aws INNOVATE

MODERN APPLICATIONS EDITION

27&28 October 2021

Effective security for modern applications

Sumit Patel

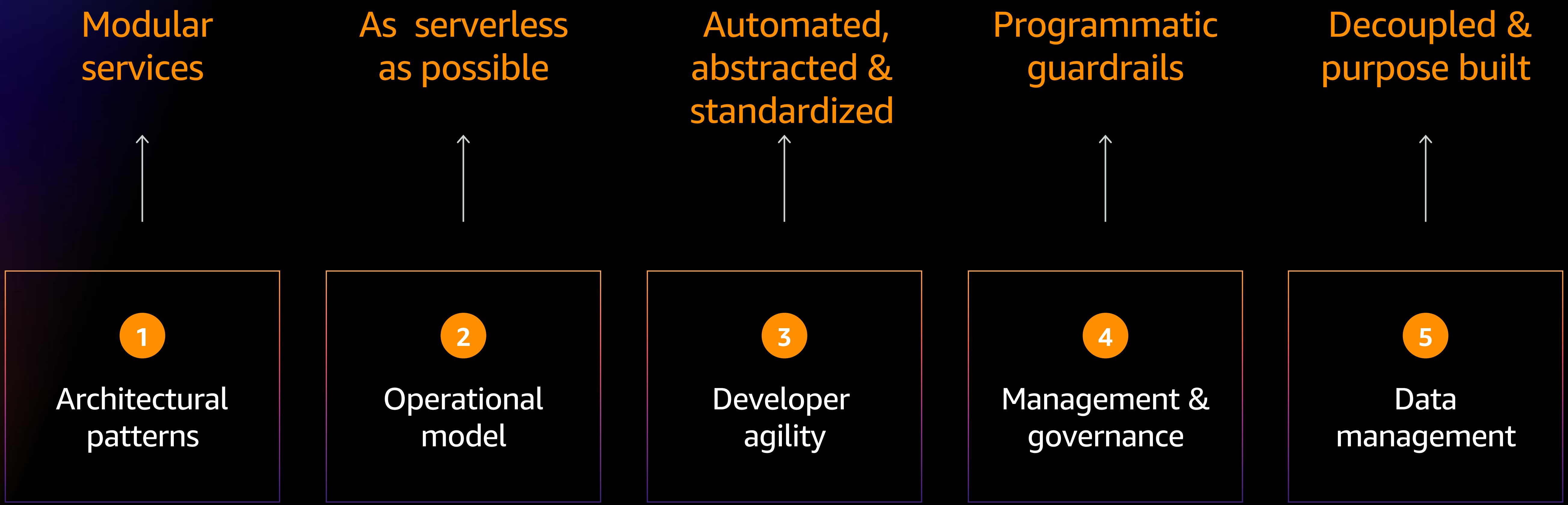
Solutions Architect
Amazon Web Services

Agenda

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

What is modern application development?

Modern applications



Modular services

As serverless as possible

Automated, abstracted & standardized

Programmatic guardrails

Decoupled & purpose built

1 Architectural patterns

2 Operational model

3 Developer agility

4 Management & governance

5 Data management

Modernization changes how you work

Builders

Start from scratch

Goal is innovation

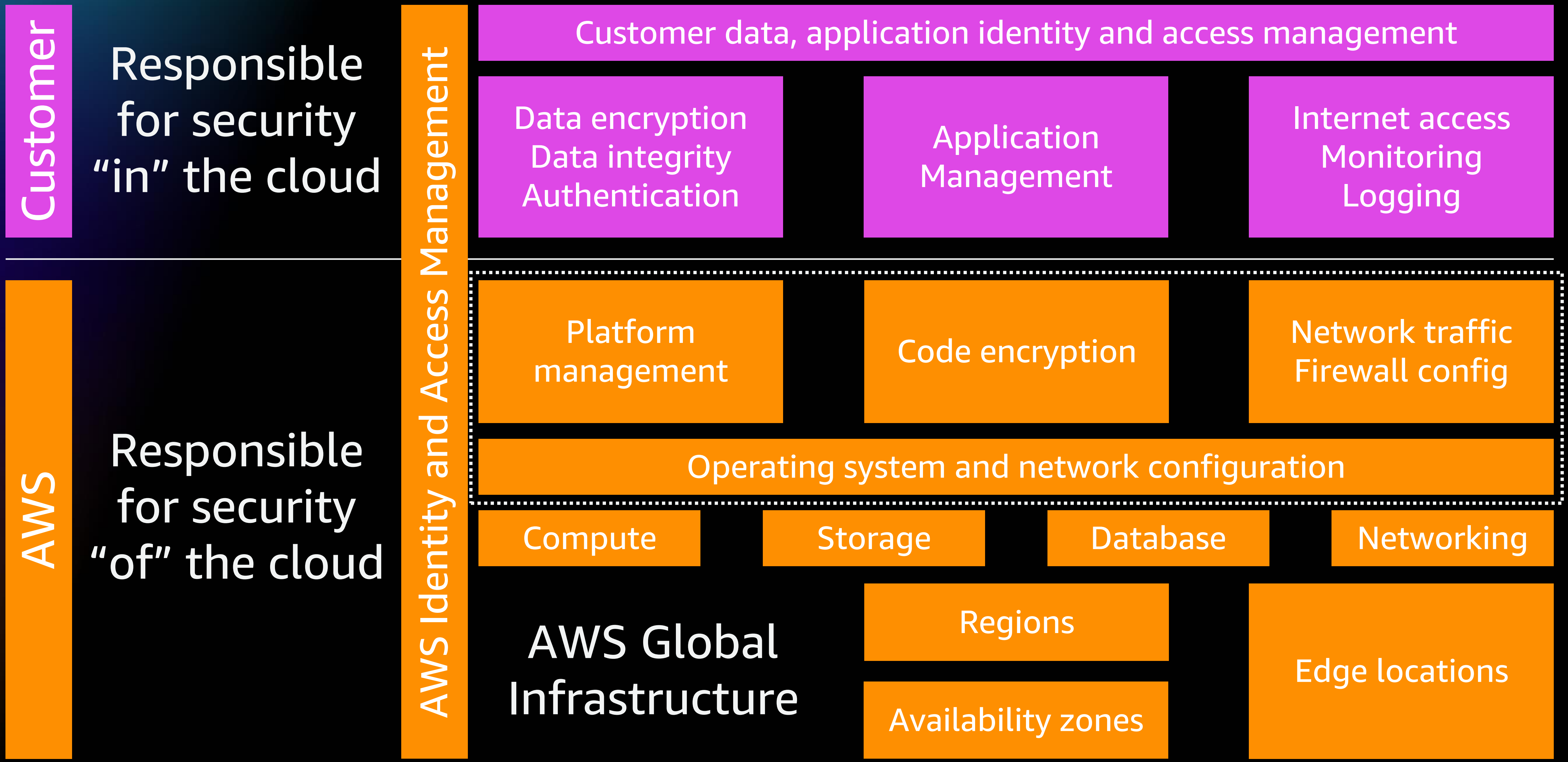
Operators

Deploy, debug, & monitor

Goal is low risk & high reliability/availability

Know your responsibility

AWS Shared Responsibility Model



Customer

Responsible for security “in” the cloud

AWS

Responsible for security “of” the cloud

AWS Identity and Access Management

Customer data, application identity and access management

Data encryption
Data integrity
Authentication

Application
Management

Internet access
Monitoring
Logging

Platform management

Code encryption

Network traffic
Firewall config

Operating system and network configuration

Compute

Storage

Database

Networking

AWS Global Infrastructure

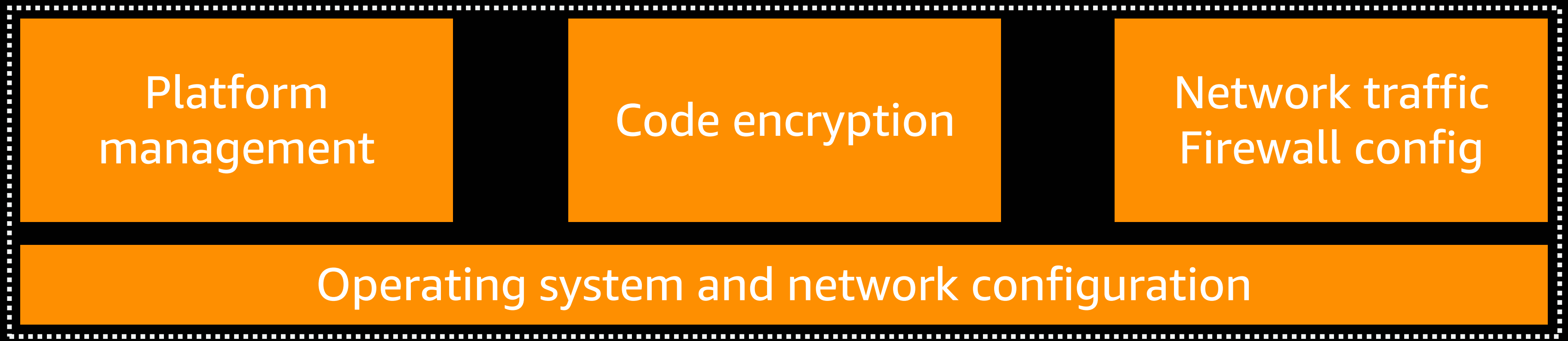
Regions

Availability zones

Edge locations

AWS Shared Responsibility Model

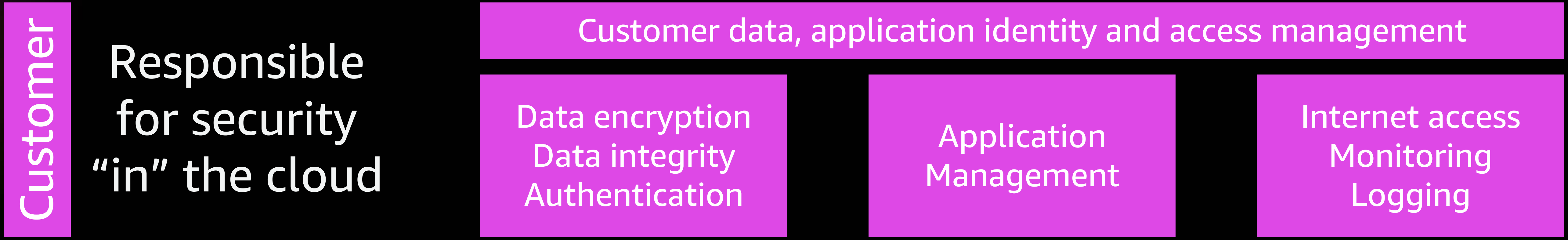
AWS assumes responsibility for these serverless applications components


Platform management
Code encryption
Network traffic Firewall config
Operating system and network configuration

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



Customer

Responsible for security “in” the cloud

Customer data, application identity and access management

Data encryption
Data integrity
Authentication

Application
Management

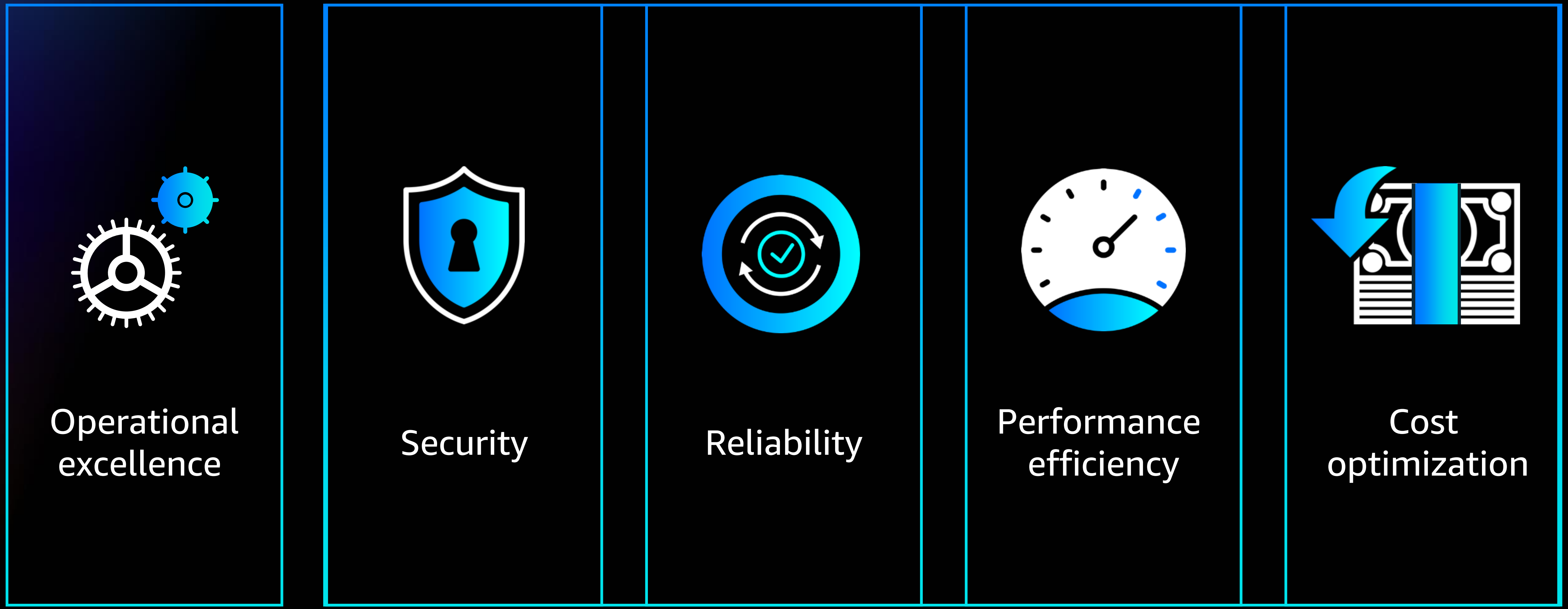
Internet access
Monitoring
Logging

Approaching your security considerations

AWS Well-Architected Framework

- Operational excellence
- Security
- Reliability
- Performance efficiency
- Cost optimization

