AWS re:Invent

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

AMZ303

Amazon’s approach to DevSecOps practices

Nat Natarajan (he/him)
Senior Manager, Solution Architects
AWS

Radu Malliu (he/him)
Senior Solution Architect
AWS

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



Nat Natarajan



Radu Malliu

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

Agenda

- Security practices at Amazon
- What is DevSecOps
- Amazon’s DevSecOps journey
- How Amazon practices DevSecOps
- Key takeaways
- Q&A and discussion

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

“At AWS, Security is the top priority”

Stephen Schmidt

VP and CISO, AWS

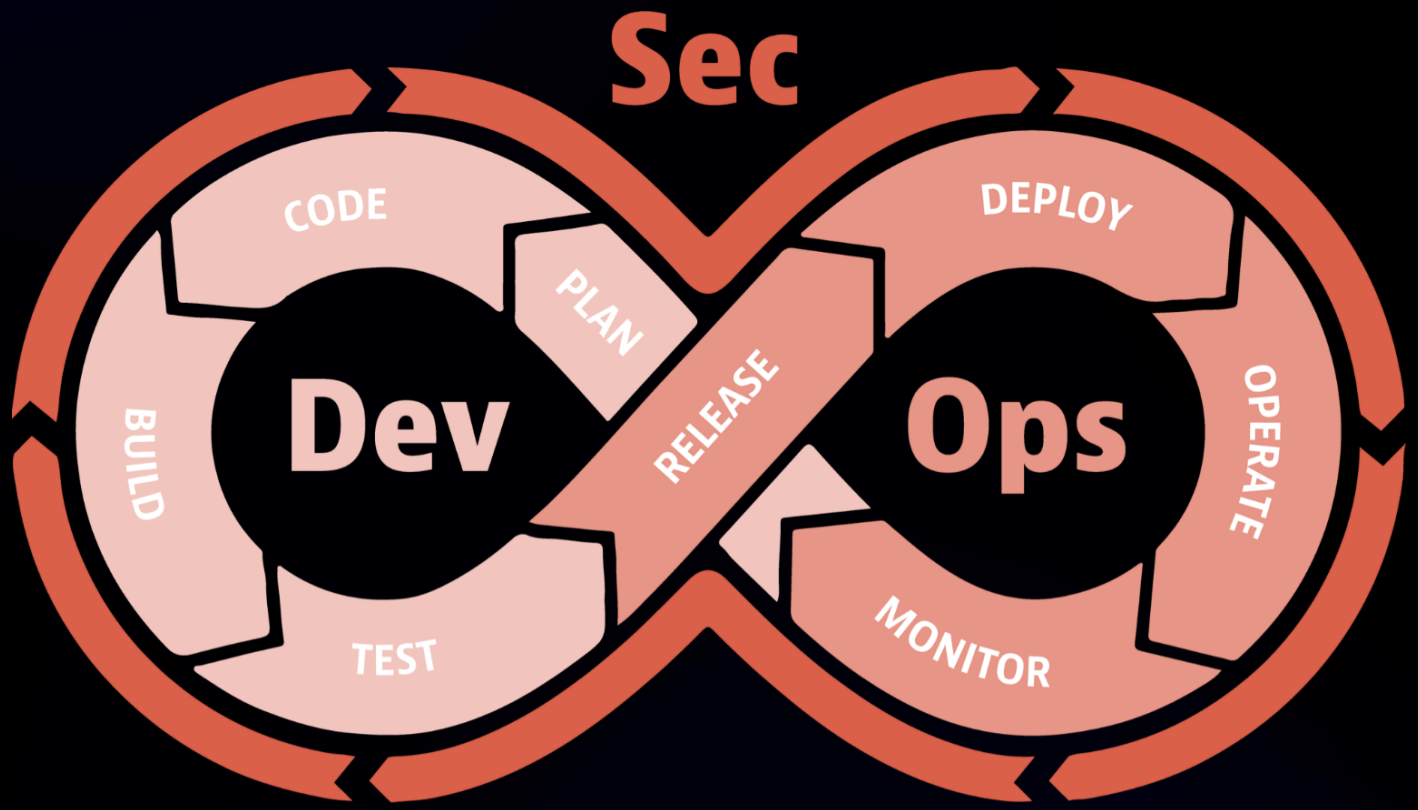
“Security is everyone's job now, not just the security teams”

