AWS

SUMMIT

Automated Compliance and Governance

Quis custodiet custodes?

Dr. Thomas Fuhrmann & Jeremias Reith
AWS Professional Services

05/18/2017

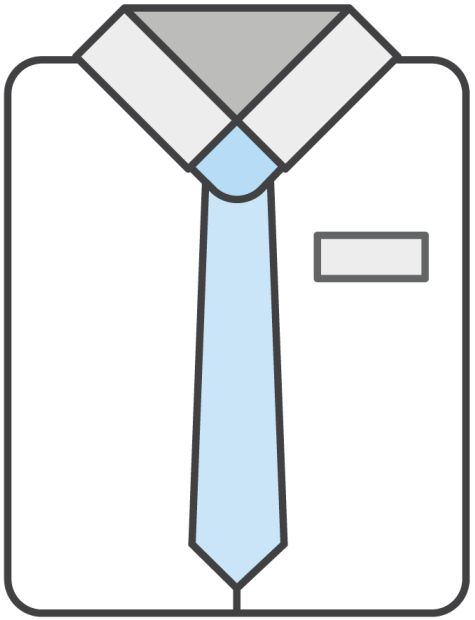
amazon web services

Quis custodiet ipsos custodes?

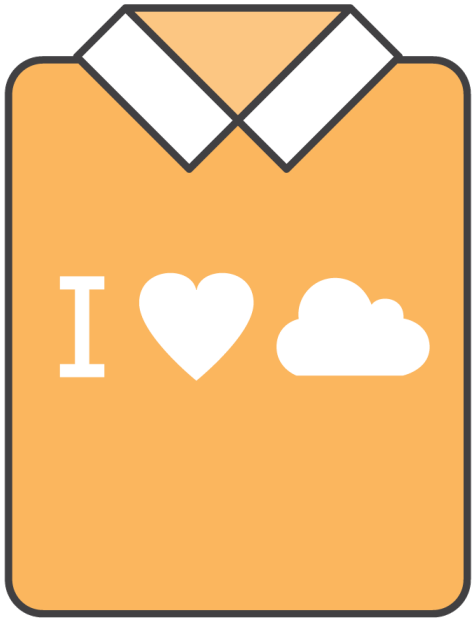
Quis custodiet ipsos custodes?

Juvenal, ca. 60 – 130 AD

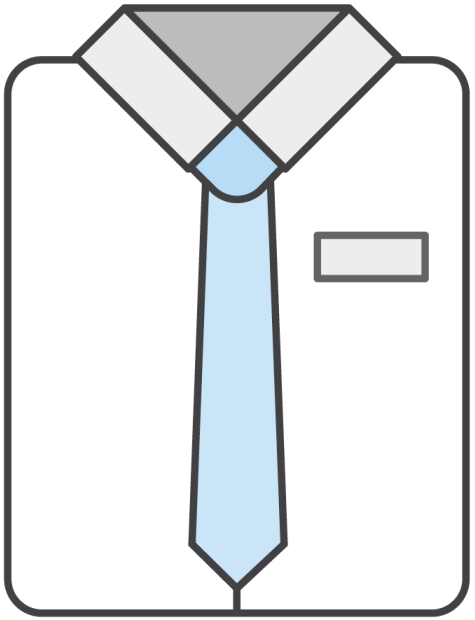
How to be compliant while still being agile?



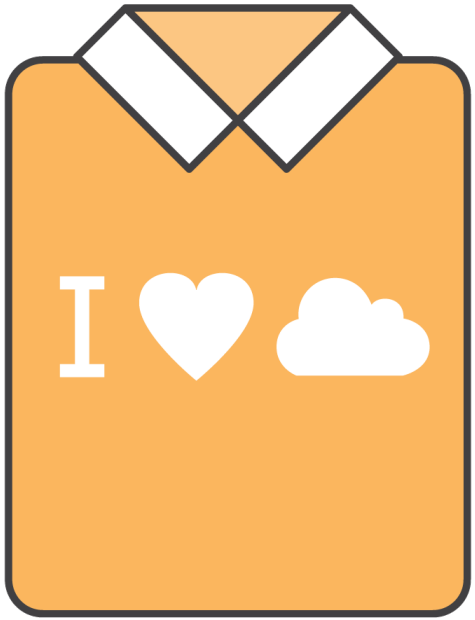
vs.



