

AWS re:Invent

NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

COP206-R

Build a complete DevSecOps pipeline on AWS

George Rolston

Senior Solutions Architect,
Cloud Foundations
AWS

Brian Terry

Senior PSA - ISV Integrations,
CloudFormation
AWS



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

Agenda

1. DevSecOps and shift left overview
2. Our DevSecOps tools
3. Workshop architecture
4. Start building!

Why AWS Cloud Operations?



Return on Investment (ROI)

241% ROI
over 3 years*



Staff productivity

62% more
efficient IT
infrastructure
staff



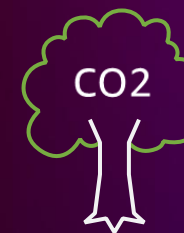
Operational resilience

57% decrease
in downtime



Business agility

37% decrease
in time
to market

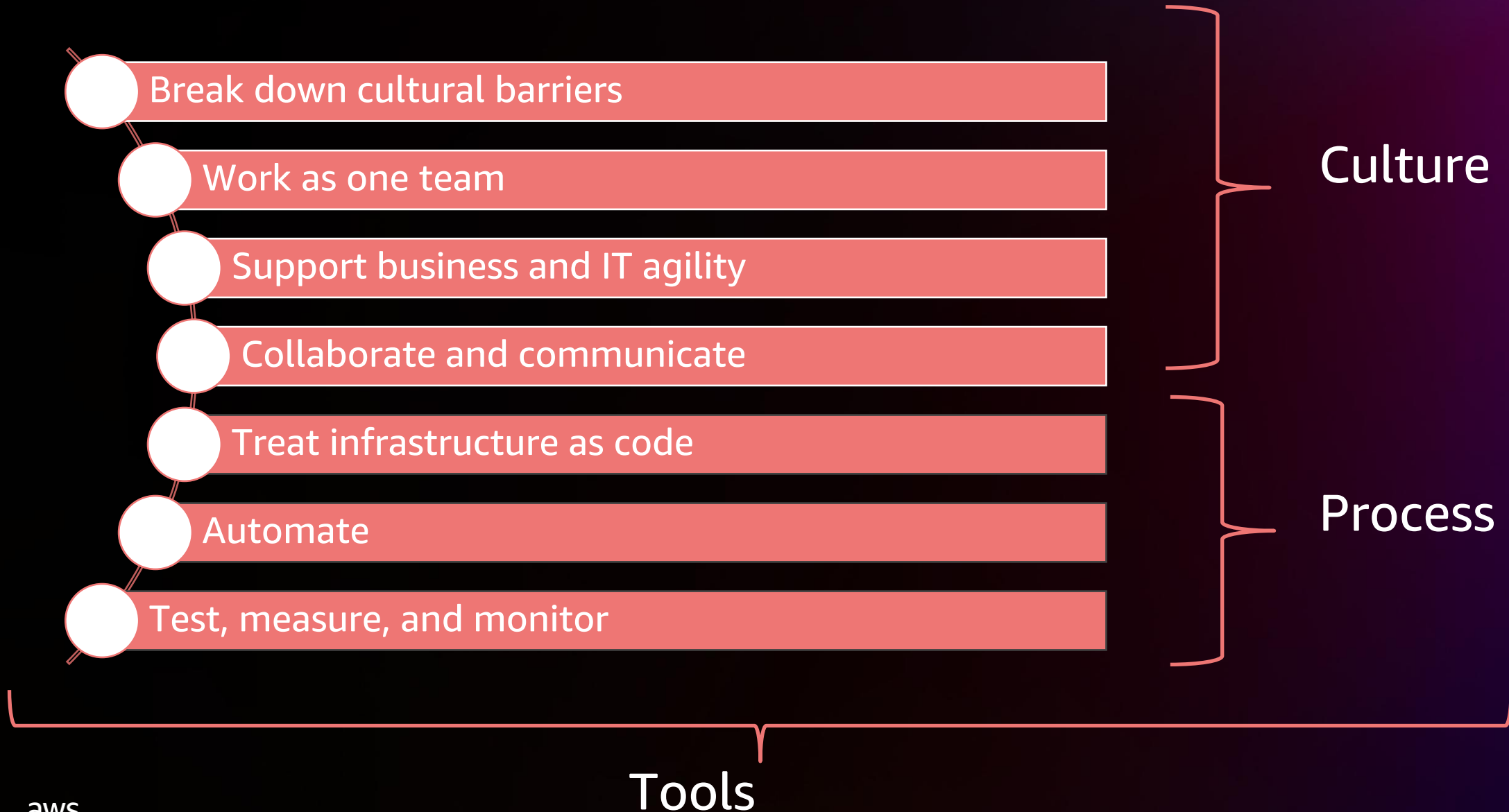


Carbon savings

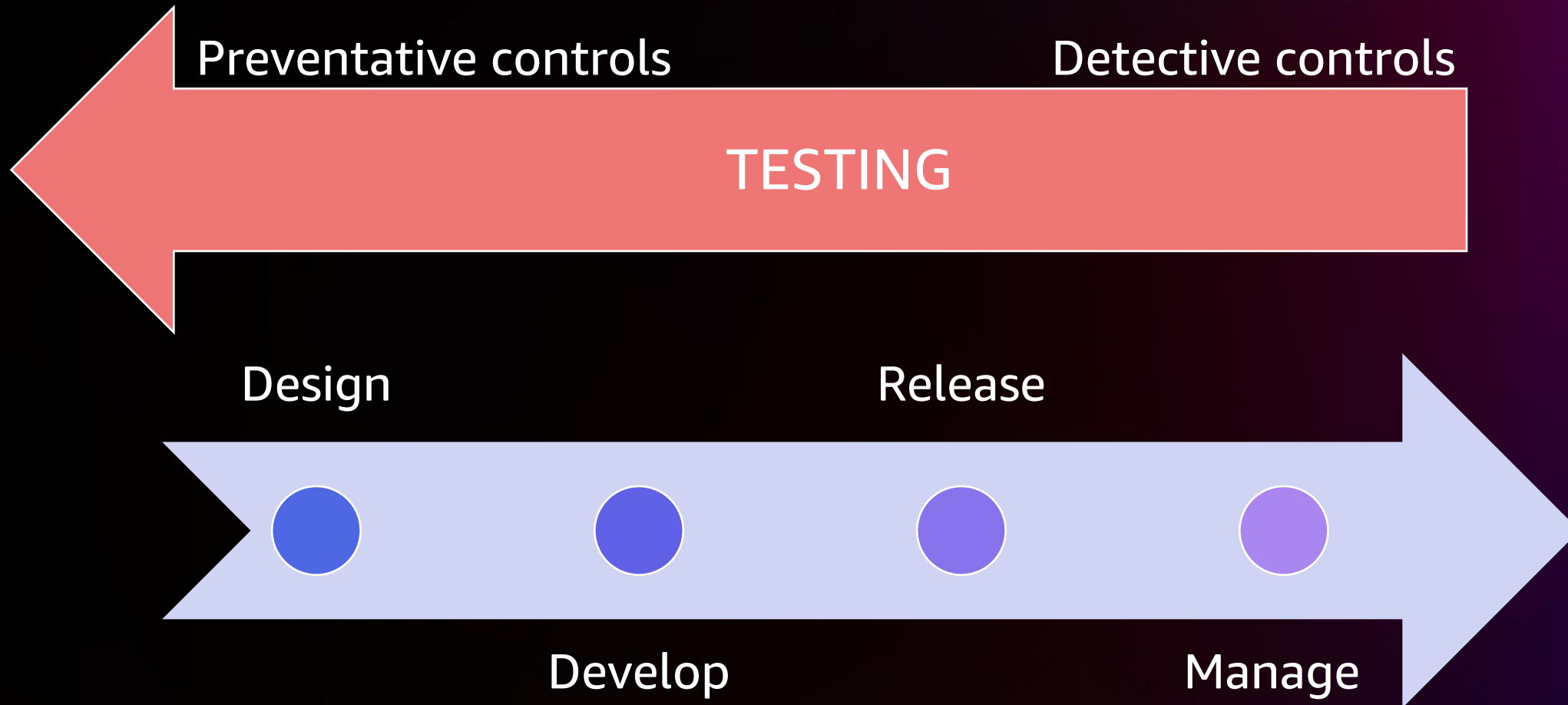
88% reduction
in carbon
footprint of
IT operations



