aws INNOVATE

MODERN APPLICATIONS EDITION

20 October, 2022

aws

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

Elevate your security posture for modern applications

Michael Stringer

Principal Security Solutions Architect
Amazon Web Services

aws

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

Agenda

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

Agenda

- What is modern application development

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

Agenda

- What is modern application development
- Know your responsibilities

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

Agenda

- What is modern application development
- Know your responsibilities
- How to approach your security considerations

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

Agenda

- What is modern application development
- Know your responsibilities
- How to approach your security considerations
- Embed that knowledge for future workloads

aws

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

Agenda

- What is modern application development
- Know your responsibilities
- How to approach your security considerations
- Embed that knowledge for future workloads
- Modern security operations

aws

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

What is modern application development?

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

Modern Applications

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

Modern Applications

Modular services

1

Architectural patterns

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

Modern Applications

Modular services

As serverless as possible

1

Architectural patterns

2

Operational model

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

Modern Applications

Modular services

As serverless as possible

Automated, Abstracted & Standardized

1

Architectural patterns

2

Operational model

3

Developer Agility

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

Modern Applications

Modular services

As serverless as possible

Automated, Abstracted & Standardized

Programmatic Guardrails

1 Architectural patterns

2 Operational model

3 Developer Agility

4 Management & Governance

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

Modern Applications

Modular services	As serverless as possible	Automated, Abstracted & Standardized	Programmatic Guardrails	Decoupled & Purpose built
↑	↑	↑	↑	↑
1	2	3	4	5
Architectural patterns	Operational model	Developer Agility	Management & Governance	Data management

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

Modernization changes how you work

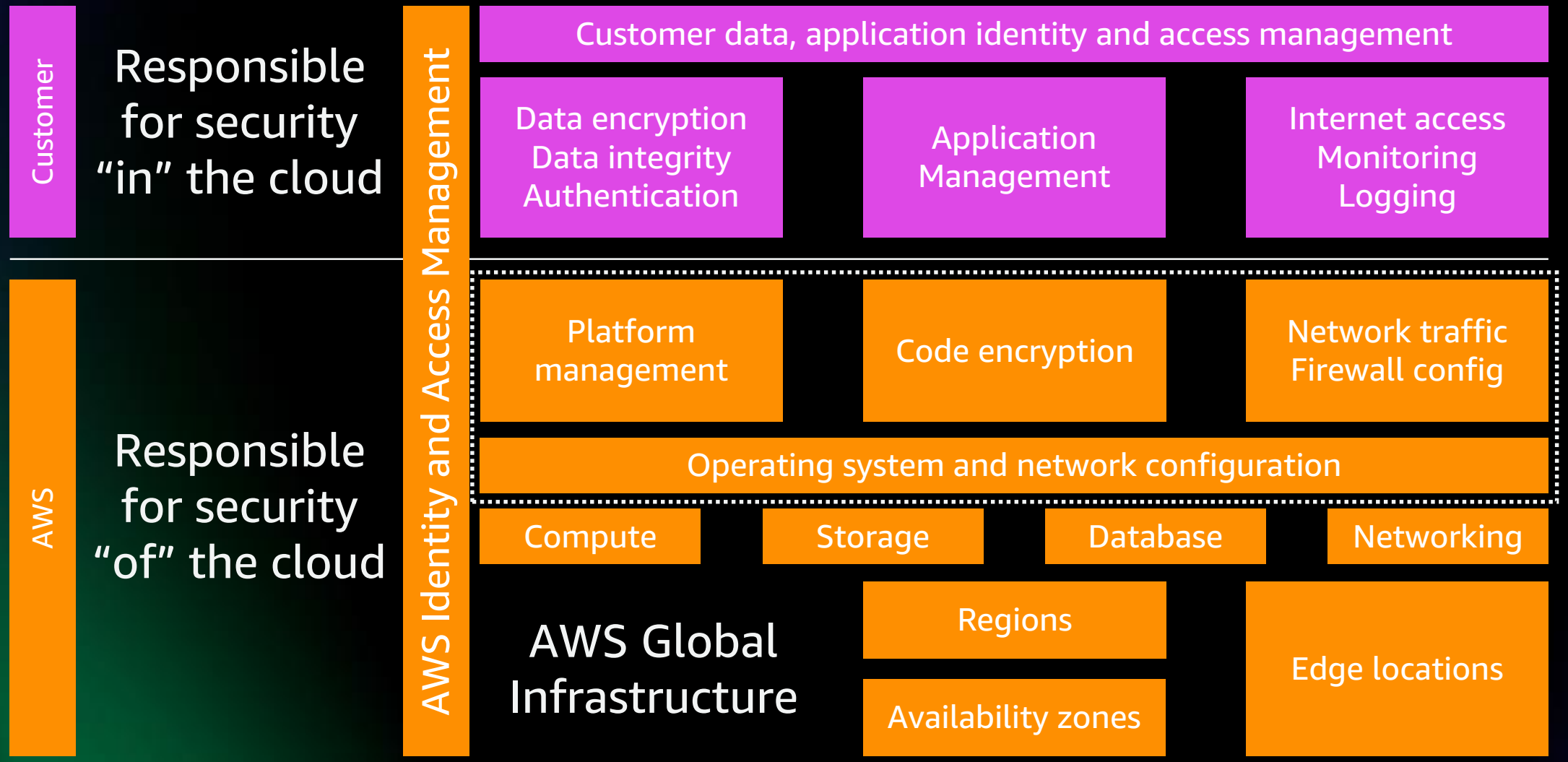
Builders	Operators
Start from scratch Goal is innovation	Deploy, debug, & monitor Goal is low risk & high reliability/availability

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

Know your responsibility

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

AWS Shared Responsibility Model



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

AWS Shared Responsibility Model

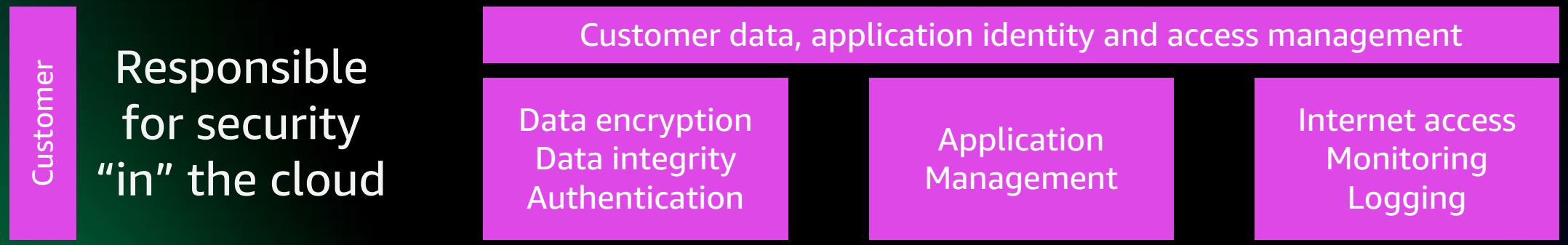
AWS assumes responsibility for these serverless applications components

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

AWS Shared Responsibility Model

Security is not “effortless” with serverless. It still takes work!

- Application layer security
- Authentication and authorization
- Data encryption and integrity
- Observability

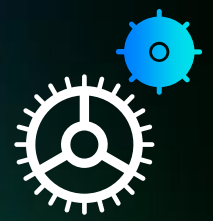


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Approaching your security considerations