Werner Vogels

CTO, Amazon Web Services

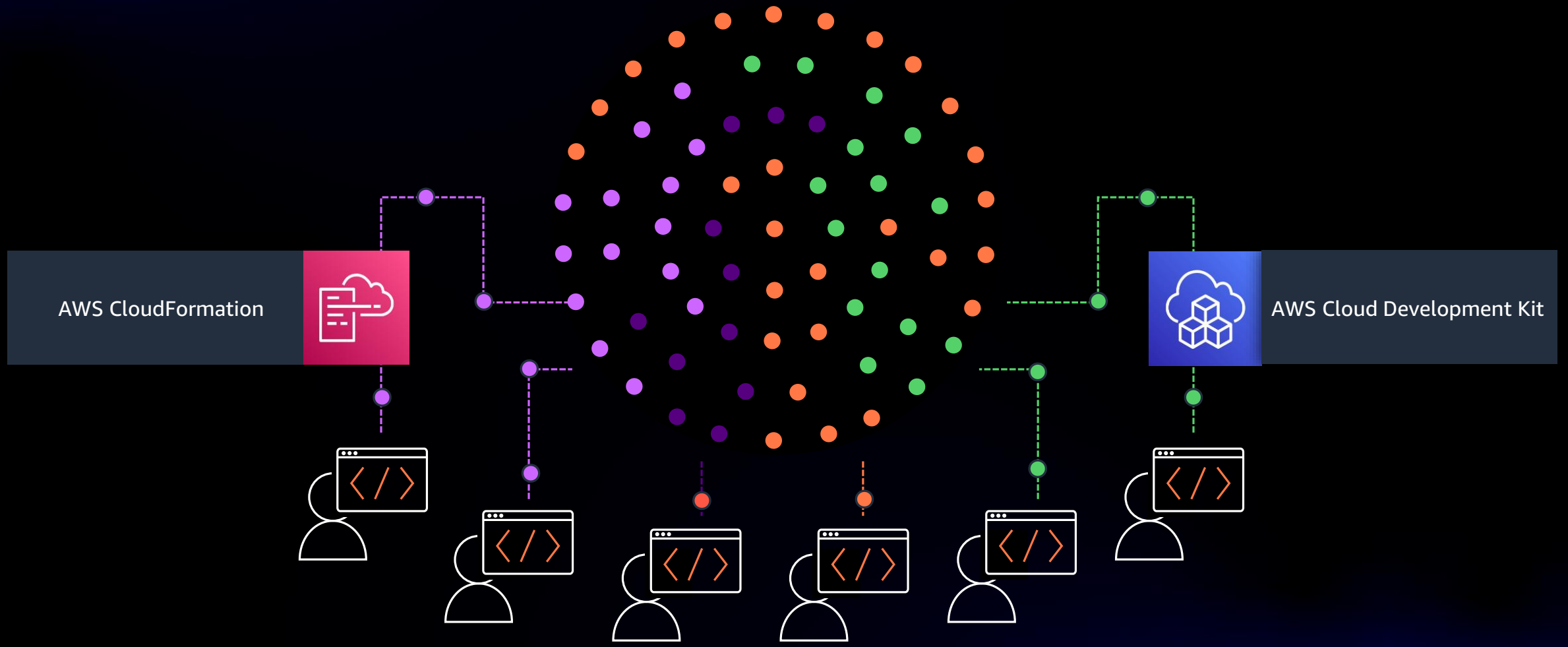
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is DevSecOps