AWS Well-Architected Framework



Operational excellence

Security

Reliability

Performance efficiency

Cost optimization

AWS Well-Architected Framework

Security

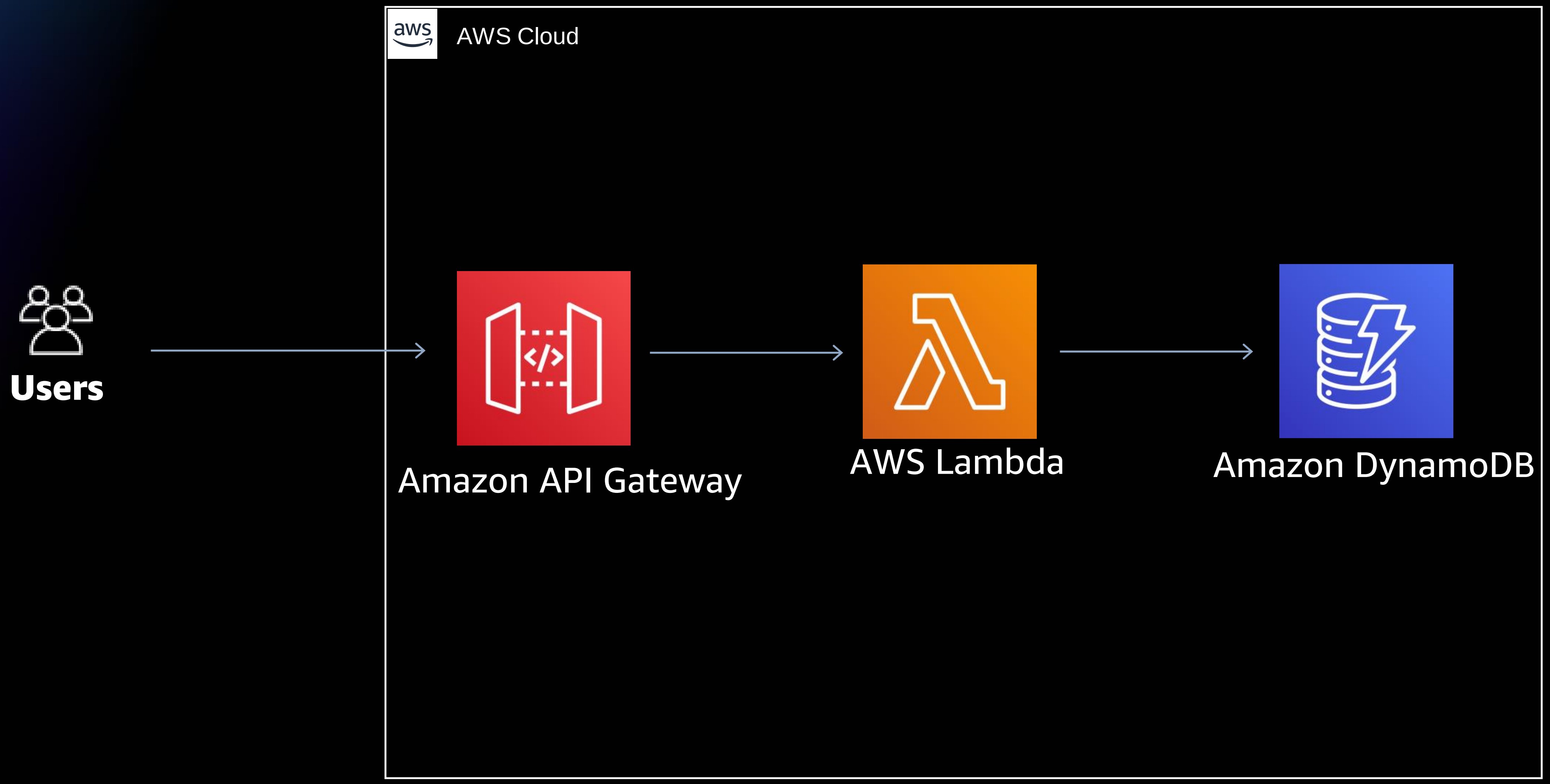
How to be secure

Best Practice Areas

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

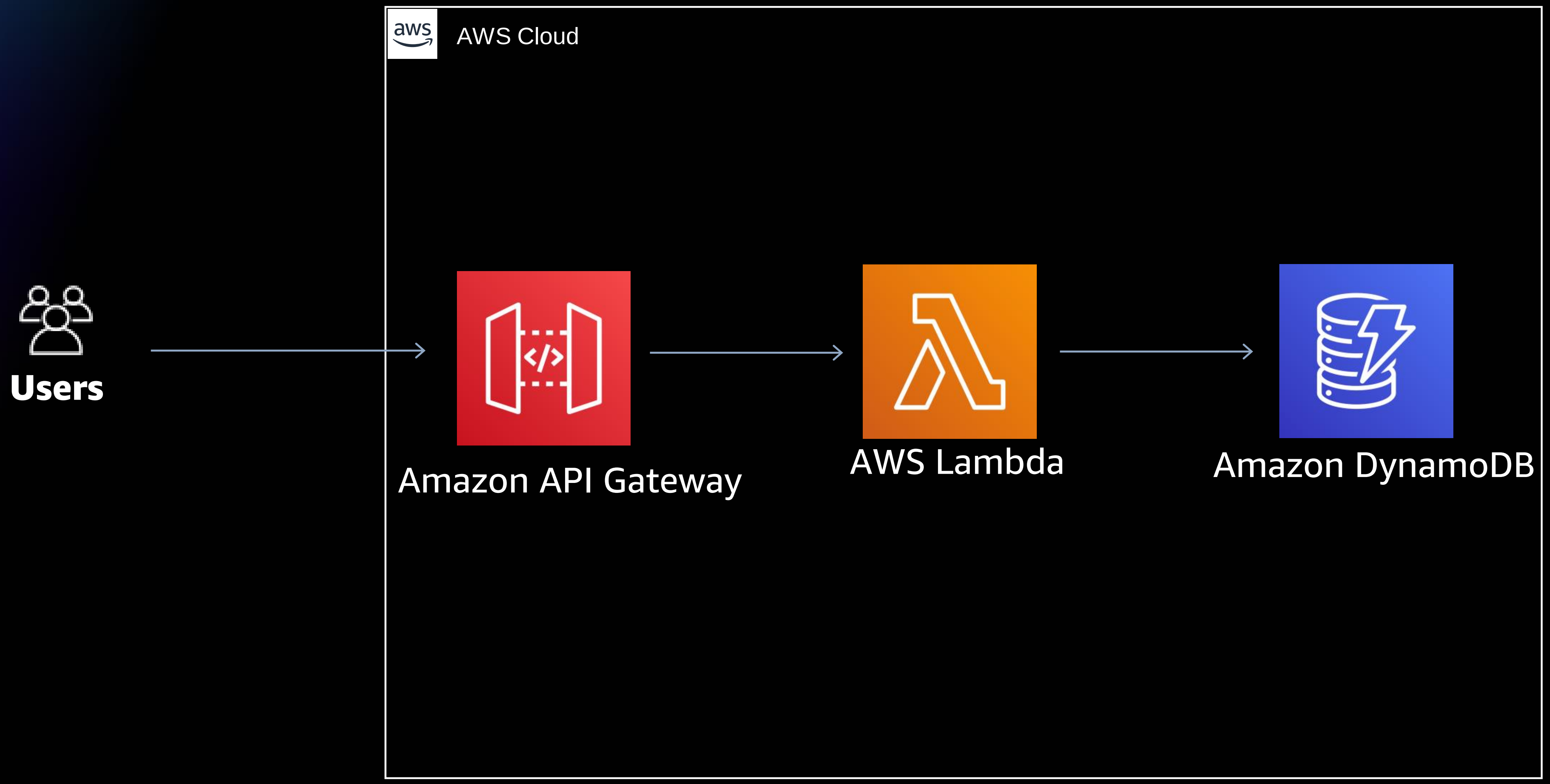
Sample modern application

Sample modern application



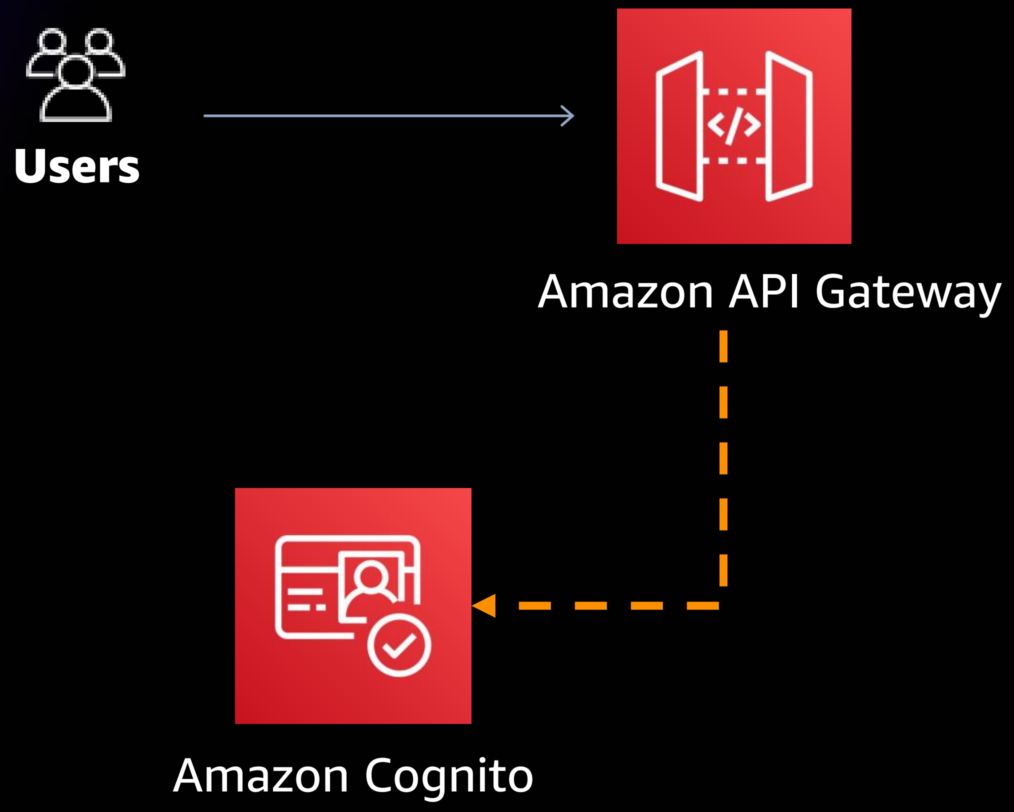
Sample modern application

Identity and access management



Sample modern application

Identity and access management



Mutual TLS Authentication

IAM permissions

- Use IAM policies and AWS credentials to grant access

AWS 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

Sample modern application

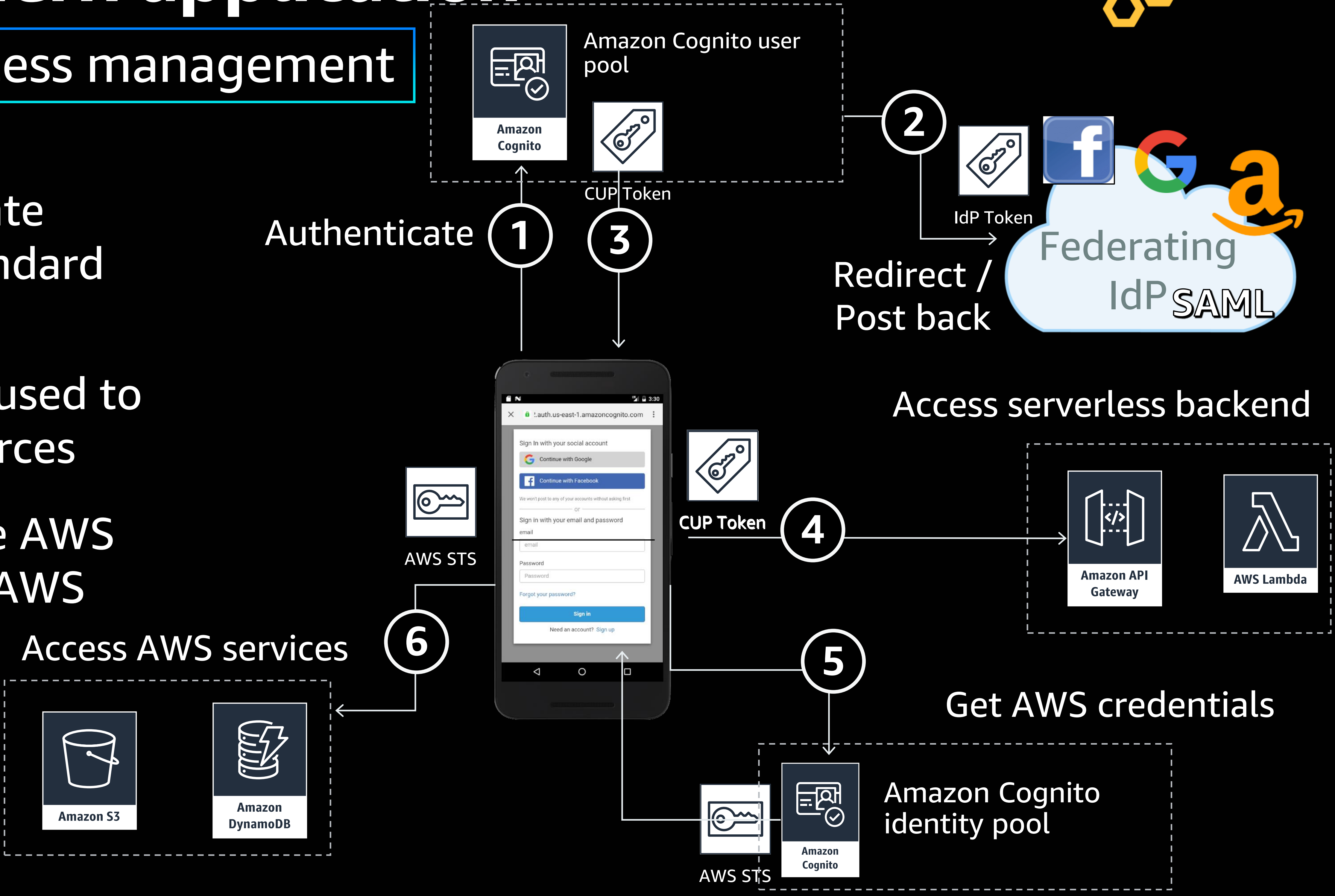
Identity and access management

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



Sign In with your social account

Continue with Google

Continue with Facebook

We won't post to any of your accounts without asking first

or

Sign in with your email and password

email

email

Password

Password

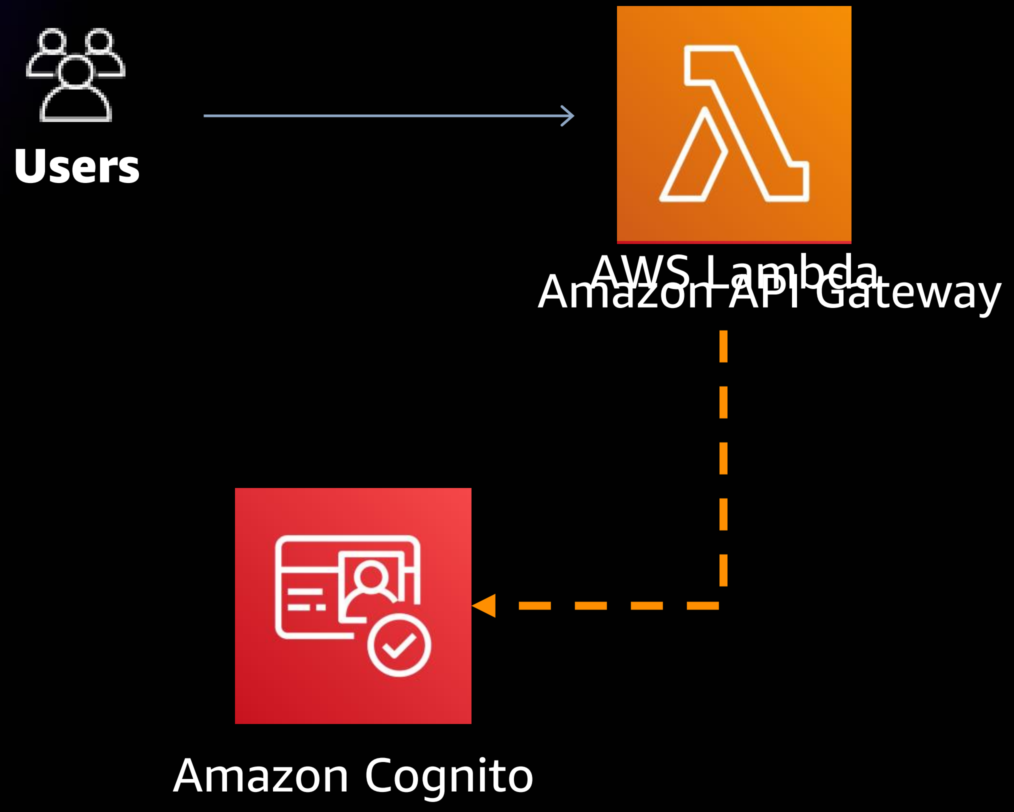
Forgot your password?

Sign in

Need an account? Sign up

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

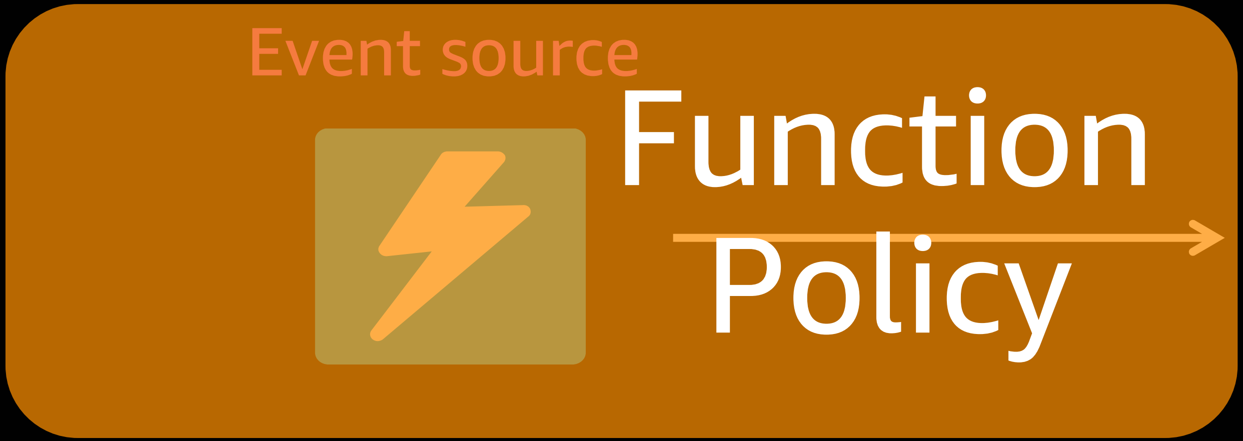
Sample modern application

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



Event source

Function Policy

Sample modern application

Identity and access management

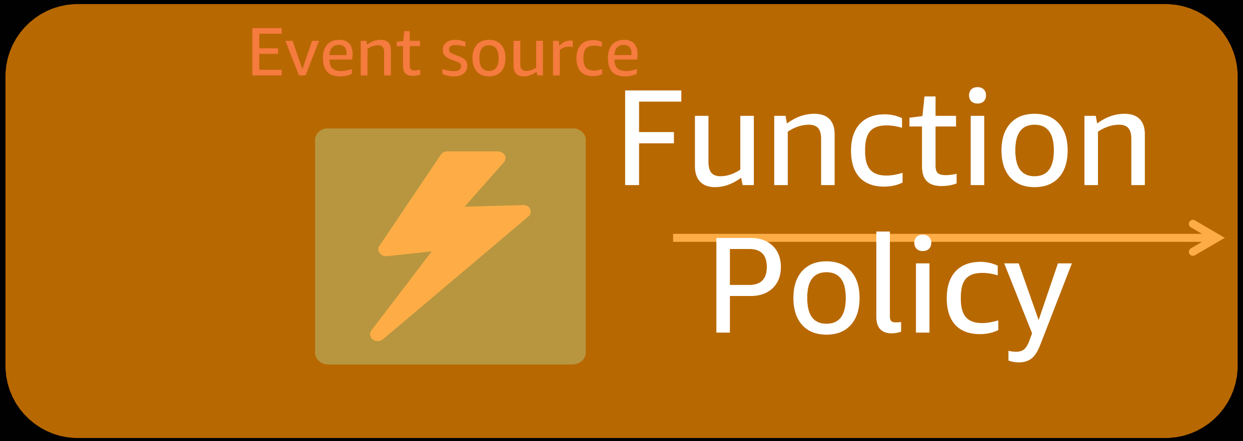
AWS Lambda

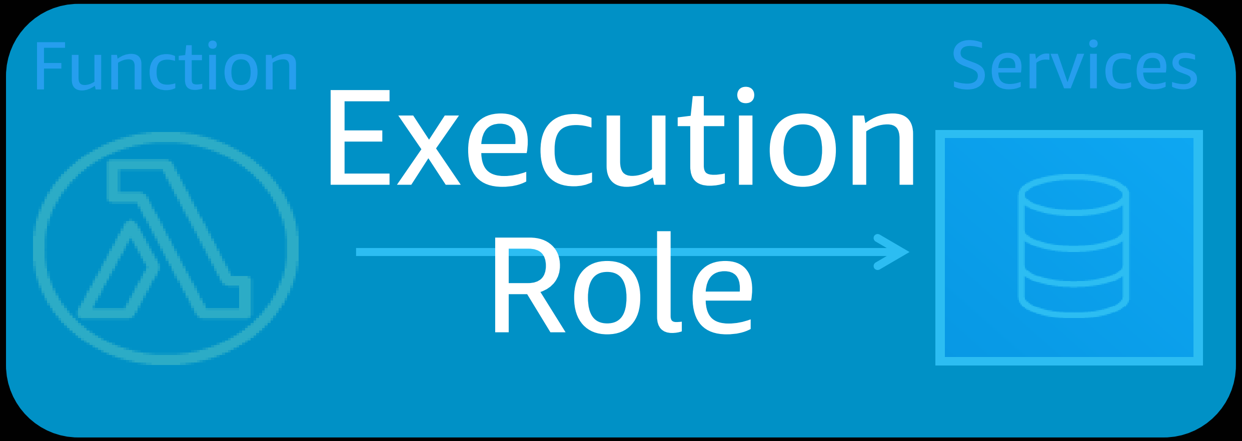
Function policies:

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

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





Sample modern application

Identity and access management

Amazon DynamoDB

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?

In English: Allowed to take all Amazon DynamoDB actions

Sample modern application

Identity and access management

Amazon DynamoDB

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

In English: Allowed to read and write individual items in Amazon DynamoDB

Sample modern application

Identity and access management

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

Amazon DynamoDB

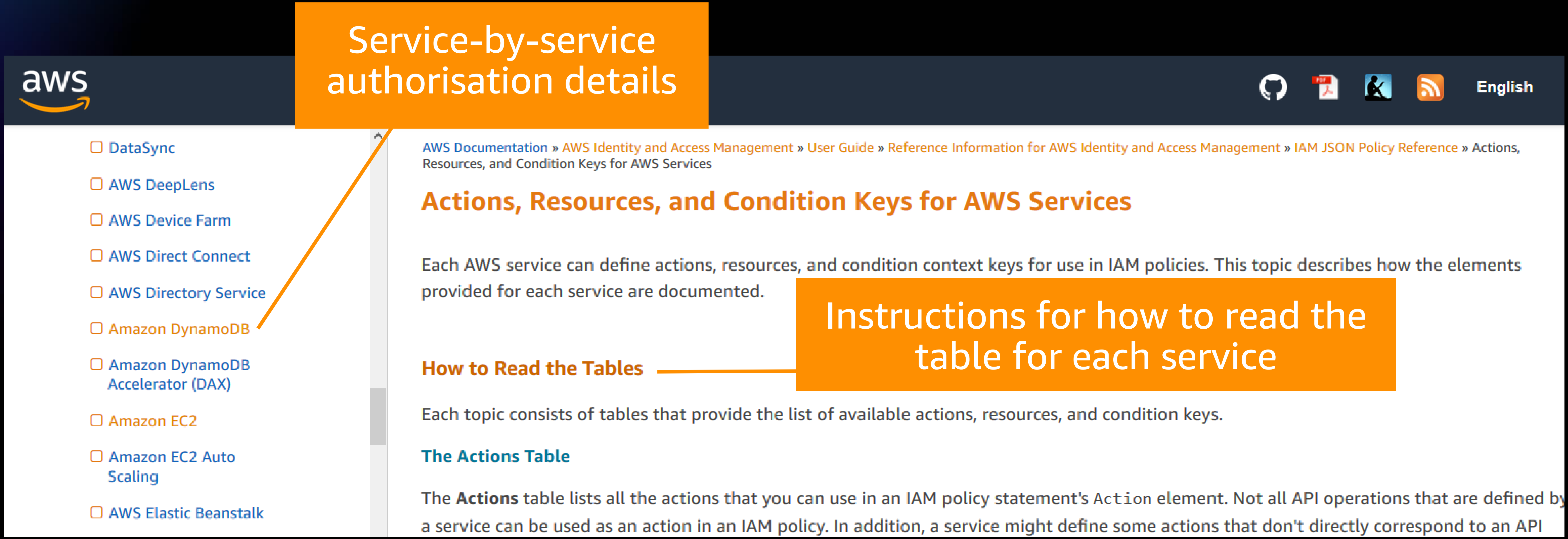
In English: Allowed to take specific DynamoDB actions on a specific table

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

Sample modern application

Identity and access management

Amazon DynamoDB



Service-by-service authorisation details

Instructions for how to read the table for each service

- □ 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.

