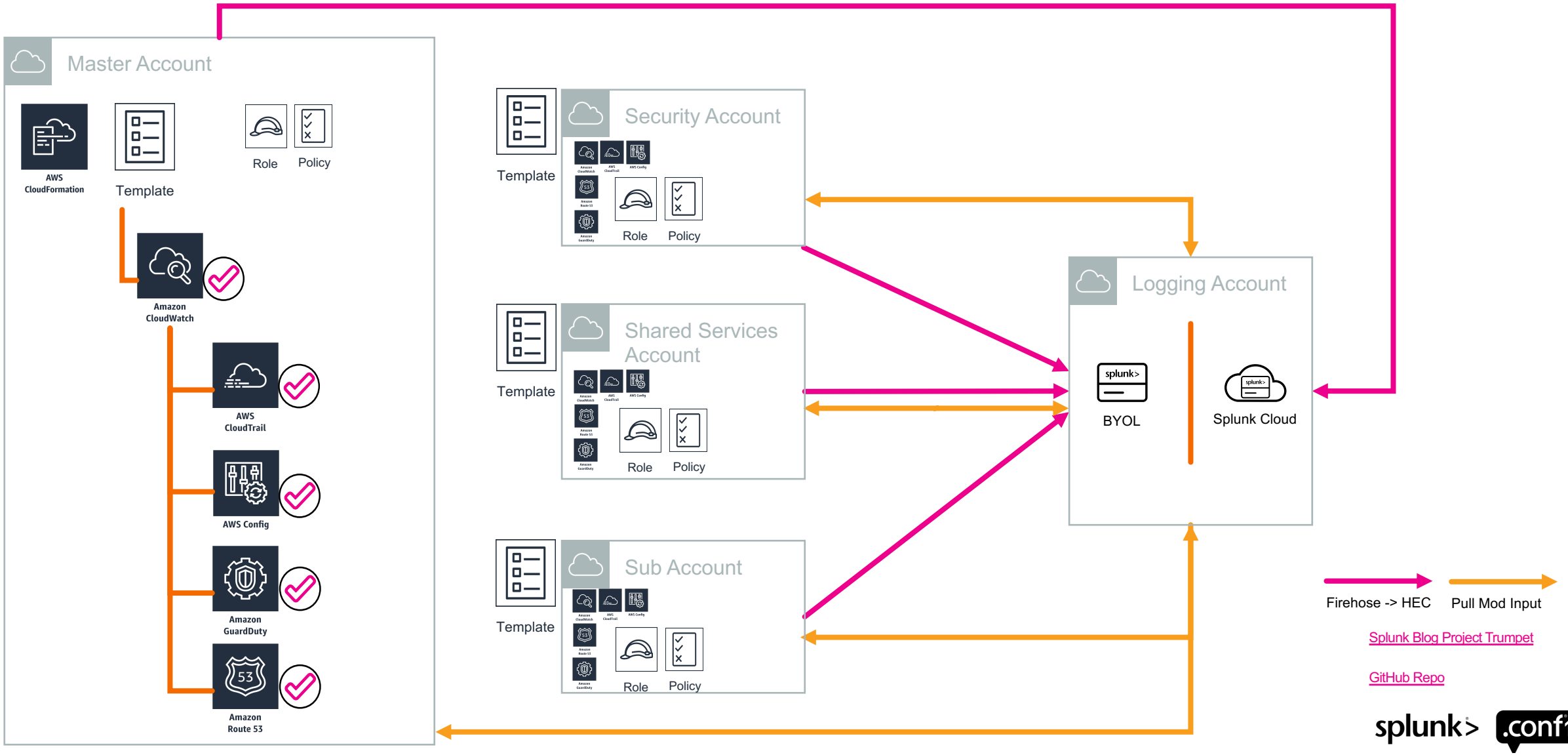
```
bash$ cd credentials/
bash$ python credentials_smusher.py
bash$ ls
all_account_credentials.json
```

Step 3 – Save File

Credentials

all_account_credentials.json

Grand Central Workflow



splunk> .conf19

Demo

splunk> turn data into doing™

AWS Organization Master Accounts

0 accounts.