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

AWS Well-Architected Framework



Operational Excellence

Security

Reliability

Performance Efficiency

Cost Optimization

Sustainability

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

AWS Well-Architected Framework

Security

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

AWS Well-Architected Framework

Security

How to be secure

Best Practice Areas

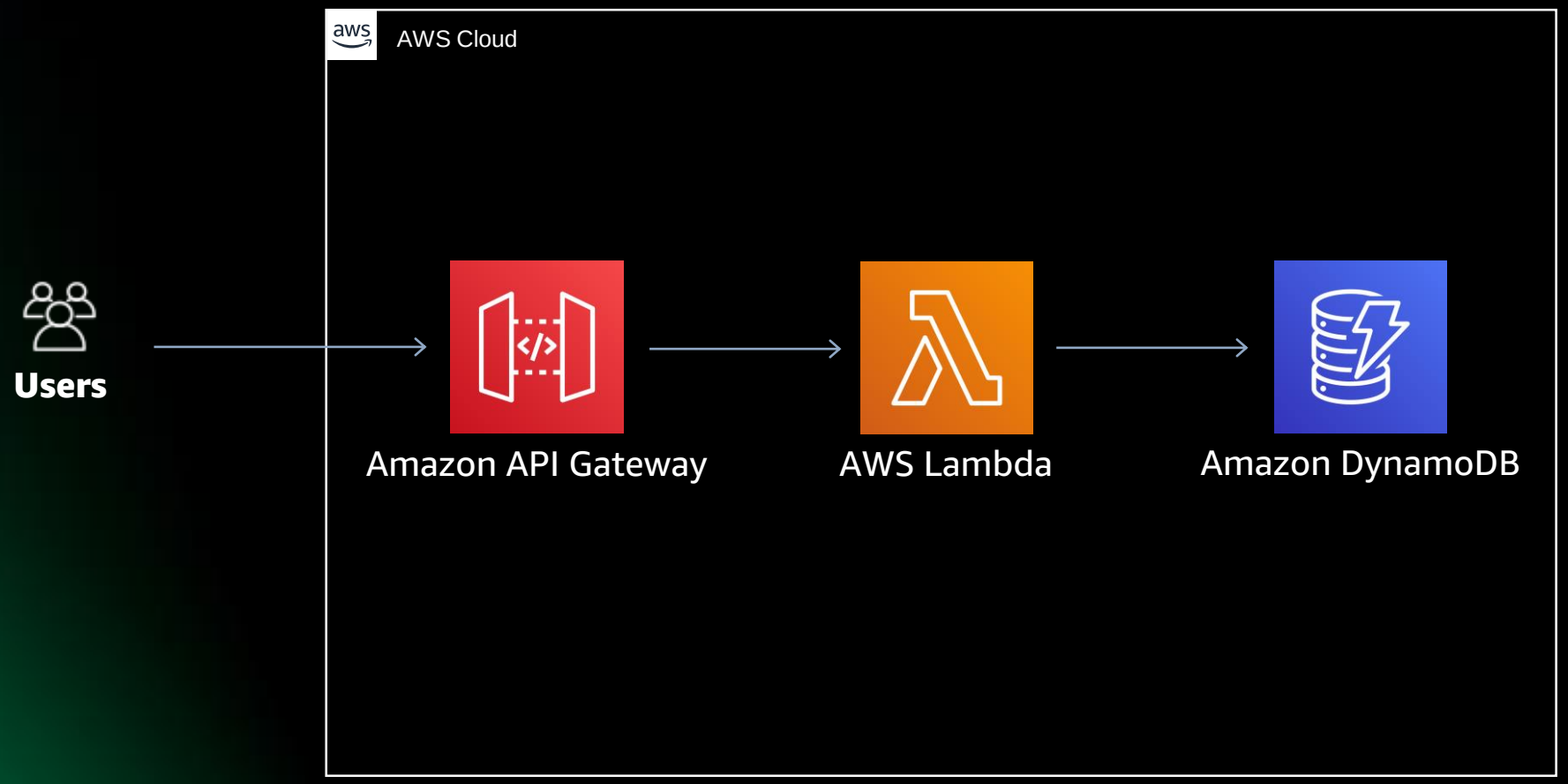
- Identity and access management
- Detection
- Infrastructure protection
- Data protection
- Incident response