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

DevSecOps and infrastructure as code

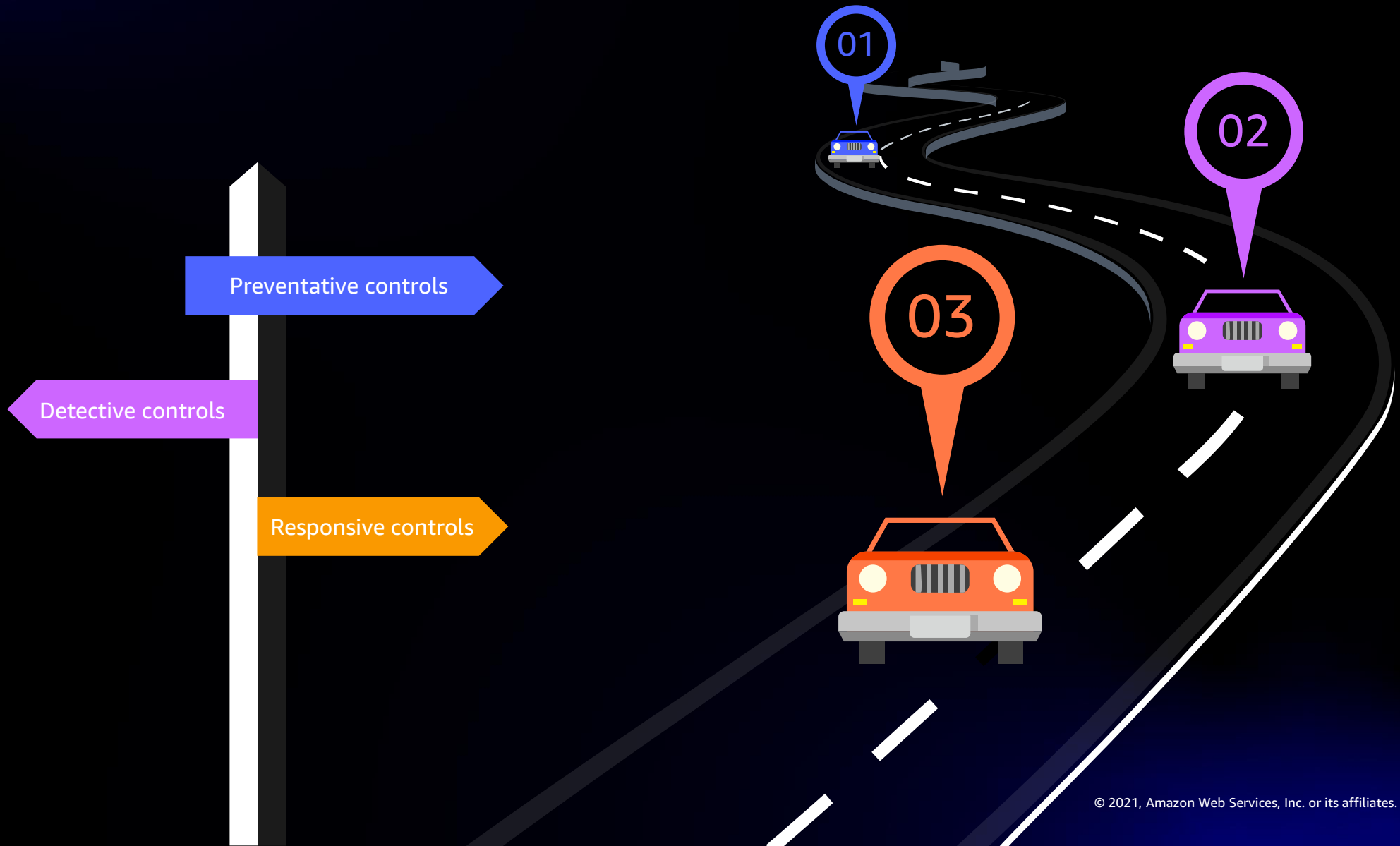


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How Amazon practices DevSecOps

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

Paving the road: Guardrails not gates



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

How Amazon practices DevSecOps

Write



AWS CDK



AWS CloudFormation

- Use a library of secure-by-default constructs
- Implemented in CDK
- Allows engineers to focus on adding value, since security configurations are delivered out of the box

