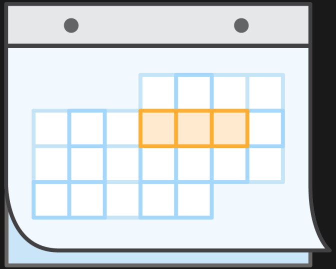
Implementing DevSecOps

Evolving Security Culture

Iolaire McKinnon
Security, Risk and Compliance, Amazon Web Services
2017-04-20

Agenda

- What is DevSecOps?
- Where do we Start?
- Demo! DevSecOps Pipeline on AWS
- Key Takeaways



What is DevOps?

Cultural Philosophy + Practices + Tools

What is DevSecOps?

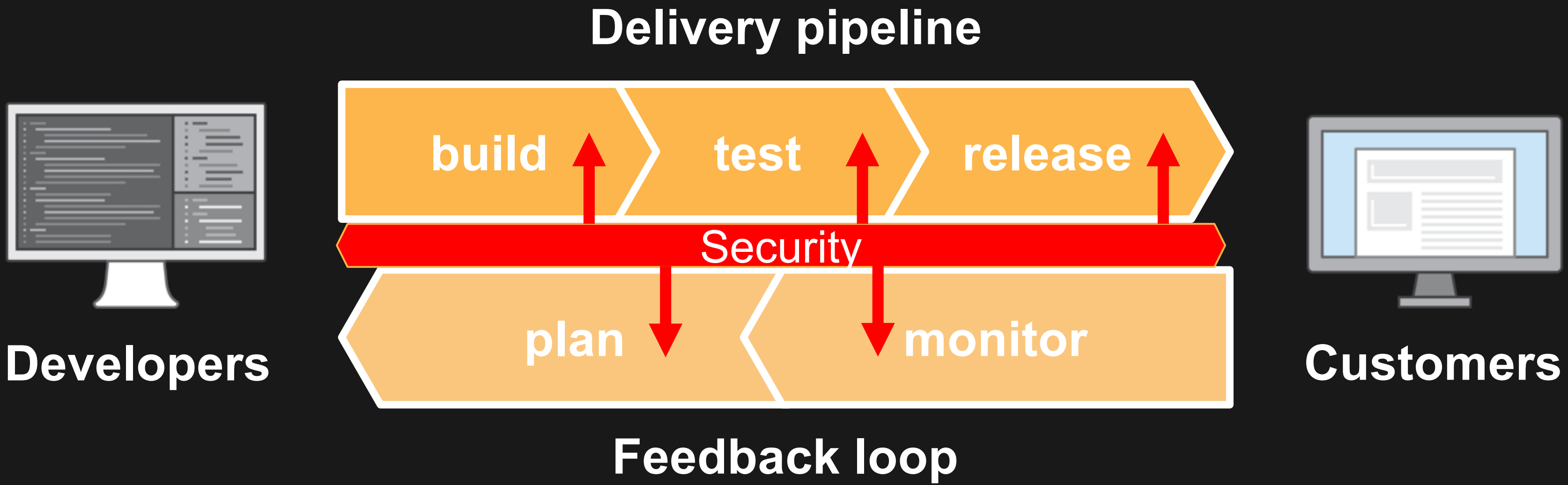
Automated + Continuous + Visible

How to win at DevSecOps

- Customer (Developer) mindset
- Successful DevSecOps is about not blocking a rapid pace of innovation.

- Security is built in, automated, and up to date.
- Security as a (self) service, but with strong audit
- Moving faster than Developers

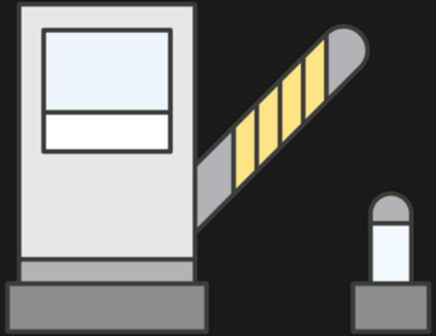
Why this Matters – Agility!



DevOps = Efficiencies that speed up this lifecycle
DevSecOps = Validate building blocks without slowing lifecycle

It was Secure when it was signed off…

- DevOps is agile, and changes happen fast
- How do we ensure continuity of Security?
- Interesting security events should be broadly visible
- Extreme visibility can lead to amplification of old problems:
    - Increased Monitoring Noise
    - Identifying relevant events: Signal vs Noise



Where to Start?

