AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

SEC307-R2

Integrating AWS IAM Access Analyzer into CI/CD pipelines

Katie Williams
Sr. Solutions Architect
AWS

Victor Feinman
Sr. Solutions Architect
AWS

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

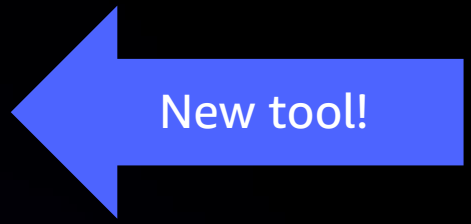
Agenda

IAM Access Analyzer overview

Why validate IAM policies in your pipeline?

Workshop architecture

IAM Policy Validator for AWS CloudFormation



Get building!

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IAM Access Analyzer

Preview access

Preview public and cross-account access based on proposed permissions

Validate policies

Validate identity and resource policies against best practice security checks and detect errors

Generate policies

Generate fine-grained IAM policies based on access activity found in AWS CloudTrail

Analyze access continuously

Identify resources with public, cross-account, or cross-organization access in your AWS account and remediate broad access

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Why validate IAM policies in your pipeline?



BUILDERS

Free builders to experiment and innovate quickly – and safely



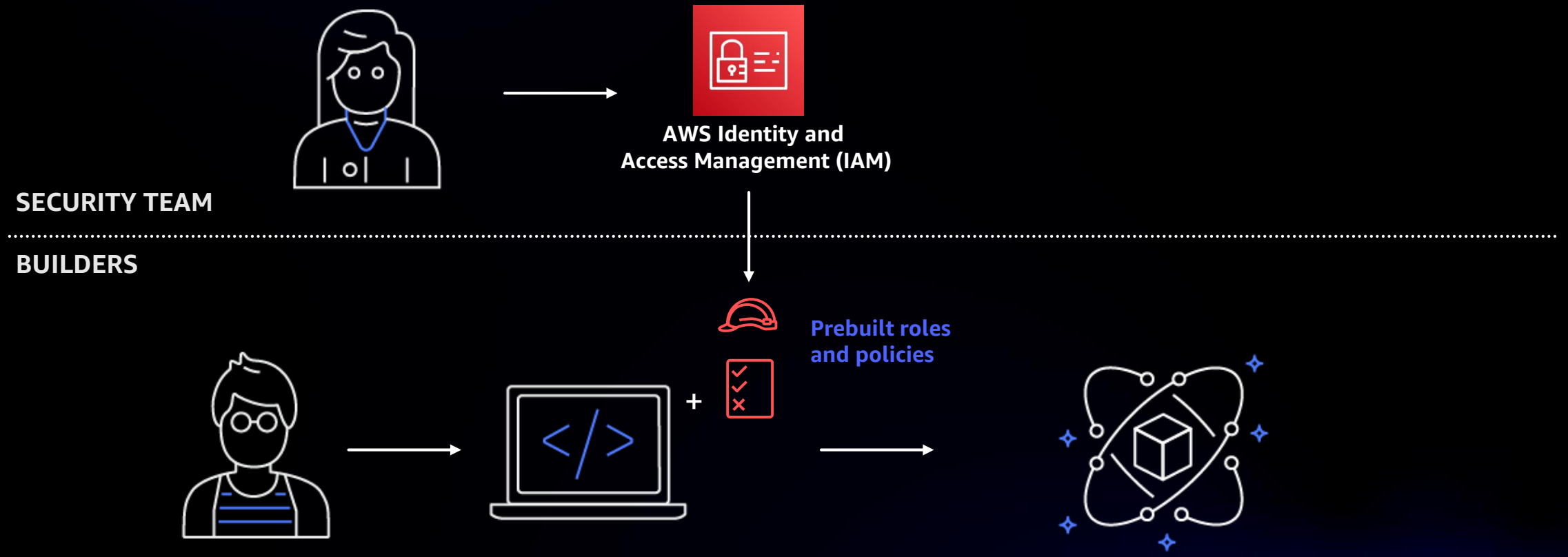
SECURITY TEAM

Free the security team to focus on high-value tasks that enable the business

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Centralized IAM approach

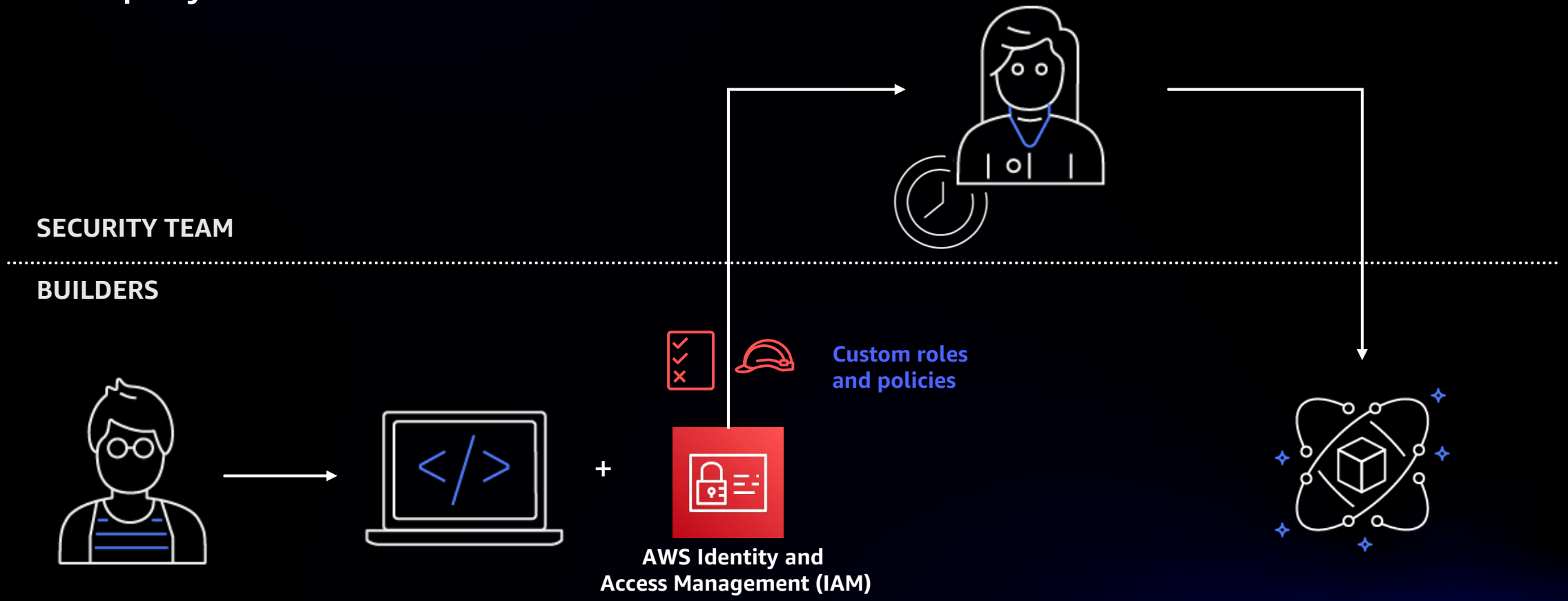
Security team creates and deploys all IAM roles/policies; builders have no access to IAM



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Gated IAM approach

Builders codify the IAM roles and policies, but need the security team to approve and deploy



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Automated policy validation approach

Builders codify the IAM roles/policies; the security team uses automated policy validation to perform many of the security checks that were previously manual



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Automated policy validation approach

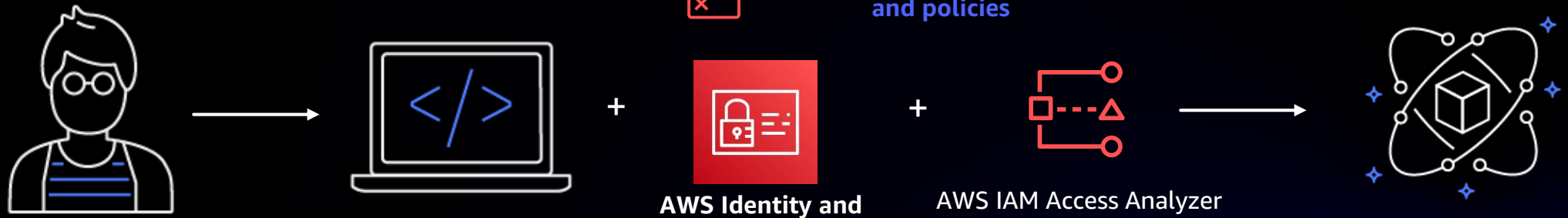
Builders codify the IAM roles/policies; the security team uses automated policy validation to perform many of the security checks that were previously manual



