
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

DOP404-R

Proactive security and compliance for infrastructure-as-code resources

Brian Terry

Sr. Solutions Architect – ISV Integrations, AWS Marketplace
AWS

Ben Perak

Principal Product Manager
AWS

Casey Lee

Principal DevOps Consultant
AWS

Luke Heidecke

Sr. Specialist, DevOps
AWS

Rahul Garg

Principal Product Manager
AWS

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

- Shift left – What's that?
- How does this apply to IaC?
- Tool of the trade
- Workshop architecture
- Start building

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Shift left – What's that?

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Shift left

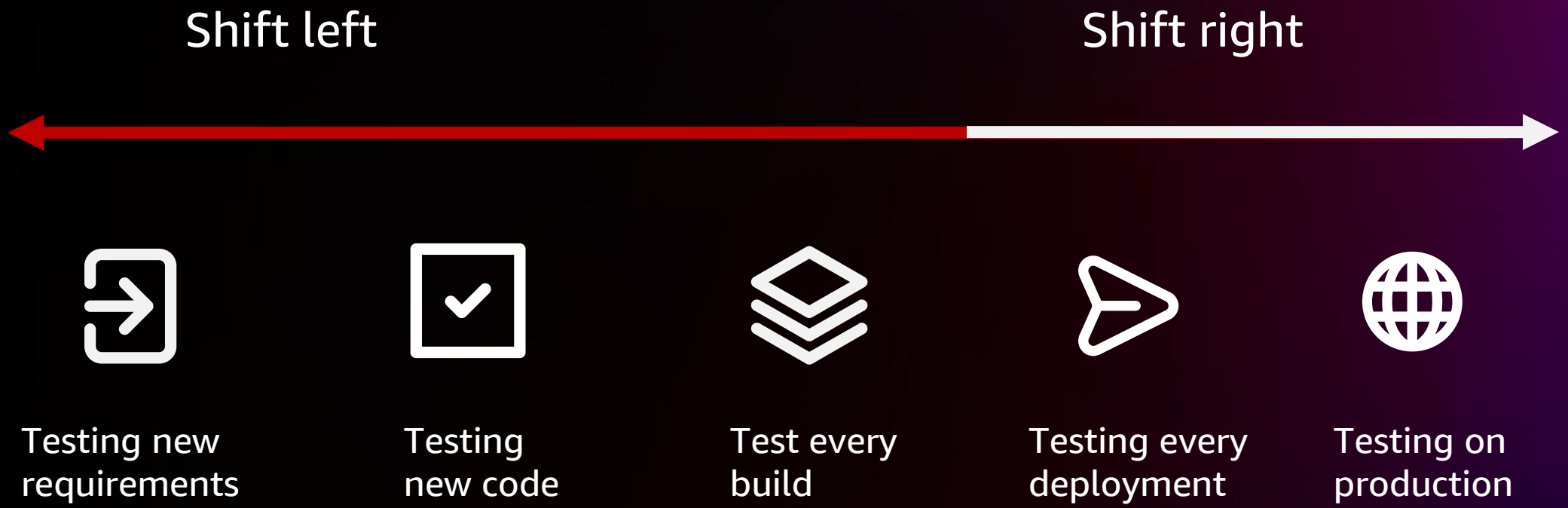
Shift left is a practice intended to find and prevent defects early in the software delivery process.