Trusted Advisor

- Catches common account misconfigurations

CloudTrail and CloudWatch

- Logs, Alerts, and Events

AWS Config Rules

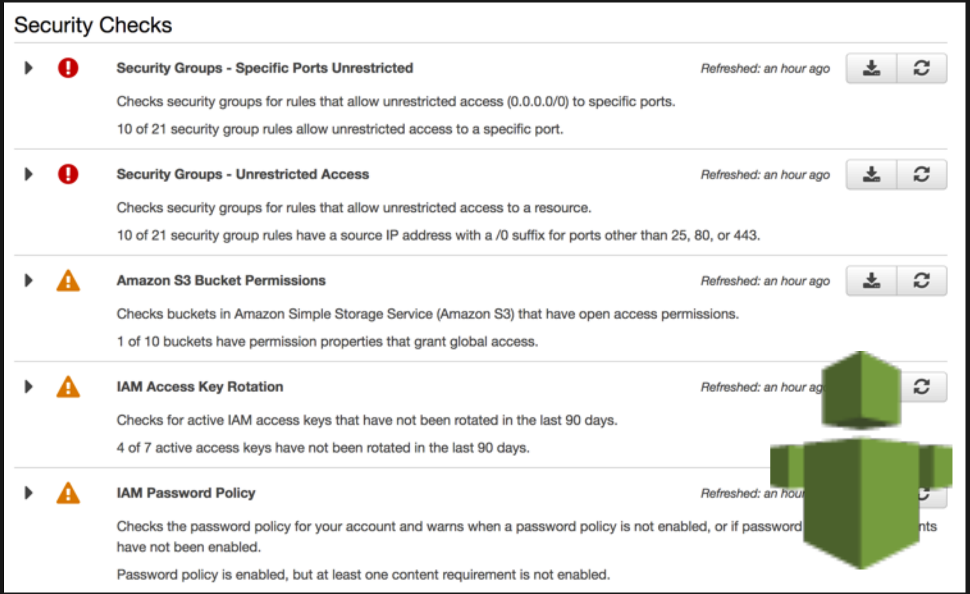
- Audit change and respond to non-compliance

AWS Trusted Advisor

- ✓ Real-time status
- ✓ Weekly reports
- ✓ Core checks are free
- ✓ Rule events can raise notifications

With a paid support plan:

- ✓ AWS Support API access
- ✓ Full access to hundreds of checks



Security Checks

▸ ❗ **Security Groups - Specific Ports Unrestricted** *Refreshed: an hour ago*

Checks security groups for rules that allow unrestricted access (0.0.0.0/0) to specific ports.

10 of 21 security group rules allow unrestricted access to a specific port.

▸ ❗ **Security Groups - Unrestricted Access** *Refreshed: an hour ago*

Checks security groups for rules that allow unrestricted access to a resource.

10 of 21 security group rules have a source IP address with a /0 suffix for ports other than 25, 80, or 443.

▸ ⚠ **Amazon S3 Bucket Permissions** *Refreshed: an hour ago*

Checks buckets in Amazon Simple Storage Service (Amazon S3) that have open access permissions.

1 of 10 buckets have permission properties that grant global access.

▸ ⚠ **IAM Access Key Rotation** *Refreshed: an hour ag*

Checks for active IAM access keys that have not been rotated in the last 90 days.

4 of 7 active access keys have not been rotated in the last 90 days.