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

Write time – Secure-by-default constructs

```
const bucket = new SecureBucket(this, 'Bucket', {
        encryption: s3.BucketEncryption.KMS,
        enforceSSL: true
});

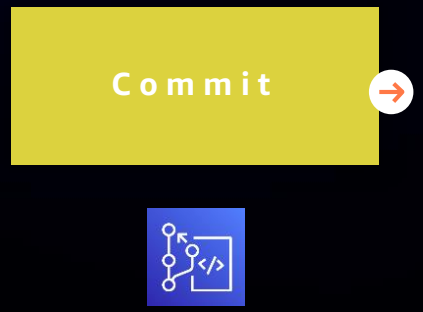
mote.AssertRestricted(bucket);
```

```
Error: The resource cannot handle Restricted data: Buckets containing HighlyConfidential+ data must enforce transport security.

BUILD SUCCEEDED
```

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

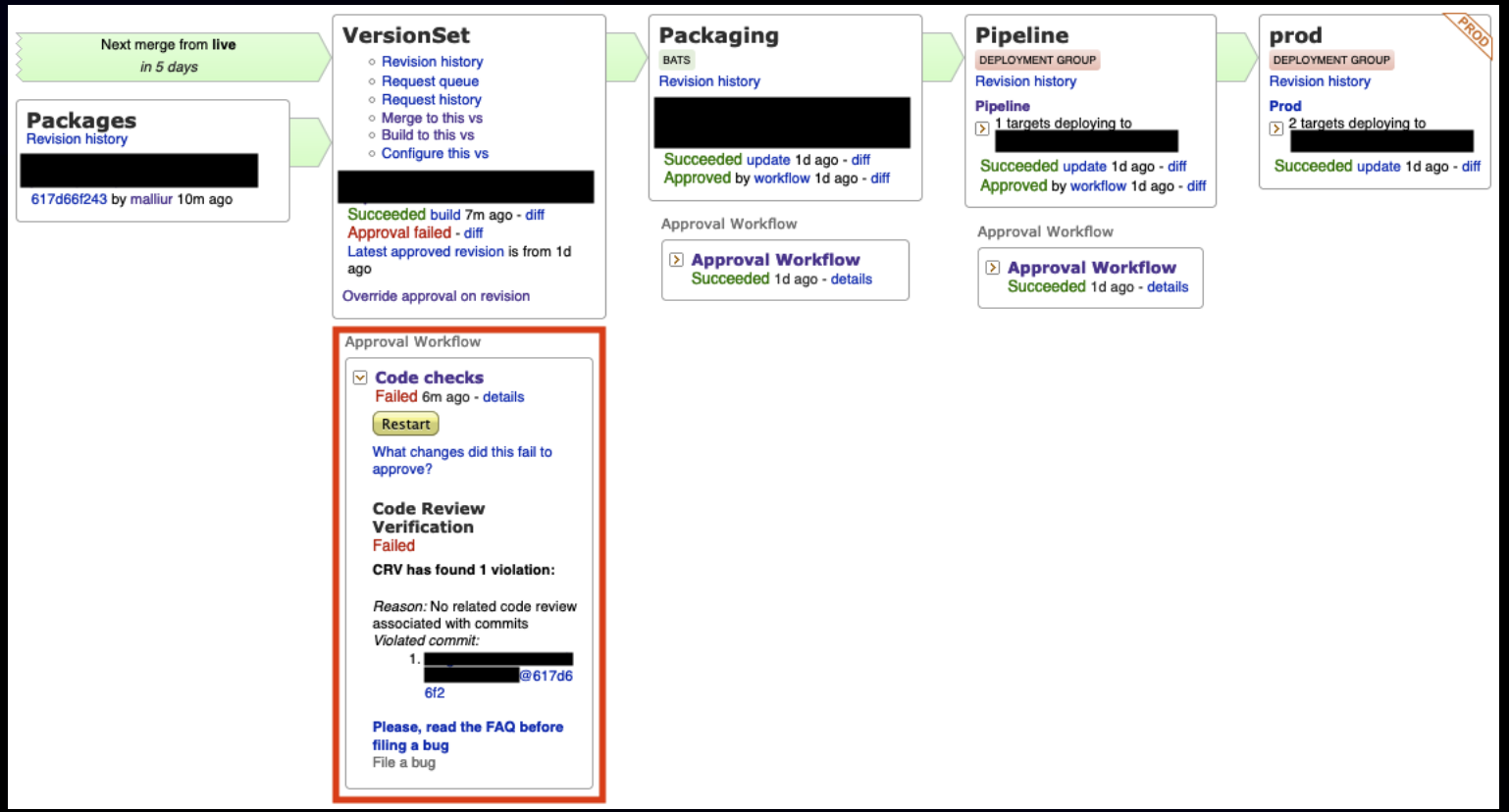
How Amazon practices DevSecOps



- Integrate checks in pipelines that verify all changes have a matching review
- Can be implemented with CodeCommit and AWS Lambda
- Ensures all changes are vetted via a review process

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

Commit time – Ensure change reviews



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

How Amazon practices DevSecOps



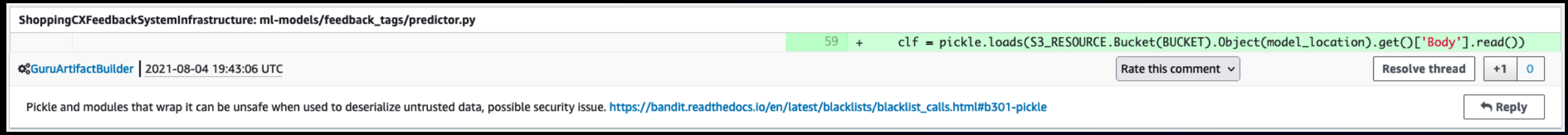
- Implement static code analysis to scan for inefficient code, do linting, etcetera
- Implemented via Code Guru Reviewer