New Organization Master Account

Account Name	Account ID	Account Type	Actions
No accounts found.			

AWS Accounts

0 accounts.

Bulk Credential Upload | Bulk Data Deployment | New Account

Filter by Organization Master Accounts.

Select...

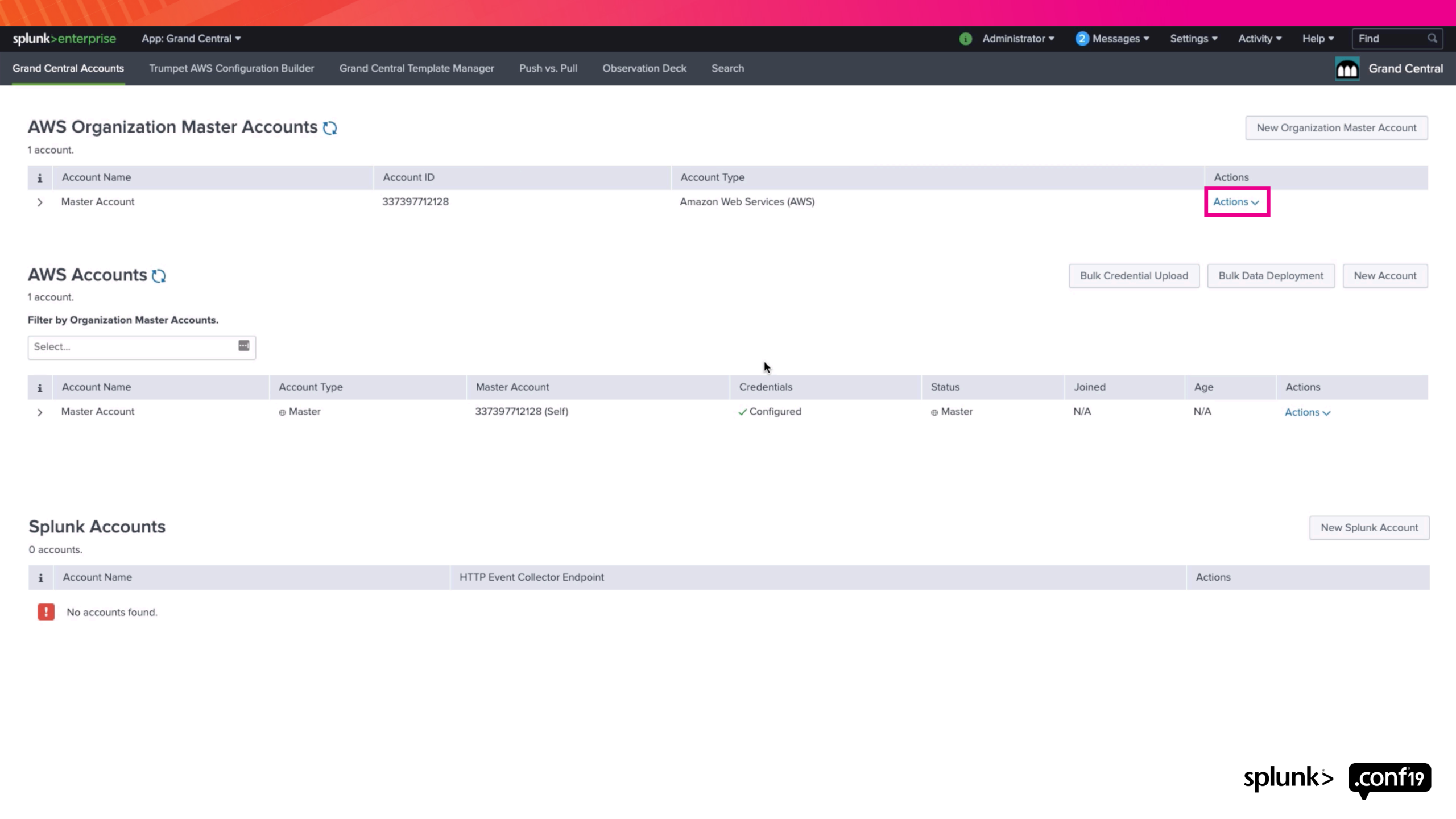
Account Name	Account Type	Master Account	Credentials	Status	Joined	Age	Actions
No accounts found.							

