AZURE NIGERIA USER MEETUP GROUP

SPEAKERS

DAVID OKEYODE
CLOUD SECURITY CONSULTANT (MVP)

UCHECHUKWU MPAMMAH
MCT (TECH TRAINER)

SATURDAY, 29 | 08 | 2020

3 PM (WAST WEST AFRICA SUMMER TIME UTC + 1)

EVENT LINK

HTTP://BIT.LY/AZUREHANDSONAUGUSTMEETUP

AZURE NIGERIA USER GROUP

BY COMMUNITY | FOR COMMUNITY

David Okeyode (MVP)

- Independent Cloud Security Consultant
- Over a decade of experience in Cybersecurity (consultancy, design, implementation)
- Over 6 years of experience as a trainer
- BLOG: https://azurehangout.com

asegunlolu

@asegunlolu

Microsoft Most Valuable Professional

Microsoft Certified Azure AI Engineer Associate

Microsoft Certified Azure Developer Associate

Microsoft Certified Azure Administrator Associate

Microsoft Certified Azure Security Engineer Associate

Microsoft Certified Azure Solutions Architect Expert

Microsoft Certified Azure DevOps Engineer Expert

aws certified Solutions Architect Professional

aws certified Security Specialty

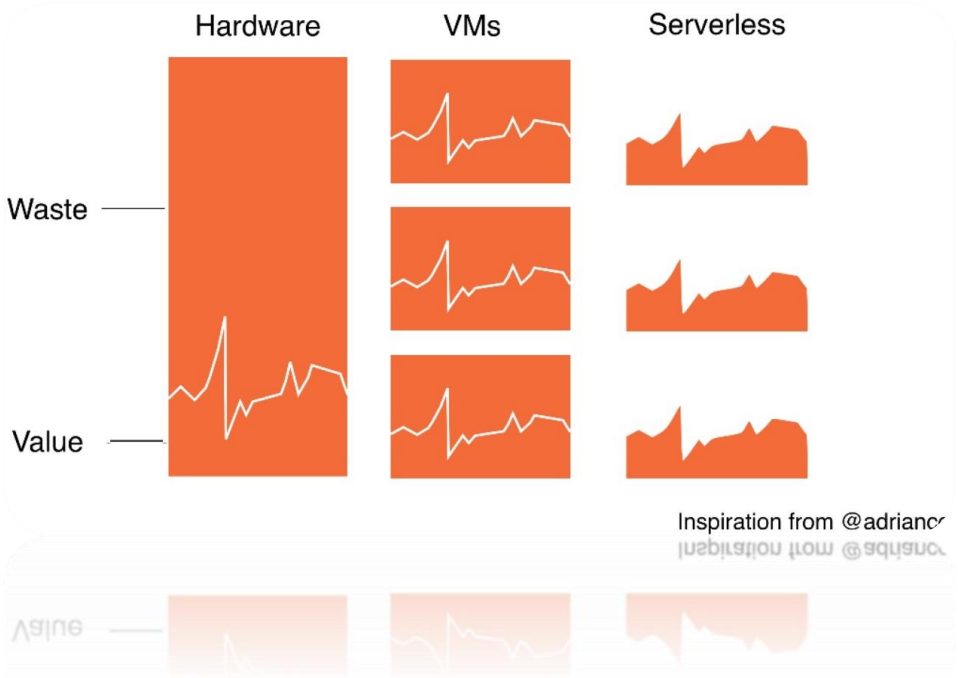
Agenda

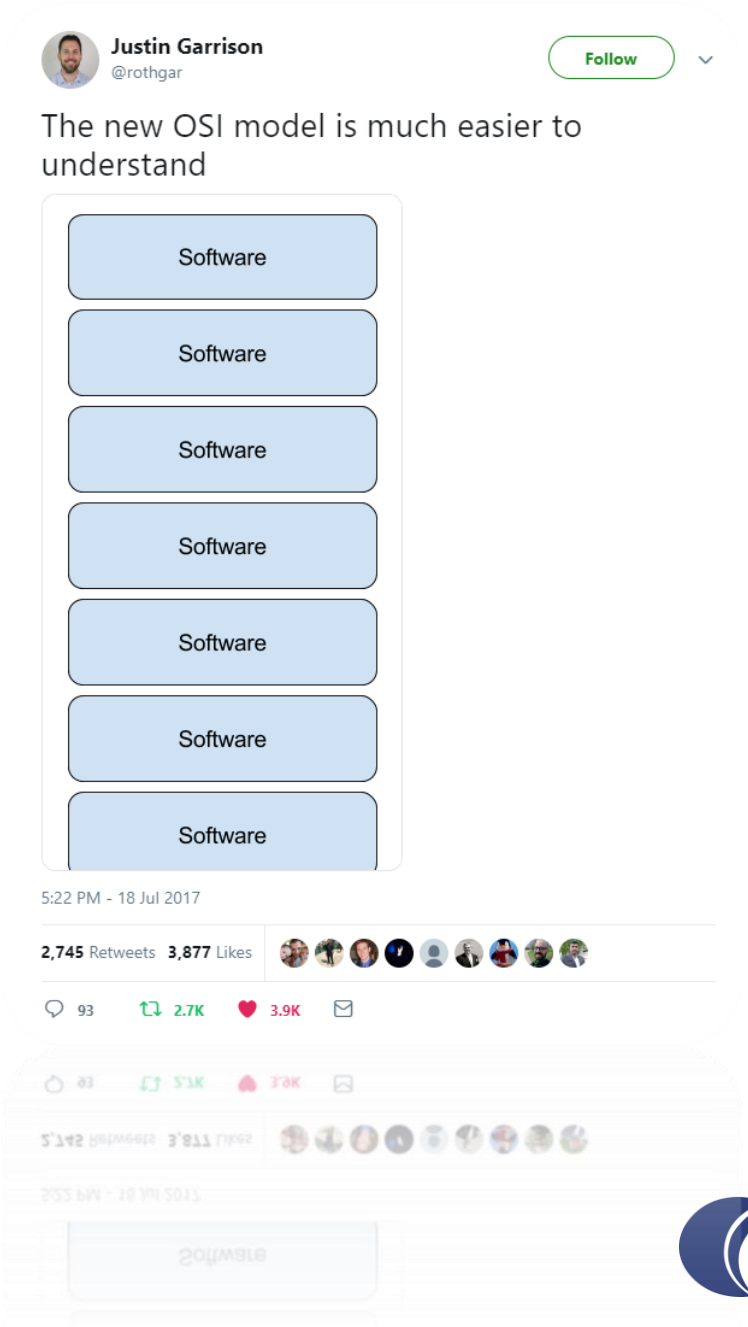
- The changes in the world
- Cloud security overview
- Security challenges of DevOps
- Implementing automated IaC security checks
- Tools for automated IaC security checks in Azure