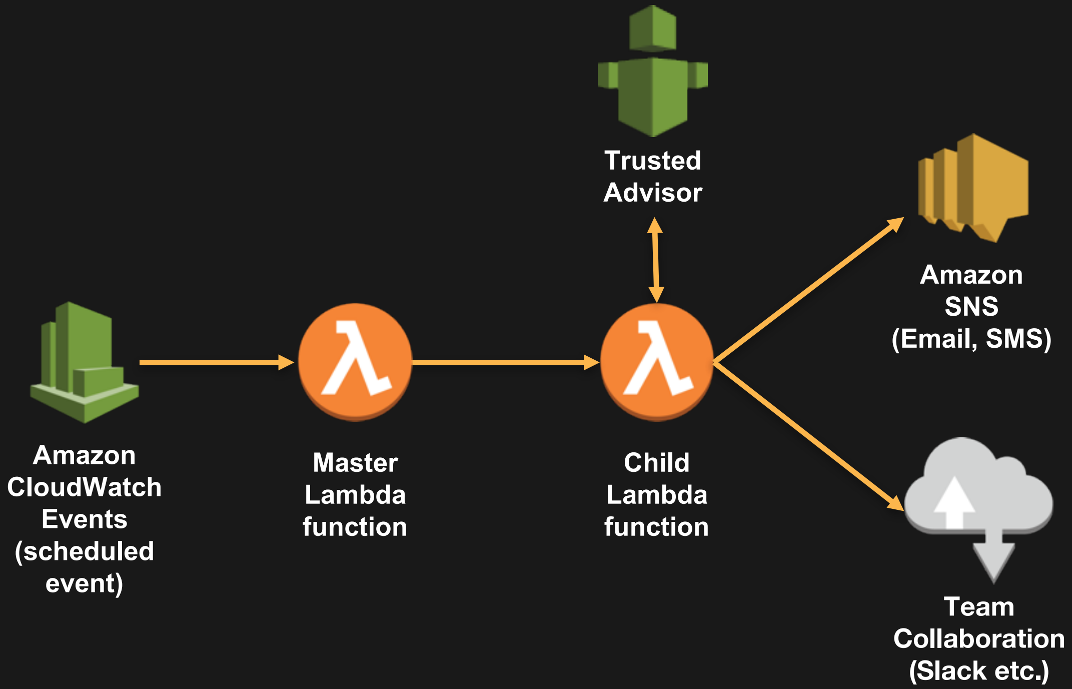
▸ ⚠ **IAM Password Policy** *Refreshed: an hou*

Checks the password policy for your account and warns when a password policy is not enabled, or if password nts have not been enabled.

Password policy is enabled, but at least one content requirement is not enabled.

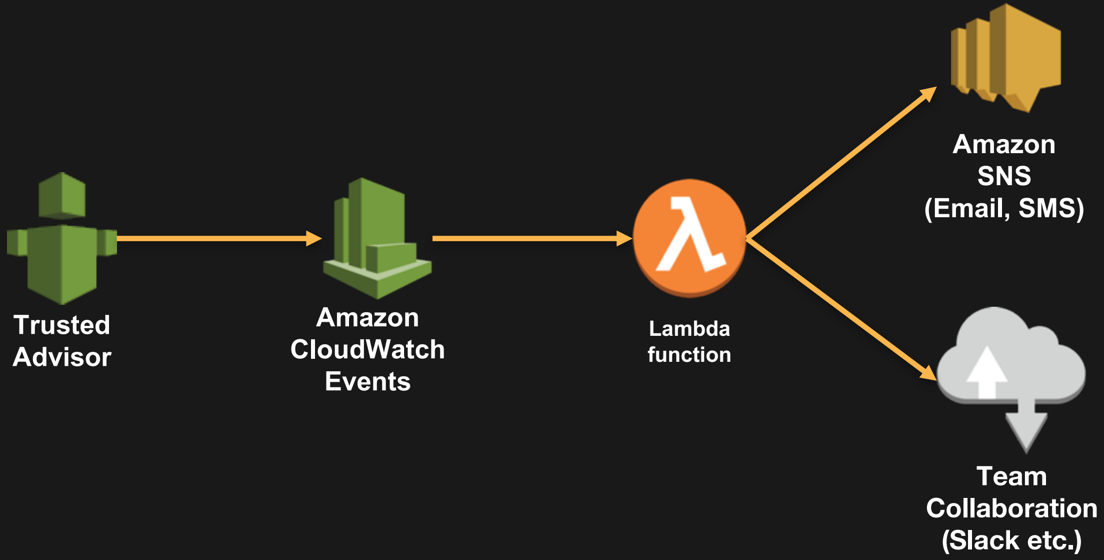
You can use CloudWatch Events to detect and react to changes in the status of Trusted Advisor checks.

