Multi-region Terraform Deployments with Terraform Built CI/CD on AWS

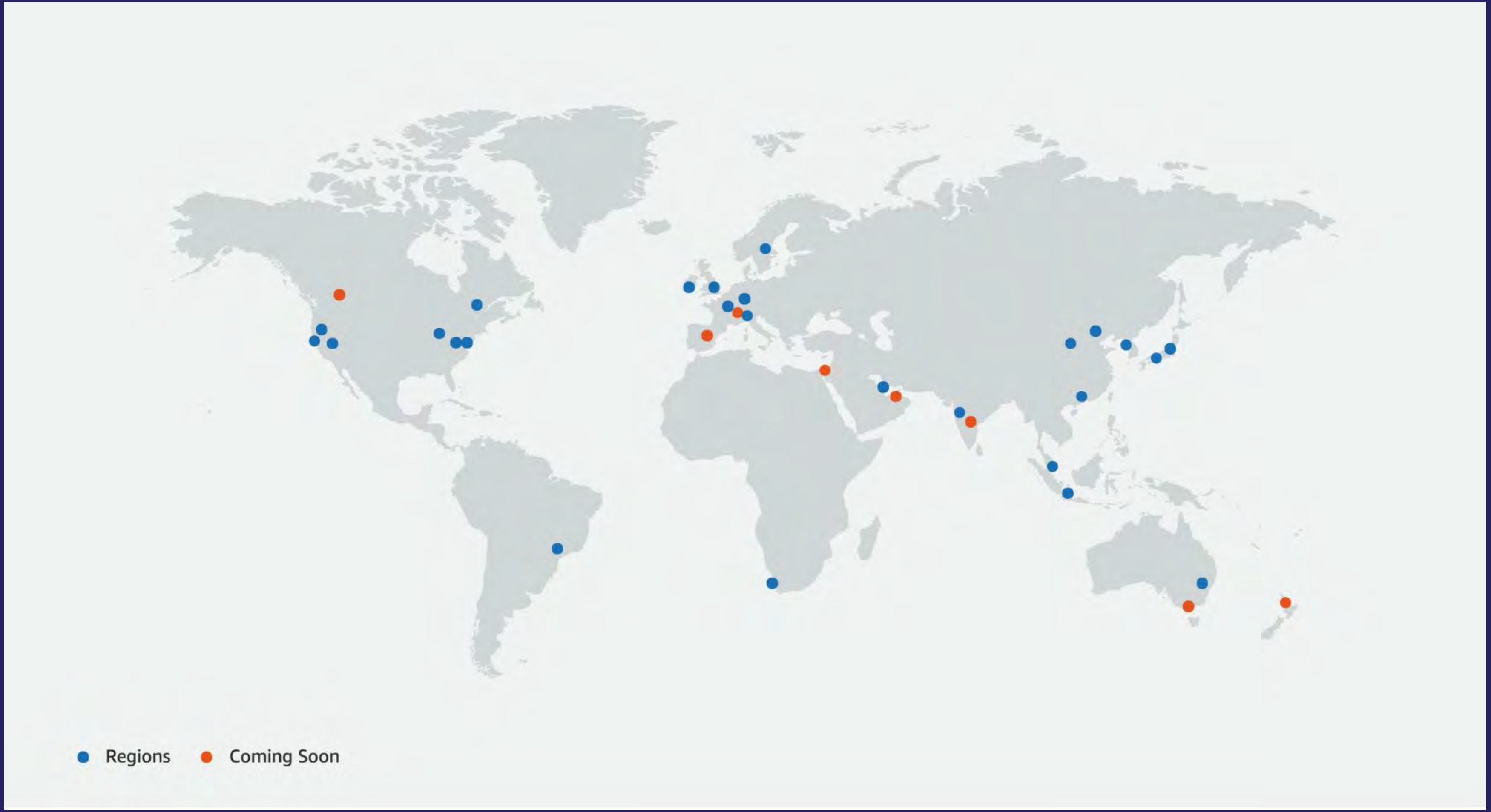
Lerna Ekmekcioglu

Sr. Solutions Architect, AWS
https://www.linkedin.com/in/lerna/

Jack Iu

Principal Solutions Architect, AWS
https://www.linkedin.com/in/jackiu

WHY multi-region deployment?



Managing multi-region resources is complex!