- Ensures that code that does not meet the bar is caught before release

aws

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

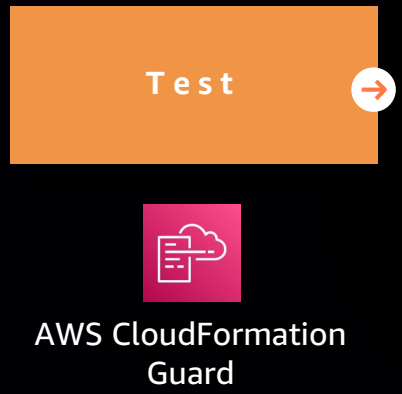
Build time – Static analysis





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

How Amazon practices DevSecOps



- Validate generated CloudFormation templates against set of security rules (for example, no security groups allowing ingress from /0 CIDR)
- Implemented via CloudFormation Guard
- Ensures that any deviations from best practices around resource configurations are caught at test time

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

Test time – Scanning of resource definitions

```
const sg = new SecurityGroup(this, 'SG', {
        vpc: vpc
});

sg.addIngressRule(
        Peer.anyIpv4(),
        Port.tcp(80)
);
```

RuleName	Status	Message	Context	Resource
aws_ec2_security_group_should_not_be_overly_permissive	FAIL	Security Group should not b overly permissive	undefined	"{\"Resolved\":{\"String\":[\"/Resources/SGADB53937/Properties/SecurityGroupIngress/0/CidrIp\",\"0.0.0.0/0\"]}}"