How to be compliant while still being agile?

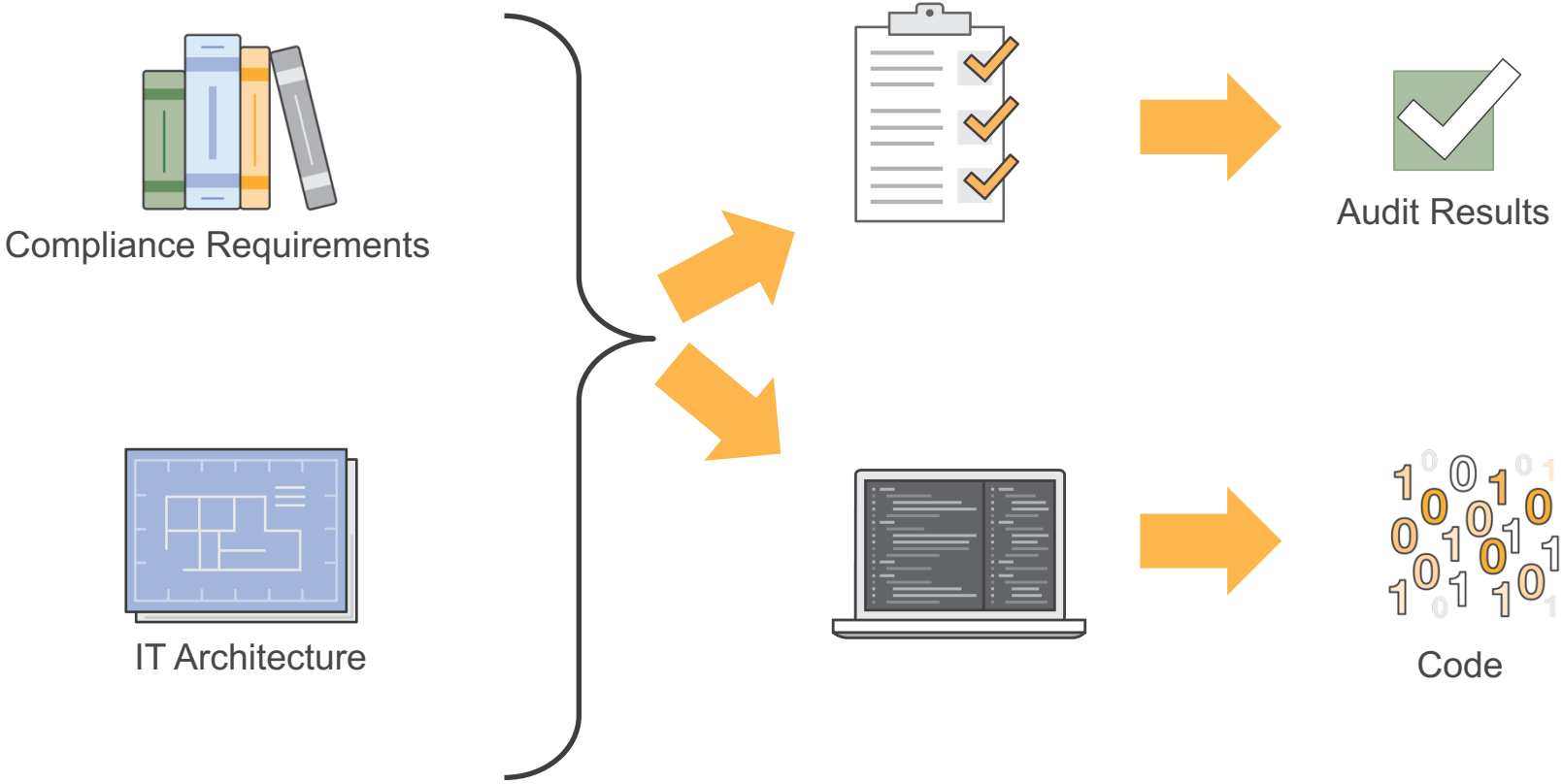