Defined by Larry Smith in 2001

https://bit.ly/3VDdDWN

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Application testing

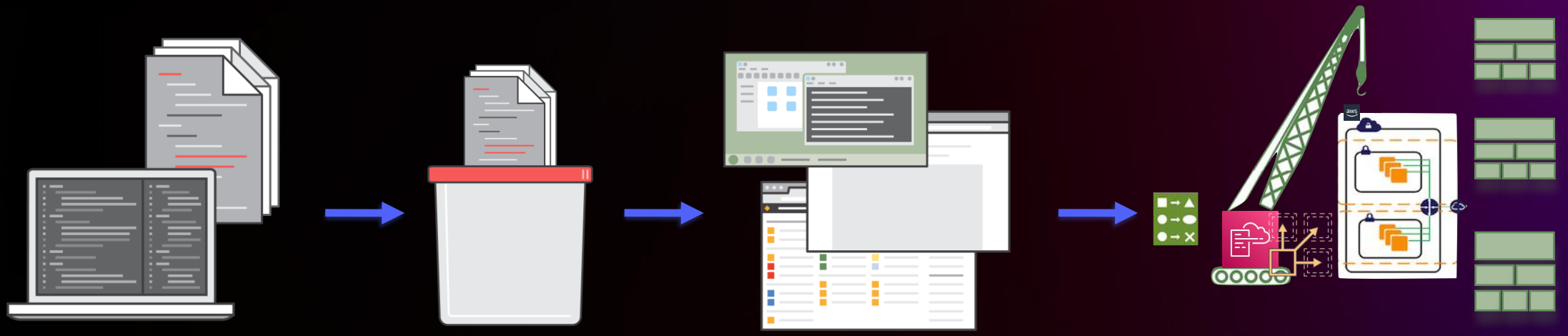


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How does this apply to IaC?

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Infrastructure as code – Recap



Code in YAML or JSON directly or use sample templates

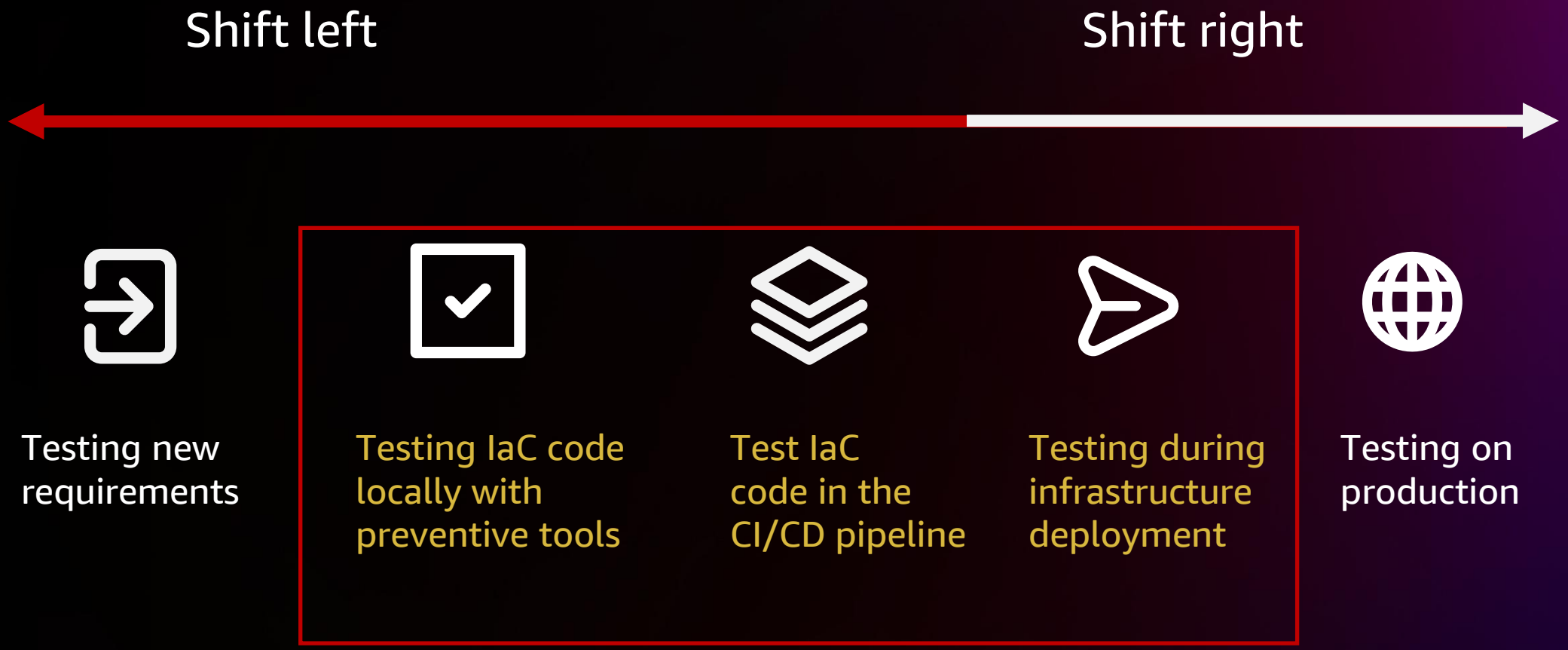
Upload local files or files from an Amazon S3 bucket