Splunk Accounts

0 accounts.

New Splunk Account

Account Name	HTTP Event Collector Endpoint	Actions
No accounts found.		


splunk>enterprise
App: Grand Central
Administrator
2 Messages
Settings
Activity
Help
Find
Grand Central Accounts
Trumpet AWS Configuration Builder
Grand Central Template Manager
Push vs. Pull
Observation Deck
Search
Grand Central
AWS Organization Master Accounts
1 account.
New Organization Master Account
Account Name
Account ID
Account Type
Actions
Master Account
337397712128
Amazon Web Services (AWS)
Actions
AWS Accounts
1 account.
Bulk Credential Upload
Bulk Data Deployment
New Account
Filter by Organization Master Accounts.
Select...
Account Name
Account Type
Master Account
Credentials
Status
Joined
Age
Actions
Master Account
Master
337397712128 (Self)
Configured
Master
N/A
N/A
Actions
Splunk Accounts
0 accounts.
New Splunk Account
Account Name
HTTP Event Collector Endpoint
Actions
No accounts found.
splunk> .conf19

New Search

Save As ▾ Close

```
| rest /servicesNS/nobody/grand_central/organizations | where ParentAccountId="337397712128"
```

Last 24 hours ▾

✓ 4 results (9/25/19 2:00:00.000 AM to 9/26/19 2:29:16.000 AM) No Event Sampling ▾

Job ▾ Smart Mode ▾

Events | Patterns | **Statistics (4)** | Visualization

20 Per Page ▾ Format Preview ▾

AccountId	Arn	Email	JoinedMethod	JoinedTimestamp	Name	ParentAccountId	Status	author	eai:acl.app	eai:acl.can_list	eai:acl.can_write	eai:acl.modifiable	eai:acl.owner	ea
337397712128	arn:aws:organizations::337397712128:account/o-lj5bf4m3jq/337397712128	kamilo.amir@splunk.com	INVITED	04/15/2019	master-account	337397712128	ACTIVE	system		1	1	0	system	*
390687995958	arn:aws:organizations::337397712128:account/o-lj5bf4m3jq/390687995958	kamir@caspida.com	INVITED	07/30/2019	Security Account	337397712128	ACTIVE	system		1	1	0	system	*
875456150869	arn:aws:organizations::337397712128:account/o-lj5bf4m3jq/875456150869	kamir_splunkd@west.mail.splunk.com	INVITED	08/26/2019	shared-services-account	337397712128	ACTIVE	system		1	1	0	system	*
911795064262	arn:aws:organizations::337397712128:account/o-lj5bf4m3jq/911795064262	kam@splunk.com	INVITED	04/29/2019	DevOps Account	337397712128	ACTIVE	system		1	1	0	system	*

AWS Organization Master Accounts

1 account.

New Organization Master Account

Account Name	Account ID	Account Type	Actions
Master Account	337397712128	Amazon Web Services (AWS)	Actions

AWS Accounts

4 accounts.

Bulk Credential Upload | Bulk Data Deployment | New Account

Filter by Organization Master Accounts.

Select...

Account Name	Account Type	Master Account	Credentials	Status	Joined	Age	Actions
Master Account	Master	337397712128 (Self)	Configured	Active	INVITED	164 Days (Joined 04/15/2019)	Actions
Security Account	Member	337397712128	Not Configured	Active	INVITED	58 Days (Joined 07/30/2019)	Actions
shared-services-account	Member	337397712128	Not Configured	Active	INVITED	31 Days (Joined 08/26/2019)	Actions
DevOps Account	Member	337397712128	Not Configured	Active	INVITED	150 Days (Joined 04/29/2019)	Actions

Splunk Accounts

0 accounts.