~~vs.~~

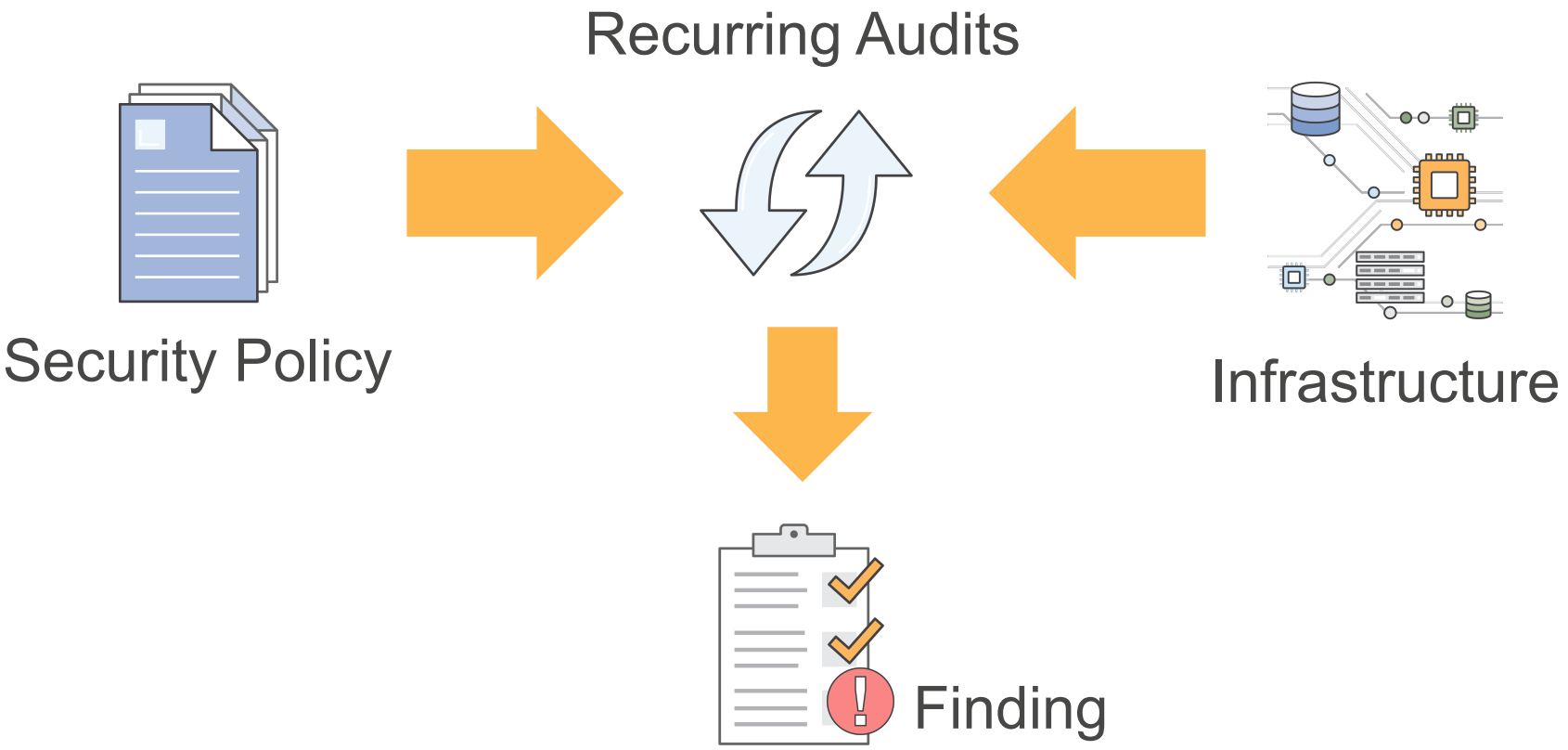


What is Test Driven Compliance?