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

CloudFormation Guard – Rule example

```
# Rule Intent: No Security Groups have a 0.0.0.0/0 ingress rule

# Expectations:
# a) SKIP: when there are no security groups with ingress rules
# b) FAIL: when any ingress rule specifies a 0.0.0.0/0 or ::/0 IP range
# c) PASS: when no ingress rules specify a 0.0.0.0/0 or ::/0 IP range

# Select all SecurityGroup resources from incoming template (payload)
let sg_resources = Resources.*[ Type == 'AWS::EC2::SecurityGroup' ]

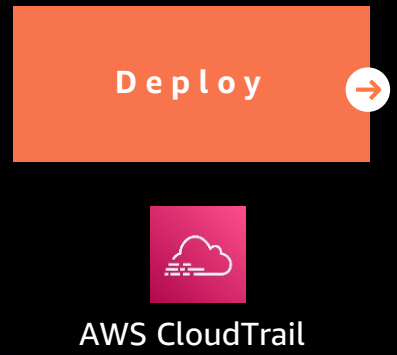
# Fetch all security groups with an ingress rule
let ingress_sg_resources = %sg_resources[
  Properties.SecurityGroupIngress exists
]

rule aws_ec2_security_group_should_not_be_overly_permissive when %ingress_sg_resources !empty {
  let ingress_ip_ranges = %ingress_sg_resources.Properties.SecurityGroupIngress[*].CidrIp

  when %ingress_ip_ranges exists {
    %ingress_ip_ranges not in ['0.0.0.0/0', '::/0'] << Security Group should not be overly permissive >>
  }
}
```

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

How Amazon practices DevSecOps



- ✓ Validate resources at deploy-time
- ✓ Implemented via scans of CloudTrail logs
- ✓ Ensures that any deviations from best practices around resource configurations are caught at deployment time and can be flagged or remediated

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

How Amazon practices DevSecOps

- ✓ Set up rules to ensure resources remain compliant with best practices for the duration of their lifecycle
- ✓ Implemented via AWS Config
- ✓ Ensures that any deviation from evolving best practices are surfaced to service owners