New Splunk Account

Account Name	HTTP Event Collector Endpoint	Actions

No accounts found.

AWS Organization Master Accounts

1 account.

New Organization Master Account

Account Name	Account ID	Account Type	Actions
Master Account	337397712128	Amazon Web Services (AWS)	Actions

AWS Accounts

5 accounts.

Bulk Credential Upload | Bulk Data Deployment | New Account

Filter by Organization Master Accounts.

Select...

Account Name	Account Type	Master Account	Credentials	Status	Joined	Age	Actions
002404001714	Individual	N/A	Configured	N/A	N/A	N/A	Actions
Master Account	Master	337397712128 (Self)	Configured	Active	INVITED	164 Days (Joined 04/15/2019)	Actions
Security Account	Member	337397712128	Configured	Active	INVITED	58 Days (Joined 07/30/2019)	Actions
shared-services-account	Member	337397712128	Configured	Active	INVITED	31 Days (Joined 08/26/2019)	Actions
DevOps Account	Member	337397712128	Configured	Active	INVITED	150 Days (Joined 04/29/2019)	Actions

Splunk Accounts

0 accounts.

New Splunk Account

Account Name	HTTP Event Collector Endpoint	Actions

No accounts found.

AWS Organization Master Accounts

1 account.

New Organization Master Account

Account Name	Account ID	Account Type	Actions
Master Account	337397712128	Amazon Web Services (AWS)	Actions

AWS Accounts

5 accounts.

Bulk Credential Upload | Bulk Data Deployment | New Account

Filter by Organization Master Accounts.

Select...

Account Name	Account Type	Master Account	Credentials	Status	Joined	Age	Actions
002404001714	Individual	N/A	Configured	N/A	N/A	N/A	Actions
Master Account	Master	337397712128 (Self)	Configured	Active	INVITED	164 Days (Joined 04/15/2019)	Actions
Security Account	Member	337397712128	Configured	Active	INVITED	58 Days (Joined 07/30/2019)	Actions
shared-services-account	Member	337397712128	Configured	Active	INVITED	31 Days (Joined 08/26/2019)	Actions
DevOps Account	Member	337397712128	Configured	Active	INVITED	150 Days (Joined 04/29/2019)	Actions