Security and Compliance Requirements

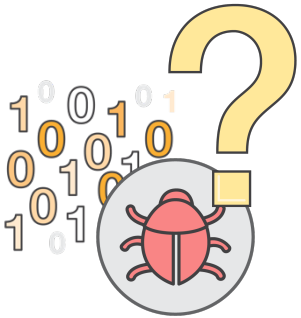


Traditional Audits are Done Manually

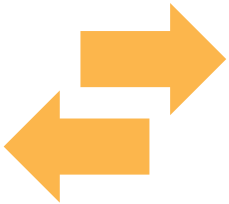


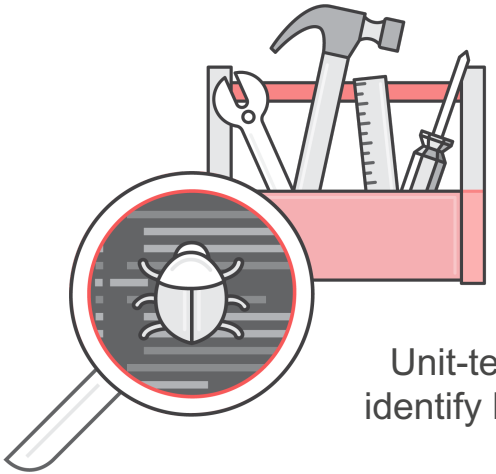

Automating
Compliance?

Unit Tests and Test-Driven Development



Code

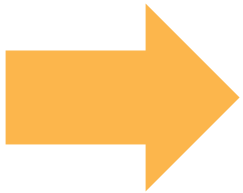




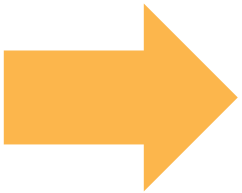
Unit-tests
identify bugs

Test-Driven Compliance: Control as Code

Risk

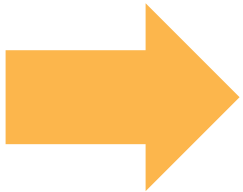


Requirement

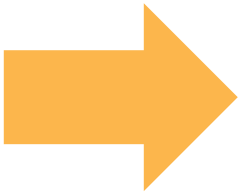


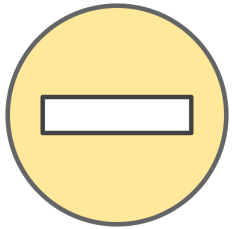
Control as Code

Data Leakage



Encryption in transit



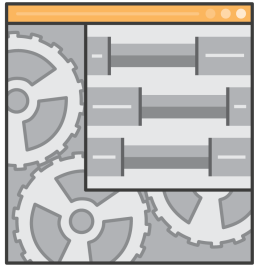


Flag insecure protocols

Continuous Delivery Pipeline for Software

Code

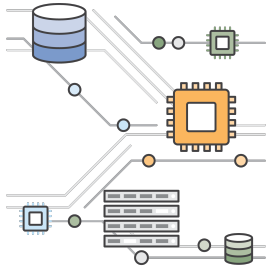
build → test → deploy



App

Continuous Delivery Pipeline for Infrastructure?