Create stack using console, API, or CLI

Stacks and resources are provisioned

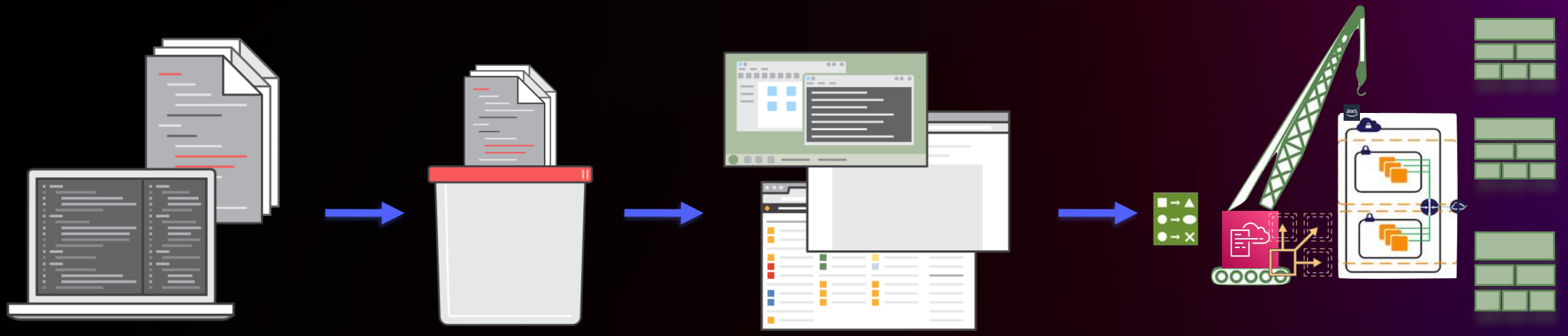
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Shift-left application testing



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Infrastructure as code – Expanded



Testing IaC code locally with preventive tools

Upload local files or files from an Amazon S3 bucket

Test IaC code in the CI/CD pipeline

Testing during infrastructure deployment

aws

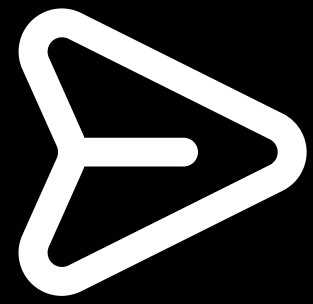
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Tool of the trade from right to left

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Config Rules

- Reactive validation
- Automatic remediation
- You can use prebuilt rules
- Build your own
- ”Always on”



Testing after infrastructure deployment

Shift left

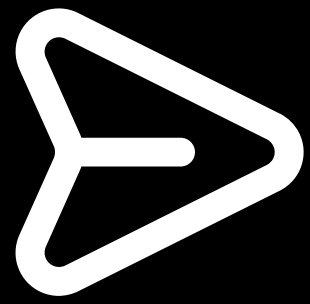
Shift right



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Systems Manager Automation documents