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

Sample Modern Application

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

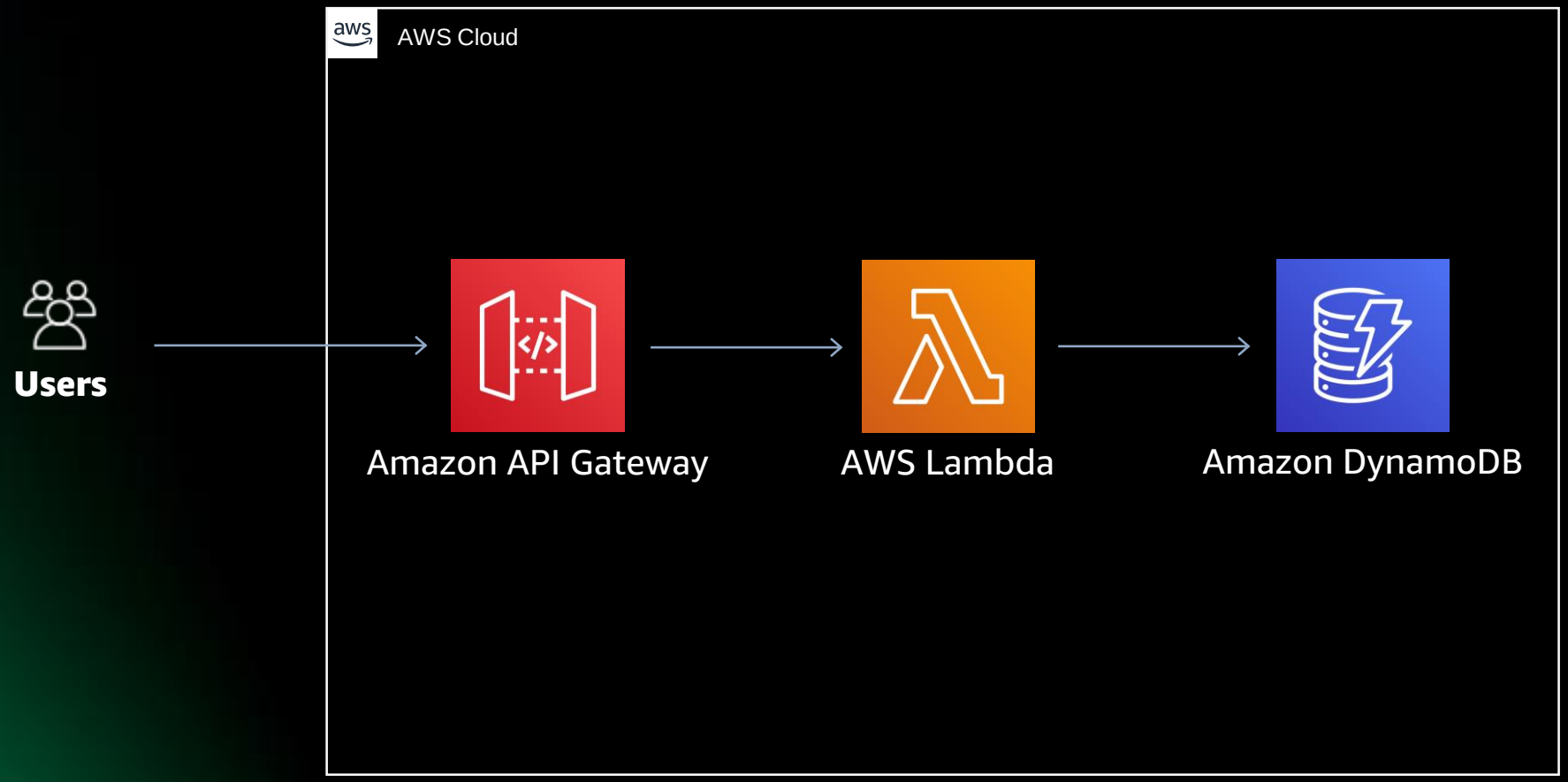
Sample modern application



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

Sample modern application

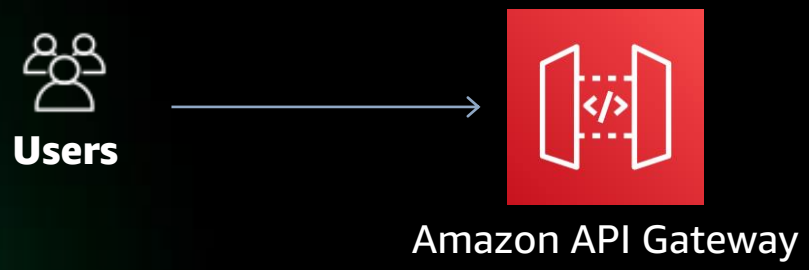
Identity and access management



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

Sample modern application

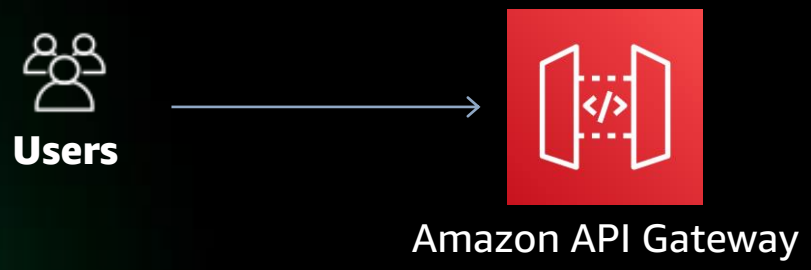
Identity and access management



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

Sample modern application

Identity and access management



Mutual TLS Authentication

IAM permissions

- Use IAM policies and AWS credentials to grant access

Lambda Authorizers

- Use a Lambda function to validate a bearer token, e.g., OAuth or SAML

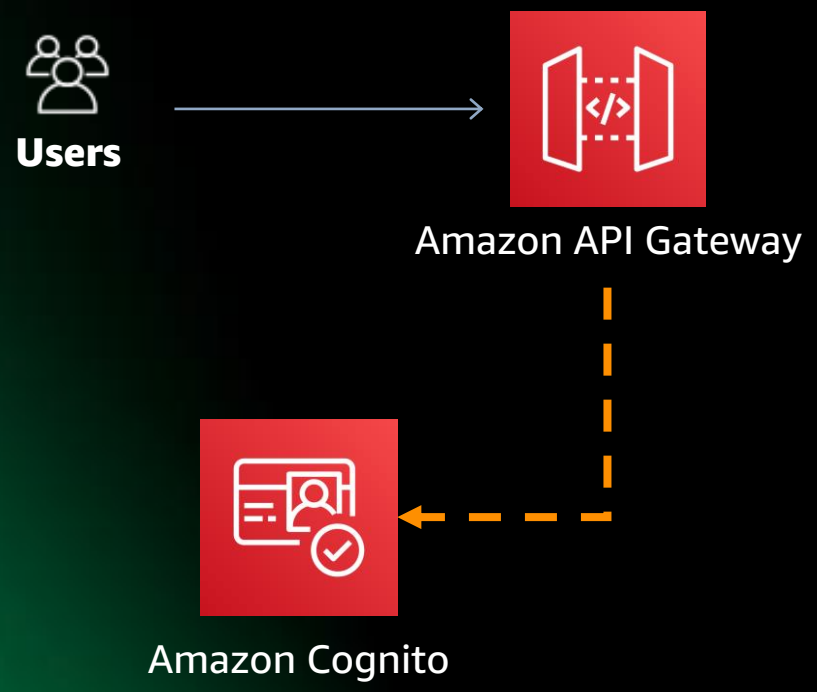
Resource Policies

- Can restrict based on IP, VPC, AWS Account ID

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

Sample modern application

Identity and access management



Mutual TLS Authentication

IAM permissions

- Use IAM policies and AWS credentials to grant access

Lambda Authorizers

- Use a Lambda function to validate a bearer token, e.g., OAuth or SAML

Resource Policies

- Can restrict based on IP, VPC, AWS Account ID

Cognito User Pools

- Create a completely managed user management system

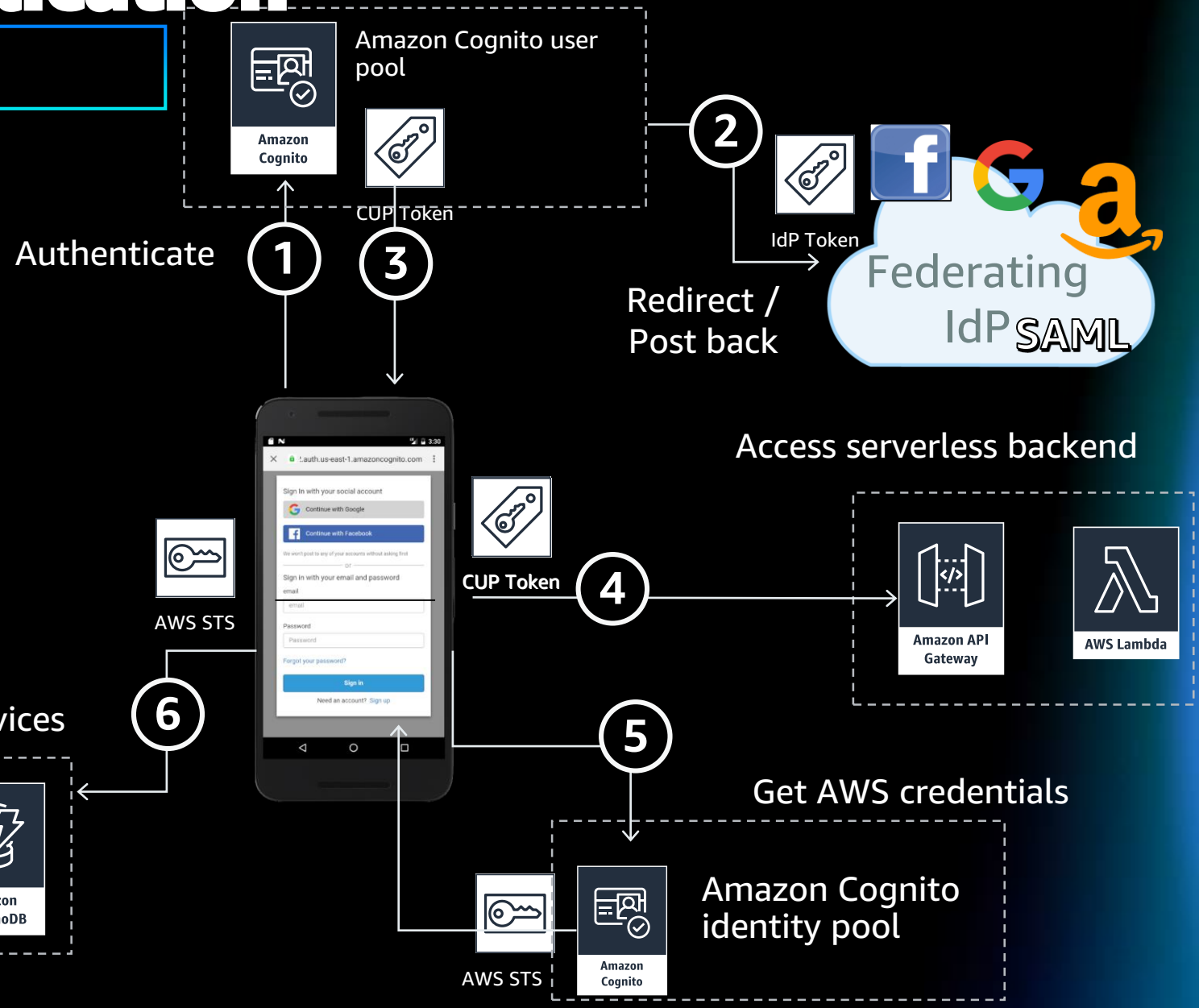
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sample modern application

Identity and access management

Amazon Cognito

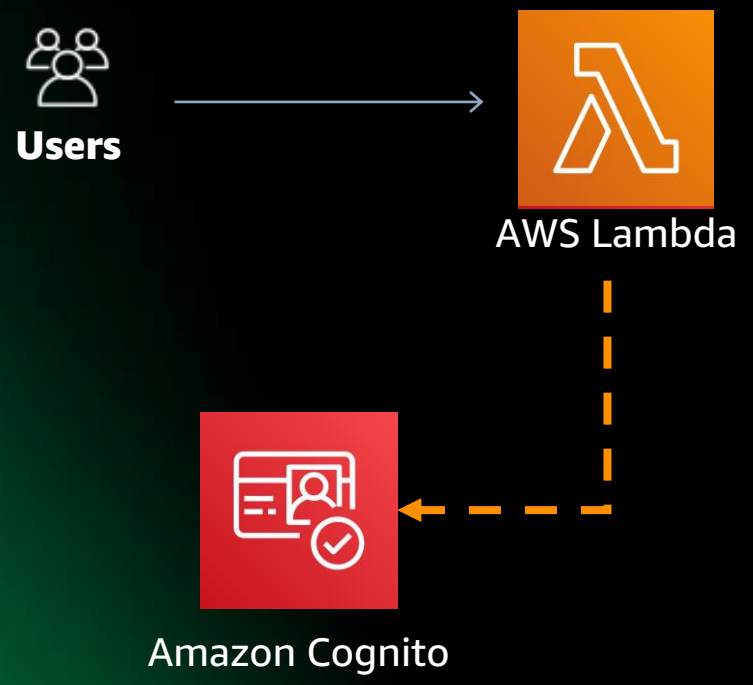
- User pools authenticate users and returns standard tokens
- User pool tokens are used to access backend resources
- Identity pools provide AWS credentials to access AWS services