AZURE HANGOUT

3 Major Movements

- Waterfall → Agile → DevOps
- Monolith → Microservices
- Datacenter → Cloud





AZURE HANGOUT

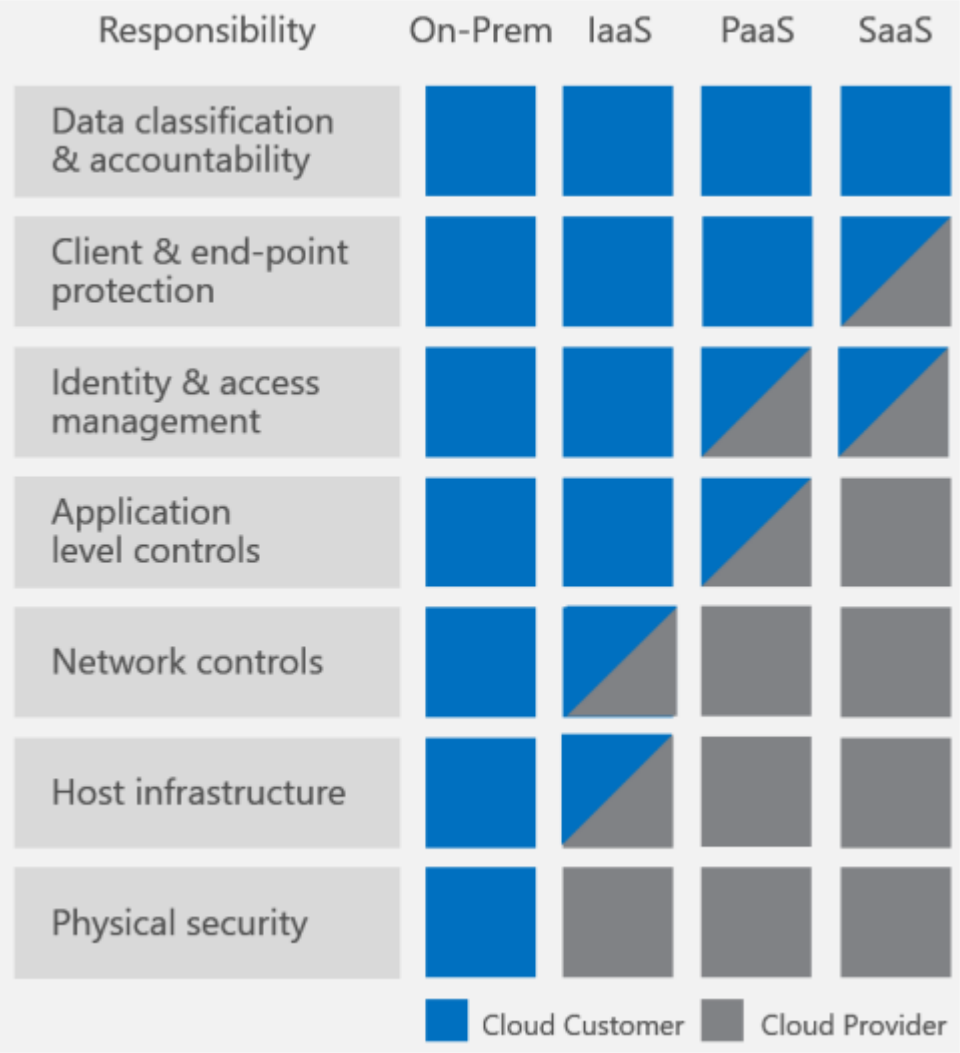
Components of DevOps

- Application Development
  - Any language
- Infrastructure as Code (IaC)
  - Azure ARM templates, Terraform templates
- Source Control Management (SCM)
  - Azure Repos, GitHub, Bit Bucket
- Continuous Integration/Continuous Development (CICD)
  - Azure Pipelines, Jenkins, GitLab