Example: Trusted Advisor Polling



https://github.com/awslabs/aws-limit-monitor/

Example: Trusted Advisor Events



http://docs.aws.amazon.com/awssupport/latest/user/cloudwatch-events-ta.html

Example: AWS CloudTrail & CloudWatch Logs

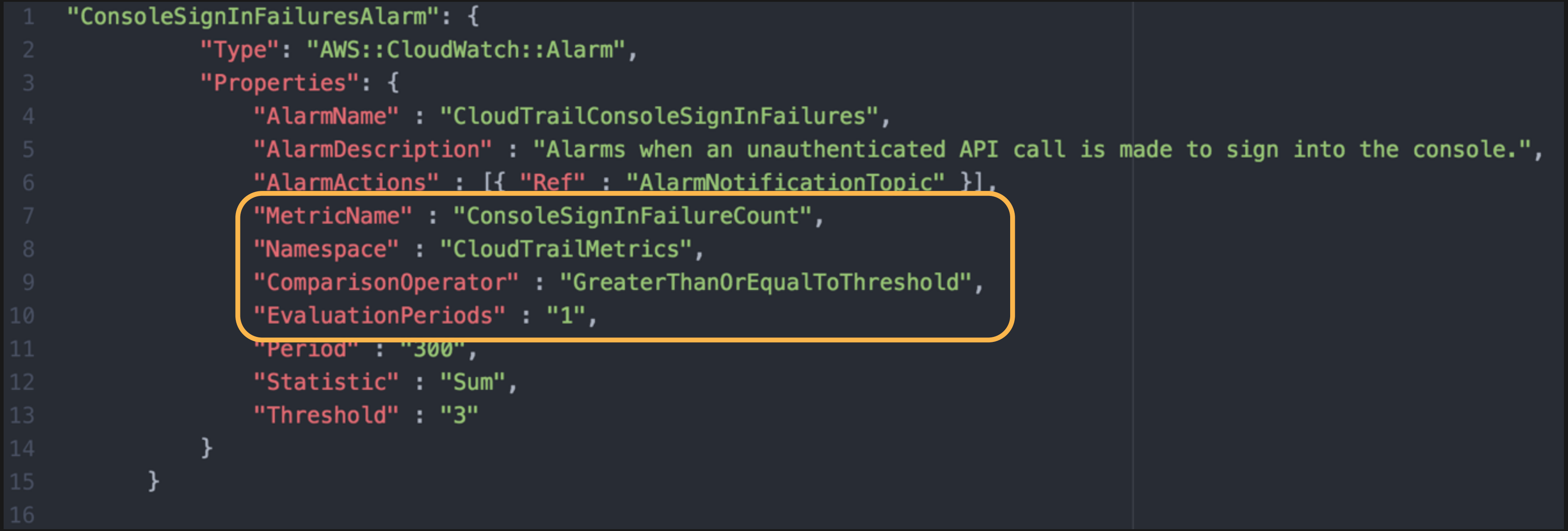
AWS CloudTrail is:
A service that enables governance, compliance, operational auditing, and risk auditing of your AWS account

CloudTrail feeds into CloudWatch Logs

What this enables:

- Log, continuously monitor, and retain events related to API calls across your AWS infrastructure.
- Provide a history of AWS API calls for your account.
- Pass events into your existing tools for further review
- Alarm on events which are relevant for your cloud security

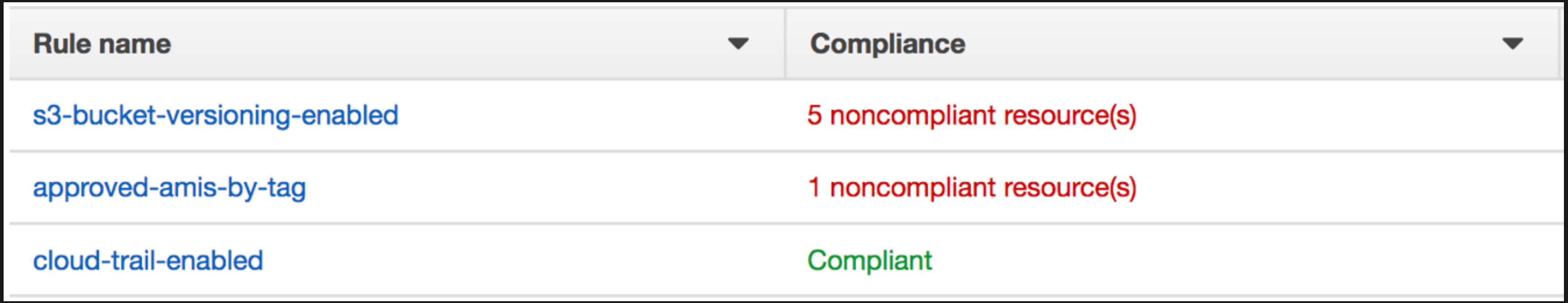
Example: CloudTrail / CloudWatch Logs



```
"ConsoleSignInFailuresAlarm": {
          "Type": "AWS::CloudWatch::Alarm",
          "Properties": {
              "AlarmName" : "CloudTrailConsoleSignInFailures",
              "AlarmDescription" : "Alarms when an unauthenticated API call is made to sign into the console.",
              "AlarmActions" : [{ "Ref" : "AlarmNotificationTopic" }],
              "MetricName" : "ConsoleSignInFailureCount",
              "Namespace" : "CloudTrailMetrics",
              "ComparisonOperator" : "GreaterThanOrEqualToThreshold",
              "EvaluationPeriods" : "1",
              "Period" : "300",
              "Statistic" : "Sum",
              "Threshold" : "3"
          }
      }
```