How to Read the Tables

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

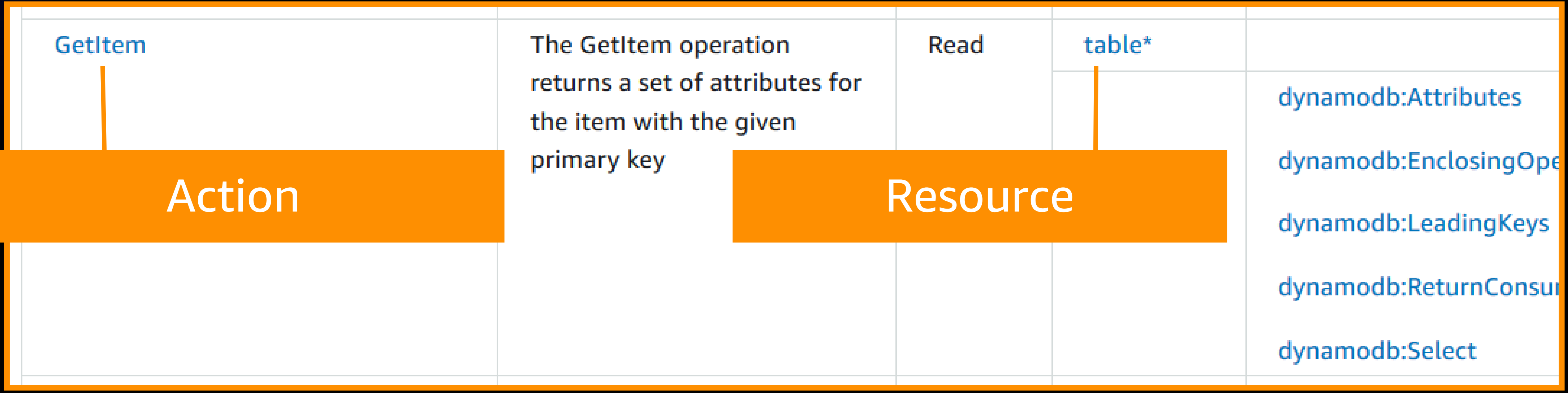
The Actions Table

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

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

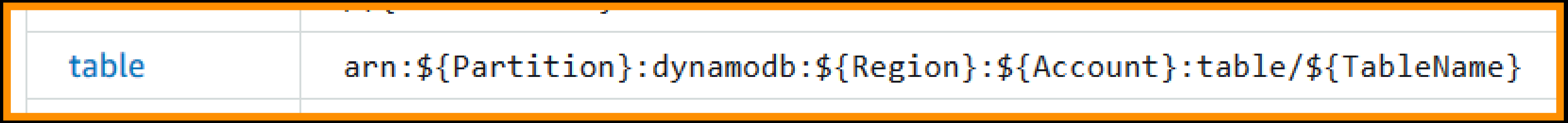


table	arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}

Resource ARN format

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

Sample modern application compliance

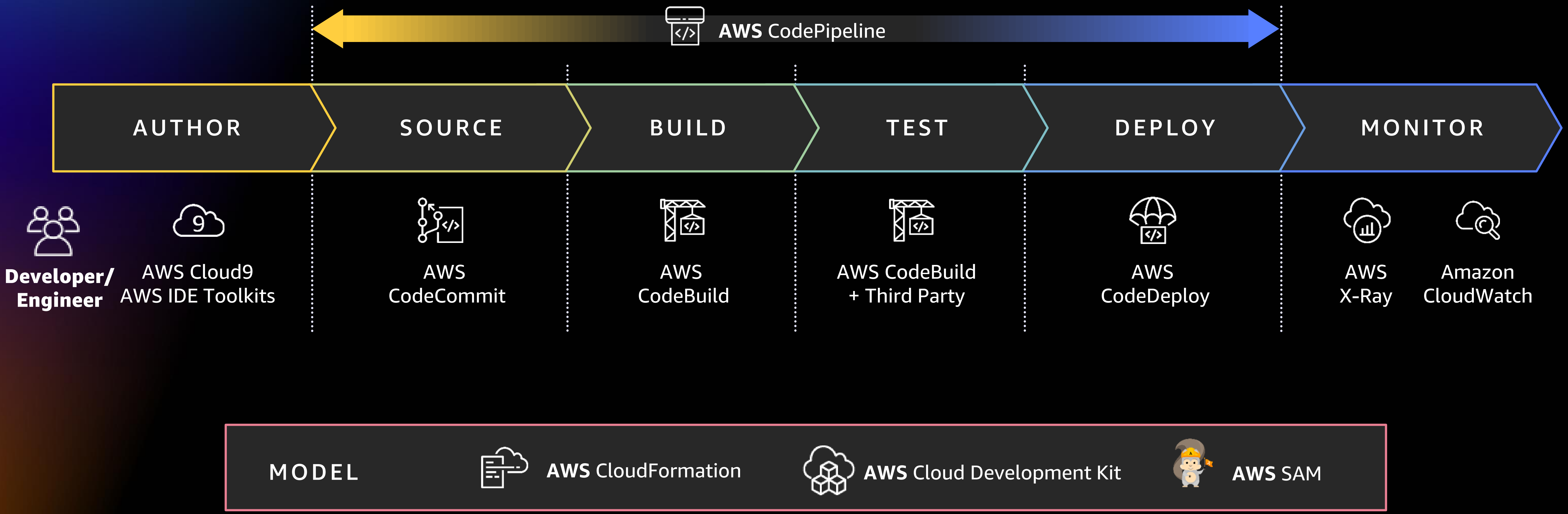
- Compliance-ready for SOC, PCI, FedRAMP, HIPAA, and others

Service	SOC	PCI	ISO	FedRAMP	HIPAA
Amazon API Gateway	☑	☑	☑	☑	☑
AWS Lambda	☑	☑	☑	☑	☑
Amazon DynamoDB	☑	☑	☑	☑	☑
Amazon Cognito	☑	☑	☑	☑	☑

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

Embed your knowledge (DevSecOps)