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

Sample modern application

Identity and access management



Mutual TLS Authentication

IAM permissions

- Use IAM policies and AWS credentials to grant access

Lambda Authorizers

- Use a Lambda function to validate a bearer token, e.g., OAuth or SAML

Resource Policies

- Can restrict based on IP, VPC, AWS Account ID

Cognito User Pools

- Create a completely managed user management system

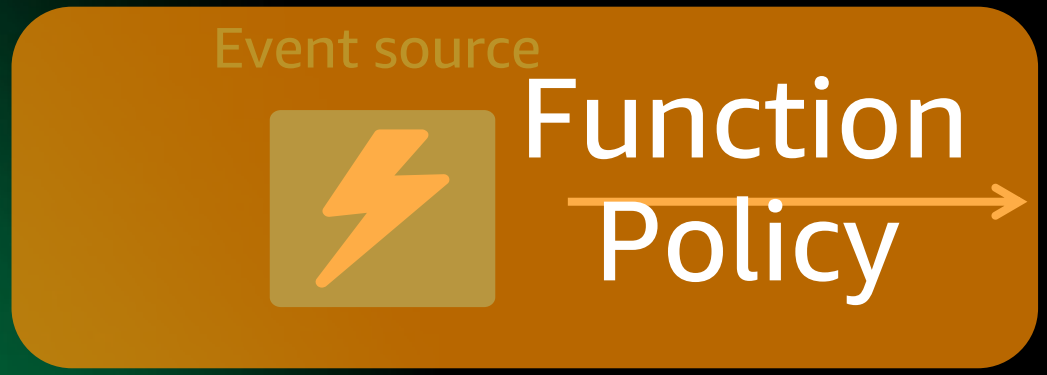
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sample modern application

Identity and access management

Function policies:

- "Actions on bucket X can invoke Lambda function Z"
- Resource policies allow for cross account access
- Used for sync and async invocations



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

Sample modern application

Identity and access management

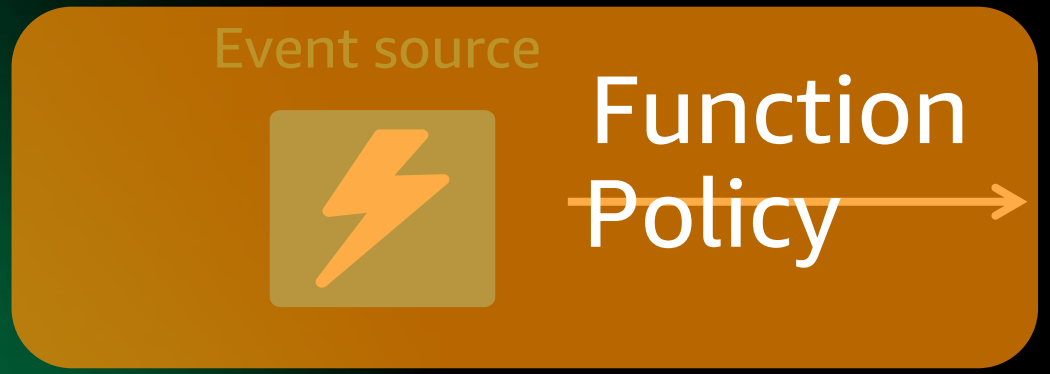
Function policies:

- "Actions on bucket X can invoke Lambda function Z"
- Resource policies allow for cross account access
- Used for sync and async invocations

AWS Lambda

Execution role:

- "Lambda function A can read from DynamoDB table users"
- Define what AWS resources/API calls can this function access via IAM
- Used in streaming invocations



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

Sample modern application

Identity and access management

Amazon DynamoDB

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

Sample modern application

Identity and access management

Amazon DynamoDB

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "dynamodb:*"
      ],
      "Resource": "*"
    }
  ]
}
```

Allow or deny?

What can (or can't) you do?

What can (or can't) you do it to?

Translation: Allowed to take all Amazon DynamoDB actions

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

Sample modern application

Identity and access management

Amazon DynamoDB

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "dynamodb:GetItem",
        "dynamodb:PutItem"
      ],
      "Resource": "*"
    }
  ]
}
```