http://docs.aws.amazon.com/awscloudtrail/latest/userguide/use-cloudformation-template-to-create-cloudwatch-alarms.html

Example: Config Rules

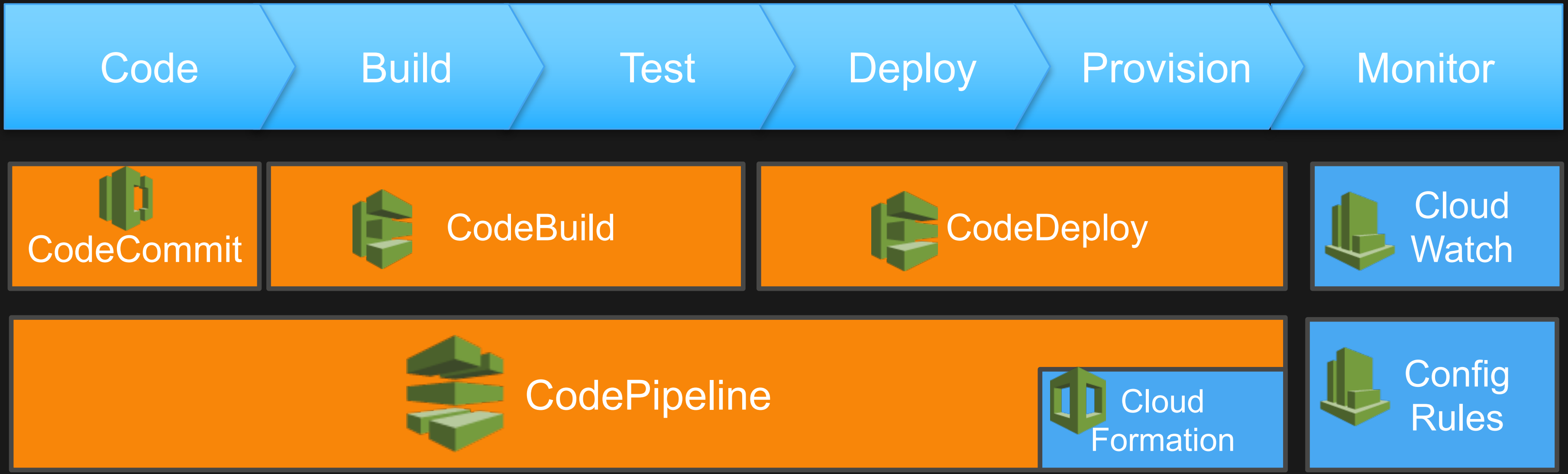


Rule name	Compliance
s3-bucket-versioning-enabled	5 noncompliant resource(s)
approved-amis-by-tag	1 noncompliant resource(s)
cloud-trail-enabled	Compliant

Many templates in AWS Console

Other Examples:
https://github.com/awslabs/aws-config-rules
https://github.com/awslabs/aws-security-benchmark