More time to manage additional guardrails and controls

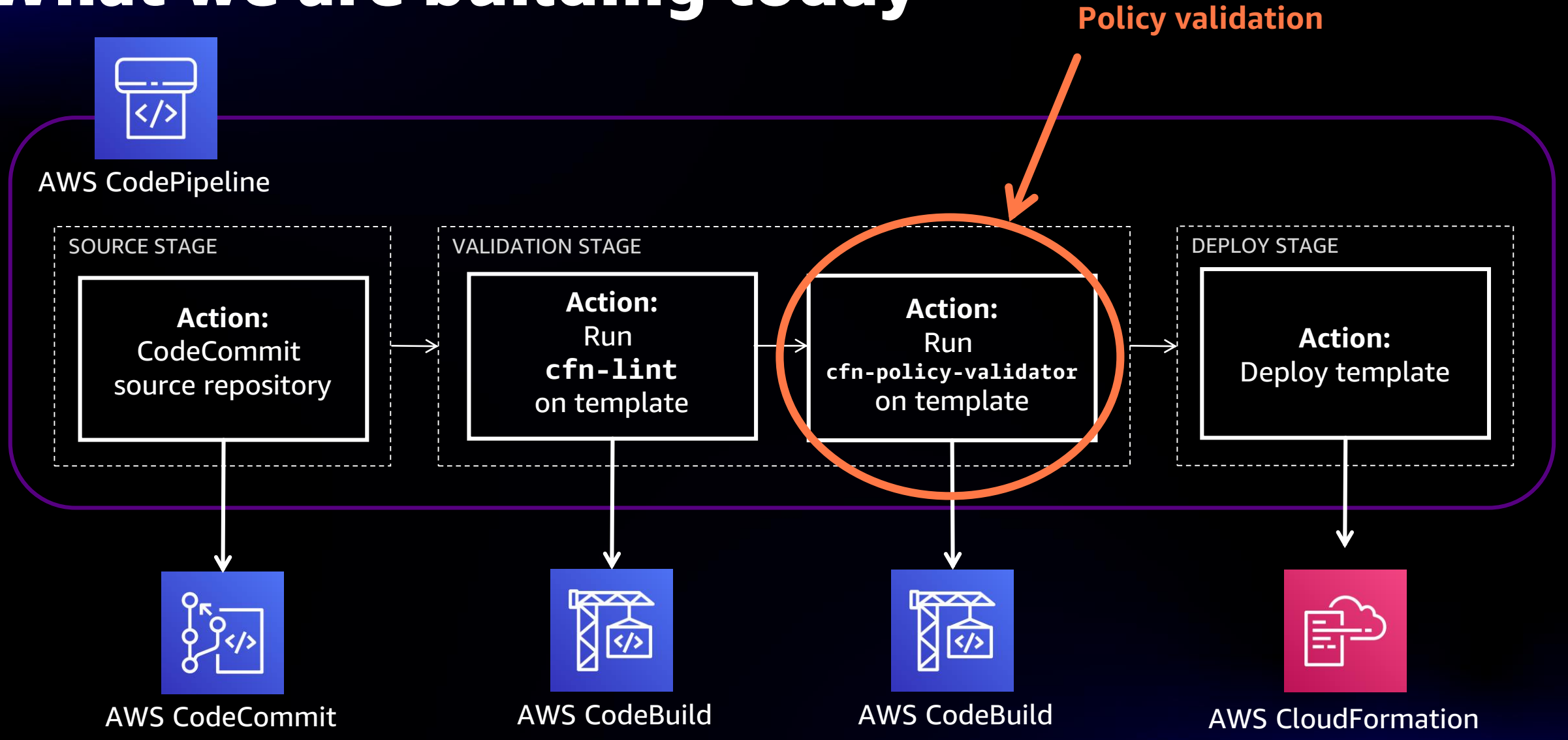
SECURITY TEAM

BUILDERS



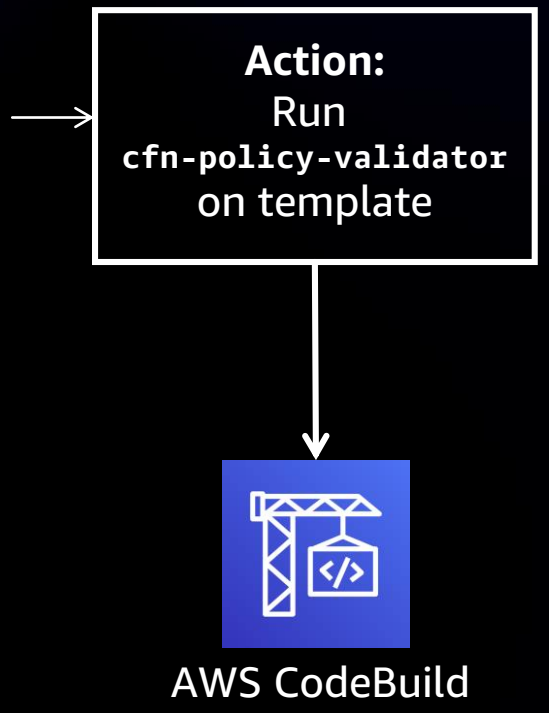
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What we are building today



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IAM Policy Validator for AWS CloudFormation



`cfn-policy-validator:` parses resource-based and identity-based IAM policies from your CloudFormation template and runs the policies through IAM Access Analyzer checks

- Runs in CI/CD pipelines that deploy CloudFormation templates
- Prevents deployments with IAM Access Analyzer findings
- Parses templates and evaluates intrinsic functions (for example, Fn::Sub or Ref) that IAM Access Analyzer can't read ← **today's challenge**

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Let’s build!

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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.

Team or Event Hash (e.g. abcd-0123456789-ef)

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

✓ Invalid Hash

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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.