Translation: Allowed to read and write individual items in DynamoDB

aws

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

Sample modern application

Identity and access management

Amazon DynamoDB

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "dynamodb:GetItem",
        "dynamodb:PutItem"
      ],
      "Resource": [
        "arn:aws:dynamodb:ap-southeast-2:111122223333:table/MyTableName"
      ]...
```

Translation: Allowed to take specific DynamoDB actions on a specific table

This is an Amazon Resource Name (ARN).
All AWS services use them, and they follow this format.

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

Sample modern application

Identity and access management

Service-by-service authorization details

Amazon DynamoDB

aws

English

- DataSync
- AWS DeepLens
- AWS Device Farm
- AWS Direct Connect
- AWS Directory Service
- Amazon DynamoDB
- Amazon DynamoDB Accelerator (DAX)
- Amazon EC2
- Amazon EC2 Auto Scaling
- AWS Elastic Beanstalk

AWS Documentation » AWS Identity and Access Management » User Guide » Reference Information for AWS Identity and Access Management » IAM JSON Policy Reference » Actions, Resources, and Condition Keys for AWS Services

Actions, Resources, and Condition Keys for AWS Services

Each AWS service can define actions, resources, and condition context keys for use in IAM policies. This topic describes how the elements provided for each service are documented.

Instructions for how to read the table for each service

How to Read the Tables

Each topic consists of tables that provide the list of available actions, resources, and condition keys.

The Actions Table

The **Actions** table lists all the actions that you can use in an IAM policy statement's `Action` element. Not all API operations that are defined by a service can be used as an action in an IAM policy. In addition, a service might define some actions that don't directly correspond to an API

aws

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

Sample modern application

Identity and access management

Amazon DynamoDB

GetItem	The GetItem operation returns a set of attributes for the item with the given primary key	Read	table*	dynamodb:Attributes dynamodb:EnclosingOpe dynamodb:LeadingKeys dynamodb:ReturnConsu dynamodb:Select

Action

Resource

table	arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}

"arn:aws:dynamodb:ap-southeast-2:111122223333:table/MyTableName"

Resource ARN format

aws

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

Sample modern application compliance

- Compliance-ready for SOC, PCI, IRAP, HIPAA, and others

Service	SOC	PCI	ISO	IRAP	HIPAA
Amazon API Gateway	✓	✓	✓	✓	✓
AWS Lambda	✓	✓	✓	✓	✓
Amazon DynamoDB	✓	✓	✓	✓	✓
Amazon Cognito	✓	✓	✓	✓	✓

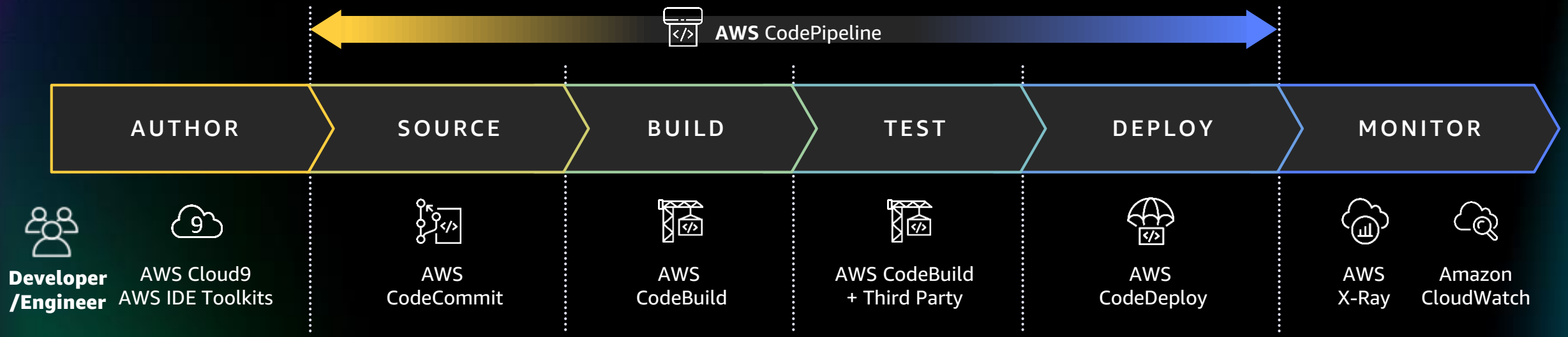
Learn more at https://aws.amazon.com/compliance/services-in-scope/

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

Embed your knowledge (DevSecOps)

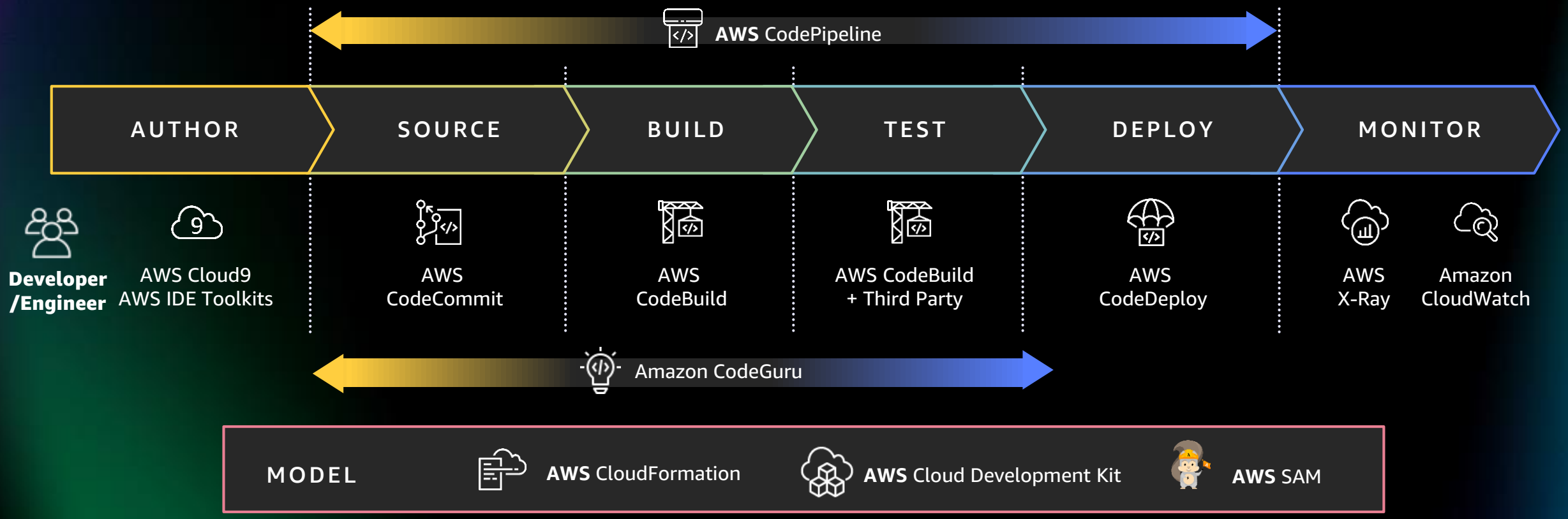
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Developer Tools for modern software delivery



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

AWS Developer Tools for modern software delivery



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

Amazon CodeGuru in your software workflow

Amazon CodeGuru Reviewer

Amazon CodeGuru Profiler

Built-in code reviews with actionable recommendations

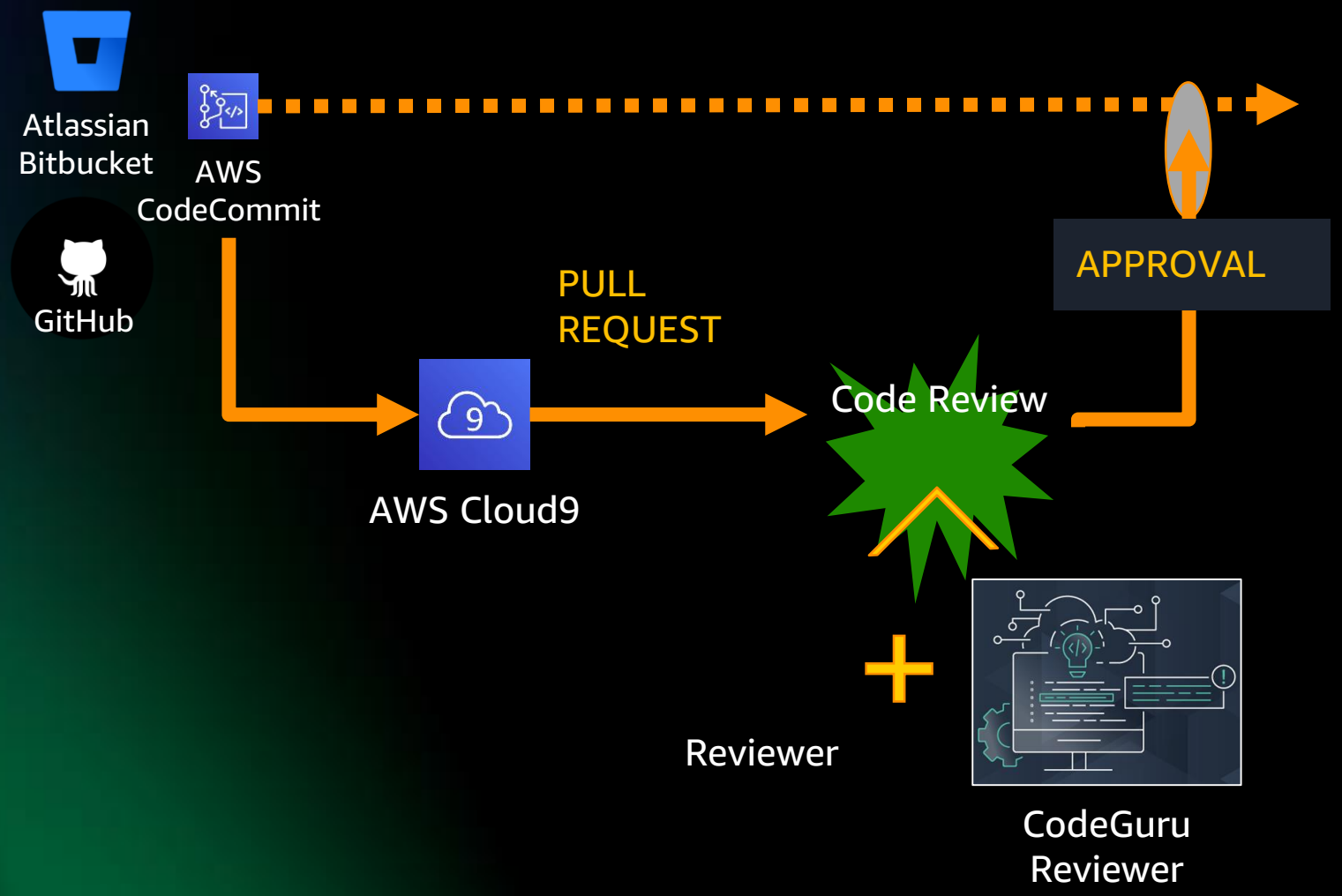
Detect and optimise the expensive lines of code

Easily identify performance and cost improvements in production environment

aws

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

Code review with Amazon CodeGuru Reviewer



- AWS API security best practices
- Java crypto library best practices
- Secure web applications
- AWS security best practices

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

Examples of Amazon CodeGuru Security findings

```
import com.amazonaws.auth.AWSCredentials;
import com.amazonaws.auth.BasicAWSCredentials;

static String myKeyId ="AKIAX742FUDUQXXXXXXX";
static String mySecretKey = "MySecretKey";

public static void main(String[] args) {
            AWSCredentials creds = getCreds(myKeyId,
mySecretKey);
}

static AWSCredentials getCreds(String id, String key) {
return new BasicAWSCredentials(id, key);
}
```

Main.java Line: 50 Security

Your code uses hardcoded AWS credentials which might allow unauthorized users access to your AWS account. These attacks can occur a long time after the credentials are removed from the code. We recommend that you set AWS credentials with environment variables or an AWS profile instead. You should consider deleting the affected account or rotating the secret key and then scanning Amazon CloudWatch for unexpected activity. Learn more.

Relevant Locations:

- src/main/java/Main.java, line: 50
  - src/main/java/Main.java, line: 25 (The constant value)
  - src/main/java/Main.java, line: 24 (The constant value)

Was this helpful?