DevOps and CI/CD



Code

Build

Test

Deploy

Provision

Monitor

CodeCommit

CodeBuild

CodeDeploy

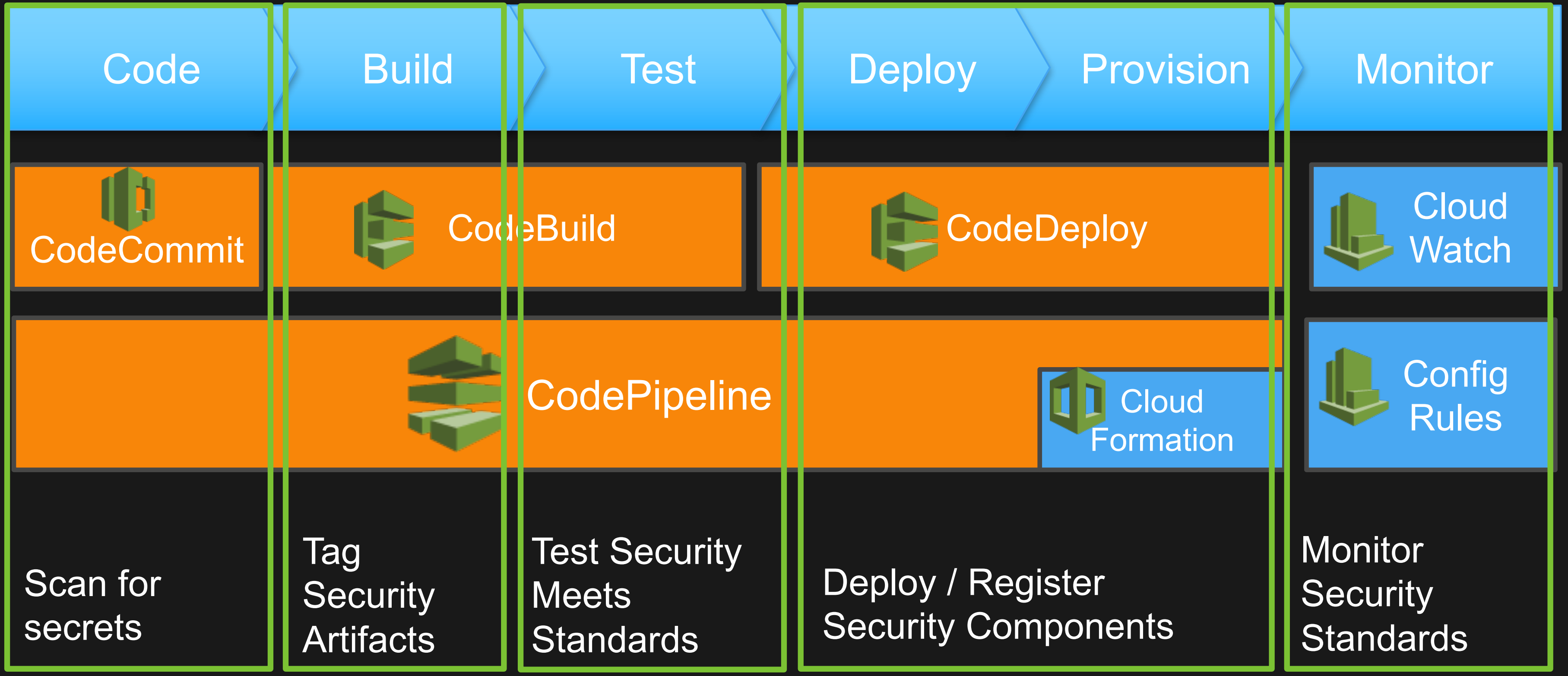
Cloud Watch

CodePipeline

Cloud Formation

Config Rules

DevSecOps: Automated, Continuous & Visible



Code

Build

Test

Deploy

Provision

Monitor

CodeCommit

CodeBuild

CodeDeploy

Cloud Watch

CodePipeline

Cloud Formation

Config Rules

Scan for secrets

Tag Security Artifacts

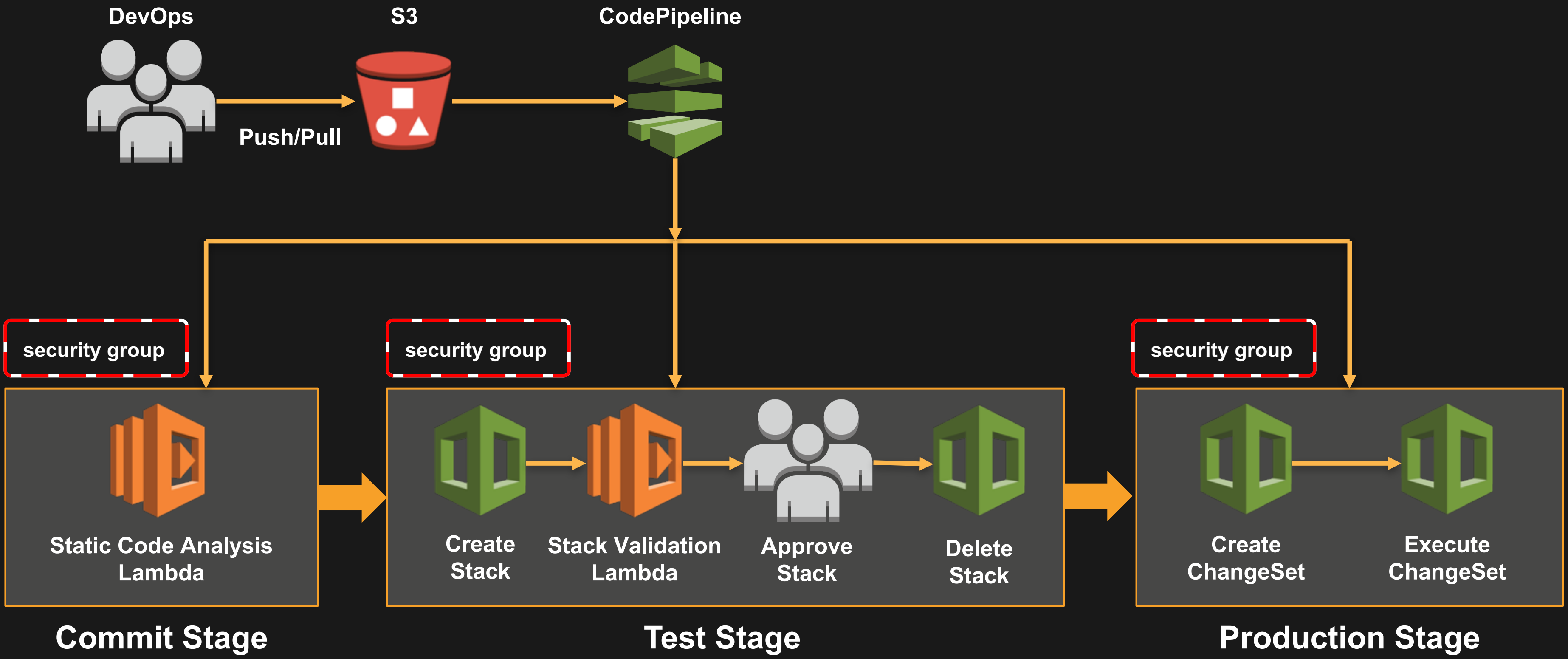
Test Security Meets Standards

Deploy / Register Security Components

Monitor Security Standards

Demo Time!
Automated Governance

Conceptual View



https://aws.amazon.com/blogs/devops/implementing-devsecops-using-aws-codepipeline/

Demo Resources

These resources are being used in this example:

An AWS CloudFormation template to create the demo pipeline.

A Lambda function to perform the static code analysis of the CloudFormation template.

A Lambda function to perform dynamic stack validation for the security groups in scope.

An S3 bucket as the sample code repository.

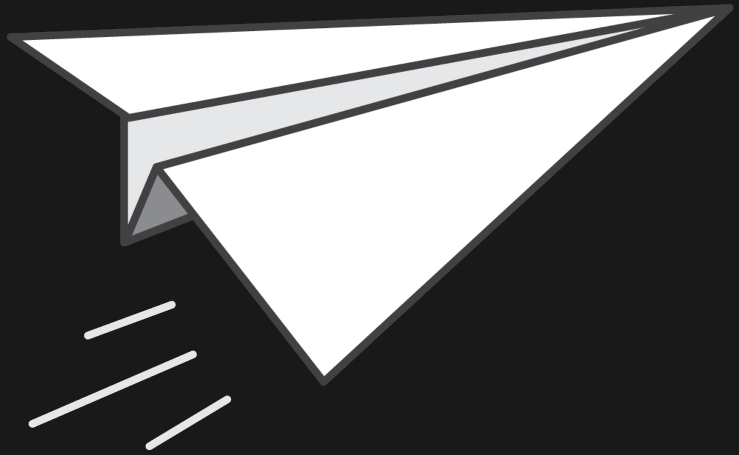
An AWS CloudFormation source template file to create the security groups.

Two VPCs to deploy the test and production security groups.

Taking Flight

Now, Solve YOUR challenges

- Developers are the Customer
- Using Agile Methods/Tools
- Build Security that is



Automated + Continuous + Visible

Resources

AWS
Trusted Advisor
http://bit.ly/AWSTrust

AWS
Config Rules
http://bit.ly/AWSRulz

Implementing
DevSecOps
http://bit.ly/AWSDSO

Thank you!

iolaire@amazon.com