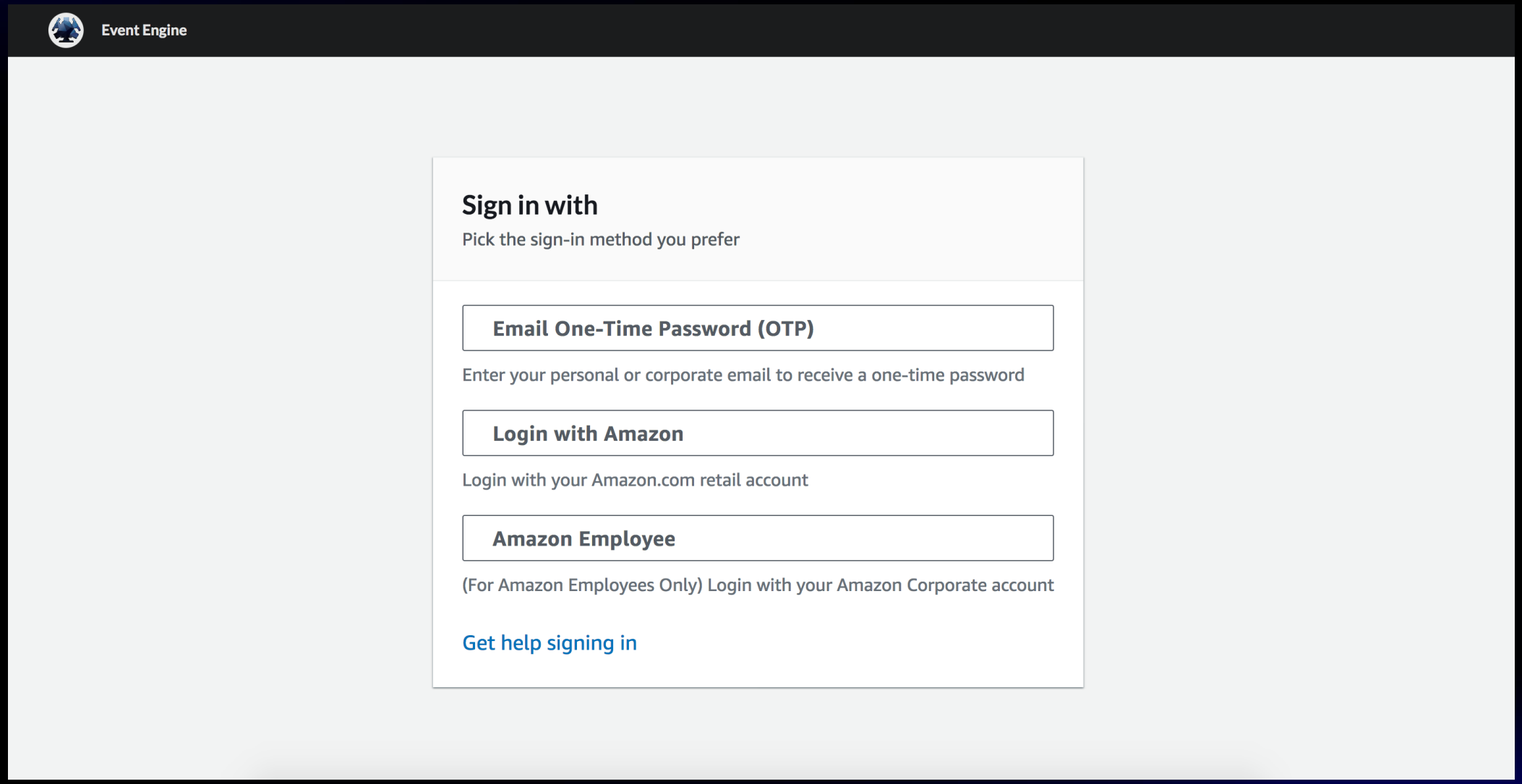
abcd-0345-df

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

✓ Accept Terms & Login

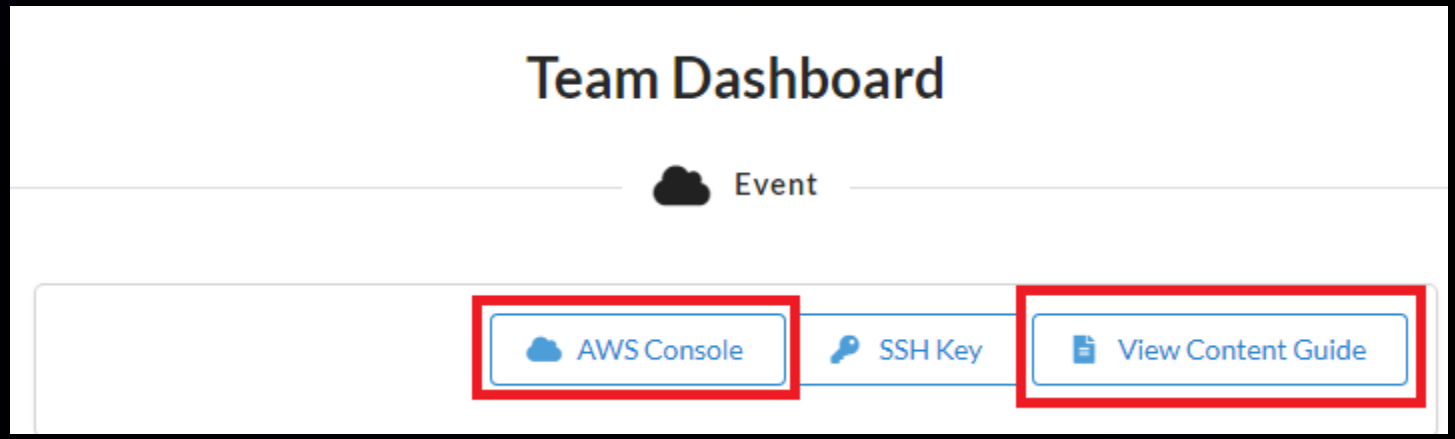
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Visit dashboard.eventengine.run



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Visit dashboard.eventengine.run



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Visit dashboard.eventengine.run

Event Hash:

d0f2-189c89b514-24

https://github.com/awslabs/aws-cloudformation-iam-policy-validator

https://github.com/aws-samples/aws-iam-access-analyzer-samples

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Katie Williams

Victor Feinman

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.