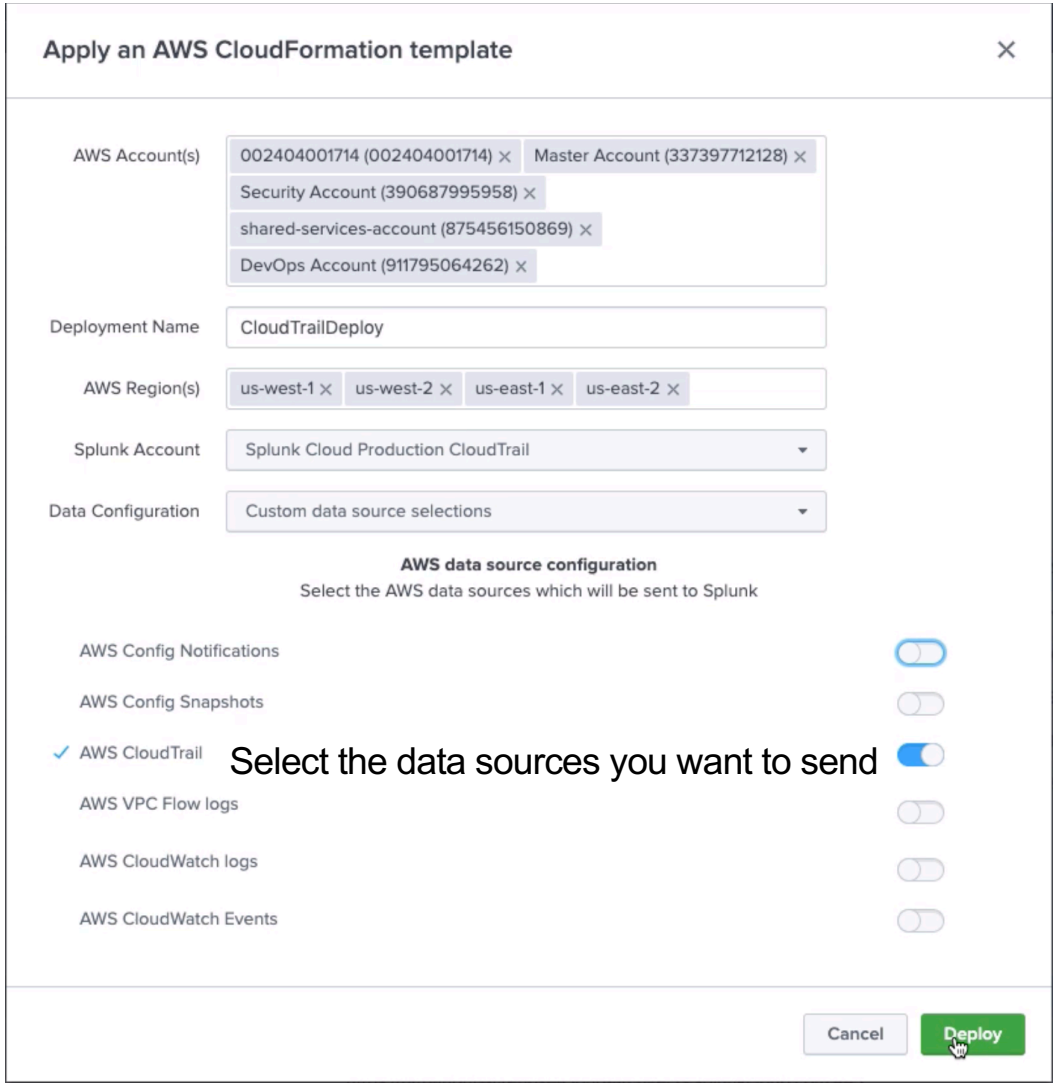
Splunk Accounts

3 accounts.

New Splunk Account

Account Name	HTTP Event Collector Endpoint	Actions
Splunk Cloud Production Config	https://http-inputs-firehose-cloud-architects.splunkcloud.com:443	Actions
Splunk Cloud Production CloudWatch Logs VPCFlow	https://http-inputs-firehose-cloud-architects.splunkcloud.com:443	Actions
Splunk Cloud Production CloudTrail	https://http-inputs-firehose-cloud-architects.splunkcloud.com:443	Actions

Send to your Splunk Endpoint



Select all the accounts

Give the deployment a name

Select all the regions

Select the data sources you want to send

splunk> .conf19

AWS Accounts

Bulk Credential Upload | Bulk Data Deployment | New Account

5 accounts.

Filter by Organization Master Accounts.

Select...

Account Name	Account Type	Master Account	Credentials	Status	Joined	Age	Actions
002404001714	★ Individual	N/A	✓ Configured	N/A	N/A	N/A	Actions

