AWS re:Invent

MGT408-R

Best practices for detecting and preventing data exposure

Claudia Charro

Enterprise Solutions Architect

Amazon Web Services

AWS re:Invent

aws

Agenda

1. Why should I pay attention to data exposure?

2. Lab to leverage a secure solution using:

   - AWS Config
   - Amazon CloudWatch Events
   - AWS Lambda
   - AWS Systems Manager

Landing zone sessions (search: “landing zone”)

SEC325-R – Architecting security & governance across your landing zone (Session)

ARC344-R – Understanding the landing zone journey (Chalk Talk)

GPSTEC203 – AWS Control Tower versus AWS Landing Zone (Chalk Talk)

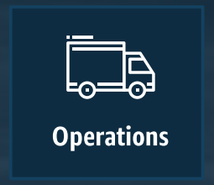
MGT307-R – Governance at scale: AWS Control Tower, AWS Organizations, and more (Chalk Talk)

MGT302-R – Enable AWS adoption at scale with automation and governance (Session)

SEC335-R – How to deploy secure workloads with AWS Control Tower (Chalk Talk)

GPSTEC324 – Automating ISV product deployment in AWS Landing Zone (Chalk Talk)

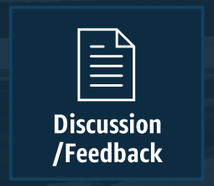
GPSTEC325 – AWS Control Tower in a nutshell and practice enablement for APN Partners



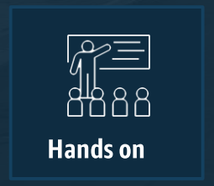
ENT320 – Cloud operations engineer: A day in the life

ENT214 – Cloud migration in the face of data-center eviction (Session)

ENT215 – Five steps AMS leverages to accelerate cloud adoption (Session)



SEC324-R – Deep dive into AWS multi-account strategies (Chalk Talk)



ARC315-R – Build end-to-end governance with AWS Control Tower (Workshop)

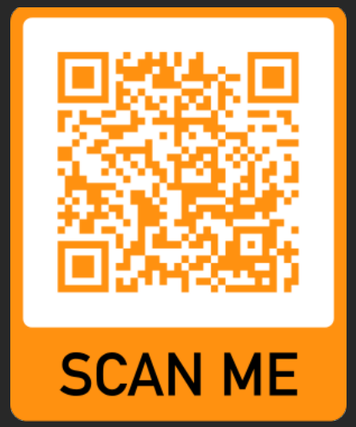
SEC347-R – DNS across a multi-account environment (Builders Session)

Agenda

In this session, learn how to configure AWS CloudTrail to detect unauthorized exposure of your data, and to configure AWS Config, Amazon CloudWatch Events, and AWS Lambda to prevent the exposure. This session also provides best practices for preventing misconfiguration of resources, including Amazon S3 and other services.

Hands-on instructions:

https://reinvent2019.aws-management.tools/mgt408/en/cont.html



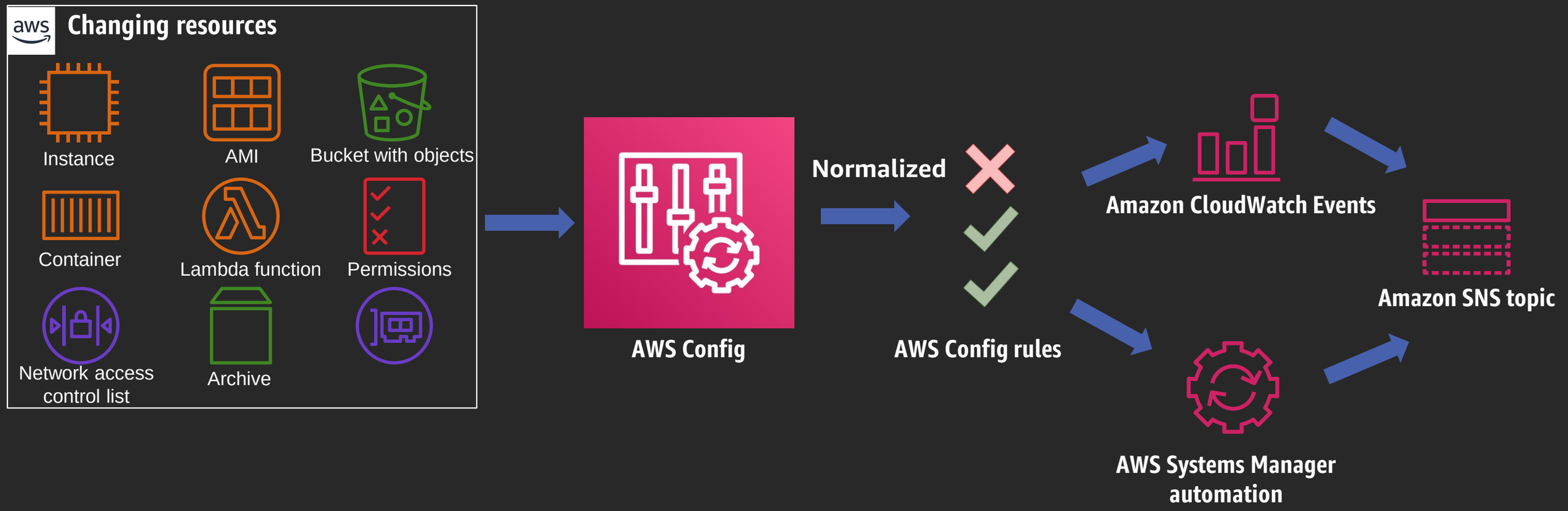
Reasons to care about data exposure

breachlevelindex.com, 2017 data

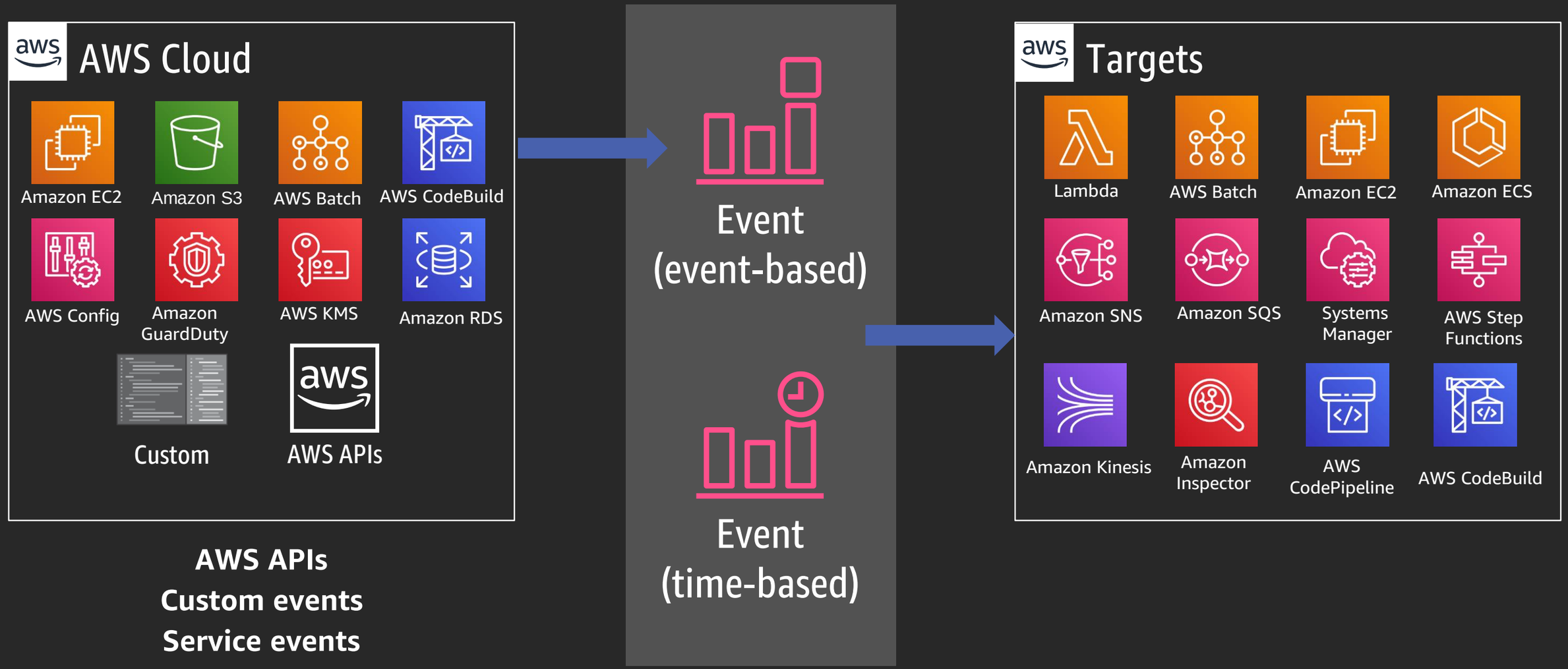
Questions to address

- Do I have adequate security to protect my workloads and data?
- How good is good enough?
- What security controls do I need to separate data from human interference? Do I have logs enable for each part of my workload?
- Do I have validation that the right controls were built?
- Do I have verification that the controls work as planned?
- Do I test my data security procedures?