AWS Developer Tools for modern software delivery



AWS CodePipeline

AUTHOR

SOURCE

BUILD

TEST

DEPLOY

MONITOR

Developer/ Engineer

AWS Cloud9
AWS IDE Toolkits

AWS
CodeCommit

AWS
CodeBuild

AWS CodeBuild
+ Third Party

AWS
CodeDeploy

AWS
X-Ray

Amazon
CloudWatch

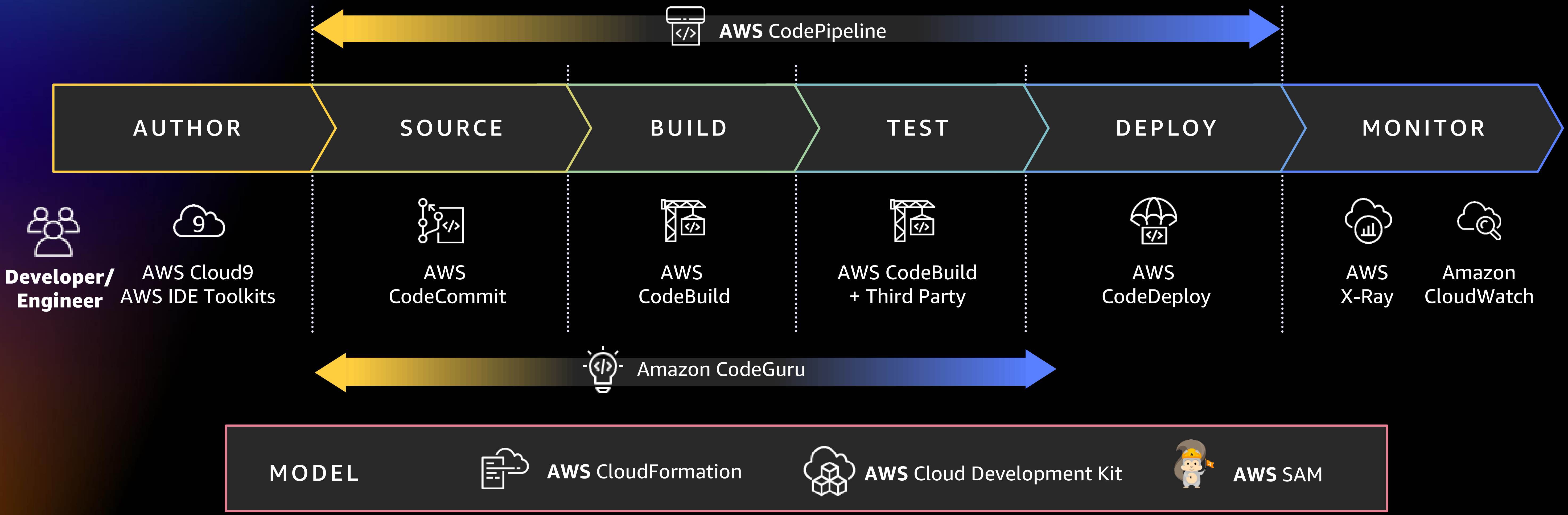
MODEL

AWS CloudFormation

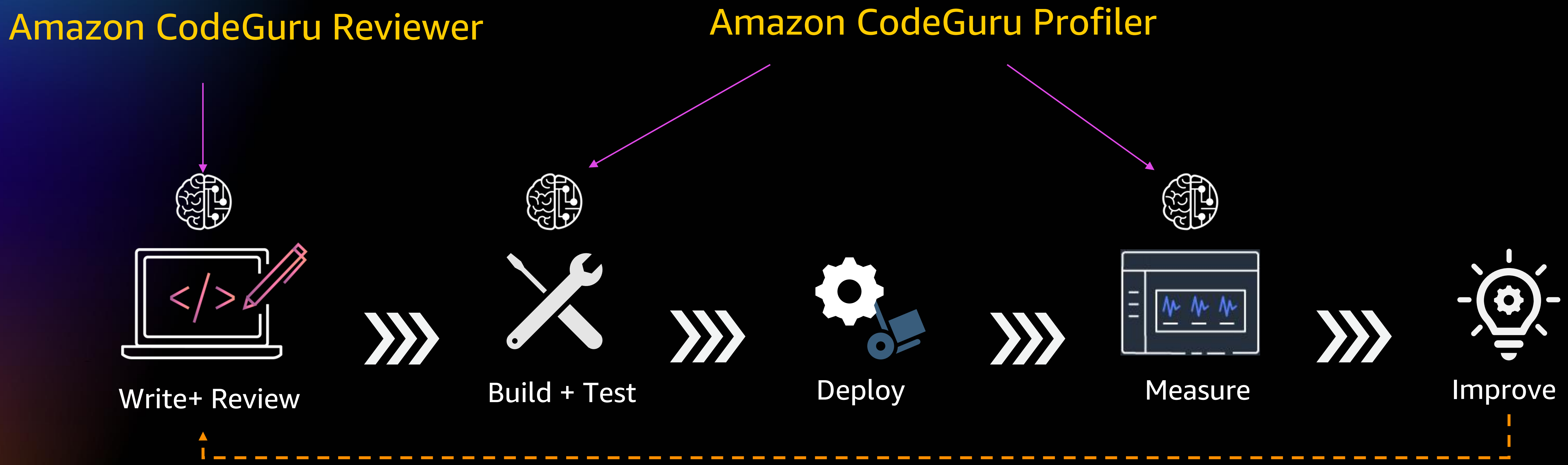
AWS Cloud Development Kit

AWS SAM

AWS Developer Tools for modern software delivery



Amazon CodeGuru in your software workflow

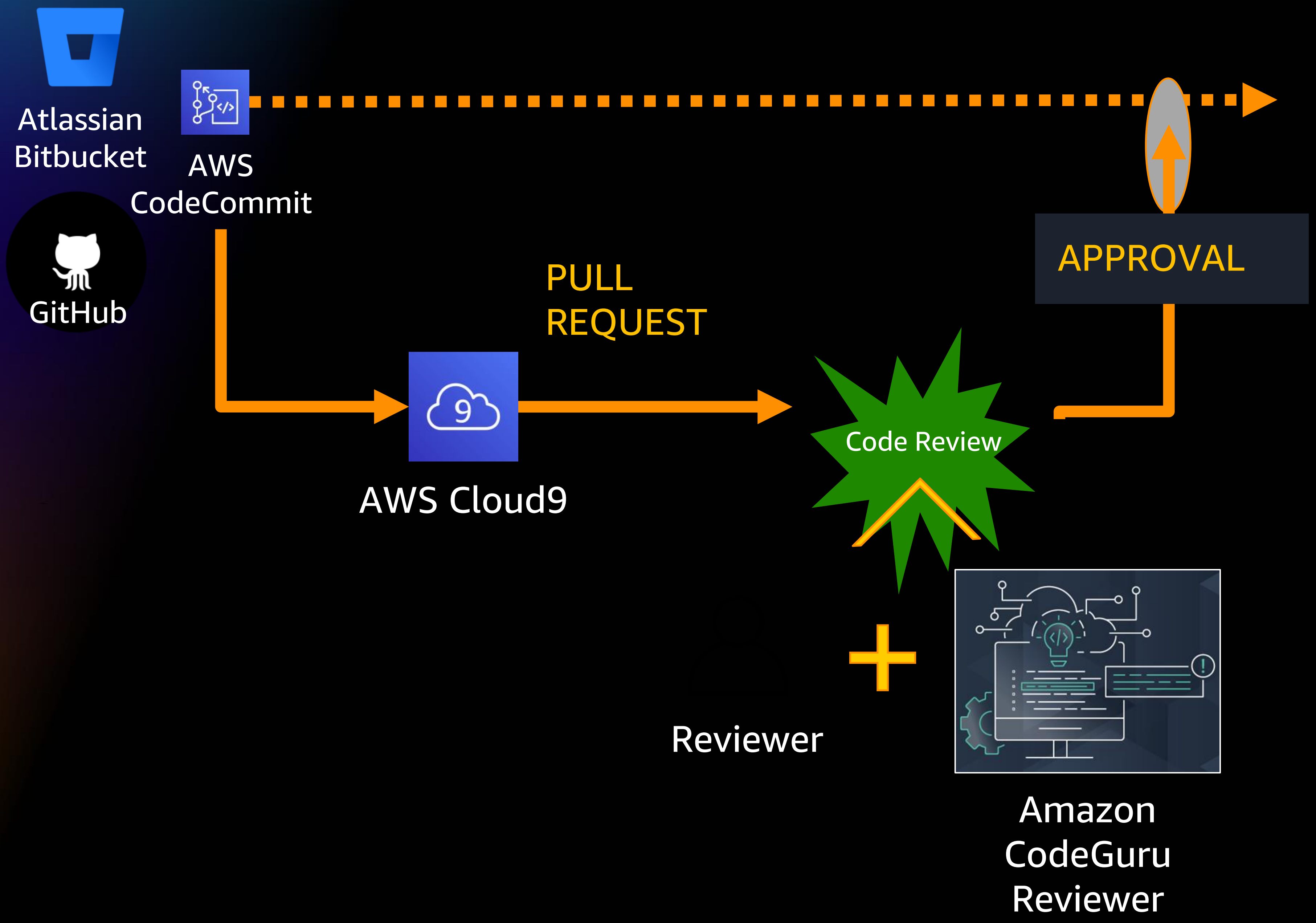


Built-in code reviews with actionable recommendations

Detect and optimize the expensive lines of code

Easily identify performance and cost improvements in production environment

Code review with Amazon CodeGuru Reviewer



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

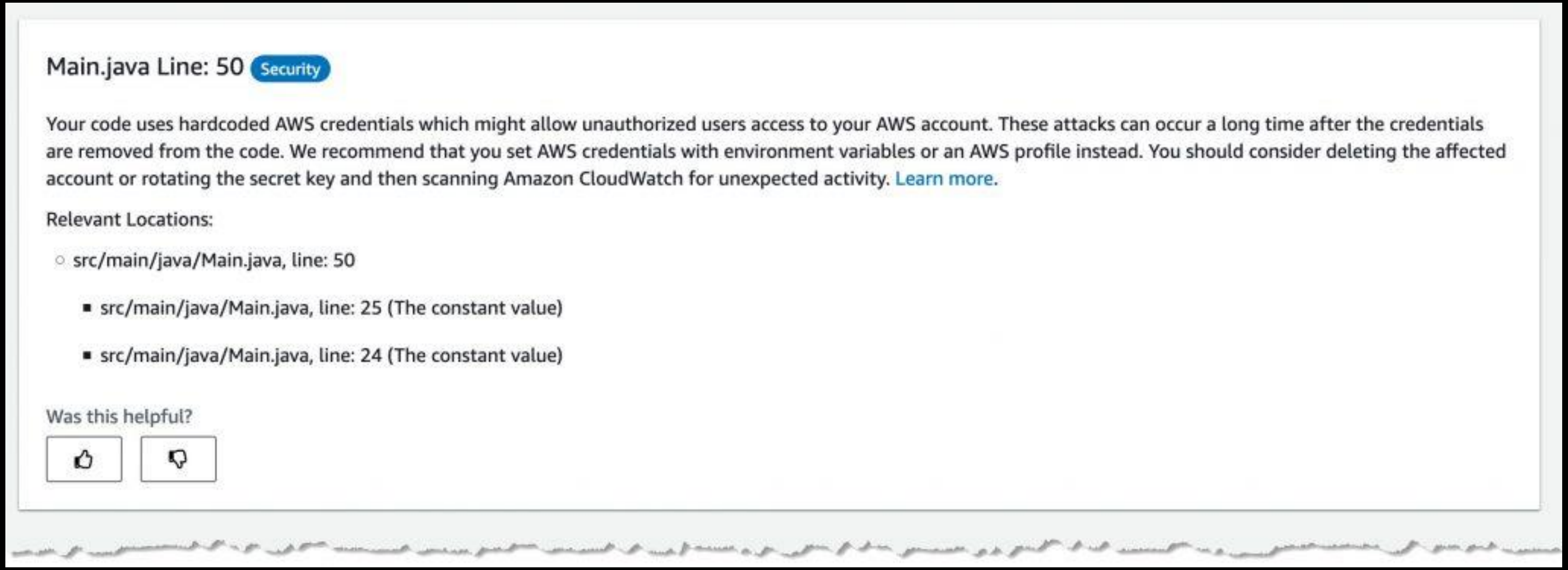
Examples of Amazon CodeGuru Security findings

```java
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.

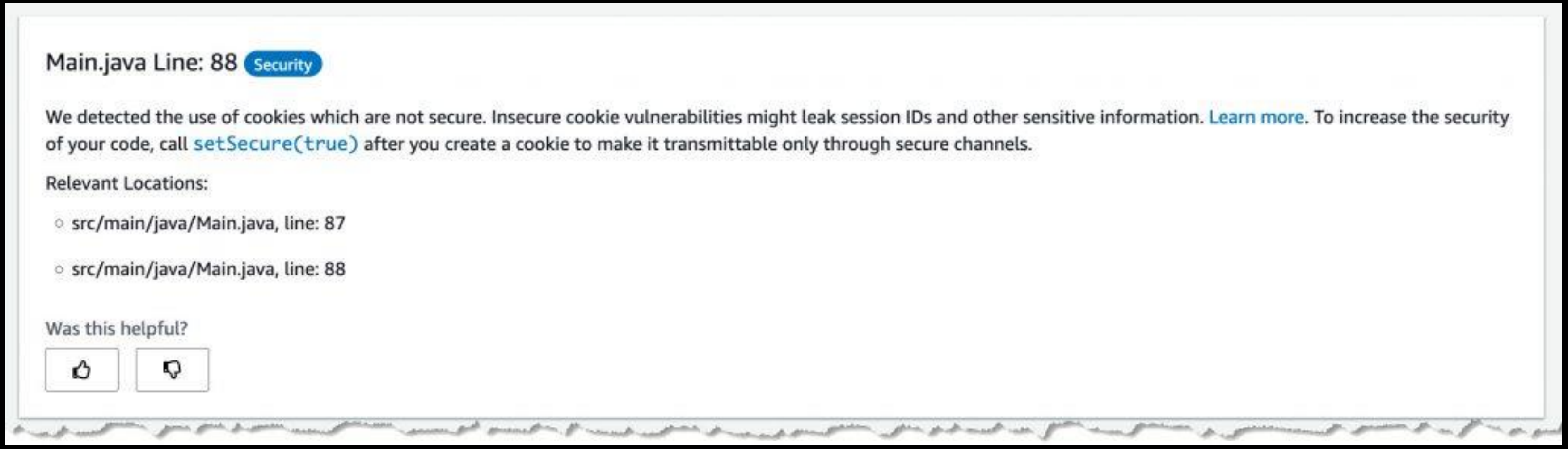
Relevant Locations:

- 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?

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