```
import javax.servlet.http.Cookie;

public static void createCookie() {
            Cookie cookie = new Cookie("name",
"value");
}
```

Main.java Line: 88 Security

We detected the use of cookies which are not secure. Insecure cookie vulnerabilities might leak session IDs and other sensitive information. Learn more. To increase the security of your code, call `setSecure(true)` after you create a cookie to make it transmittable only through secure channels.

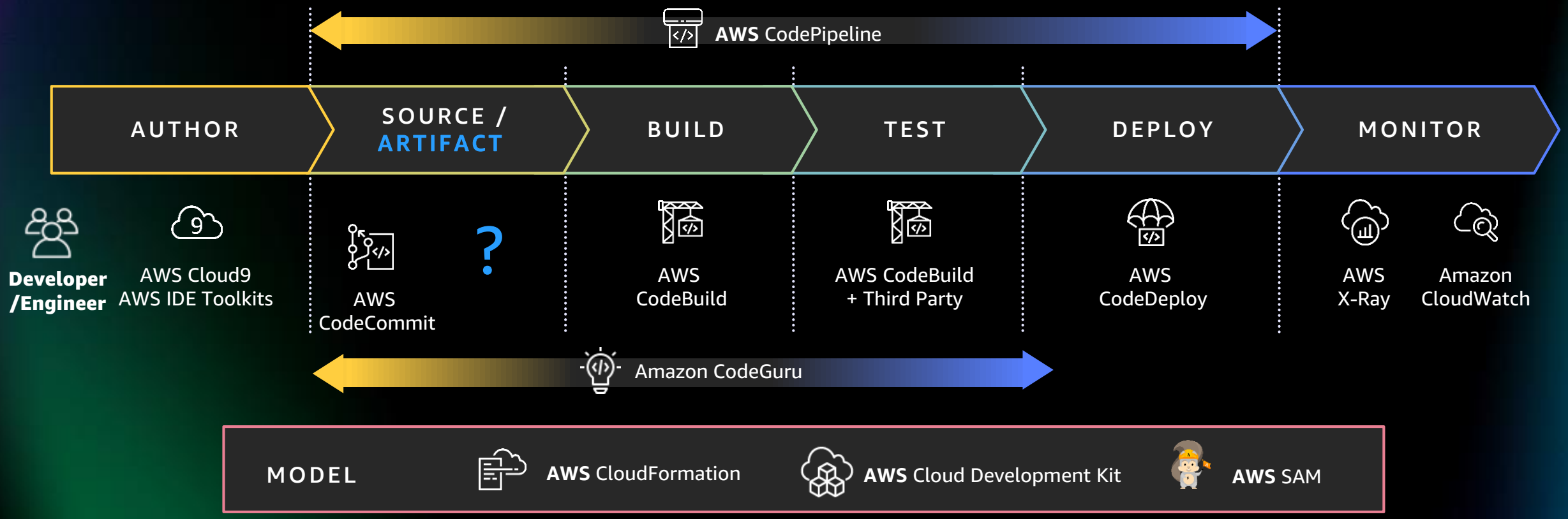
Relevant Locations:

- src/main/java/Main.java, line: 87
- src/main/java/Main.java, line: 88

Was this helpful?

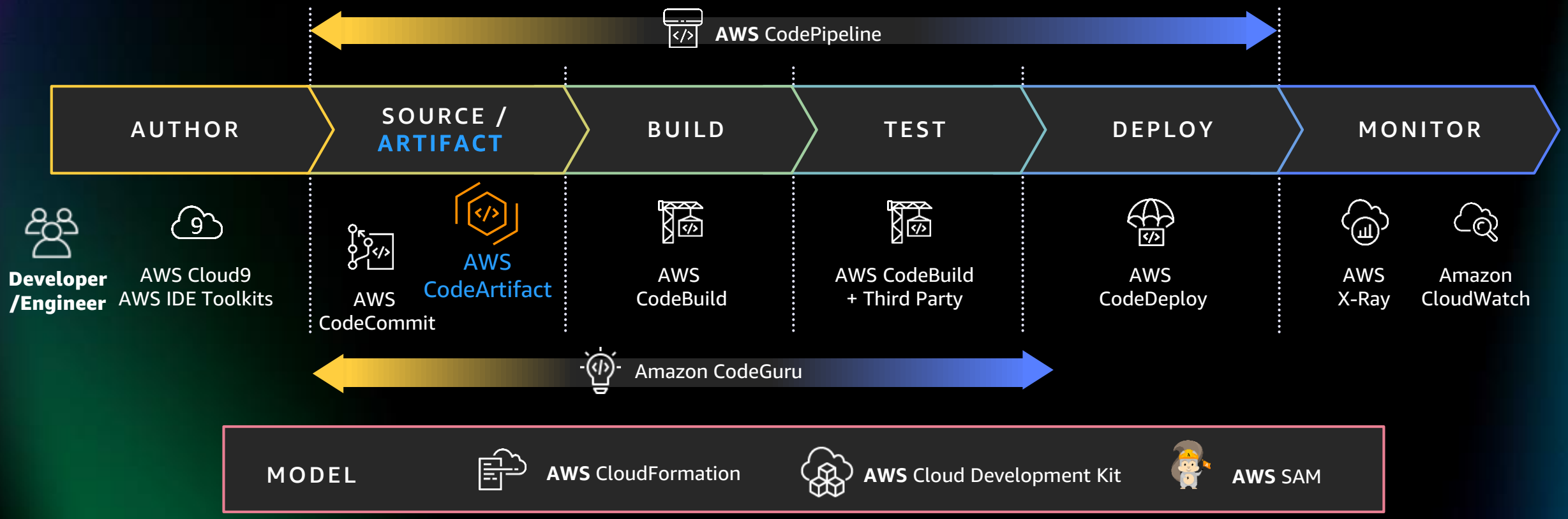
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Developer Tools for modern software delivery