- AWS Config applies remediation using AWS Systems Manager Automation documents
- You can either choose to manually or automatically remediate noncompliant resources
- Create your own custom remediation actions



Testing after infrastructure deployment

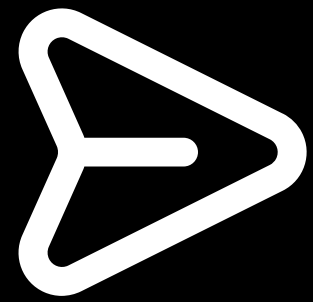
Shift left

Shift right

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS CloudFormation hooks





- Proactive validation
- Automatic enforcement
- Prebuilt hooks
- Build your own
- ”Always on”

Testing during infrastructure deployment

Shift left

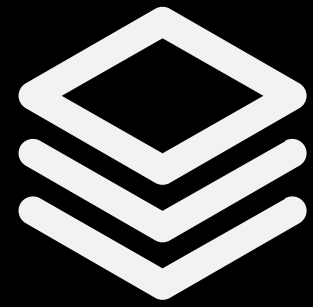
Shift right



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS CodePipeline

- Use CFN-Guard to validate compliance
- Deploy AWS CloudFormation



Test IAC code in the CICD pipeline

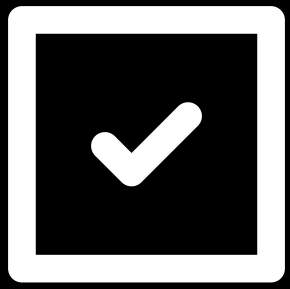
Shift left

Shift right

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS cdk-nag – Policy as code

- Open source policy-as-code tool
- Predefined rules for AWS solutions, HIPAA, NIST 800-53 and PCI DSS 3.2.1
- Validate AWS CDK applications
- Any **AWS CDK** configuration



Testing IAC code locally with preventive tools

Shift left

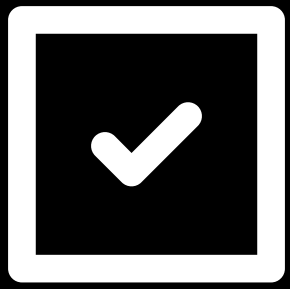
Shift right



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS CFN-Guard – Policy as code

- Open source policy-as-code tool
- Write rules to validate compliance
- Validate AWS CloudFormation
- Any JSON or YAML doc configuration
- **Terraform state files**
- **Kubernetes configurations**



Testing IAC code locally with preventive tools

Shift left

Shift right



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Introduction to CloudFormation hooks

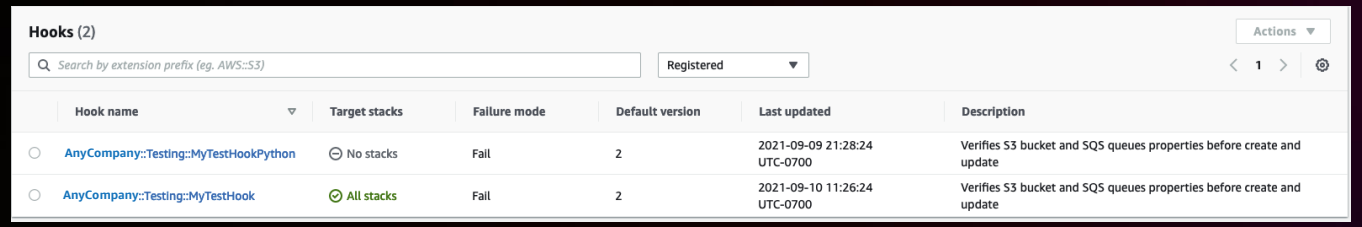
Template

```
AWSTemplateFormatVersion: "2010-09-09"
Resources:
  S3Bucket:
    Type: AWS::S3::Bucket
    Properties: {}
```

```
resultStatus = HookStatus.FAILED;
resultMessage = "Bucket Encryption not enabled for bucket with name: " + bucket.getBucketName();
```