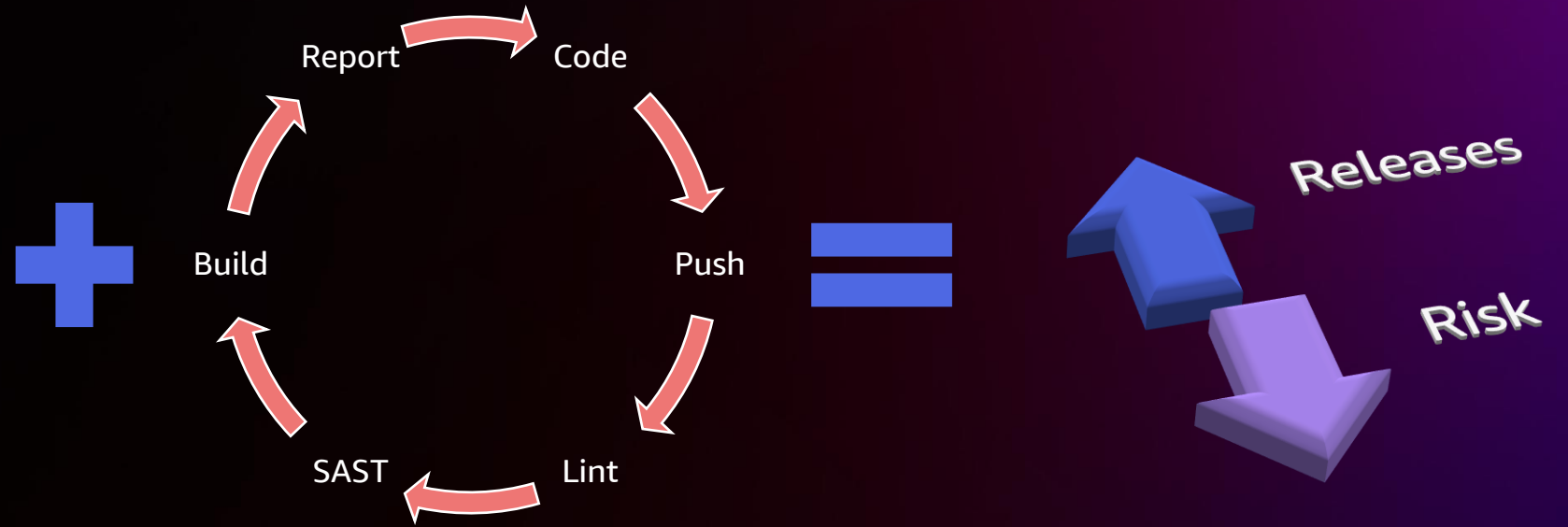
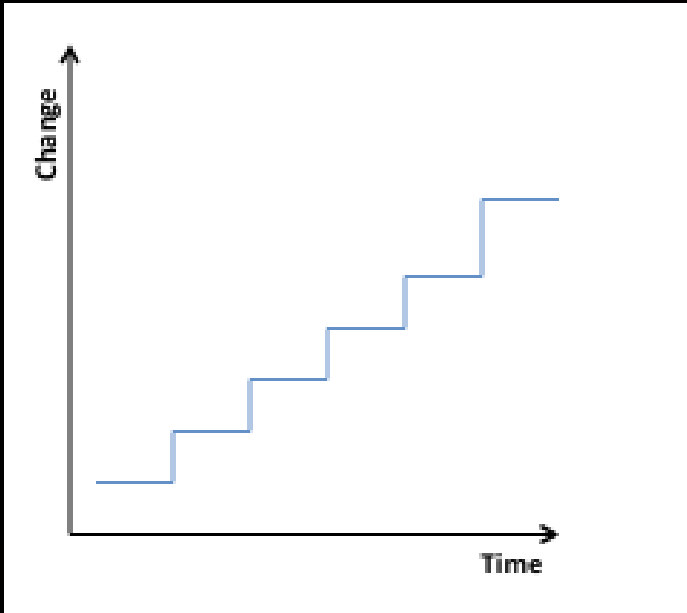
DevSecOps and shift left overview