Code

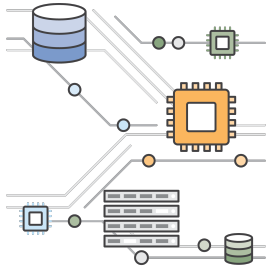


Infrastructure

Continuous Delivery Pipeline for Infrastructure

Code

build → test → deploy

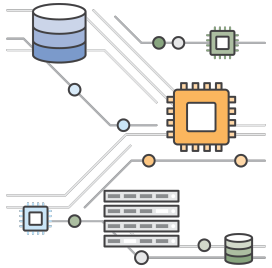


Infrastructure

Continuous Delivery Pipeline for Infrastructure

Code

build → test → deploy

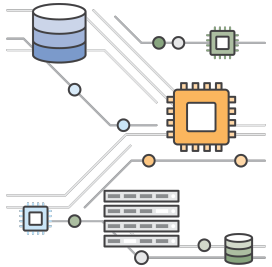


Infrastructure

Continuous Delivery Pipeline for Infrastructure

Code

build → test → audit → deploy



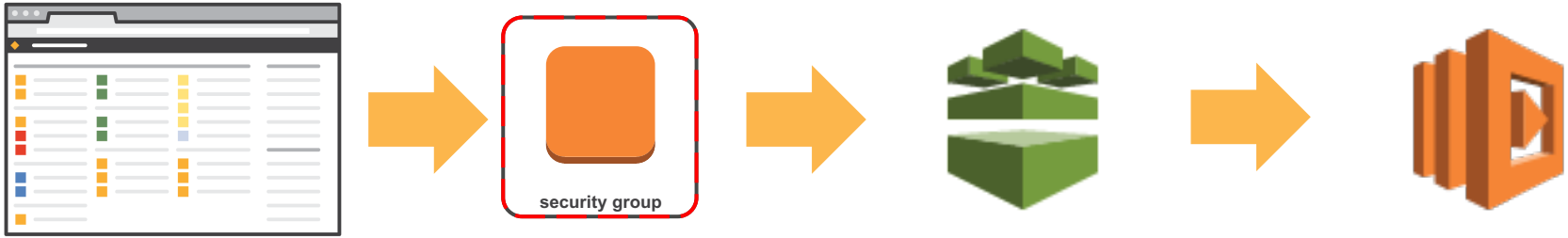
Infrastructure

Test-Driven Compliance for in-place Changes?

Change via AWS Console

HTTP (Port 80) added to Security Group

Using AWS Config Rules to Act on Changes



Change via AWS Console

HTTP (Port 80) added to Security Group

Config Rule checking Security Group

Lambda function acting on incidents

How to Leverage Config Rules to do that

EC2 Instance i-790e73c5

at June 29, 2016 9:54:21 AM CEST (UTC+02:00)

Manage resources

29th June 2016 8:18:01 AM

29th June 2016 9:42:56 AM

29th June 2016 9:52:59 AM

Now

2

2

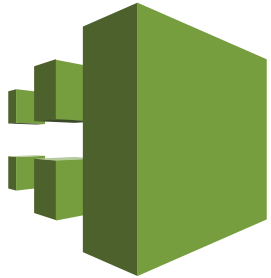
Configuration Details

View Details

Amazon Resource Name	arn:aws:ec2:eu-central-1[redacted]instance/i-790e73c5	**Instance Type**	t2.nano
Resource type	AWS::EC2::Instance	**Instance state**	running
Resource ID	i-790e73c5	**Private DNS**	ip-172-31-11-169.eu-central-1.compute.internal
Availability zone	eu-central-1b	**Private Ips**	172.31.11.169
Created at	June 29, 2016 8:15:55 AM	**Public DNS**	ec2-52-59-30-188.eu-central-1.compute.amazonaws.com
Tags (1)	Name:Demo	**AMI ID**	ami-ea26ce85