Account Details Edit

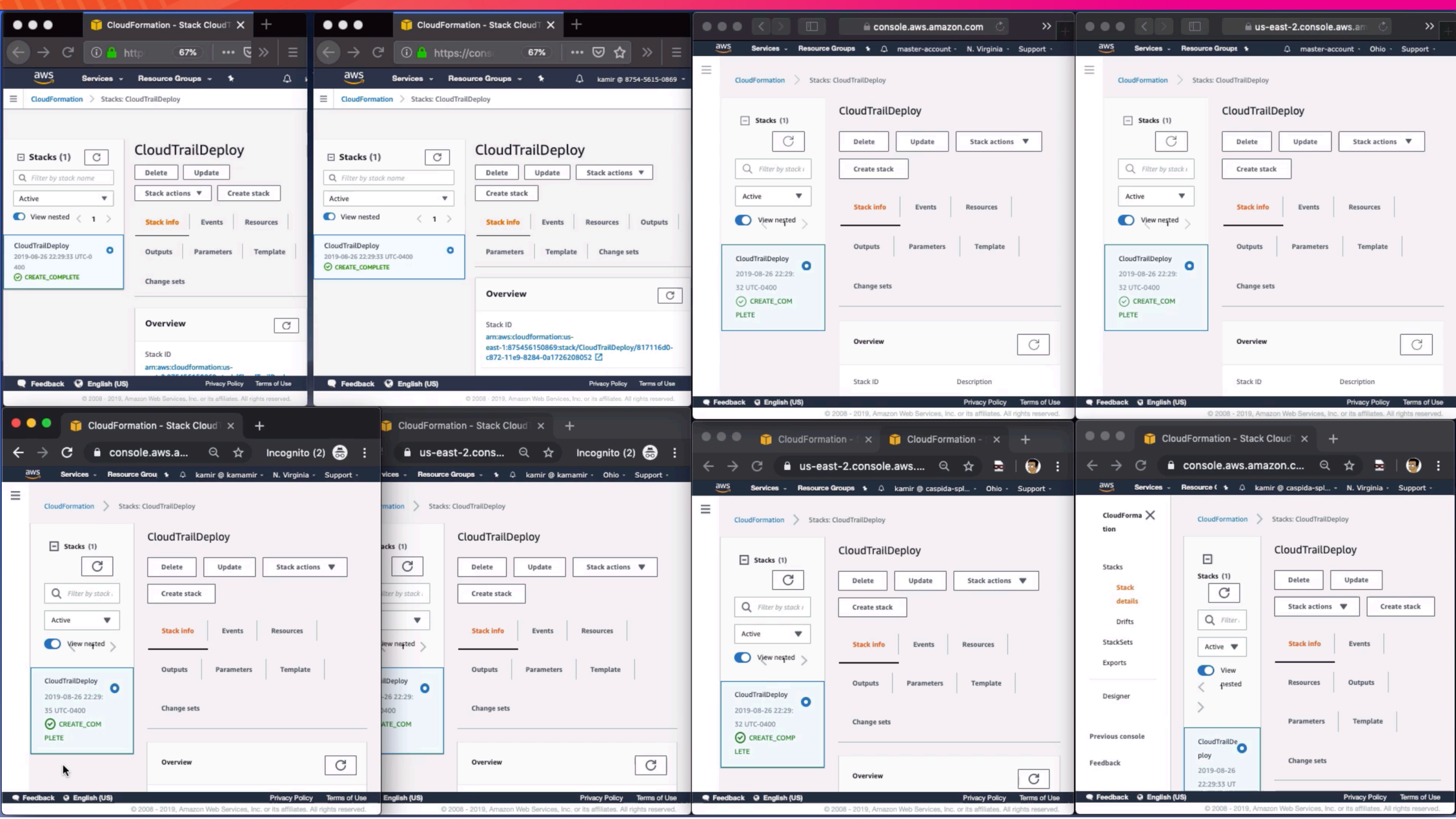
AWS Account ID 002404001714
AWS Account Key AKIAQBD2KE6ZBYHBVT4Q
AWS Account ARN ..... arn:aws:iam::002404001714:user/Grand_Central_Deployer
AWS Account Email ..... N/A
Tags ..... N/A

Data Collection

Deploy Data Collection

4 deployments.

Region	CloudTrail Status	Deployment Name	Data Collection Launch Status	Data Collection Deployment Status	Actions
us-west-1	✓ Deployed	CloudTrailDeploy	✓ Launched	Deploying	Actions
us-west-2	✓ Deployed	CloudTrailDeploy	✓ Launched	Deploying	Actions
us-east-1	✓ Deployed	CloudTrailDeploy	✓ Launched	Deploying	Actions
us-east-2	✓ Deployed	CloudTrailDeploy	✓ Launched	Deploying	Actions


CloudFormation - Stack CloudT
Services
Resource Groups
CloudFormation
Stacks: CloudTrailDeploy
Stacks (1)
CloudTrailDeploy
Delete
Update
Stack actions
Create stack
Active
View nested
Stack info
Events
Resources
Outputs
Parameters
Template
Change sets
Overview
Stack ID
Feedback
English (US)
Privacy Policy
Terms of Use

Observation Deck

Edit | Export ▾ | ...