DevSecOps and shift left overview



DevSecOps formula for success



AWS CloudFormation Guard – Policy as code

Open source policy-as-code tool

- <https://github.com/aws-cloudformation/cloudformation-guard>

A policy-as-code domain-specific language (DSL)

Current version 2.1.3

- Any JSON- or YAML-formatted configuration data, such as:
 - **Terraform state files**
 - **Kubernetes configurations**



AWS CloudFormation Guard Rules Registry

Open source library of rule templates and rule sets

<https://github.com/aws-cloudformation/aws-guard-rules-registry>

aws-cloudformation / aws-guard-rules-registry Public

Code Issues 39 Pull requests Discussions Actions Projects 1 Wiki Security Insights

main 3 branches 3 tags

Go to file Add file Code

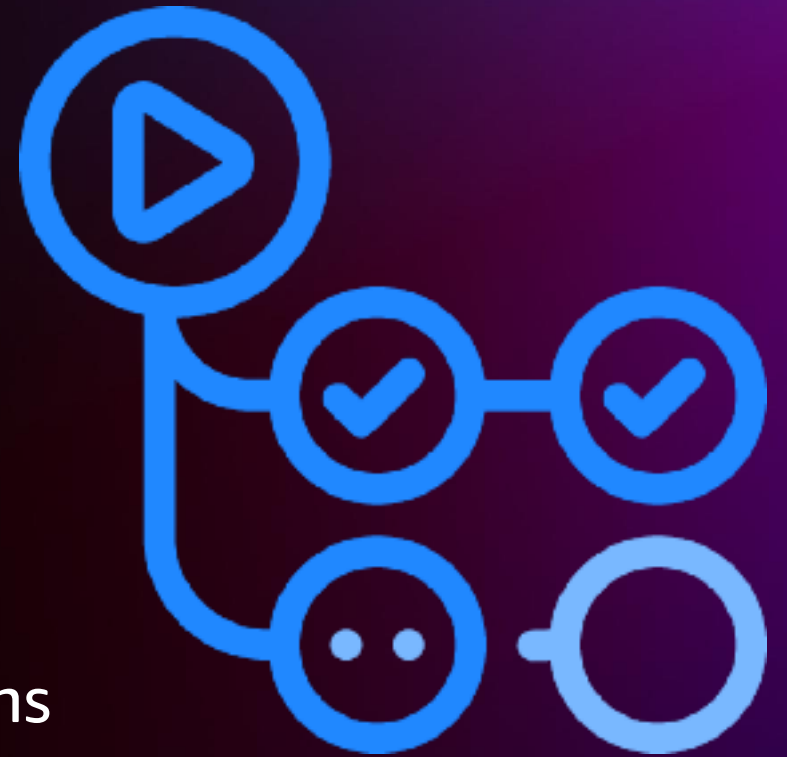
grolston feat: elb cloudfront (#227) 4e83476 1 hour ago 56 commits

github	feat: resource map (#222)	last month
docker	feat: Make docker image work with non-root users (#219)	last month
docs	feat: resource map (#222)	last month
mappings	feat: elb cloudfront (#227)	1 hour ago
rules/aws	feat: elb cloudfront (#227)	1 hour ago
.gitignore	feat: ec2 (#191)	5 months ago
CODE_OF_CONDUCT.md	Initial commit	11 months ago



GitHub Actions

- CI/CD services
 - Built into GitHub
 - Similar to GitLab CI
- Supported in GitHub.com and Enterprise GitHub
- AWS GitHub Actions – <https://github.com/aws-actions>