Registered hooks



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Guard Rules Registry (Bonus)

- Open-source library of rules templates
- https://github.com/aws-cloudformation/aws-guard-rules-registry
- Delivers consumable templates for public use
- Best-effort complement for detective controls
- Support DevSecOps from the “shift-left” philosophy

Shift left



NEW

README.md

AWS Guard Rules Registry

AWS Guard Rules Registry is an open-source repository of AWS C
sets that help organizations *shift left* in their Software Developmer

TL;DR

Leverage the existing AWS Guard Registry Rule Sets currently a

- Read the Using Guard Rules Registry Guide for information on
integration and development processes. Then pick from the li

Contribute to the individual AWS Guard Registry Rules:

- Read the Guard Rules Development Guide for details in how to
rules. Additionally, Guard Rules Registry has several staged G
These Guard rules are to be a *best of effort* representation of
for an open issues labeled `good first issue`.

Create and contribute your own open source AWS Guard Rules

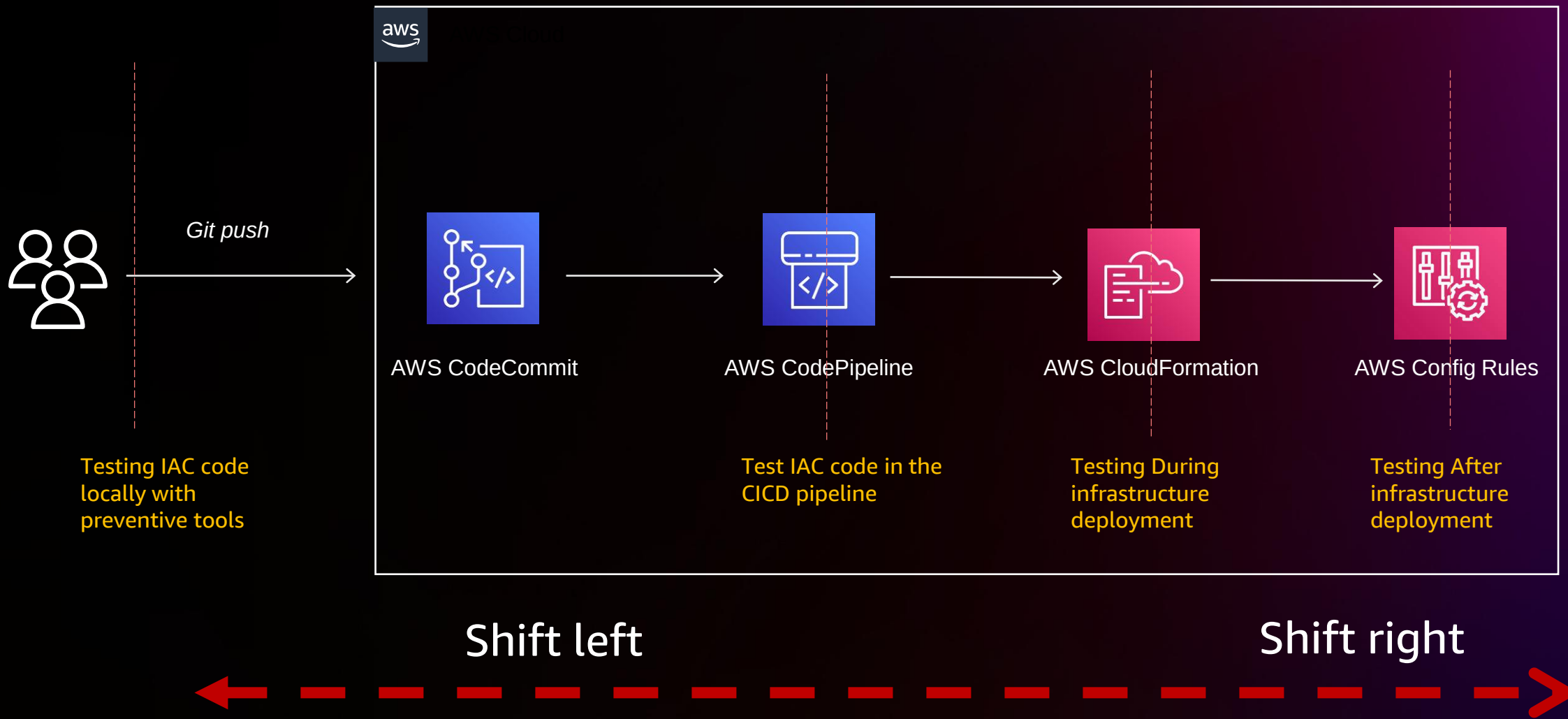
- Read the Guard Rule Sets Development Guide for details on c