View status of Accounts added to Grand Central

Time

Last 24 hours | Submit | Hide Filters

Number of Organizations

1

Number of Accounts

4

Successful Deployments

30

Map of Successful Deployments

Accounts Setup Geographically

Successful Deployments by Region

Account Filter

All

Regions

aws_account_id	Deployments	Regions
002404001714	9	us-east-1 us-east-2 us-west-1 us-west-2
337397712128	8	us-east-1 us-east-2 us-west-1 us-west-2
390687995958	5	us-east-1 us-east-2 us-west-1 us-west-2
875456150869	4	us-east-1 us-east-2 us-west-1 us-west-2
911795064262	4	us-east-1

Better Together

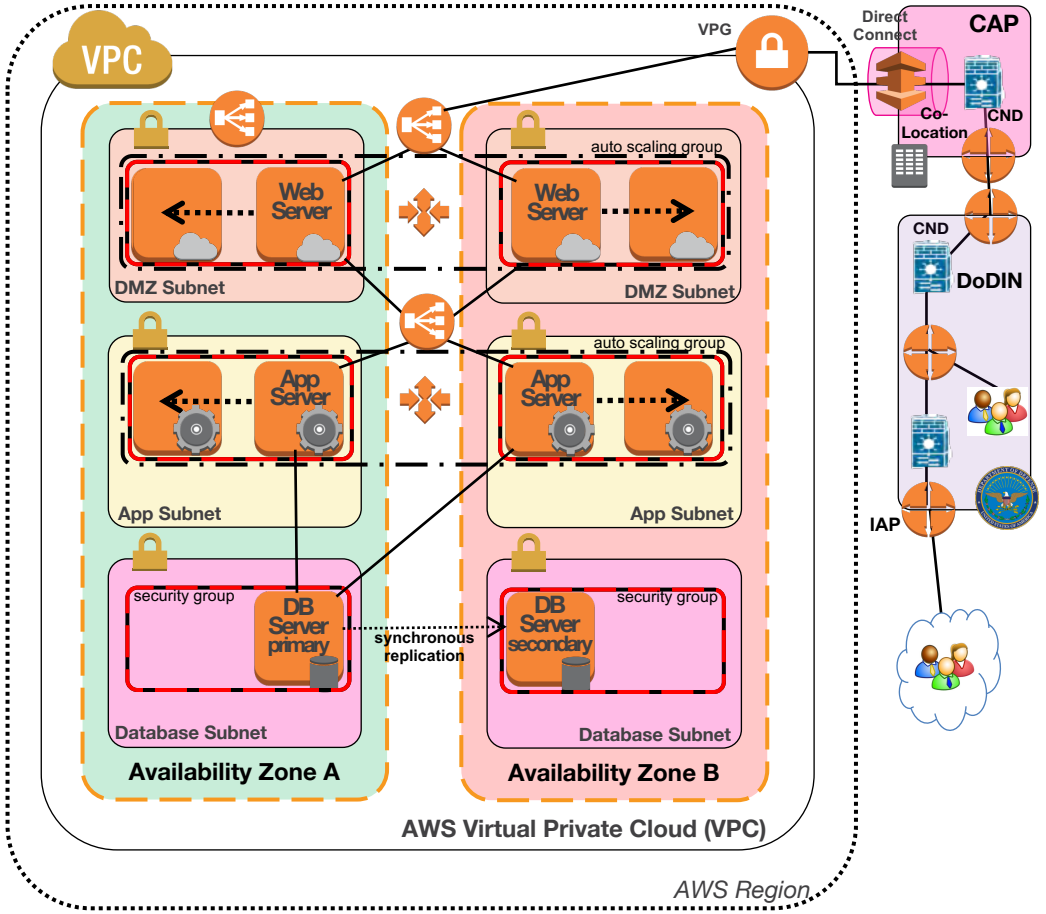
splunk> .conf19

Like Peas and Carrots

Detect and respond #1

Many customers are working with Controlled Unclassified Data (CUI) or FOUO data. A DoD SRG Impact Level 4 compliant Architecture does not have an Internet Gateway (IGW).