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



Main.java Line: 88 Security

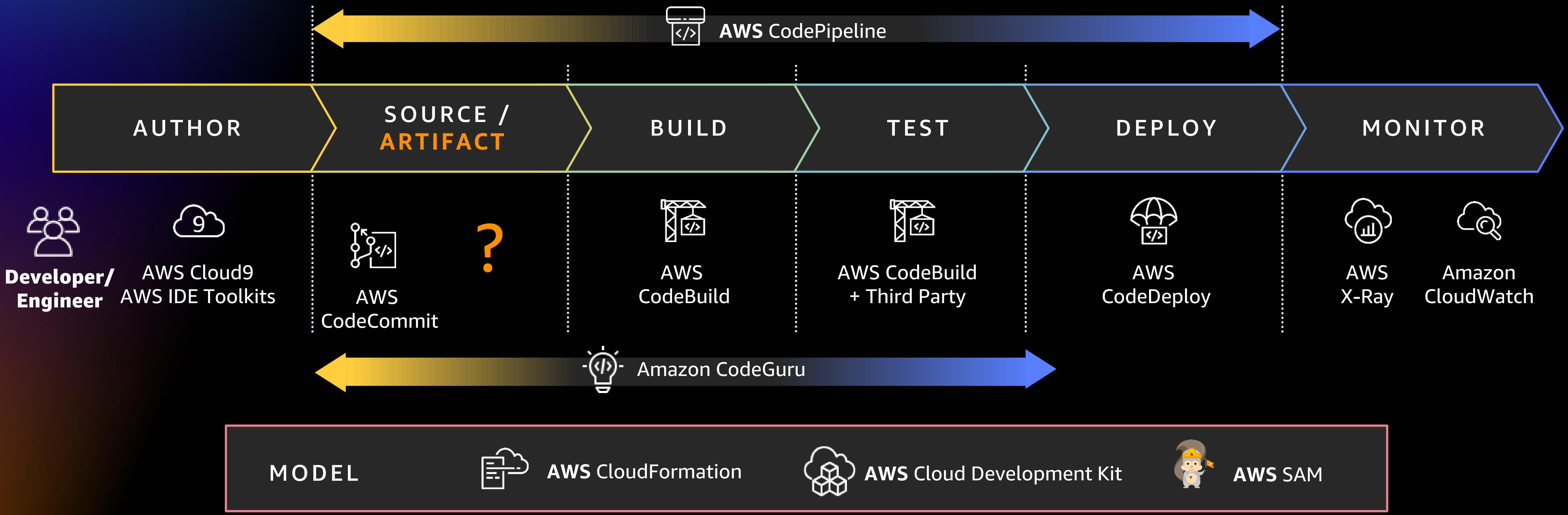
We detected the use of cookies which are not secure. Insecure cookie vulnerabilities might leak session IDs and other sensitive information. Learn more. To increase the security of your code, call `setSecure(true)` after you create a cookie to make it transmittable only through secure channels.

Relevant Locations:

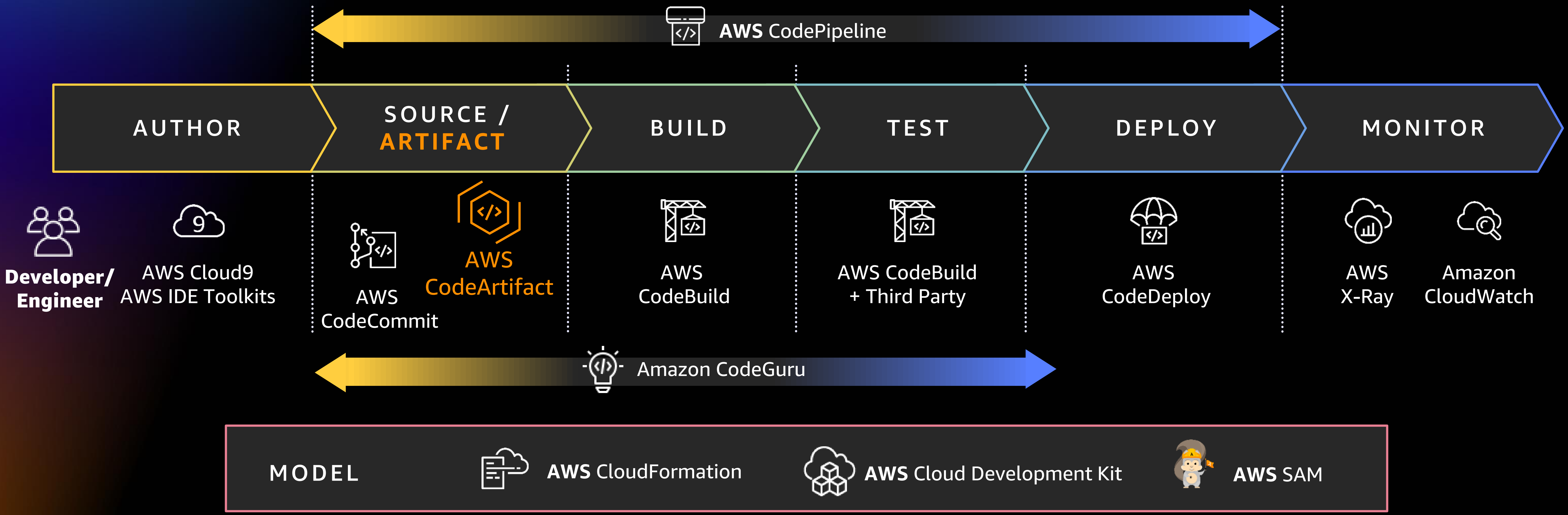
- src/main/java/Main.java, line: 87
- src/main/java/Main.java, line: 88

Was this helpful?

AWS Developer Tools for modern software delivery



AWS Developer Tools for modern software delivery



AWS CodePipeline

AUTHOR

SOURCE / ARTIFACT

BUILD

TEST

DEPLOY

MONITOR

Developer/ Engineer

AWS Cloud9
AWS IDE Toolkits

AWS CodeCommit

AWS CodeArtifact

AWS CodeBuild

AWS CodeBuild + Third Party

AWS CodeDeploy

AWS X-Ray

Amazon CloudWatch

Amazon CodeGuru

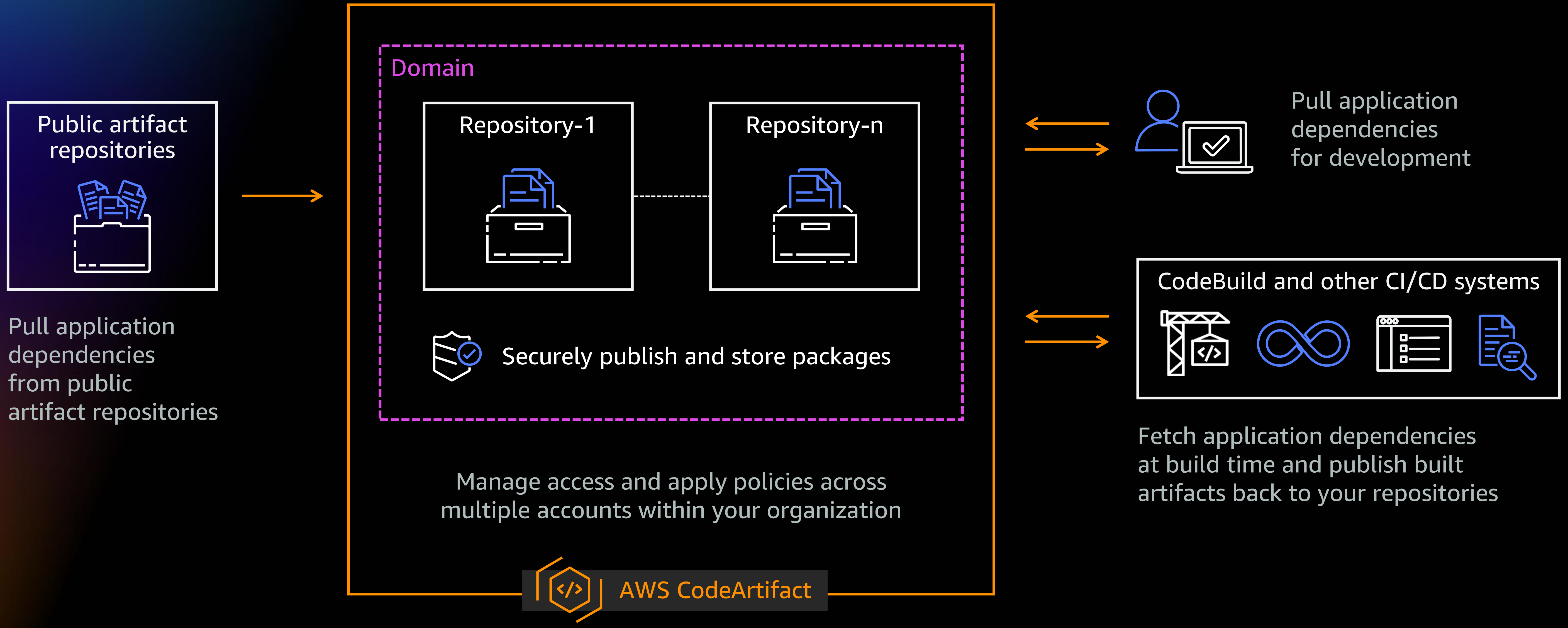
MODEL

AWS CloudFormation

AWS Cloud Development Kit

AWS SAM

AWS CodeArtifact overview



Public artifact repositories
Domain
Repository-1