AZURE HANGOUT

Cloud Security Overview

Cloud Security is a Shared Responsibility



The Customer is responsible for the **security** of **each asset layer**

The Customer is responsible for providing **host** security

The Customer is responsible for **authenticating user/service access**

The Customer is responsible for securing application infrastructure

The Customer is responsible for securing and inspecting network traffic

Customer/Microsoft is responsible for the security '*of*' the Cloud

Microsoft is responsible for the Physical Security '*of*' the Cloud

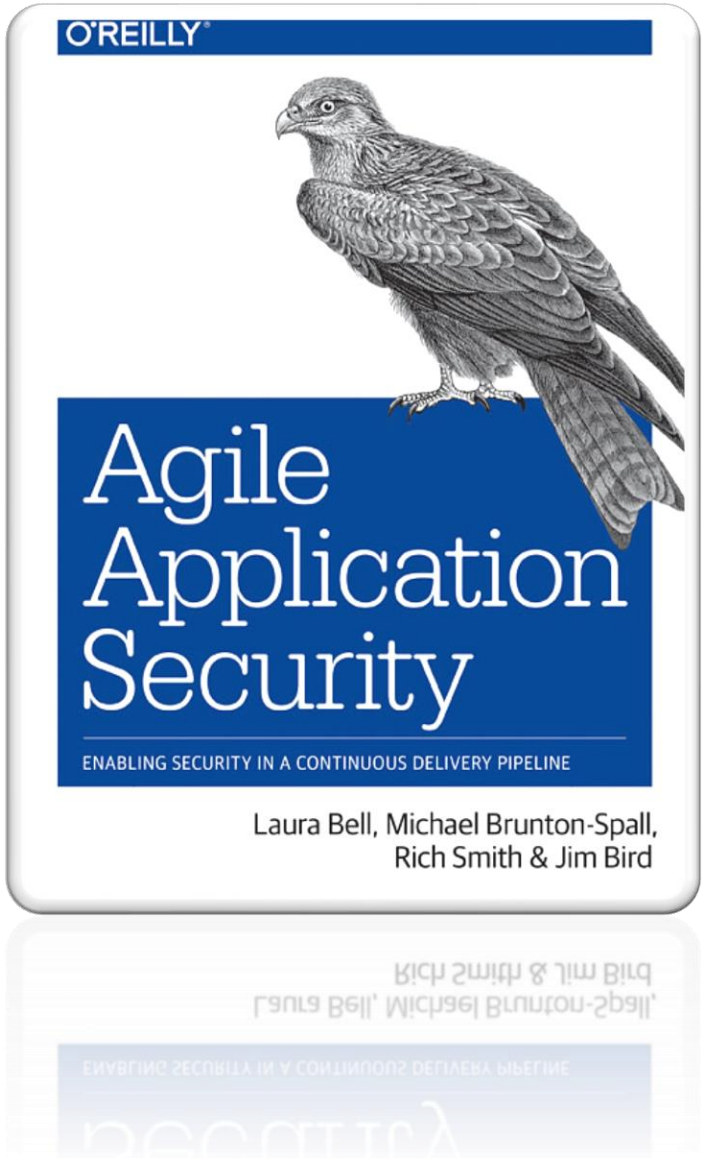
Source: Microsoft TechNet – Shared Responsibilities for Cloud Computing

AZURE HANGOUT

Security Challenges of DevOps

- DevOps workflows are heavily automated, security checks for application and infrastructure code often are manual
- Development, operations and security teams are measured differently - delivery vs stability vs protection

Security Challenges of DevOps

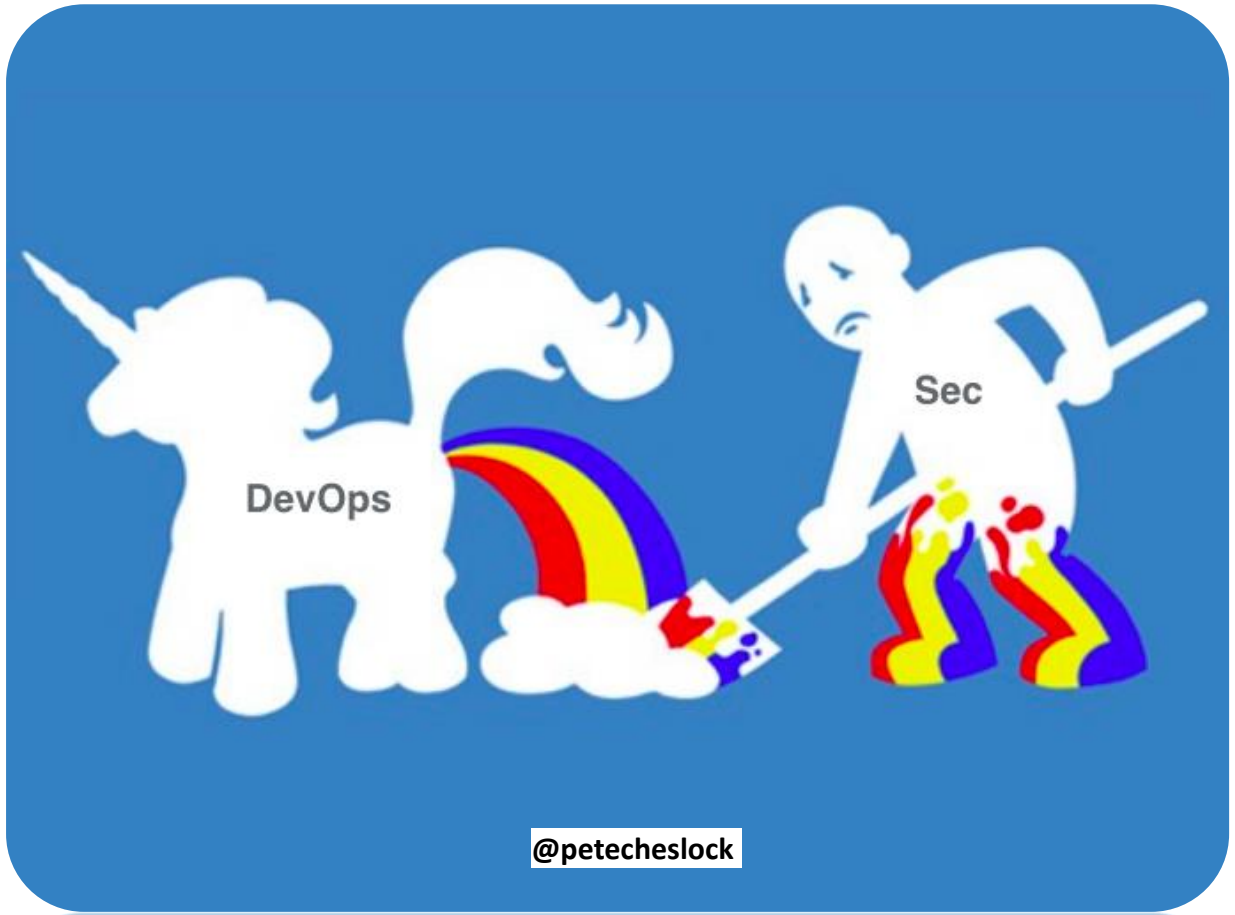


"Many Security teams work with a worldview where their goal is to inhibit change as much as possible"