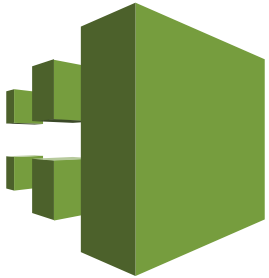
AWS Config

Example in AWS CloudTrail (1/2)




```
"awsRegion": "eu-west-1",
"eventID": ”xxxxxxxx-1234-xxxx-xxxx-xxxxxxxxxxxx",
"eventName": "AttachVolume",
"eventSource": "ec2.amazonaws.com",
"eventTime”: "2016-06-29T07:50:10Z",
"eventType": "AwsApiCall",
"eventVersion": "1.03",
"recipientAccountId": ”123456789012",
"requestID": "xxxxxxxx-4321-xxxx-xxxx-xxxxxxxxxxxx",
"requestParameters": {
    "deleteOnTermination": false,
    "device": "sdg",
    "instanceId": "i-790e73c5",
    "volumeId": "vol-5b5674e1 »
},
```

Example in AWS CloudTrail (2/2)



```
        "sourceIPAddress": "10.0.0.1",
        "userAgent": "signin.amazonaws.com",
        "userIdentity": {
            "accessKeyId": "ABC123DEF456XYZ789AB",
            "accountId": ”123456789012",
            "arn": "arn:aws:iam::123456789012:user/fuhrmt",
            "invokedBy": "signin.amazonaws.com",
            "principalId": "ABCD1234DEFG45678HIJK",
            "sessionContext": {
                "attributes": {
                    "creationDate": "2016-06-29T06:02:27Z",
                    "mfaAuthenticated": ”true"
                }
            },
            "type": "IAMUser",
            "userName": “fuhrmt"
        }
    },
```

Compliance Violation Raises Alarm

CloudTrail

records actions in S3

Lambda checks for compliance

SNS sends alarms

Example in AWS Config Rules (1/2)


```
{
    "version": "1.0",
    "invokingEvent":
"{\"configurationItemDiff\":{\"changedProperties\":{\"Relationships.0\":{\"previousValu
e\":null,\"updatedValue\":{\"resourceId\":\"i-
790e73c5\",\"resourceName\":null,\"resourceType\":\"AWS::EC2::Instance\",\"name\":\"Is
attached to Instance\"},\"changeType\":\"CREATE\"},...}",
    "ruleParameters": "{}",
    "resultToken": "...",
    "eventLeftScope": false,
    "executionRoleArn": "arn:aws:iam::xxx:role/service-role/config-role-eu-central-1",
    "configRuleArn": "arn:aws:config:eu-central-1:xxx:config-rule/config-rule-xyzxyz",
    "configRuleName": ”DemoConfigRule",
    "configRuleId": "config-rule-xyzxyz",
    "accountId": ”123456789012”
}
```

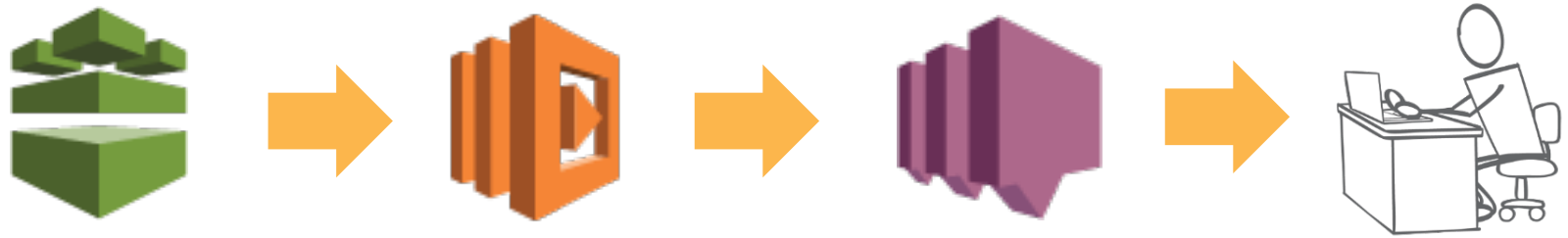
Example in AWS Config Rules (2/2)


```
{ "configurationItem" : {
    "ARN": "arn:aws:ec2:eu-central-1:123456789012:volume/vol-5b5674e1",
    "resourceCreationTime": "2016-06-29T07:39:17.355Z",
    "configurationItemCaptureTime": "2016-06-29T07:52:59.658Z",
    "awsAccountId": "123456789012",
    "configurationItemStatus": "OK",
    "resourceType": "AWS::EC2::Volume",
    "resourceId": "vol-5b5674e1",
    "tags": {},
    "relationships": [{
        "resourceId": "i-790e73c5",
        "resourceType": "AWS::EC2::Instance",
        "name": "Is attached to Instance"
    }],
    "configuration" : { ... }
  },
  "messageType":"ConfigurationItemChangeNotification"
}
```



```
"volumeId": "vol-5b5674e1",
"state": "in-use",
"createTime": "...",
"attachments": [{...}],
"encrypted": false,
"kmsKeyId": null
```