The baseline for our hands on – AWS Config

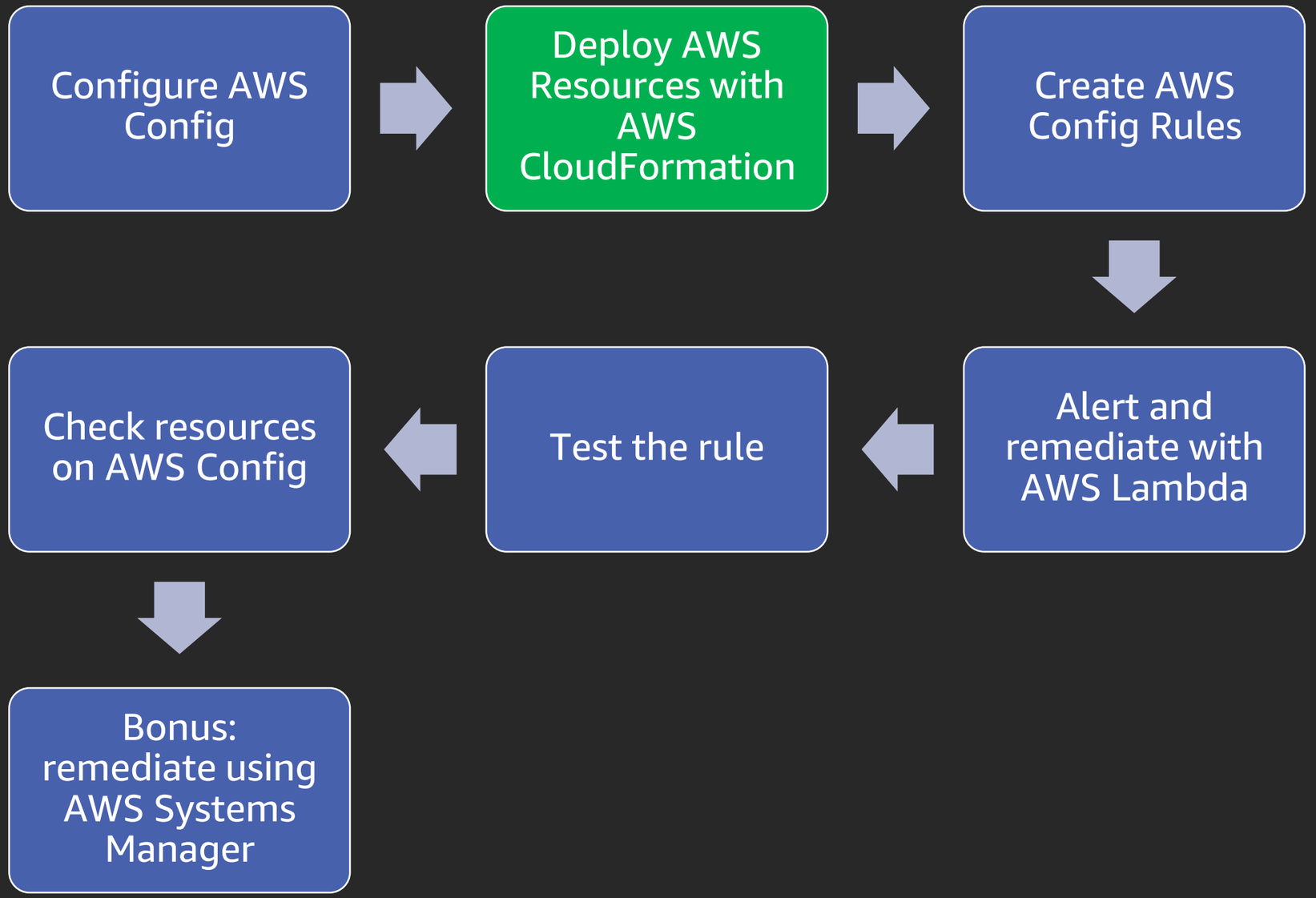


Baseline for our hands-on: Amazon CloudWatch Events



AWS APIs
Custom events
Service events

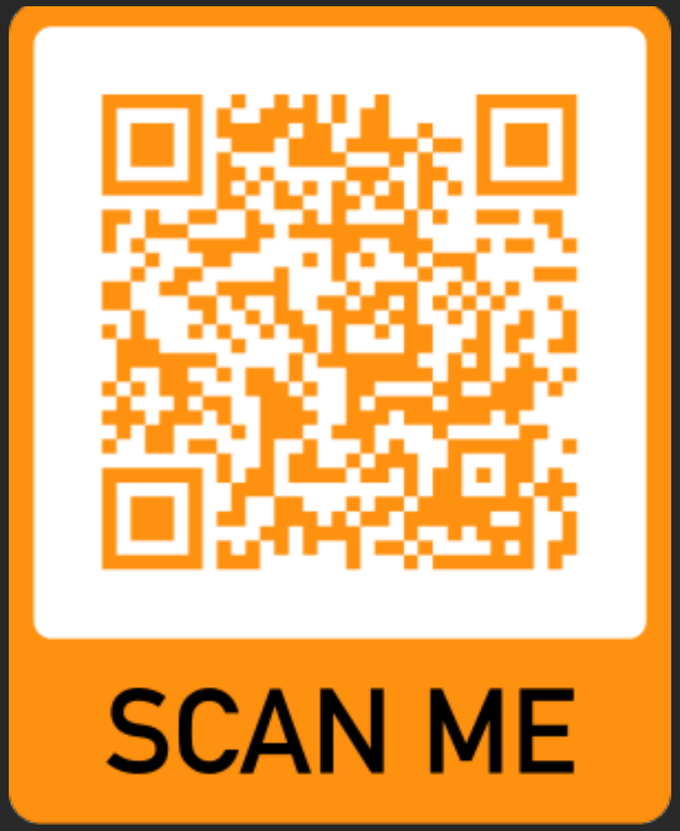
Lab Steps


Configure AWS Config
Deploy AWS Resources with AWS CloudFormation
Create AWS Config Rules
Alert and remediate with AWS Lambda
Test the rule
Check resources on AWS Config
Bonus: remediate using AWS Systems Manager