AWS for GitHub Actions

<https://amazon.com/aws>

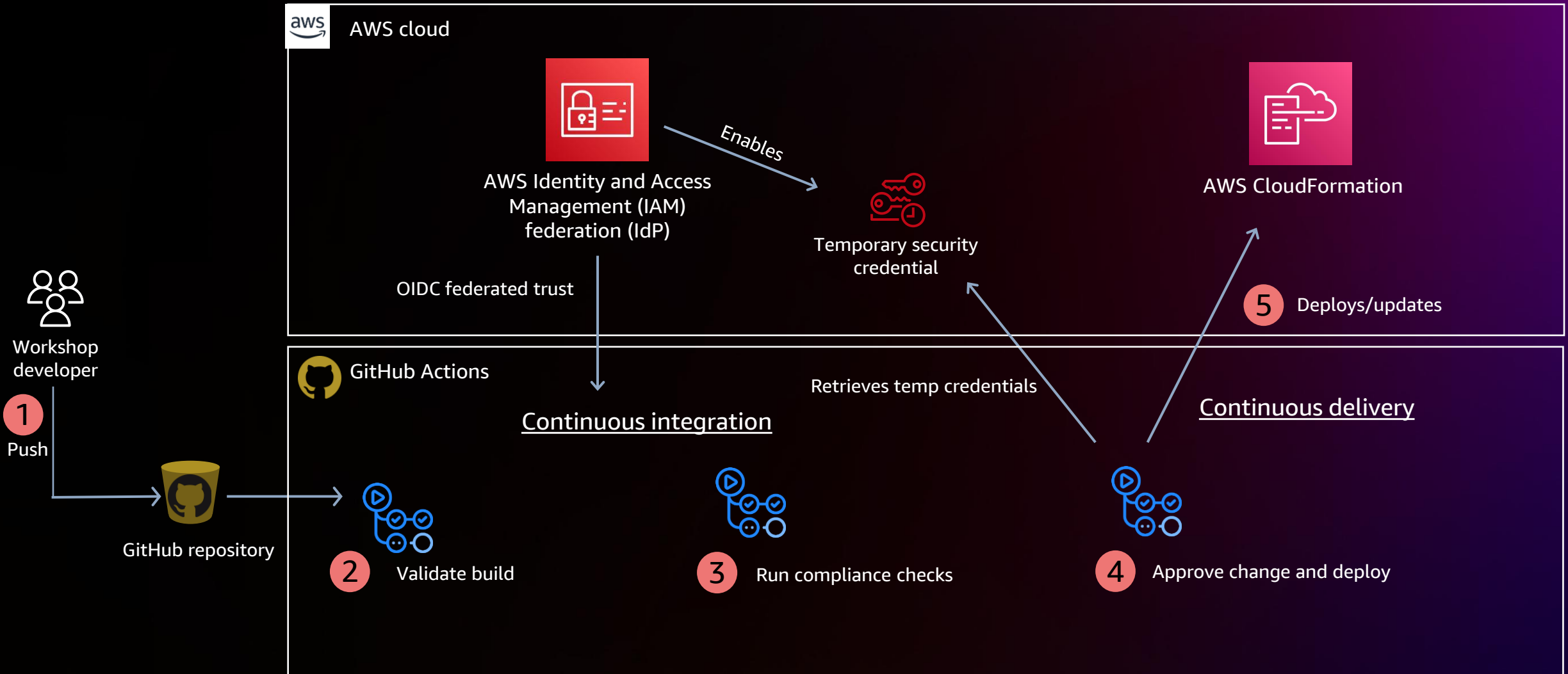
Part of Amazon

Verified

Workshop architecture



Architecture overview



Let's start building



Visit: `dashboard.eventengine.run`

Terms & Conditions:

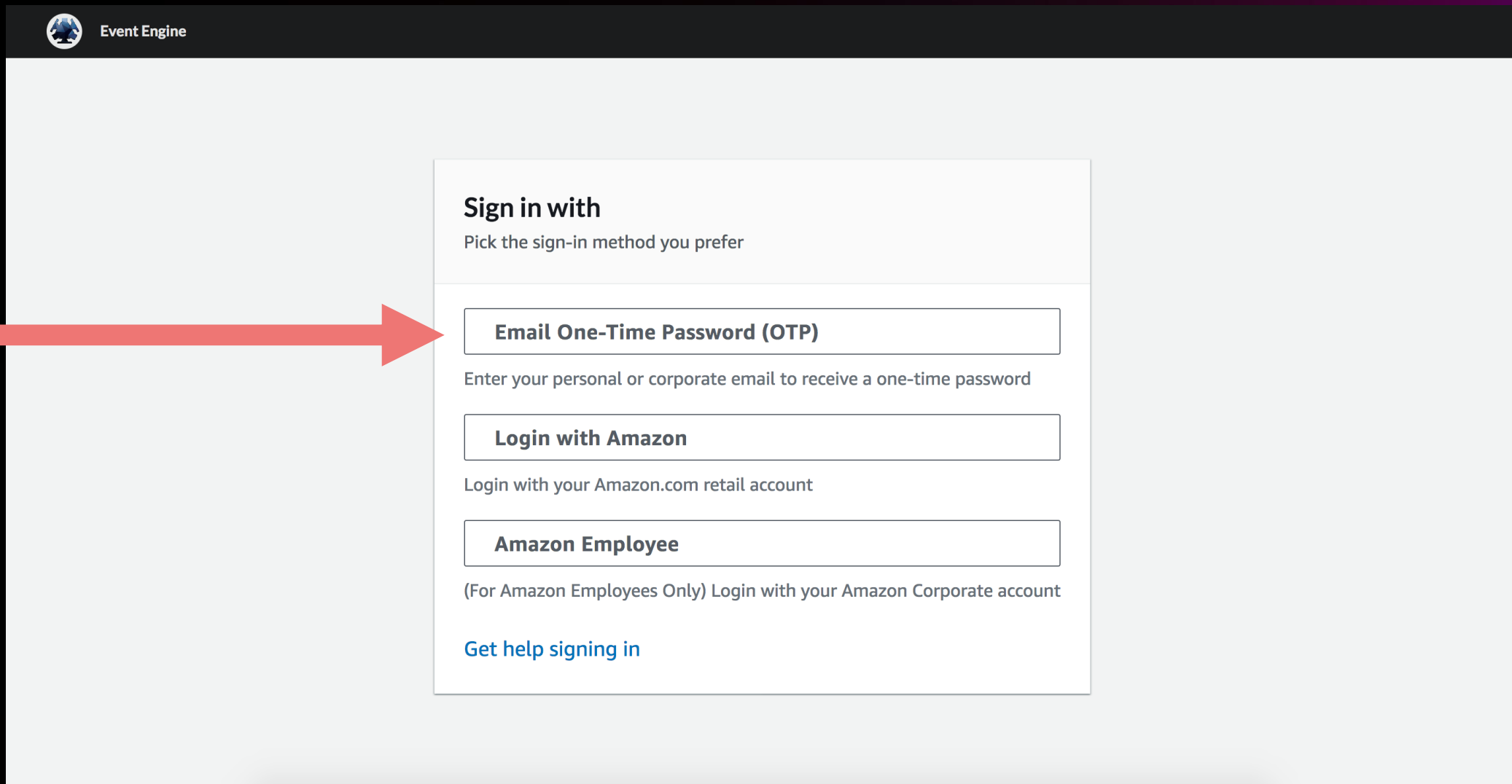
1. By using the Event Engine for the relevant event, you agree to the [AWS Event Terms and Conditions](#) and the [AWS Acceptable Use Policy](#). You acknowledge and agree that are using an AWS-owned account that you can only access for the duration of the relevant event. If you find residual resources or materials in the AWS-owned account, you will make us aware and cease use of the account. AWS reserves the right to terminate the account and delete the contents at any time.
2. You will not: (a) process or run any operation on any data other than test data sets or lab-approved materials by AWS, and (b) copy, import, export or otherwise create derivate works of materials provided by AWS, including but not limited to, data sets.
3. AWS is under no obligation to enable the transmission of your materials through Event Engine and may, in its discretion, edit, block, refuse to post, or remove your materials at any time.
4. Your use of the Event Engine will comply with these terms and all applicable laws, and your access to Event Engine will immediately and automatically terminate if you do not comply with any of these terms or conditions.

abcd-0345-df

This is the 12 or 16 digit hash that was given to you for this event or for a specific team.

✓ Accept Terms & Login

Visit: dashboard.eventengine.run



The screenshot shows the Event Engine dashboard login interface. At the top left, there is a logo and the text 'Event Engine'. The main content area is a white box with a light gray border. Inside, the heading 'Sign in with' is followed by the instruction 'Pick the sign-in method you prefer'. There are three buttons: 'Email One-Time Password (OTP)', 'Login with Amazon', and 'Amazon Employee'. A red arrow points to the 'Email One-Time Password (OTP)' button. Below each button is a brief description of the login method. At the bottom, there is a link 'Get help signing in'.