What happens if someone creates one?



Like Peas and Carrots

Detect and Respond #1

CloudTrail → CloudWatch Events → Splunk

Splunk ES raises and notable and alarm >

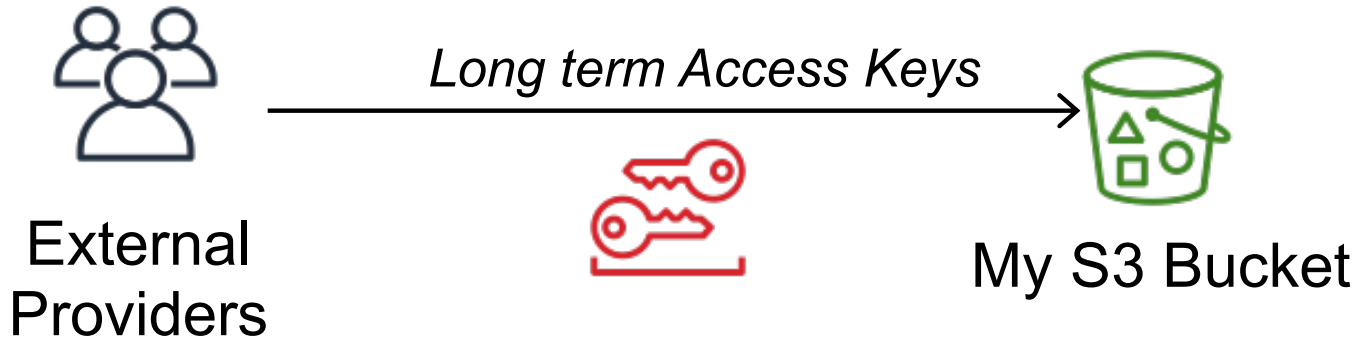
Identifies:

- Which Account
- Who did it
- When they did it
- Splunk passes notable to Phantom to delete the IGW and suspend Rights to Role (Deny Policy)

Like Peanut Butter and Jelly

Detect and Respond #2

Many customers may have external data providers or legacy, on premises, applications that may need to use IAM User Access Key/Secret Key to interact with AWS – such as putting data in an S3 bucket.



How can I know if those keys have been leaked or compromised?

Like Peanut Butter and Jelly

Detect and respond #2

CloudTrail → CloudWatch Events → Splunk

Splunk builds whitelist of acceptable SRC and usage patterns.
Alarms on Anomalies.

Identifies:

- Which Account
- WHERE they did it from
- When they did it
- Can trigger CWE/Lambda to suspend AK/SK, Call Phantom to run remediation playbook.

Like Biscuits and Gravy

Detect and respond #3

Many customers need to STIG or harden their “golden images” (called Amazon Machine Images (AMI) in AWS).

What happens if your environment is running AMI’s not authorized or really old (*2 years*)?

- Which Accounts are at risk?
- Which Mission Services?

Like Biscuits and Gravy

Detect and respond #3

Config → Config Rules → Splunk

Splunk periodically queries AWS API to “build the universe” of an account. Tracks state of EC2 instances and their history. Un-rolls the point in time state into a traceable history.

Identifies:

- Which Accounts
- How old are the AMIs
- When they did it

Key Takeaways:

Dem’take aways.
You has them

1. AWS Booth — See those demos
2. Review your organizations plan
3. Figure out your architecture for collection and archive
4. Challenge corporate conventional wisdom

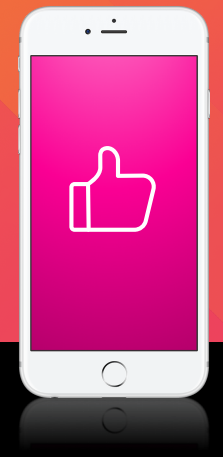
.conf19

splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION



Q&A

splunk> .conf19