Repository-n
Securely publish and store packages
AWS CodeArtifact
CodeBuild and other CI/CD systems

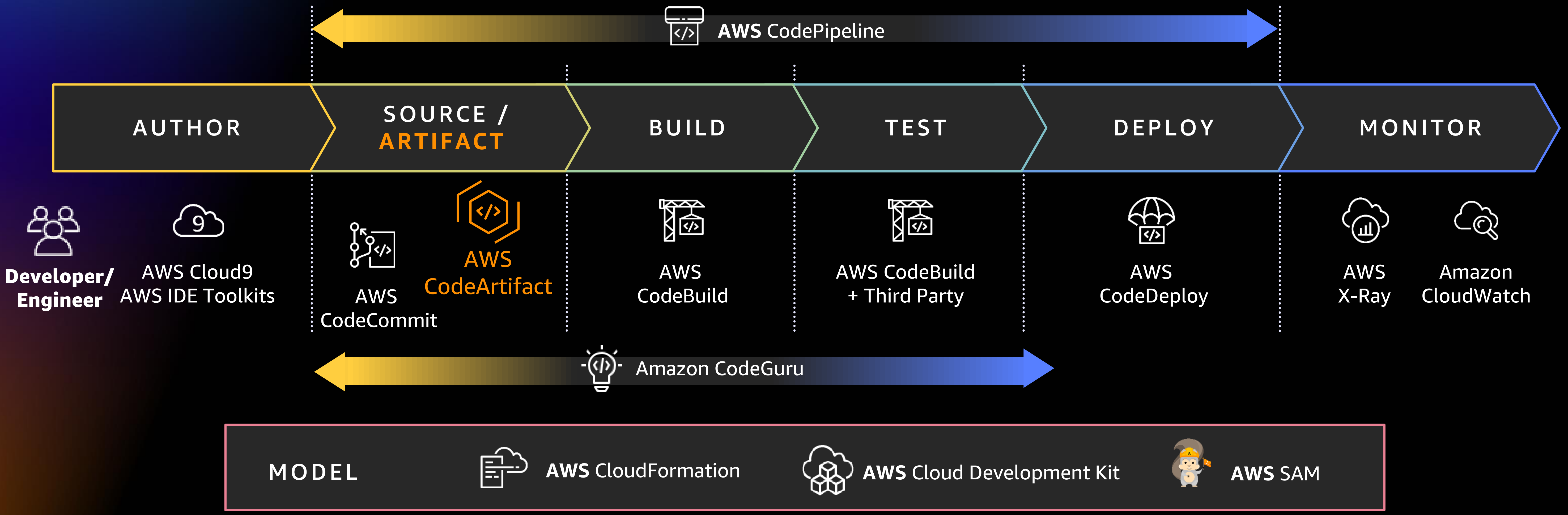
Pull application dependencies from public artifact repositories

Manage access and apply policies across multiple accounts within your organization

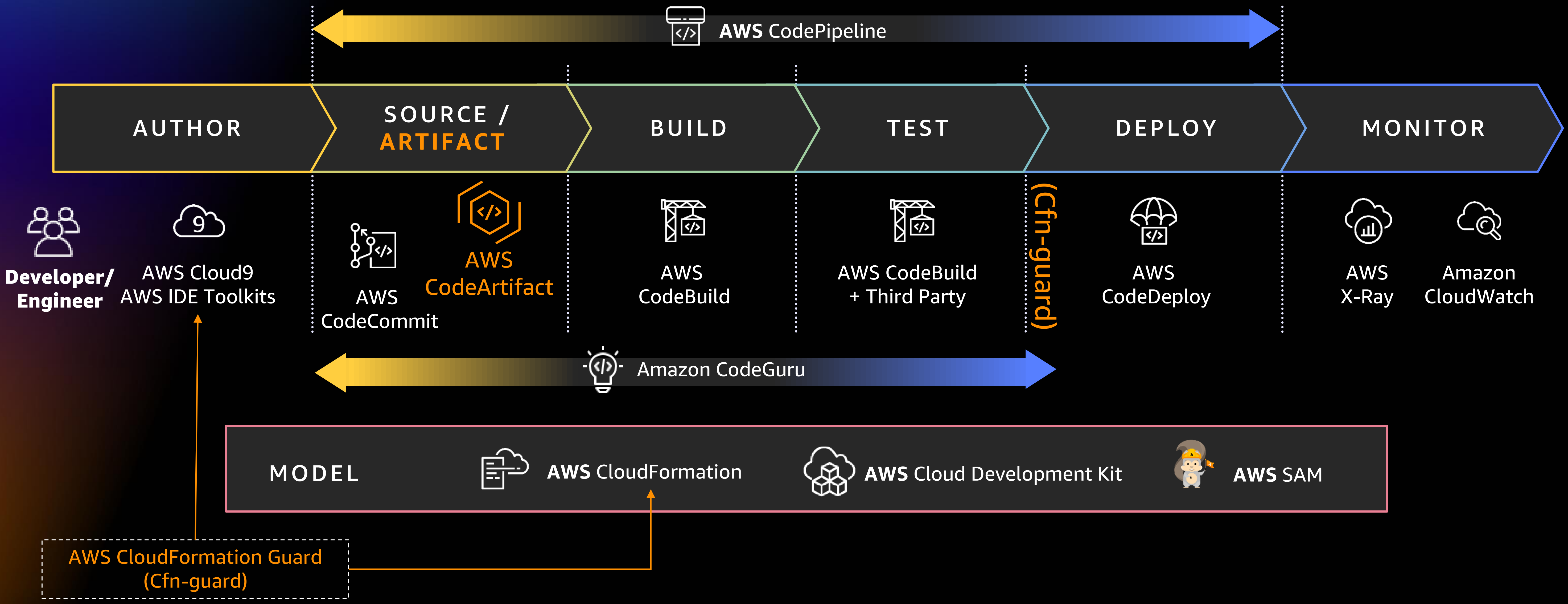
Pull application dependencies for development

Fetch application dependencies at build time and publish built artifacts back to your repositories

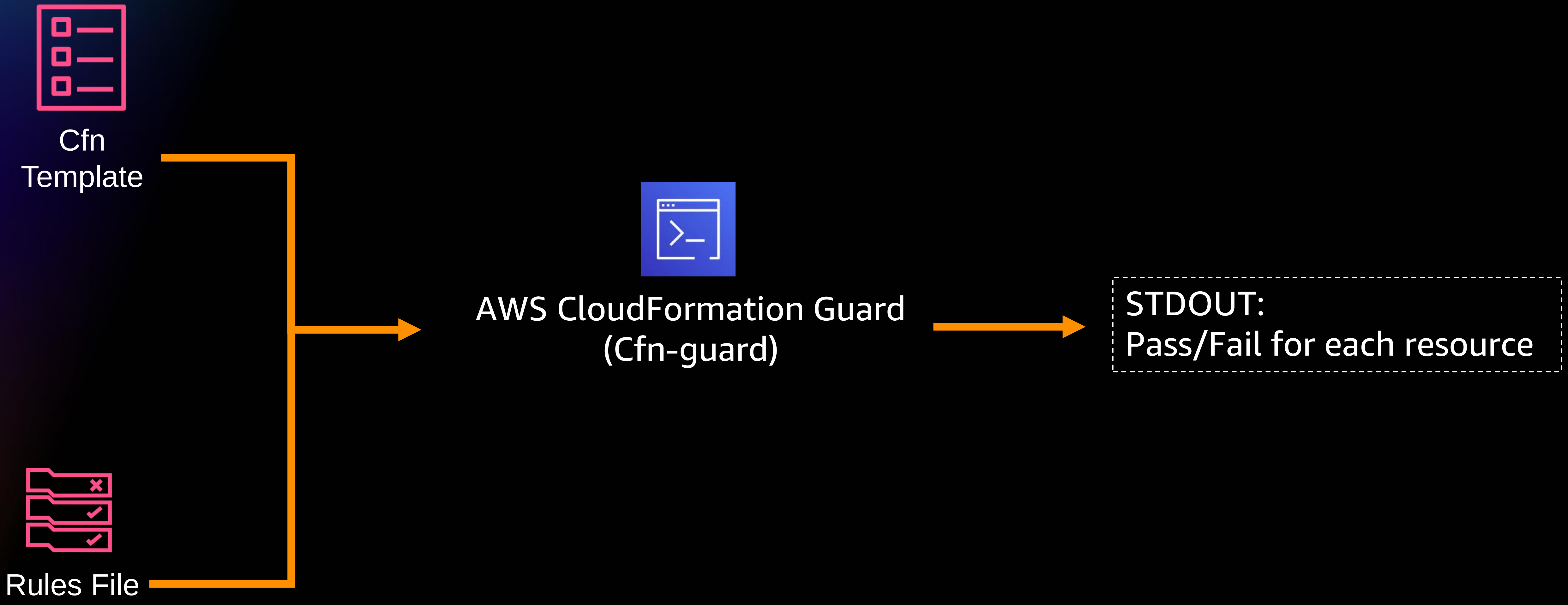
AWS Developer Tools for modern software delivery



AWS Developer Tools for modern software delivery



AWS CloudFormation Guard workflow



Cfn Template

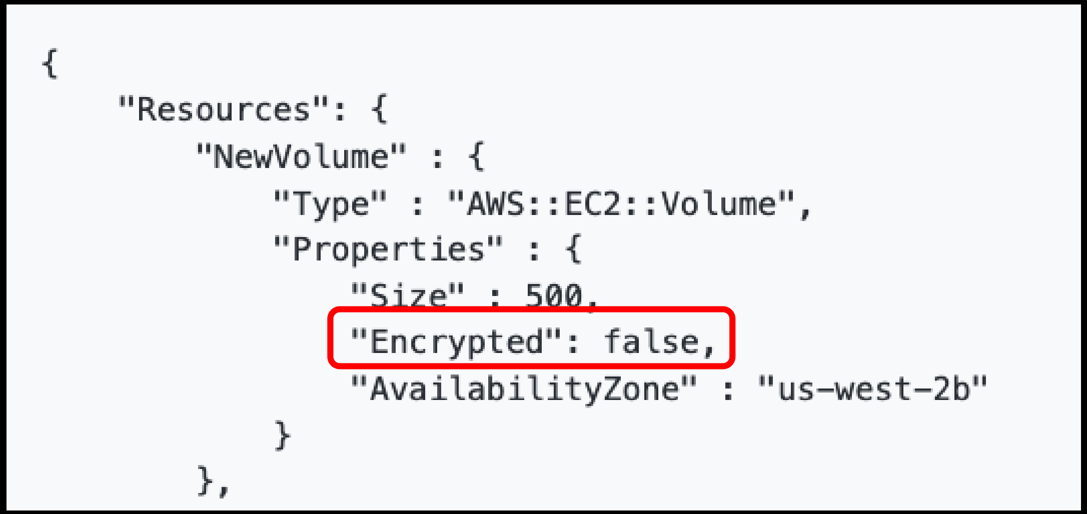
Rules File

AWS CloudFormation Guard (Cfn-guard)

STDOUT:
Pass/Fail for each resource

Example

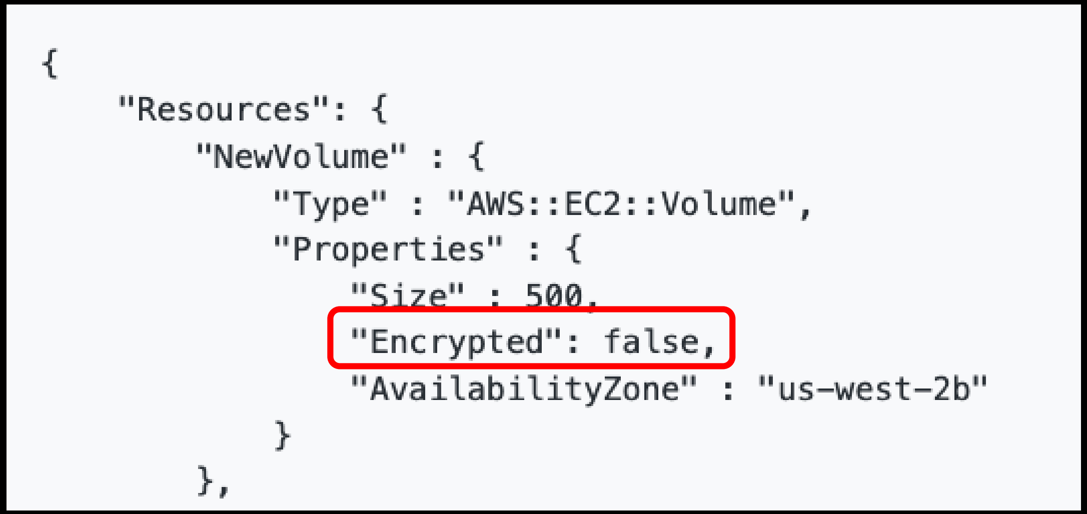
- CloudFormation template



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

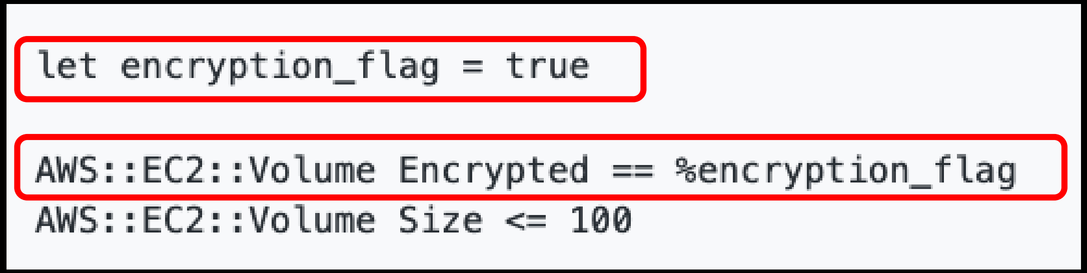
Example

- CloudFormation template



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

- Cfn-guard rules file

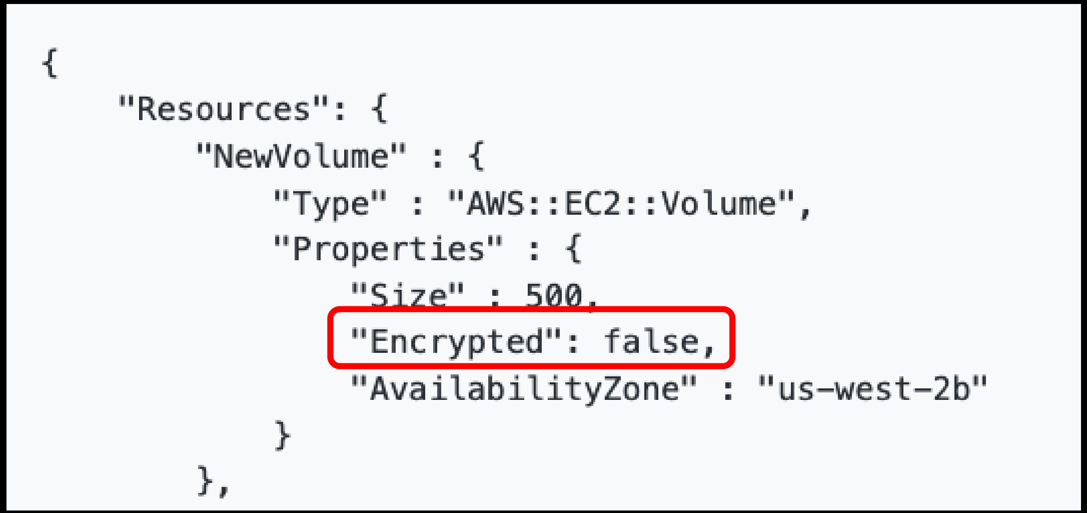