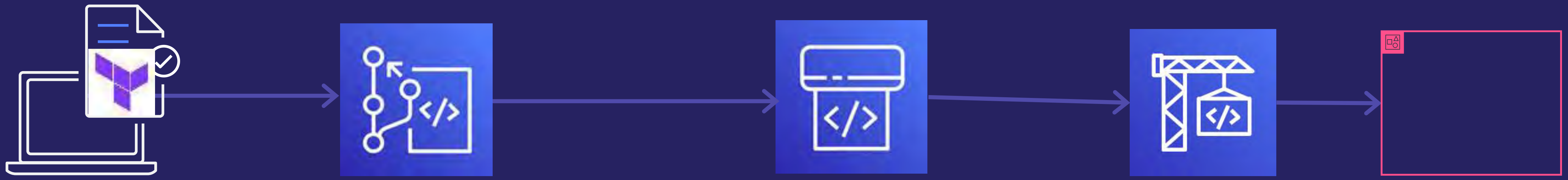
Consistency

Infrastructure as code

Deployment

Multi-region Terraform Deployments: Terraform Deployment Workflow

Terraform deployment workflow



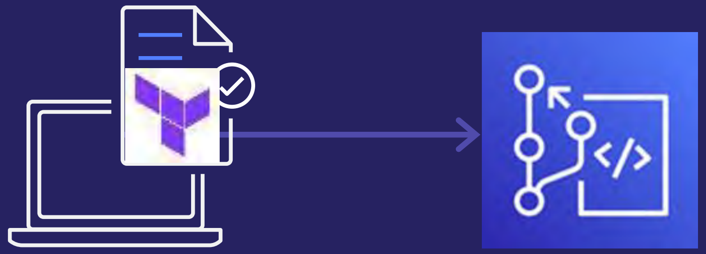
1 Infra as Code

2 Git Tag

3 Triggers Pipeline

4 Deploys into target account

Terraform deployment workflow

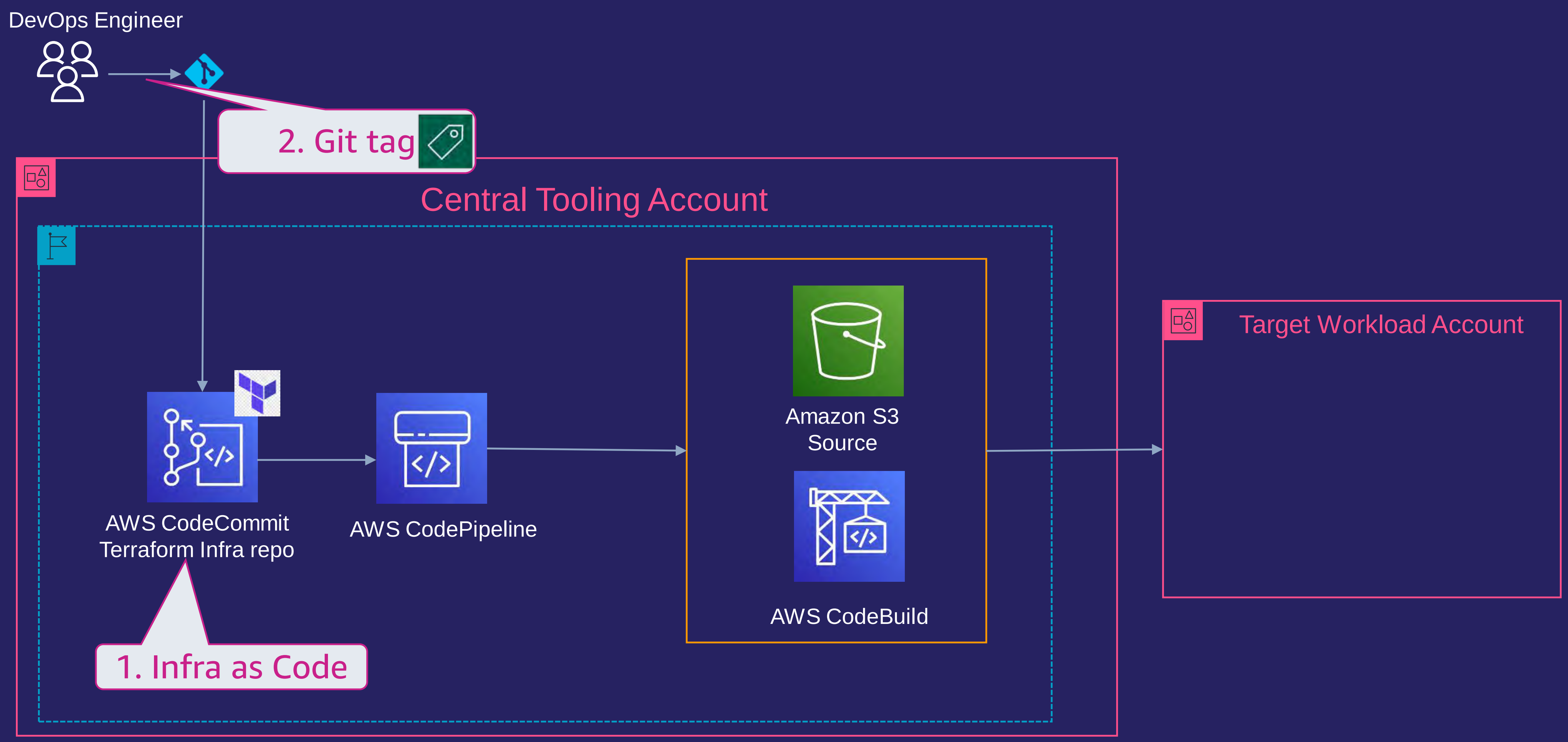


1