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Workshop architecture

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

High-level architecture overview

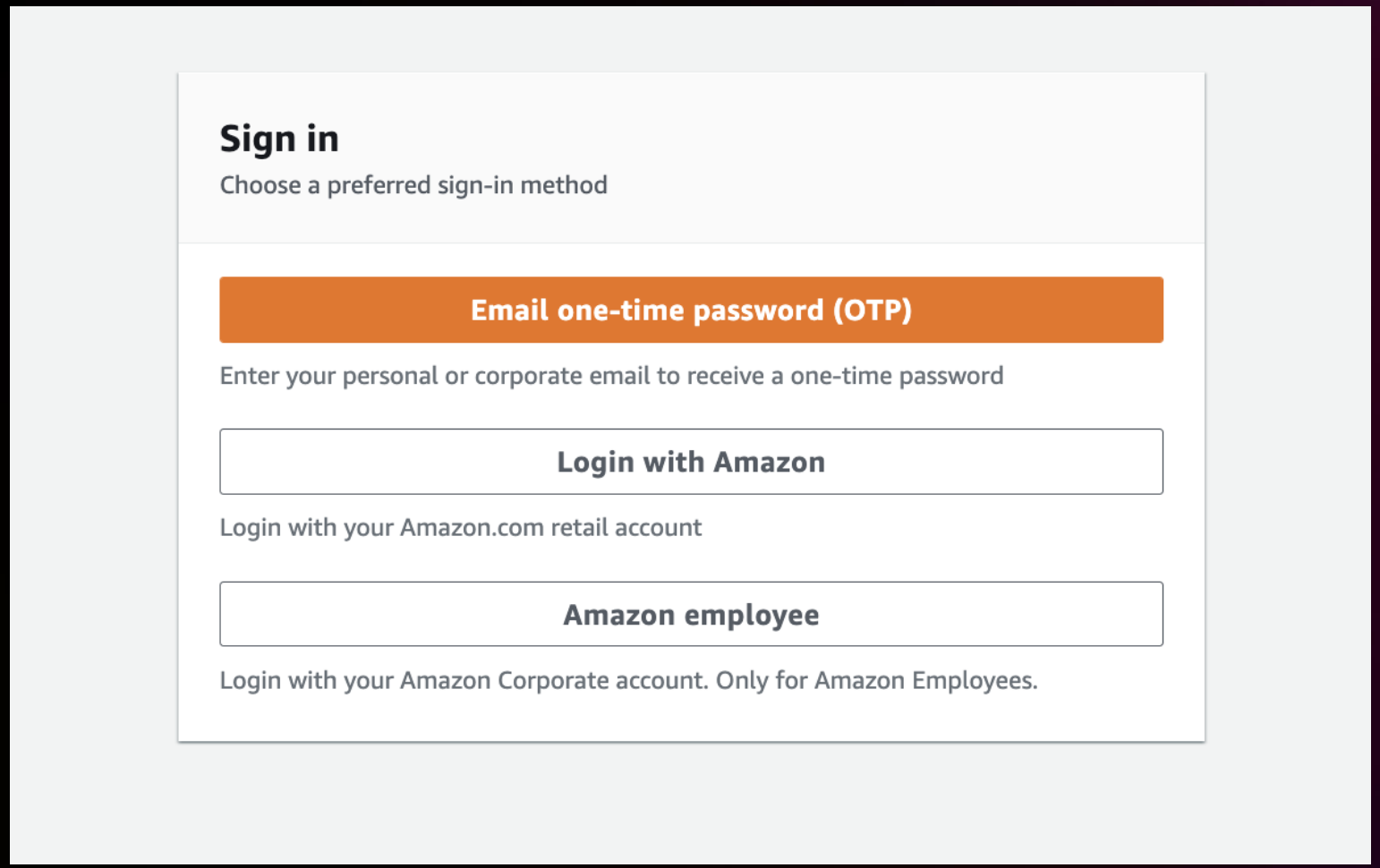