```
let encryption_flag = true

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

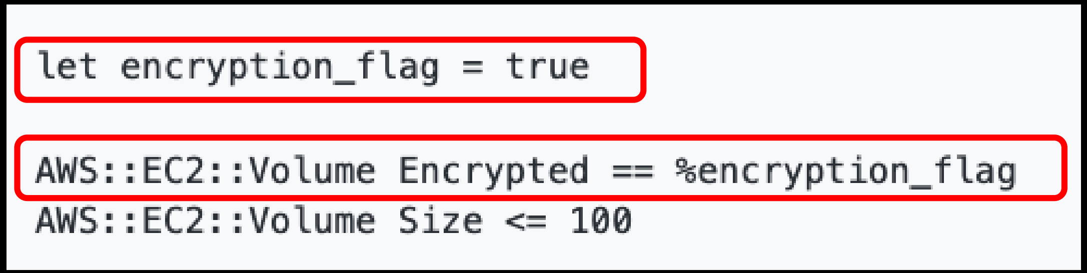
Example

- CloudFormation template



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

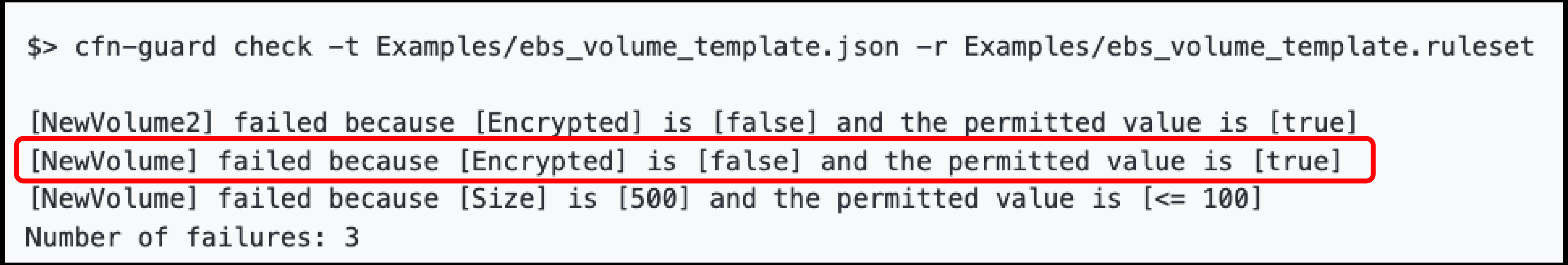
- Cfn-guard rules file



```
let encryption_flag = true

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

- Cfn-guard output



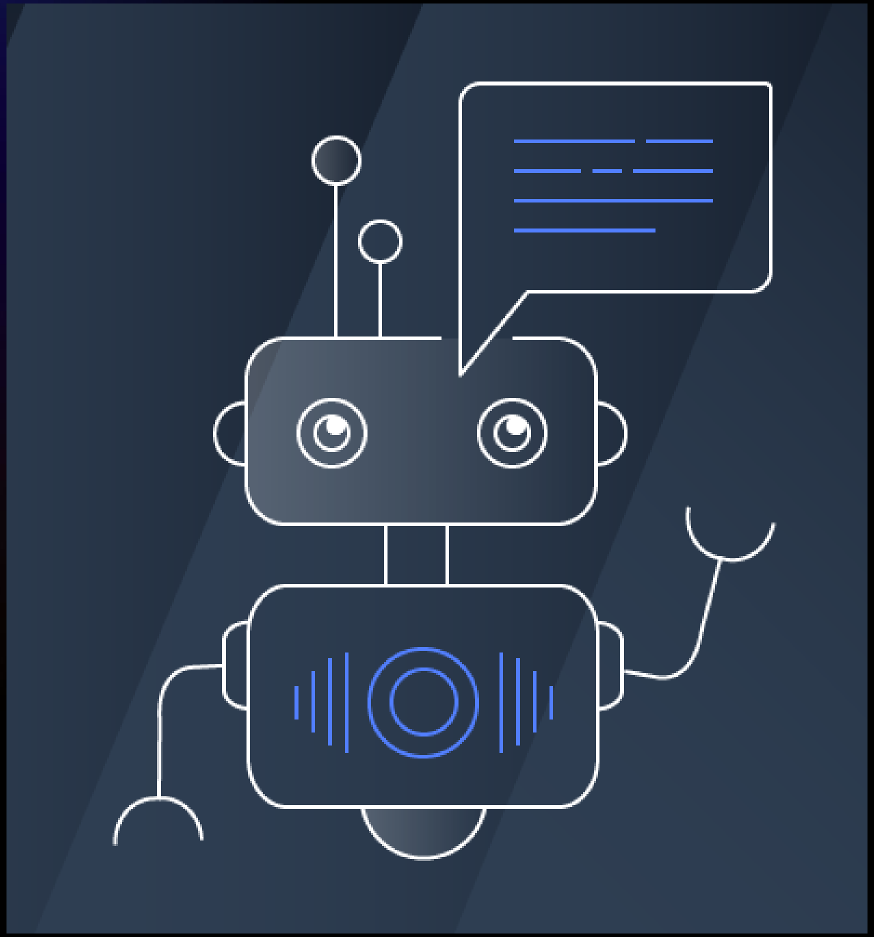
```
$> cfn-guard check -t Examples/ebs_volume_template.json -r Examples/ebs_volume_template.ruleset