AZURE HANGOUT

Security Challenges of DevOps

- We live in a DevOps world
- Changes that impacts on security posture happen CONTINUOUSLY

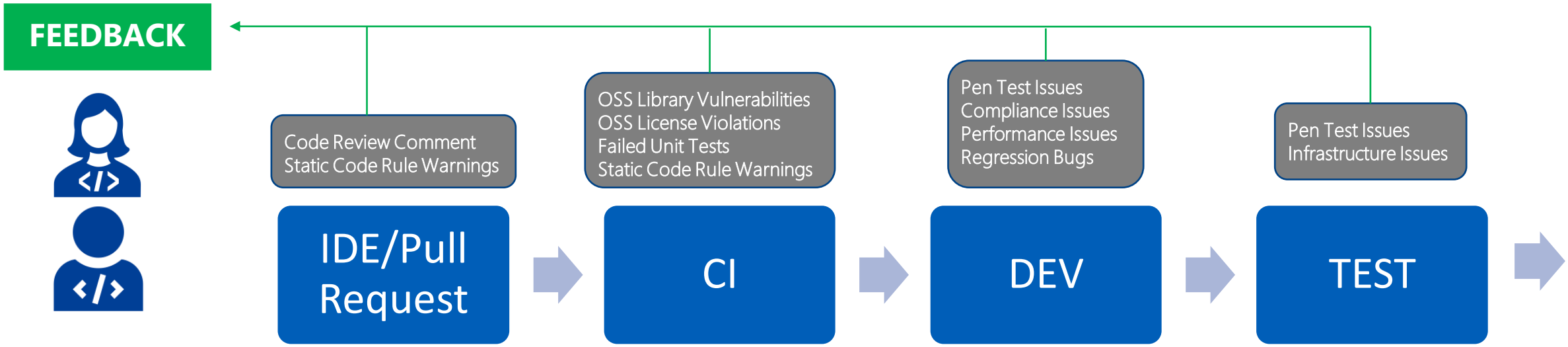


Security – We've forgotten the ecosystem

- Hackers will gain control through the weakest link
  - and slowly progress through the environment
- Hacker dwell time increasing

AZURE HANGOUT

Continuous Security Validation



Application CI/CD	Static Code Analysis Code Review Work Item Linking	Static Code Analysis OSS Vulnerability Scan Unit Tests Code Metrics	Passive Pen Test Encryption validation Infrastructure Scan	Infrastructure Scan
Scheduled Test Runs			Load Performance Testing Automated Regression Testing Infrastructure Scan	Active Pen Test Infrastructure Scan

- Continuous security validation should be added at each step from development through production