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Let’s start building

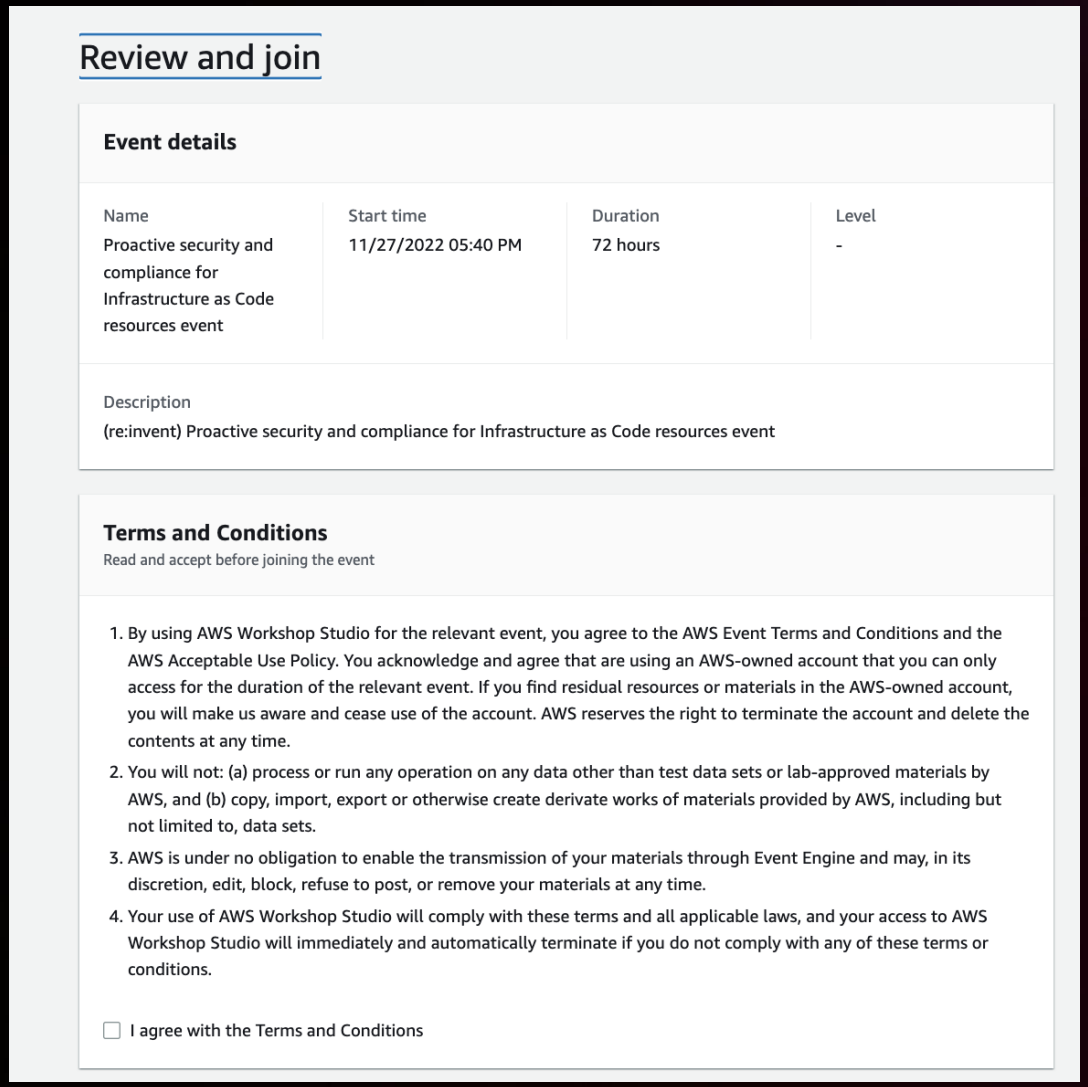
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Visit: http://bit.ly/3EHf3YM