[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
```

Modern security operations

AWS Chatbot: Bring AWS to Slack and Amazon Chime

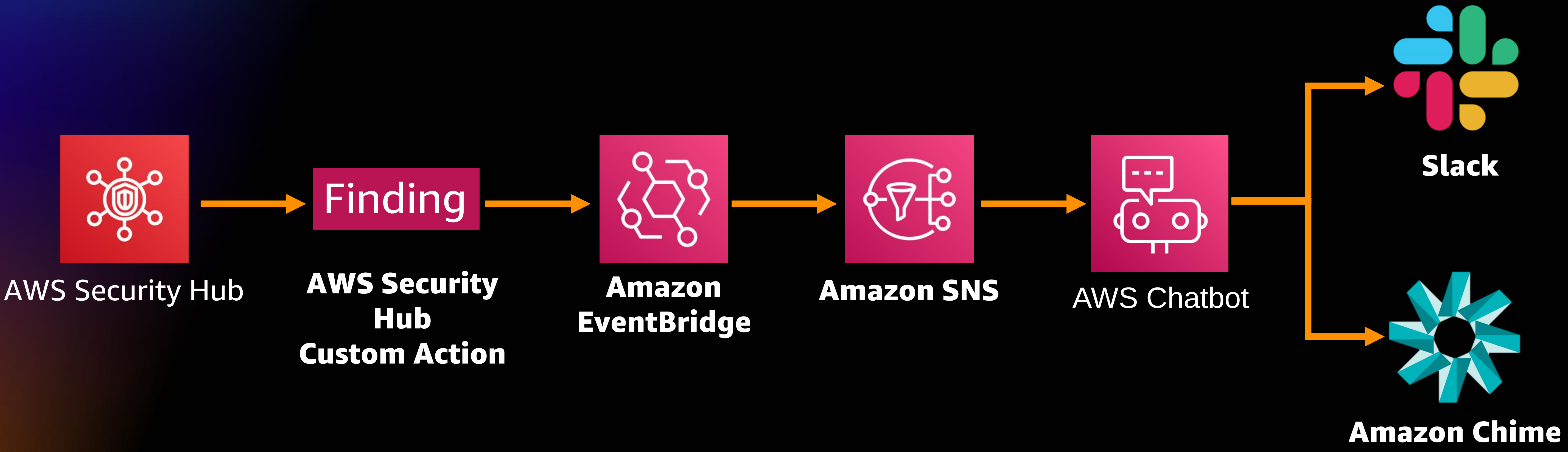
AWS Chatbot



Interactive agent for ChatOps on AWS

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

Enabling AWS Security Hub integration with AWS Chatbot



AWS Security Hub

Finding

AWS Security Hub Custom Action

Amazon EventBridge

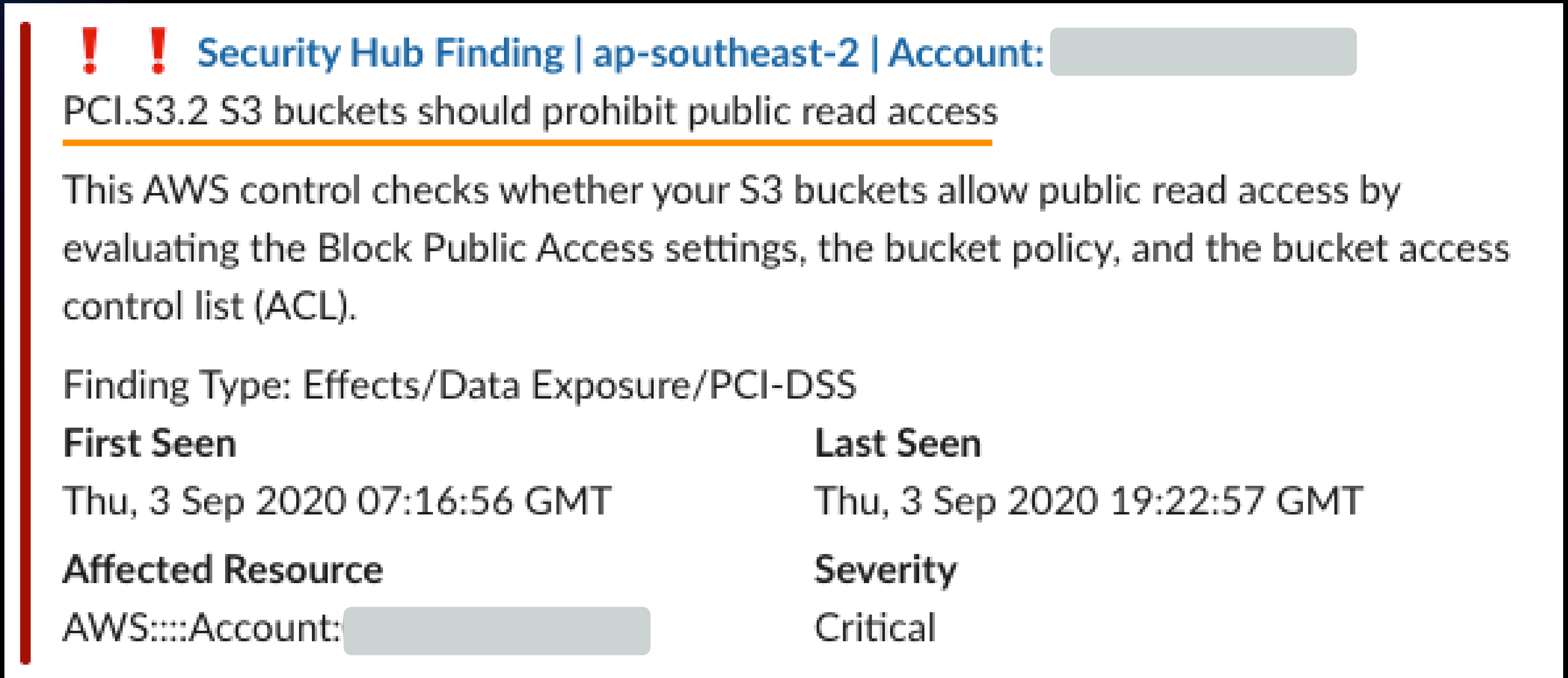
Amazon SNS

AWS Chatbot

Slack

Amazon Chime

Security Hub PCI notifications



❗ ❗ Security Hub Finding | ap-southeast-2 | Account: [redacted]

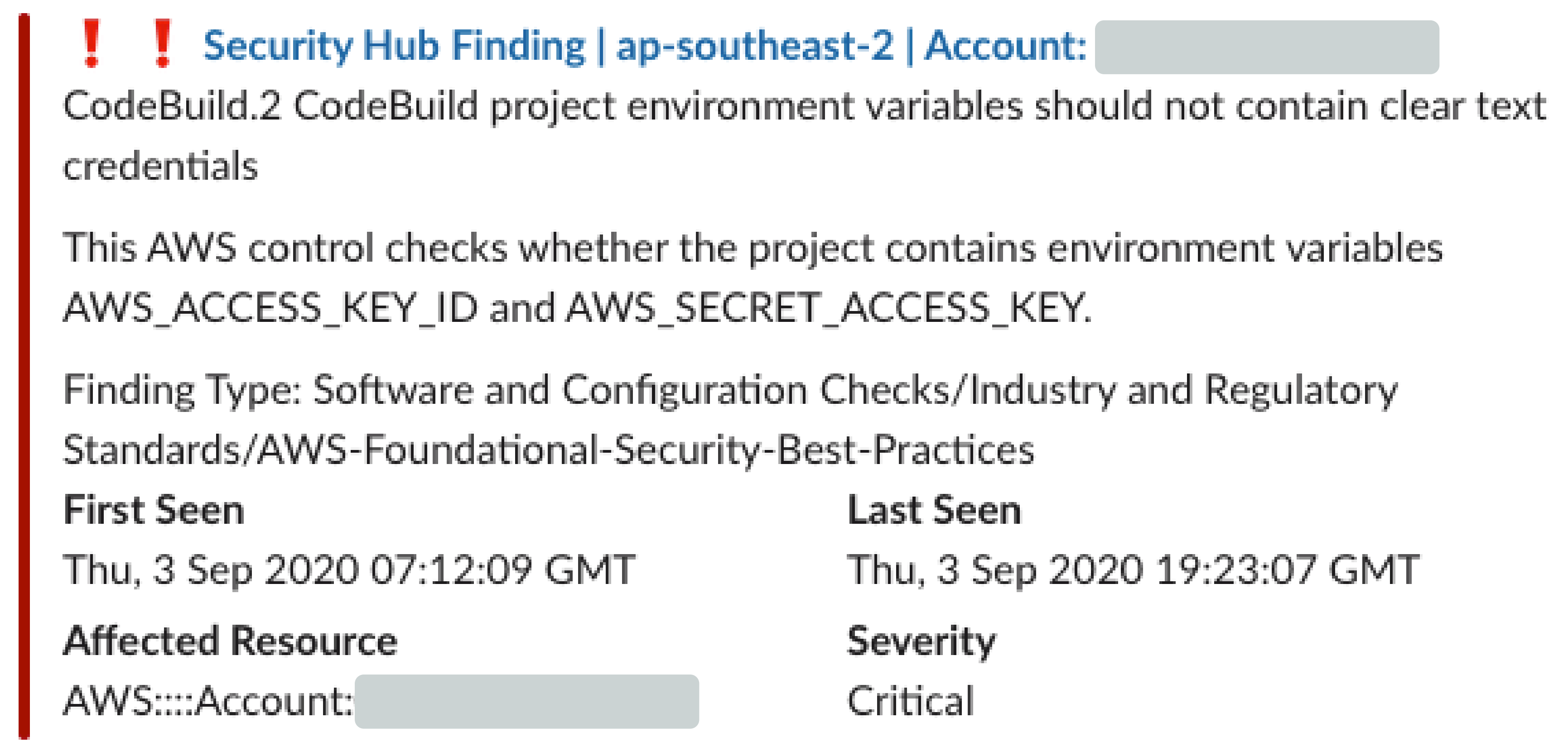
PCI.S3.2 S3 buckets should prohibit public read access

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:[redacted]	Critical

Security Hub CodeBuild notifications



❗ ❗ Security Hub Finding | ap-southeast-2 | Account: [redacted]

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
Thu, 3 Sep 2020 07:12:09 GMT

Last Seen
Thu, 3 Sep 2020 19:23:07 GMT

Affected Resource
AWS::::Account:[redacted]

Severity
Critical

Let’s recap

Resources

Resource Links

AWS Shared Responsibility Model :
https://aws.amazon.com/compliance/shared-responsibility-model/

AWS Well-Architected Framework:
https://aws.amazon.com/architecture/well-architected/
https://aws.amazon.com/blogs/aws/new-serverless-lens-in-aws-well-architected-tool/

Enabling AWS Security Hub integration with AWS Chatbot:
https://aws.amazon.com/blogs/security/enabling-aws-security-hub-integration-with-aws-chatbot/

AWS Serverless Security Workshop:
https://github.com/aws-samples/aws-serverless-security-workshop

Visit the Modern Applications Resource Hub for more resources

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

- Build modern applications on AWS e-book
- Build mobile and web apps faster e-book
- Modernize today with containers on AWS e-book
- Adopting a modern Dev+Ops model e-book
- Modern apps need modern ops e-book
- Determining the total cost of ownership: Comparing Serverless and Server-based technologies paper
- Continuous learning, continuous modernization e-book
- … and more!

https://bit.ly/3yfOvbK

Visit resource hub »

AWS Training and Certification

Accelerate modernization with continuous learning

Free digital courses, including:
Architecting serverless solutions
Getting started with DevOps on AWS

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

Hands-on classroom training (available virtually) including:
Running containers on Amazon Elastic Kubernetes Service (Amazon EKS)
Advanced developing on AWS

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

Take Developer and DevOps training today

Learn more about Modernization training for you and your team

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

Thank you!