AZURE HANGOUT

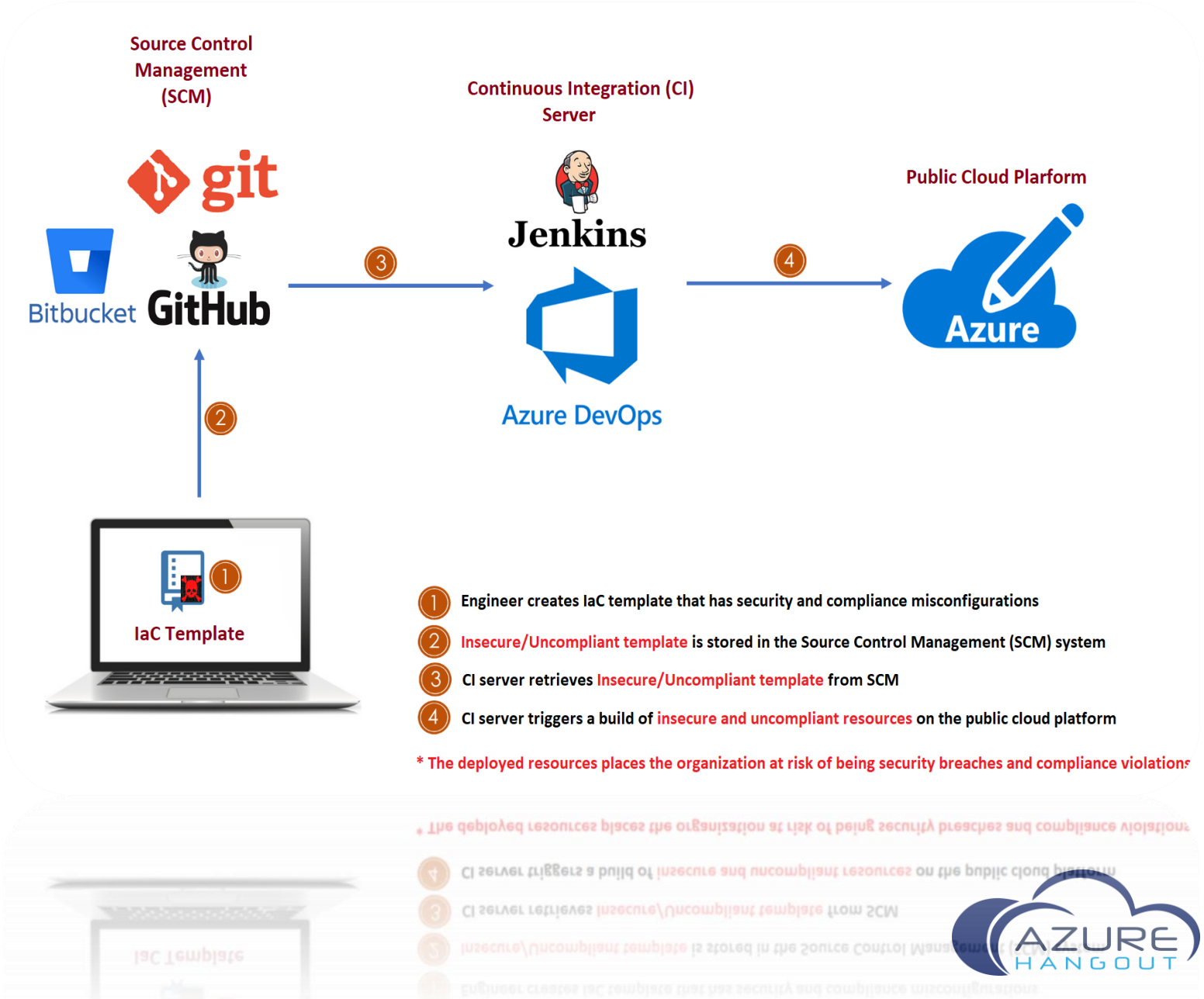
Components of DevOps

- Application Development
- Infrastructure as Code (IaC)
- Source Control Management (SCM)
- Continuous Integration/Continuous Development (CICD)

AZURE HANGOUT

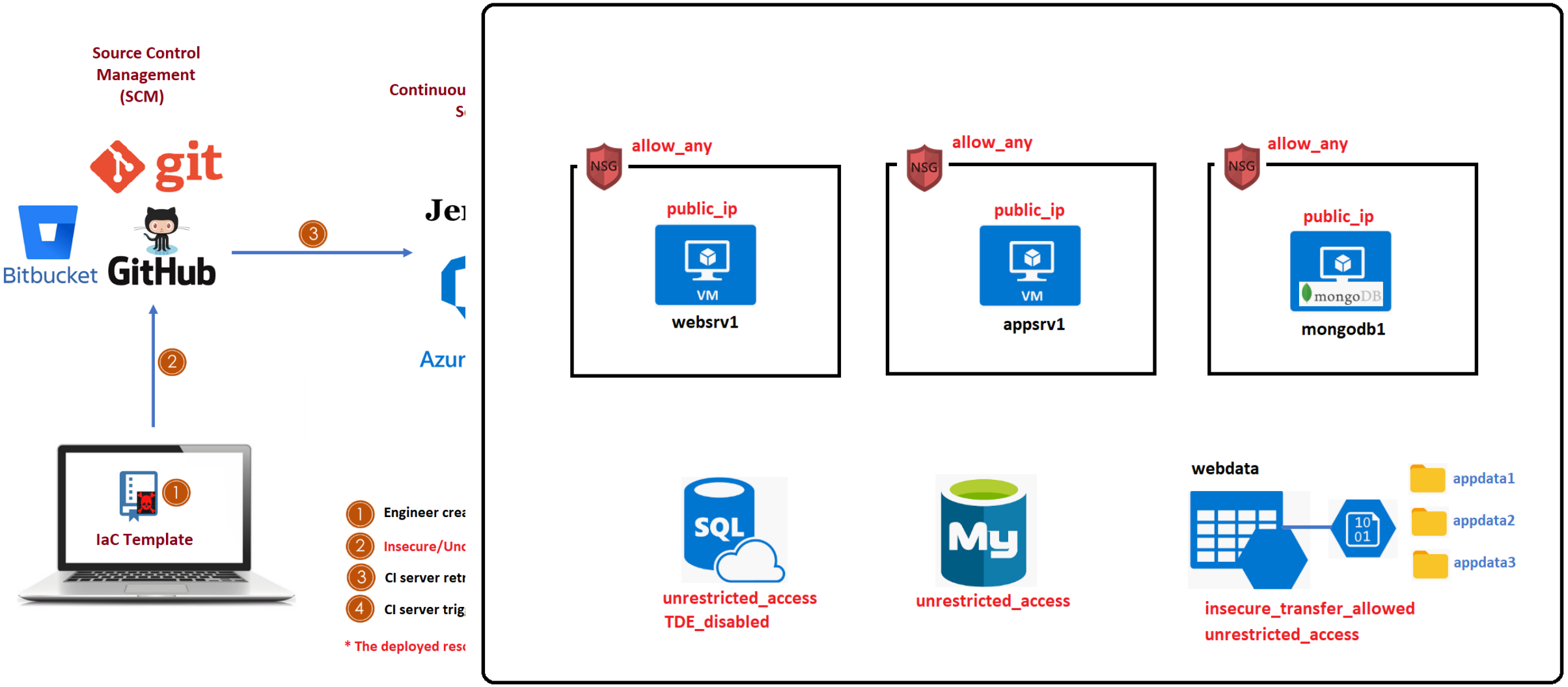
DEMO

IaC Risk without Security



AZURE HANGOUT

IaC Risk Without Security



AZURE HANGOUT

Implementing Automated IaC Security Checks

AZURE HANGOUT

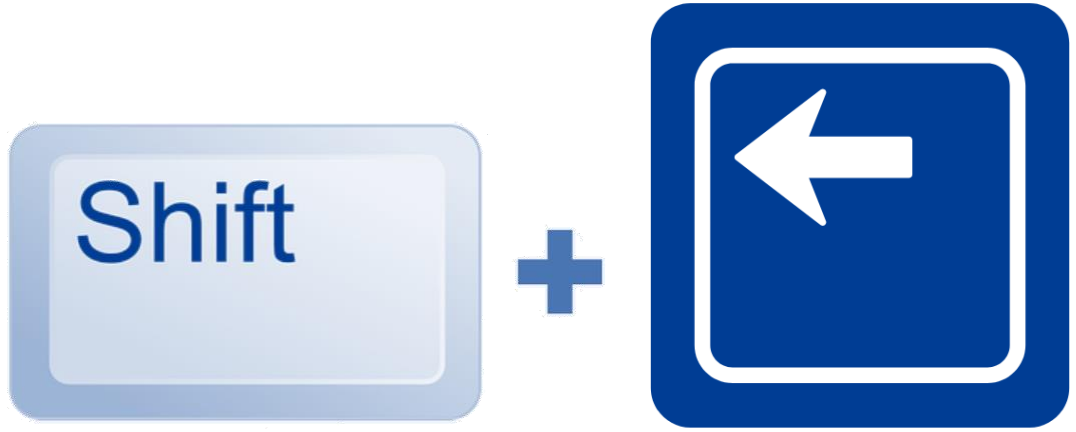
Component #1 – Focus on Automation

- Time matters in a continuous delivery world
- “Everything as Code”
- Reduce feedback loops