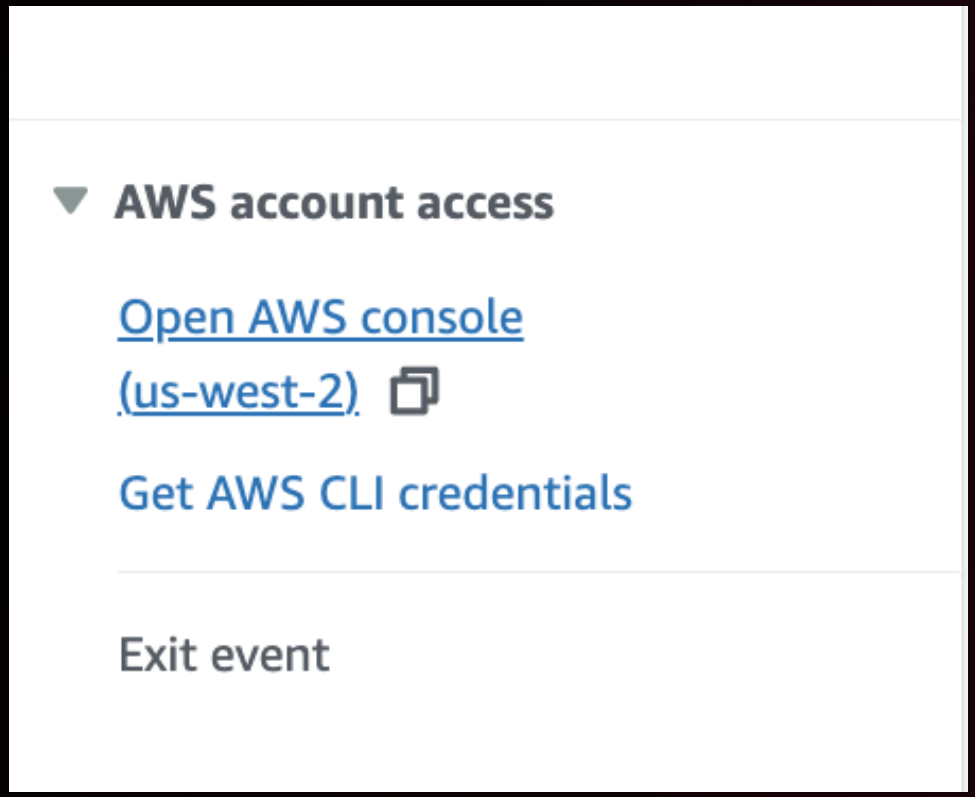
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Visit: http://bit.ly/3EHf3YM



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Visit: http://bit.ly/3EHf3YM



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Brian Terry
brianter@amazon.com
linkedin.com/in/brian-t-b3276250
Twitter: @ineedhelpbrian

Ben Perak

Casey Lee

Luke Heidecke

Rahul Garg



Please complete the session survey in the **mobile app**

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.