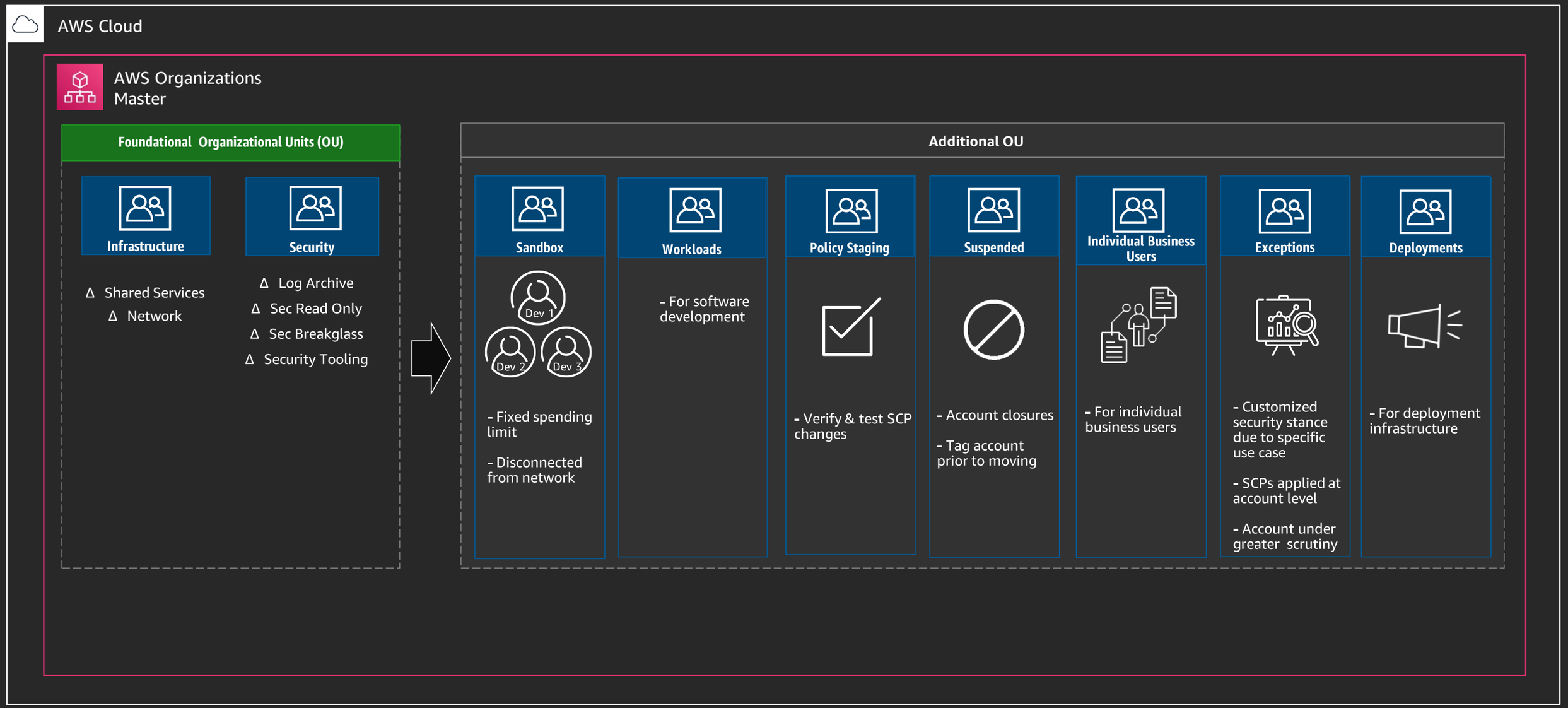
Let’s do it in the console!

Execute Lab:

https://reinvent2019.aws-management.tools/mgt408/en/cont.html



Start by organizing your accounts



Lab steps: Removing resources

Thank you!

AWS re:Invent

aws

Please complete the session survey in the mobile app.