AZURE HANGOUT

Component #2 – Focus on Shifting Left

- Security testing automated in every phase
- Security providing value through making security normal in every phase



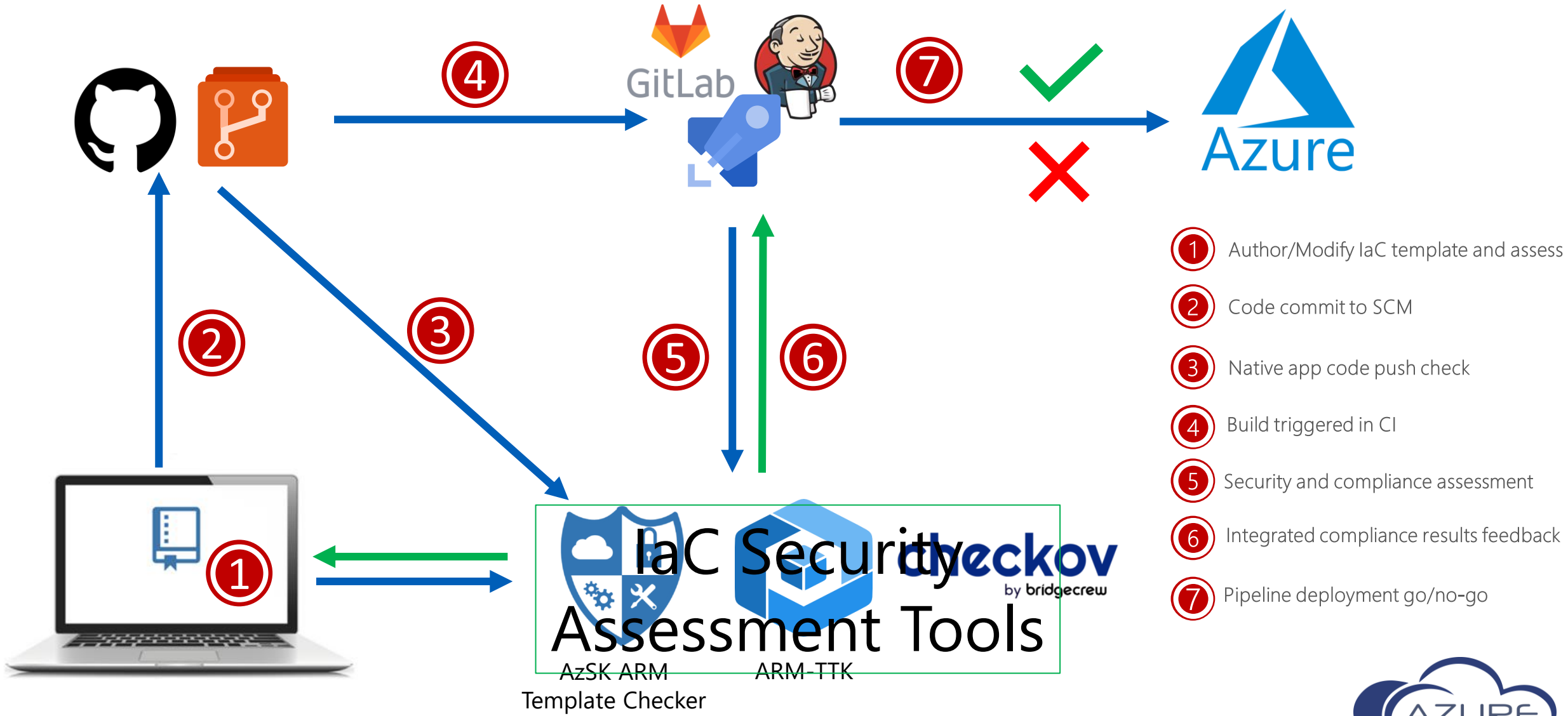
AZURE HANGOUT

Component #3 – Focus on Empowerment

- Don’t fear DevOps - Know the people, processes and tools
- Guidance Documents alone won’t work!
- Move from the "Learn-Build" cycle to the "Build-Measure-Learn" cycle
- Provide tools that works with existing agile workflows
  - API Based

AZURE HANGOUT

IaC Continuous Security Validation



1. Author/Modify IaC template and assess
2. Code commit to SCM
3. Native app code push check
4. Build triggered in CI
5. Security and compliance assessment
6. Integrated compliance results feedback
7. Pipeline deployment go/no-go

AZURE HANGOUT

AzSK ARM Template Checker

- Created by the Core Services Engineering & Operations (CSEO) division at Microsoft
- Not an official Microsoft product
- Scan the security health of our IaC Templates
- Supported resource types
  - Currently supports 42 resource providers
  - There are currently 186 resource providers
- Supported template format
  - ARM Template only
- Use Cases
  - IaC template assessment for authors/contributors (Development)
  - IaC template assessment in integration/release pipelines (CICD)

AZURE HANGOUT

Using AzSK ARM Template Checker

- Install the Secure DevOps Kit PowerShell module

```
Install-Module AzSK -AllowClobber
```

- Configure Auto-Update

```
Set-AzSKPolicySettings -AutoUpdate On
```

- To run ad-hoc tests

```
Get-AzSKARMTemplateSecurityStatus -ARMTemplatePath <Path to ARM Template>
```