Compliance Violation Raises Alarm



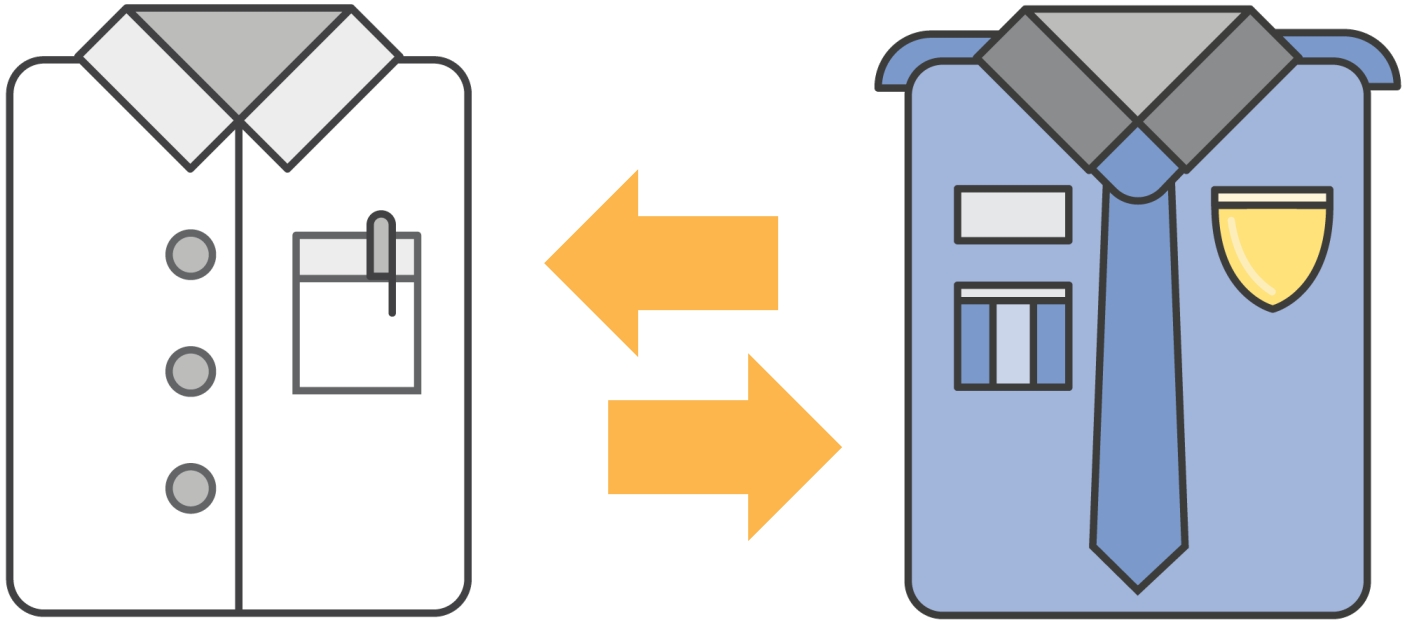
AWS Config records virtual infrastructure