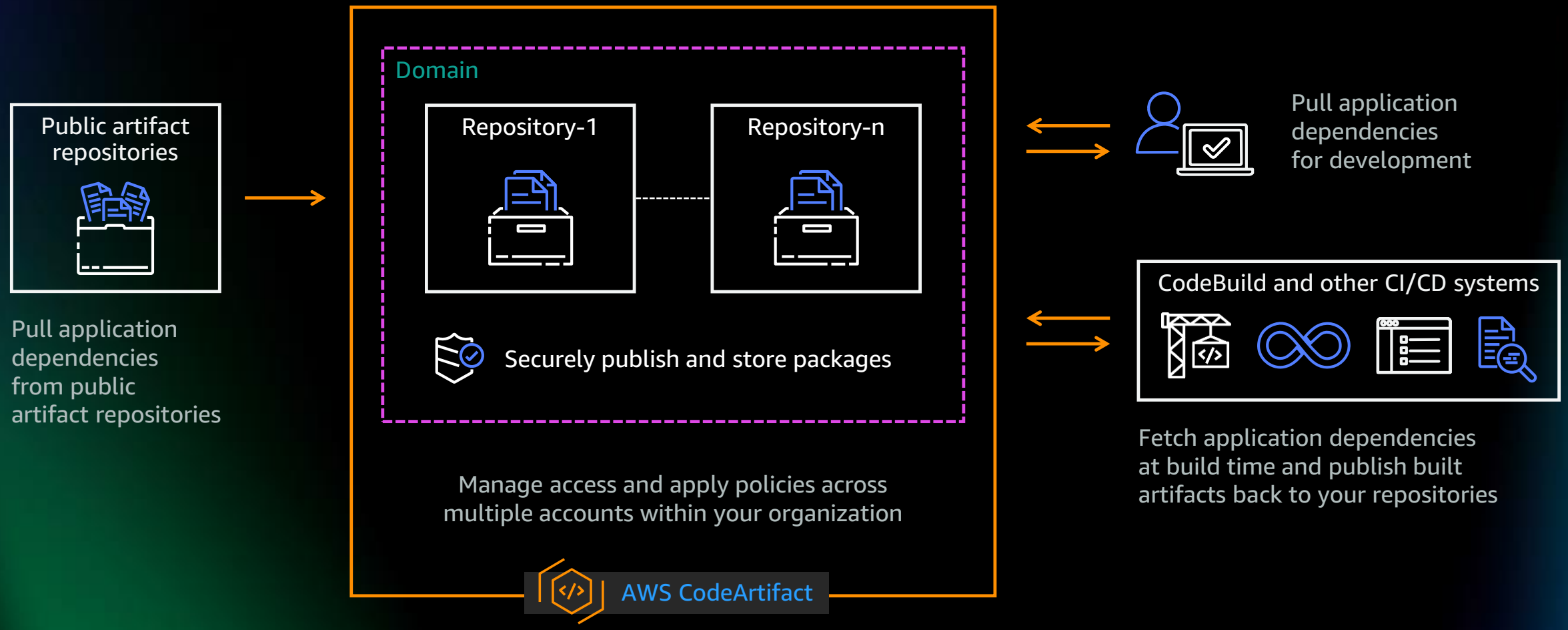
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Developer Tools for modern software delivery



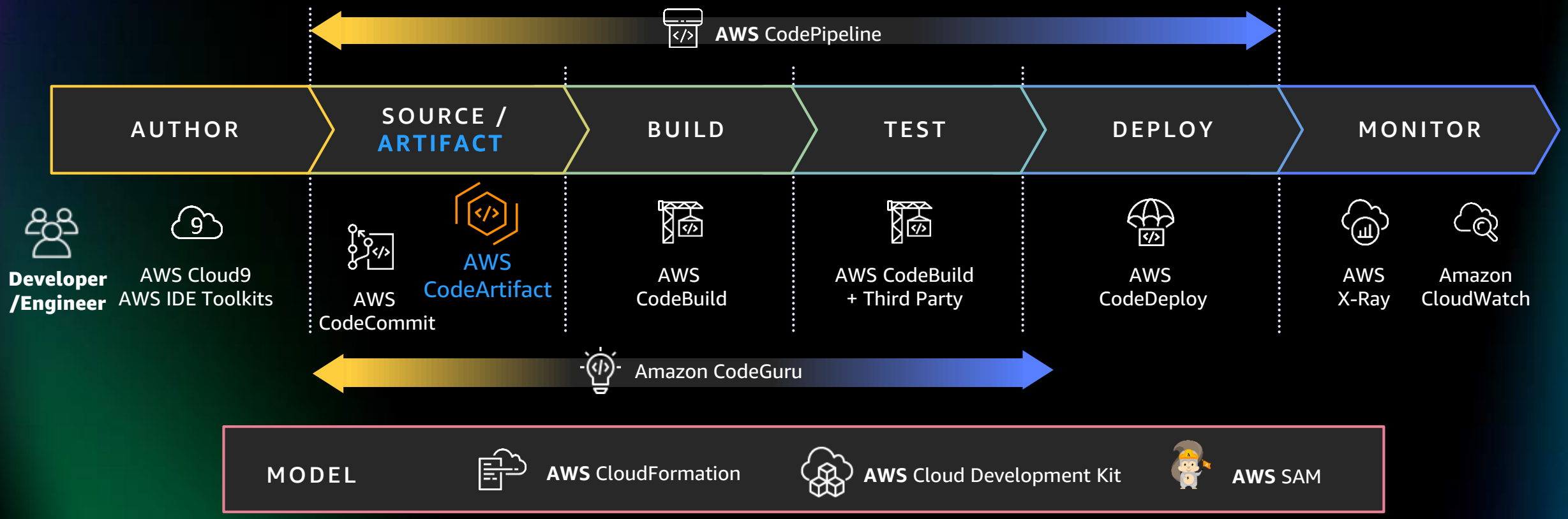
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS CodeArtifact overview



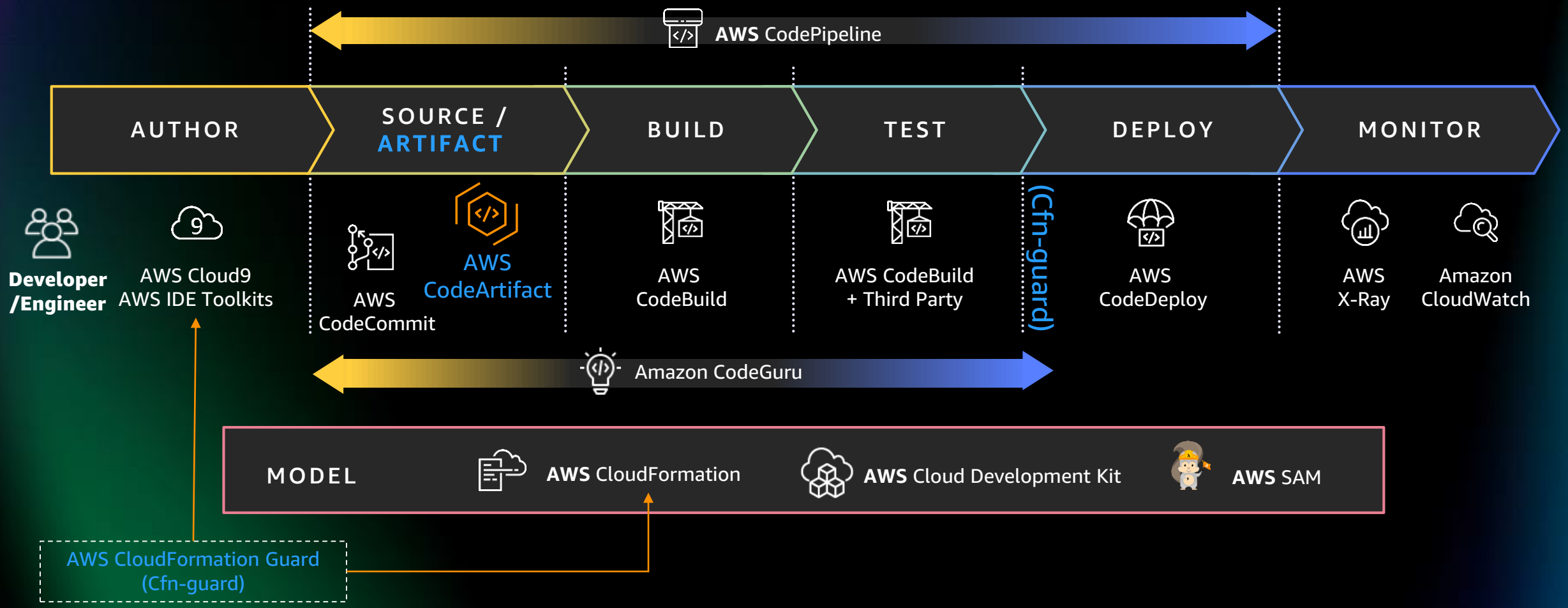
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Developer Tools for modern software delivery



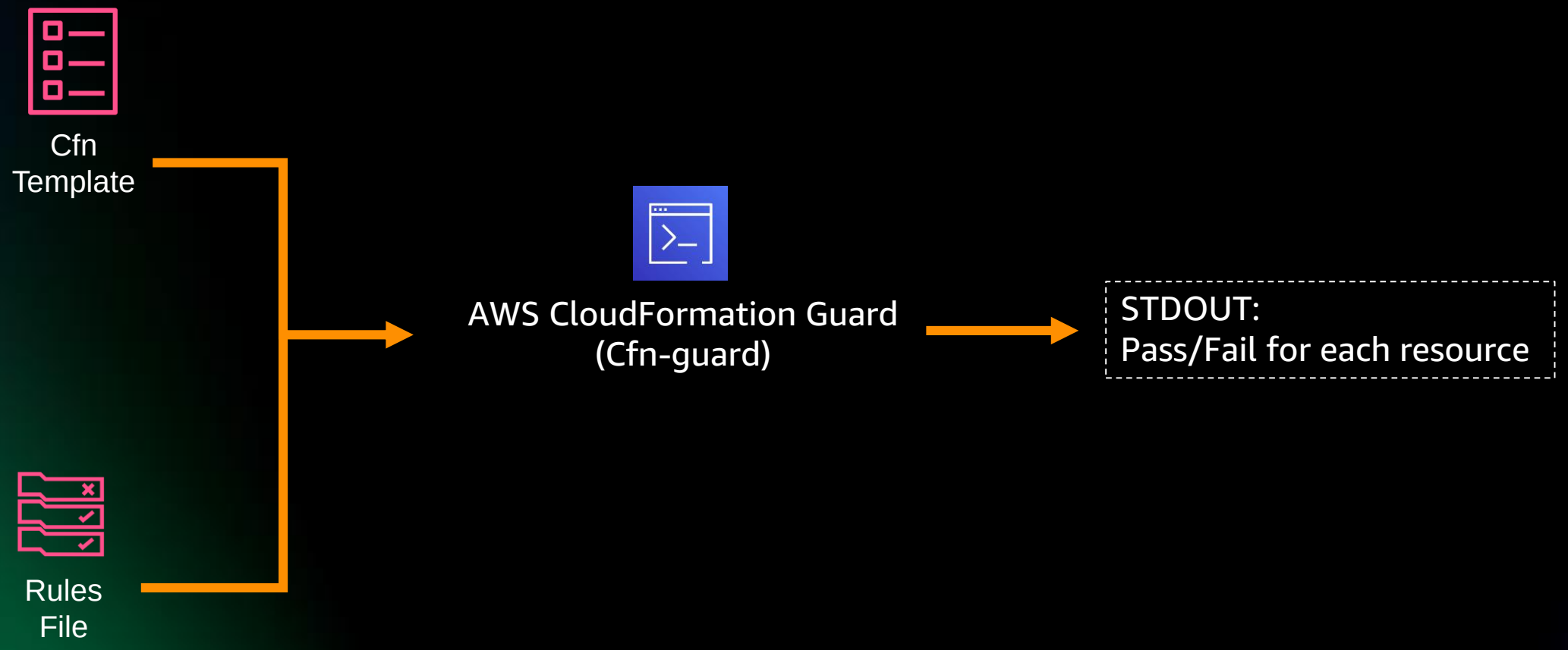
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Developer Tools for modern software delivery



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

AWS CloudFormation Guard workflow



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

Example

- CloudFormation template