- To run tests on multiple templates

```
Get-AzSKARMTemplateSecurityStatus -ARMTemplatePath $TemplateFolder
```

AZURE HANGOUT

Using AzSK ARM Template Checker

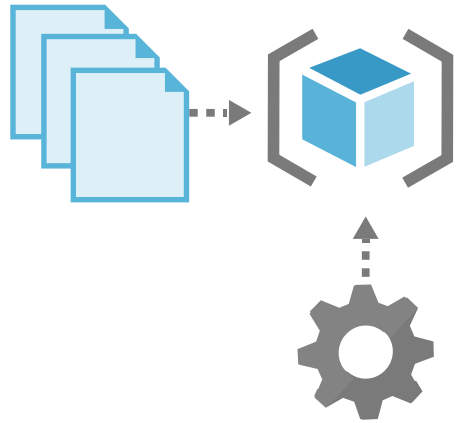
- To integrate in an Azure DevOps Pipeline
  - Secure DevOps Kit (AzSK) CICD Extensions for Azure
- The installation adds two new tasks that we can use for security assessment to our pipelines
  - AzSK Security Verification Tests
  - AzSK ARM Template Checker
- We can use the “Publish Test Result” task to publish results

AZURE HANGOUT

DEMO

AzSK ARM Template Checker

+



AZURE HANGOUT

ARM Template Test Toolkit (ARM-TTK)

- Scan IaC Templates for compliance with recommended best practices
  - Used for Azure quickstart and marketplace templates
- Returns a list of warnings with the suggested changes
- Supported template format
  - ARM Template only
- Currently supports assessment for 24 test cases
  - Secure parameters can't have hardcoded default
  - Use recent API version
  - Use latest VM images
  - Outputs can't include secrets
  - [illegible]
- Use
  - [illegible]
  - [illegible]
  - [illegible]

```
"imageReference": {
    "publisher": "Canonical",
    "offer": "UbuntuServer",
    "sku": "16.04-LTS",
    "version": "latest"
},
```

Passed

AZURE HANGOUT

Using ARM-TTK

- Download the ARM template test toolkit

```
Invoke-WebRequest -Uri https://aka.ms/arm-ttk-latest -OutFile arm-ttk-latest.zip
Expand-Archive -LiteralPath 'arm-ttk-latest.zip'
```

- Import the module into your PowerShell session

```
Import-Module .\arm-ttk.psd1
```

- To run ad-hoc tests

```
Test-AzTemplate -TemplatePath C:\Users\azureadmin\Downloads\templates\azuredeploy.json
```

- To run tests on multiple templates

```
Test-AzTemplate -TemplatePath $TemplateFolder
```

AZURE HANGOUT

Using ARM-TTK

- Download the ARM template test toolkit

```
Invoke-WebRequest -Uri https://aka.ms/arm-ttk-latest -OutFile arm-ttk-latest.zip
Expand-Archive -LiteralPath 'arm-ttk-latest.zip'
```

- Import the module into your PowerShell session

```
Import-Module .\arm-ttk.psd1
```

- To run ad-hoc tests

```
Test-AzTemplate -TemplatePath C:\Users\azureadmin\Downloads\templates\azuredeploy.json
```

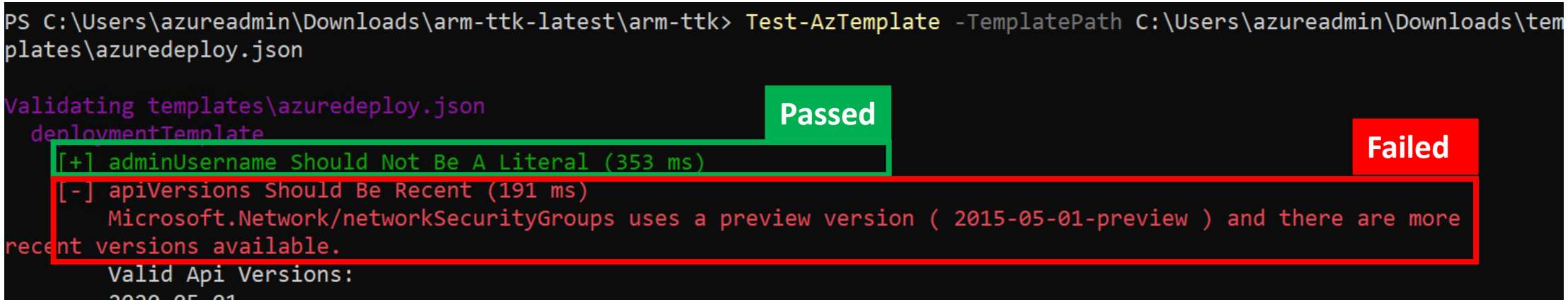
- To run tests on multiple templates

```
Test-AzTemplate -TemplatePath $TemplateFolder
```

AZURE HANGOUT

Using ARM-TTK

- To interpret results



- To select tests

```
Test-AzTemplate -TemplatePath $TemplateFolder -Test "Resources Should Have Location"
```

- To add our custom tests

```
Create new test case in \arm-ttk\testcases\deploymentTemplate
```

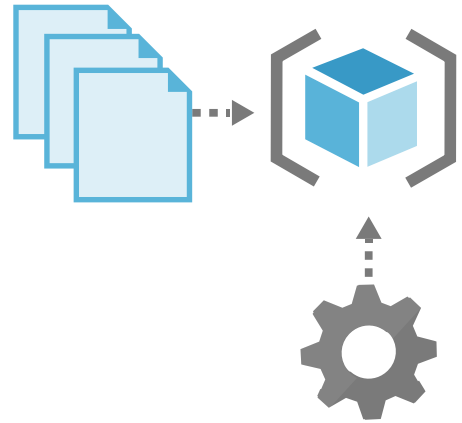
AZURE HANGOUT

Using ARM-TTK

- To integrate in an Azure DevOps Pipeline
- There are two extensions that we could use:
  - ARMTTKExtension created by Sam Cogan
  - ARM Template Tester created by Maik van der Gaag
- ARMTTKExtension created by Sam Cogan
  - Adds a new task “Run ARM TTK Test” to Azure DevOps
- We can use the “Publish Test Result” task to publish results