Config Rules checks for violations

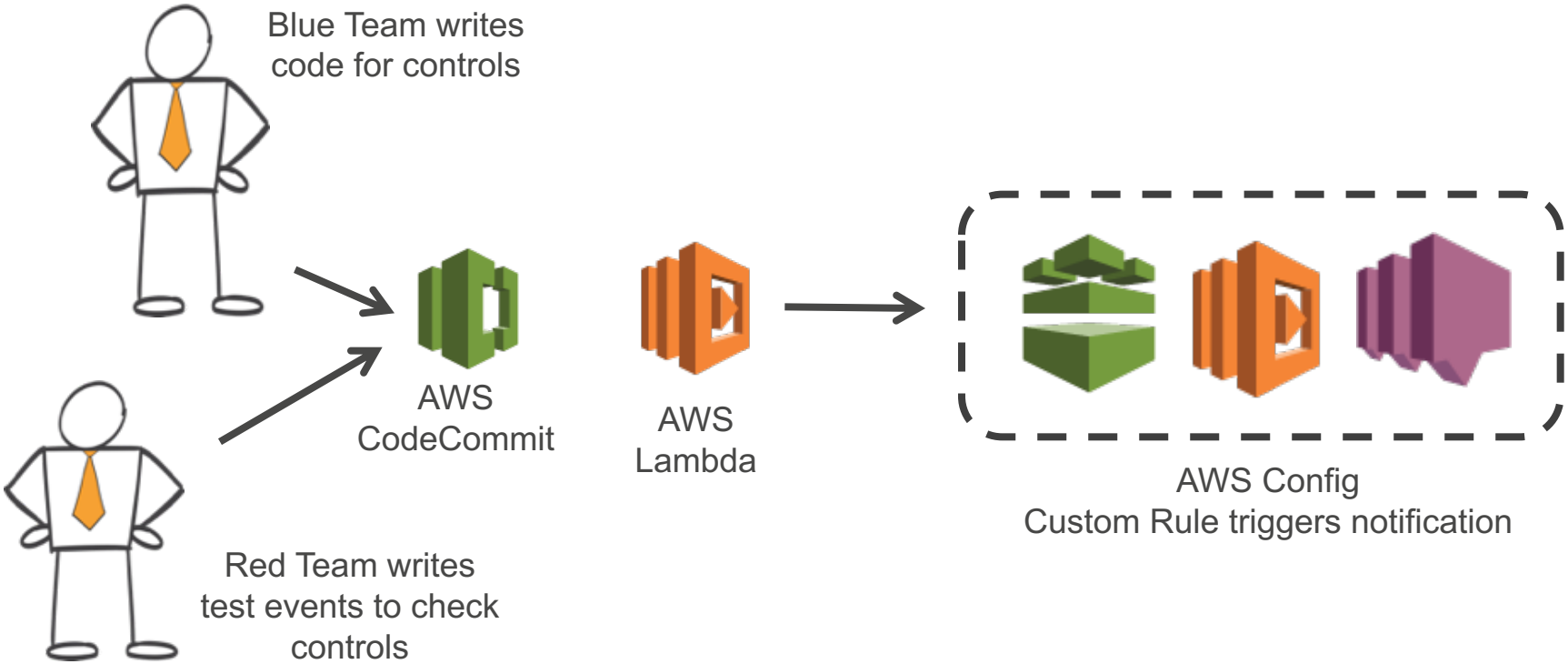
SNS sends alarms


Quis custodiet
ipsos custodes?

Red Blue Teaming



Test-Driven Compliance



Summary

- „Infrastructure as Code“ and „Controls as Code“ are best tackled with software development best practices
- Test-driven compliance automates audits
- Living „DevSecOps“ this way spares manual audits, improves quality, and speeds up development cycles

AWS

SUMMIT

Dr. Thomas Fuhrmann <fuhrmt@amazon.de>
Jeremias Reith <reithj@amazon.de>

amazon web services