```
{
    "Resources": {
        "NewVolume" : {
            "Type" : "AWS::EC2::Volume",
            "Properties" : {
                "Size" : 500,
                "Encrypted": false,
                "AvailabilityZone" : "us-west-2b"
            }
        },
```

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

Example

- CloudFormation template

```
{
    "Resources": {
        "NewVolume" : {
            "Type" : "AWS::EC2::Volume",
            "Properties" : {
                "Size" : 500,
                "Encrypted": false,
                "AvailabilityZone" : "us-west-2b"
            }
        },
```

- Cfn-guard rules file

```
let encryption_flag = true

AWS::EC2::Volume Encrypted == %encryption_flag
AWS::EC2::Volume Size <= 100
```

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

Example

- CloudFormation template

```
{
    "Resources": {
        "NewVolume" : {
            "Type" : "AWS::EC2::Volume",
            "Properties" : {
                "Size" : 500,
                "Encrypted": false,
                "AvailabilityZone" : "us-west-2b"
            }
        },
```

- Cfn-guard rules file

```
let encryption_flag = true

AWS::EC2::Volume Encrypted == %encryption_flag
AWS::EC2::Volume Size <= 100
```

- Cfn-guard output

```
$> cfn-guard check -t Examples/ebs_volume_template.json -r Examples/ebs_volume_template.ruleset

[NewVolume2] failed because [Encrypted] is [false] and the permitted value is [true]
[NewVolume] failed because [Encrypted] is [false] and the permitted value is [true]
[NewVolume] failed because [Size] is [500] and the permitted value is [<= 100]
Number of failures: 3
```

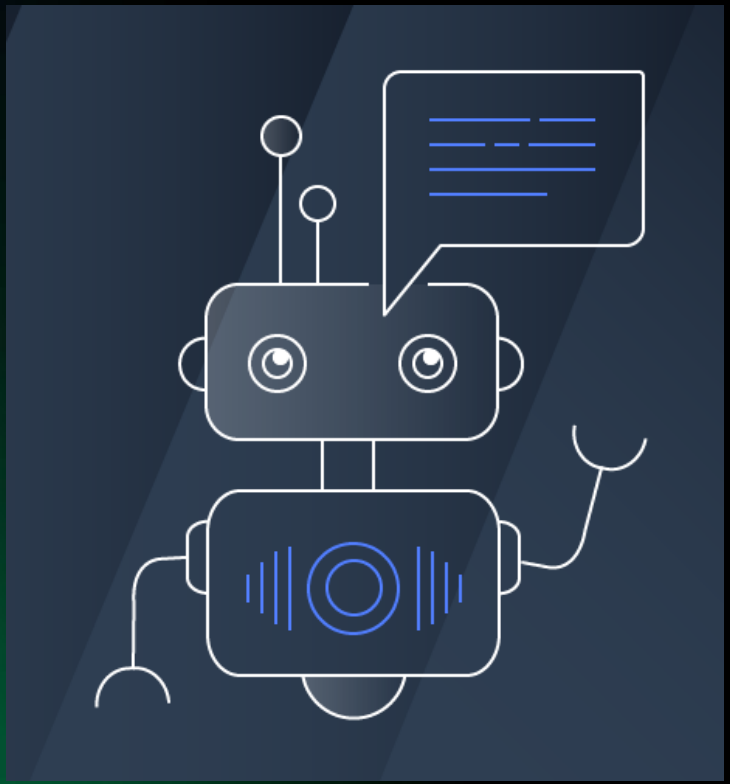
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Modern Security Operations

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

AWS Chatbot: Bring AWS to Slack and Amazon Chime

AWS Chatbot

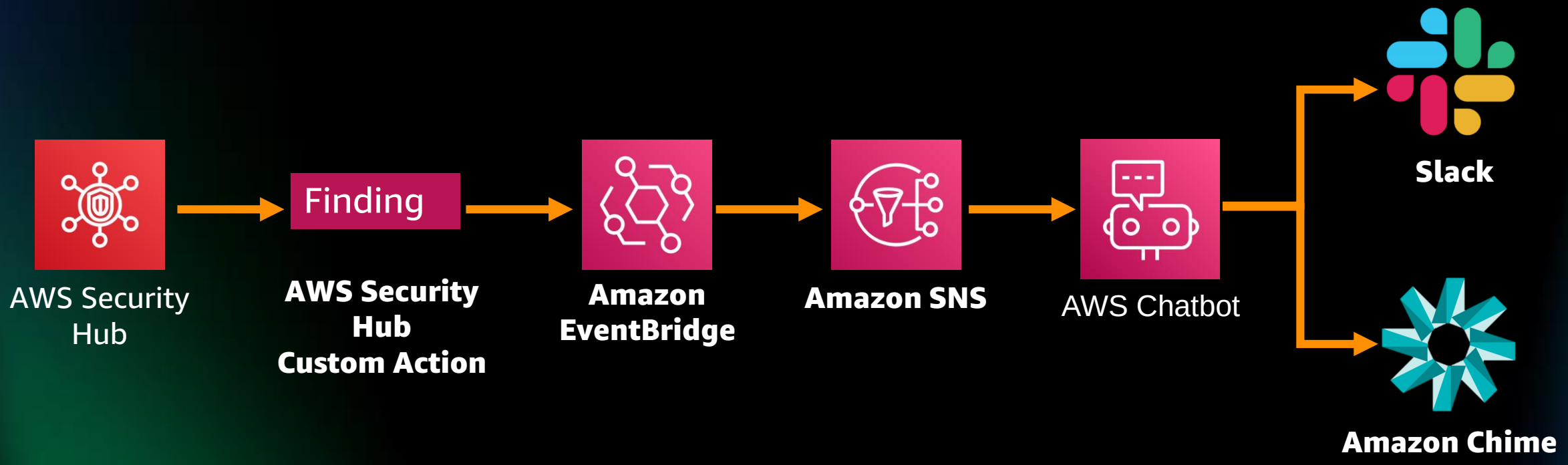


Interactive agent for ChatOps on AWS

- Centralise AWS workflows where work lives
- Get real-time updates & run commands
- Collaborate with your team
- Support for Slack and Chime

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

Enabling AWS Security Hub integration with AWS Chatbot



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

AWS Security Hub PCI notifications

❗ ❗ Security Hub Finding | ap-southeast-2 | Account:

PCI.S3.2 S3 buckets should prohibit public read access

This AWS control checks whether your S3 buckets allow public read access by evaluating the Block Public Access settings, the bucket policy, and the bucket access control list (ACL).

Finding Type: Effects/Data Exposure/PCI-DSS

First Seen	Last Seen
Thu, 3 Sep 2020 07:16:56 GMT	Thu, 3 Sep 2020 19:22:57 GMT
Affected Resource	**Severity**
AWS::::Account:	Critical

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

AWS Security Hub Codebuild notifications

❗ ❗ **Security Hub Finding | ap-southeast-2 | Account:**

CodeBuild.2 CodeBuild project environment variables should not contain clear text credentials

This AWS control checks whether the project contains environment variables AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY.

Finding Type: Software and Configuration Checks/Industry and Regulatory Standards/AWS-Foundational-Security-Best-Practices

First Seen	Last Seen
Thu, 3 Sep 2020 07:12:09 GMT	Thu, 3 Sep 2020 19:23:07 GMT
Affected Resource	**Severity**
AWS::::Account:	Critical

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

Let’s recap

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

Resource Links

AWS Shared Responsibility Model

AWS Well-Architected Framework

Enabling AWS Security Hub integration with AWS Chatbot

AWS Serverless Security Workshop

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

Visit the Modern Applications resource hub

Dive deeper with these resources to help you develop an effective plan for your modernisation journey.

- Build modern applications on AWS
- Business value of cloud modernisation
- An introduction to event-driven architectures
- Accelerate full-stack web and mobile app development
- Determining the total cost of ownership: Comparing serverless and server-based technologies
- Building event-driven architectures with AWS
- Continuous learning, continuous modernisation

https://tinyurl.com/modern-apps-aws

Visit resource hub

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

AWS Training and Certification

Get started with Free Digital Training for you and your team today

Achieve key milestones and plan your next steps with the AWS Modern Application skills training

Access 500+ free digital courses with
AWS Skill Builder

Earn an industry-recognised credential:
AWS Certified Developer – Associate
AWS Certified DevOps – Professional

Create a self-paced learning roadmap
AWS ramp-up guide - Developer
AWS ramp-up guide - DevOps

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

Thank you for attending AWS Innovate Modern Applications Edition

We hope you found it interesting! A kind reminder to **complete the survey.**
Let us know what you thought of today's event and how we can improve the event experience for you in the future.

aws-apj-marketing@amazon.com

twitter.com/AWSCloud

facebook.com/AmazonWebServices

youtube.com/user/AmazonWebServices

slideshare.net/AmazonWebServices

twitch.tv/aws

aws

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

Thank you!

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