Sign in with
Pick the sign-in method you prefer

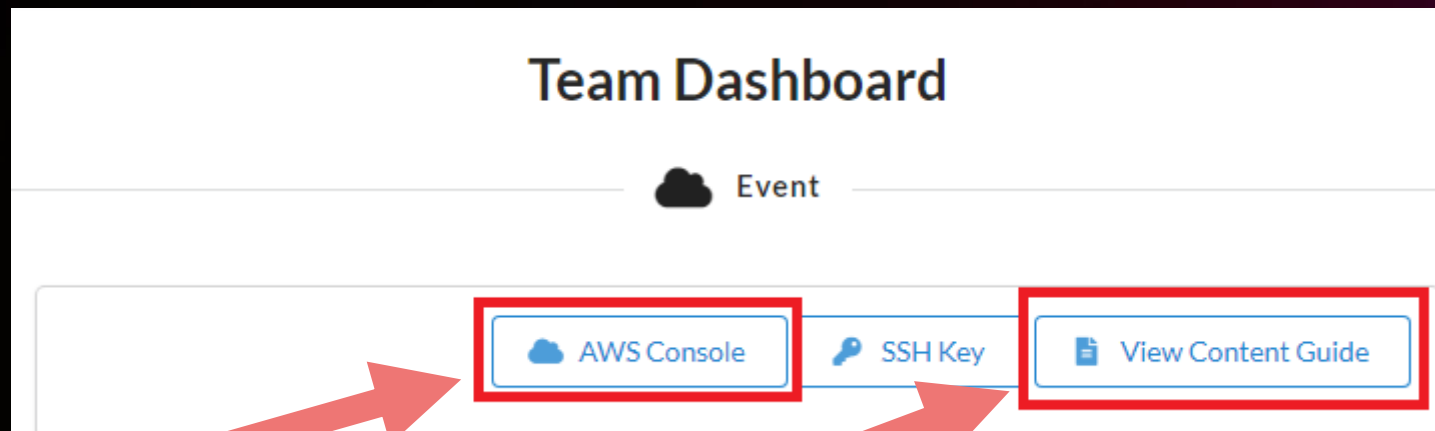
Email One-Time Password (OTP)
Enter your personal or corporate email to receive a one-time password

Login with Amazon
Login with your Amazon.com retail account

Amazon Employee
(For Amazon Employees Only) Login with your Amazon Corporate account

[Get help signing in](#)

Visit: `dashboard.eventengine.run`



Let's go!

Access <https://www.cop206.com>

Password: reinvent22-cop206



Workshop Outline

- Introduction
- Environment Setup
- CI/CD Account Aware Pipeline
- Deploy Template
- Summary

Want to see more AWS Cloud Operations?

Please complete the
session survey
in the mobile app



Ask us anything at our
kiosks in the
AWS Village Expo



Find related sessions
in our re:Invent blog



Cloud foundations and multi-account strategy sessions

Architecture



ARC205 (breakout) Establishing your cloud foundation on AWS – beyond your landing zone

ARC321 (chalk talk) Using a multi-account strategy to enable hyperscale

ARC318 (chalk talk) Best practices for disaster recovery of workloads on AWS

COP305 (breakout) Best practices for organizing and operating on AWS

Implementation



COP325 (chalk talk) Best practices for automating AWS account migration

ARC319 (chalk talk) Designing a multi-account environment for disaster recovery

DOP322 (chalk talk) Optimizing runtime performance with AWS X-Ray and Amazon CodeGuru Profiler

DOP402-R (chalk talk) Implementing DevSecOps pipelines with compliance in mind

Discussion



COP324 (chalk talk) Extend your multi-account governance with automation

ARC317-R (chalk talk) Architecting security and governance across your multi-account environment

COP323-R (chalk talk) Delegating access in a multi-account environment with IAM Identity Center

Hands-on



COP206-R (workshop) Build a complete DevSecOps pipeline on AWS

ARC301-R (workshop) Building a monitoring strategy

Thank you!

George Rolston

grolston@amazon.com

[linkedin.com/in/george-rolston](https://www.linkedin.com/in/george-rolston)

Brian Terry

brianter@amazon.com

[linkedin.com/in/brian-t-b3276250](https://www.linkedin.com/in/brian-t-b3276250)

twitter: ineedhelpbrian@



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



Access info: <https://www.cop206.com>



Password: reinvent22-cop206