Live



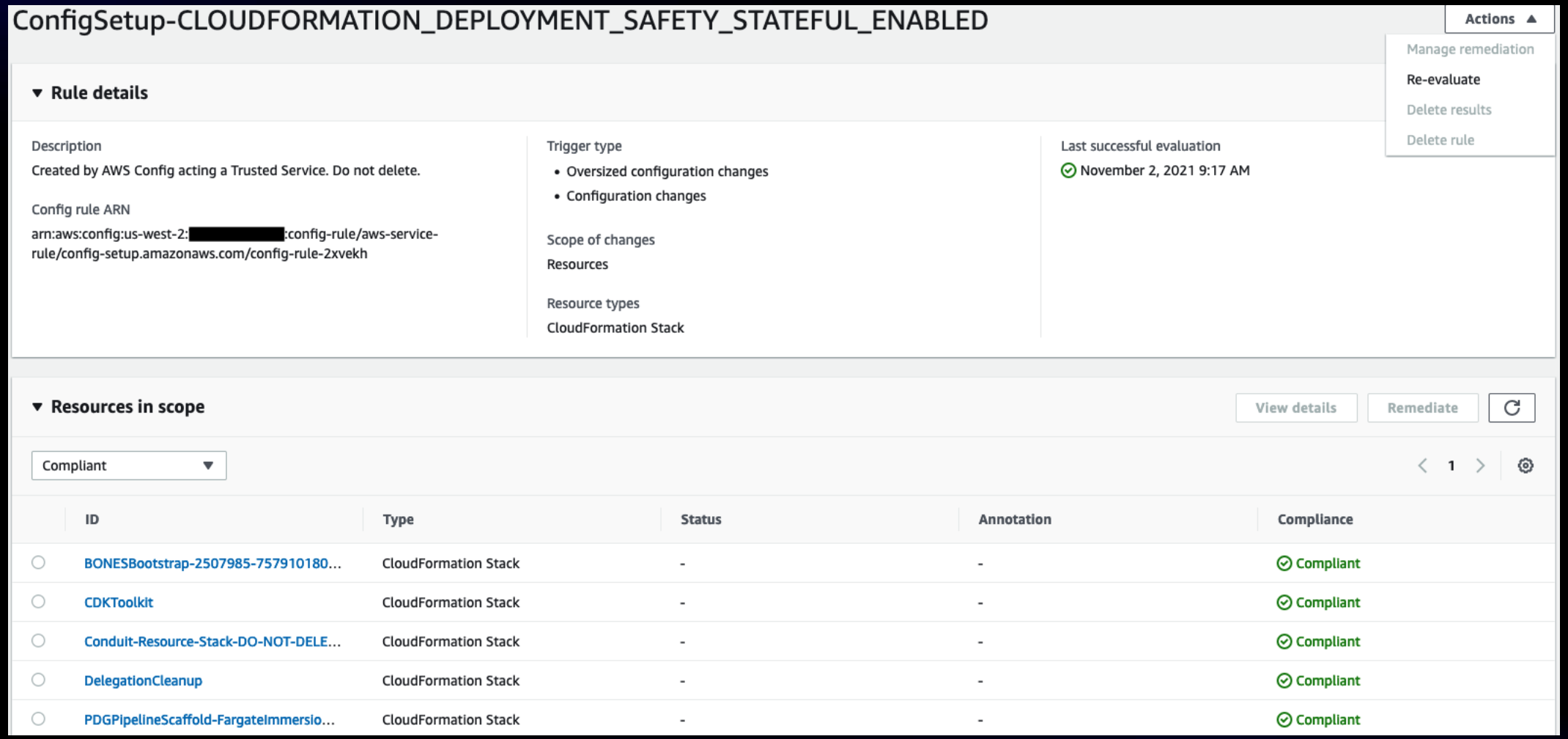
AWS CloudWatch



AWS Config

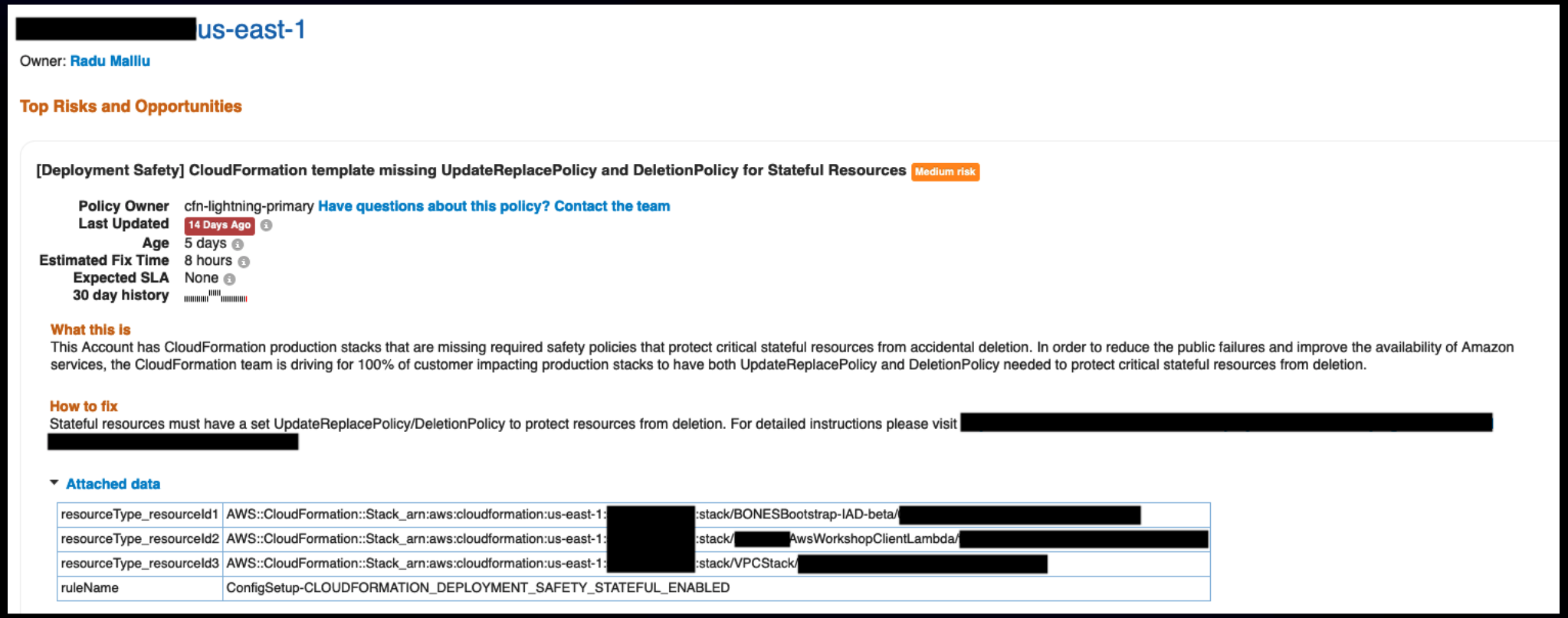
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Live – On-going review and remediation