DEMO

ARM Template Test Toolkit (ARM-TTK)



Checkov by Bridgecrew

checkov by bridgecrew

- IaC static code analysis tool for infrastructure-as-code
- Returns a list of warnings with the suggested changes
- Supported template format (for Azure)
  - ARM Template
  - Terraform Azure Templates
- Currently supports assessment for 107 security checks for Azure
  - 52 ARM Template checks
  - 55 Terraform Azure checks
- Use Cases
  - Template assessment for authors/contributors (Development)
  - IaC template assessment in integration/release pipelines (CICD)
  - Continuous security validation

AZURE HANGOUT

Using Checkov

- Download the ARM template test toolkit

```
Invoke-WebRequest -Uri https://aka.ms/arm-ttk-latest -OutFile arm-ttk-latest.zip
Expand-Archive -LiteralPath 'arm-ttk-latest.zip'
```

- Import the module into your PowerShell session

```
Import-Module .\arm-ttk.psd1
```

- To run ad-hoc tests

```
Test-AzTemplate -TemplatePath C:\Users\azureadmin\Downloads\templates\azuredeploy.json
```

- To run tests on multiple templates

```
Test-AzTemplate -TemplatePath $TemplateFolder
```

AZURE HANGOUT

DEMO

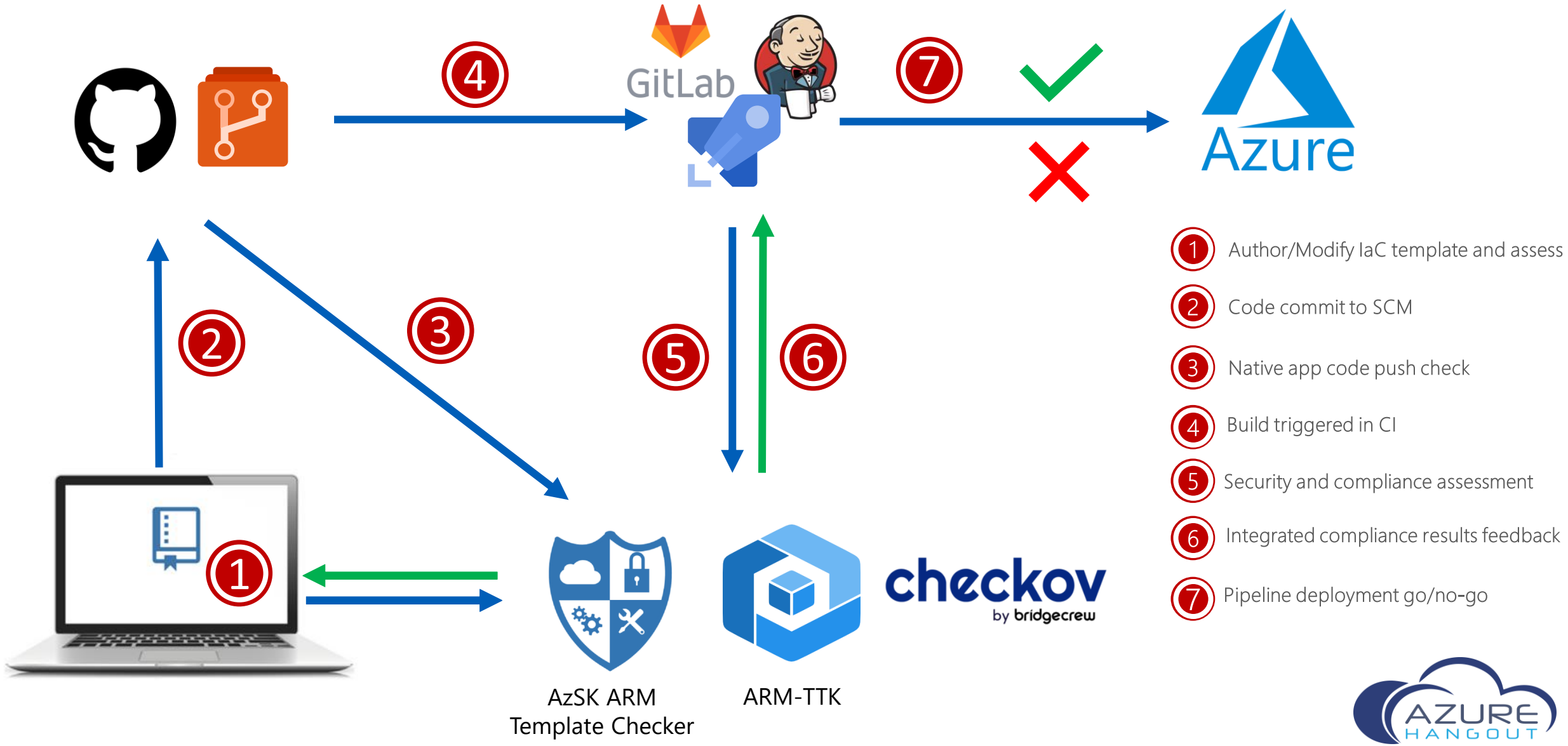
ARM Template Test Toolkit (ARM-TTK)

TerraGoat
by bridgecrew

vs checkov
by bridgecrew

AZURE HANGOUT

IaC Continuous Security Validation



1. Author/Modify IaC template and assess
2. Code commit to SCM
3. Native app code push check
4. Build triggered in CI
5. Security and compliance assessment
6. Integrated compliance results feedback
7. Pipeline deployment go/no-go

AZURE HANGOUT

David Okeyode

THANK YOU!

Q and A???

- BLOG: https://azurehangout.com

asegunlolu

@asegunlolu