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

Live – On-going review and remediation



[redacted]us-east-1

Owner: Radu Maliiu

Top Risks and Opportunities

[Deployment Safety] CloudFormation template missing UpdateReplacePolicy and DeletionPolicy for Stateful Resources Medium risk

Policy Owner	cfn-lightning-primary **Have questions about this policy? Contact the team**
Last Updated	14 Days Ago
Age	5 days
Estimated Fix Time	8 hours
Expected SLA	None
30 day history	

What this is

This Account has CloudFormation production stacks that are missing required safety policies that protect critical stateful resources from accidental deletion. In order to reduce the public failures and improve the availability of Amazon services, the CloudFormation team is driving for 100% of customer impacting production stacks to have both UpdateReplacePolicy and DeletionPolicy needed to protect critical stateful resources from deletion.

How to fix

Stateful resources must have a set UpdateReplacePolicy/DeletionPolicy to protect resources from deletion. For detailed instructions please visit [redacted]

Attached data

resourceType_resourceId1	AWS::CloudFormation::Stack_arn:aws:cloudformation:us-east-1:[redacted]:stack/BONESBootstrap-IAD-beta/[redacted]
resourceType_resourceId2	AWS::CloudFormation::Stack_arn:aws:cloudformation:us-east-1:[redacted]:stack/[redacted]AwsWorkshopClientLambda/[redacted]
resourceType_resourceId3	AWS::CloudFormation::Stack_arn:aws:cloudformation:us-east-1:[redacted]:stack/VPCStack/[redacted]
ruleName	ConfigSetup-CLOUDFORMATION_DEPLOYMENT_SAFETY_STATEFUL_ENABLED

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

Key takeaways from Amazon practices



Treat infrastructure as code



Define guardrails not gates



Establish security controls

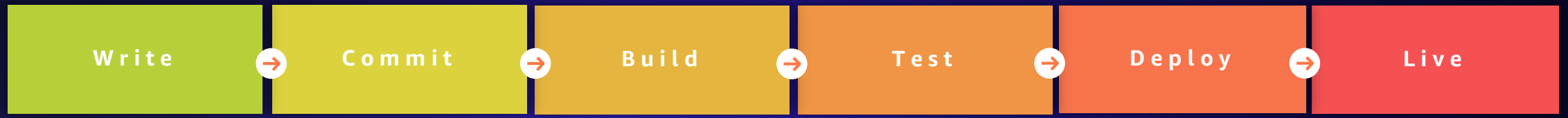


Automate as much as possible



Wrap security around pipelines

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



AWS CDK

AWS CodeCommit

Amazon CodeGuru

AWS CloudFormation Guard

AWS CloudTrail

AWS CloudWatch

AWS CloudFormation

AWS Config

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

Additional resources

- Amazon’s approach to Security during Development

https://aws.amazon.com/builders-library/amazon-approach-to-security-during-development/?did=ba_card&trk=ba_card

- AWS DevSecOps Blog

https://aws.amazon.com/blogs/security/tag/devsecops/

- AWS DevOps Blog

https://aws.amazon.com/blogs/devops/

- The Amazon Builder’s Library

https://aws.amazon.com/builders-library/?cards-body.sort-by=item.additionalFields.sortDate&cards-body.sort-order=desc&awsf.filter-content-category=*all&awsf.filter-content-type=*all&awsf.filter-content-level=*all

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

Thank you!

Nat Natarajan
natnata@amazon.com

Radu Malliu
malliur@amazon.com

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