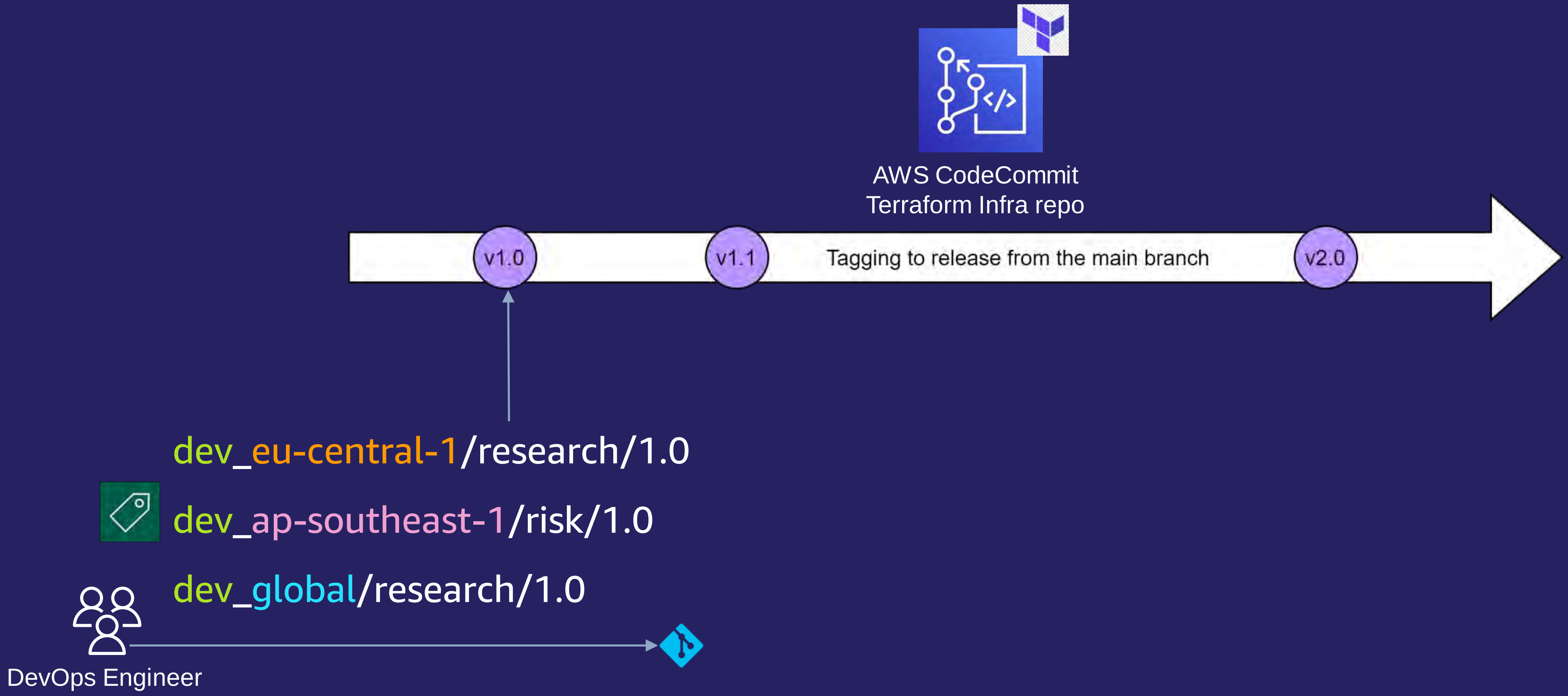
Infra as Code

2

Git Tag


DevOps Engineer
2. Git tag
Central Tooling Account
AWS CodeCommit
Terraform Infra repo
AWS CodePipeline
Amazon S3
Source
AWS CodeBuild
Target Workload Account
1. Infra as Code

MULTI REGION TERRAFORM DEPLOYMENTS WITH TERRAFORM BUILT CI/CD ON AWS



AWS CodeCommit
Terraform Infra repo

v1.0

v1.1

Tagging to release from the main branch

v2.0

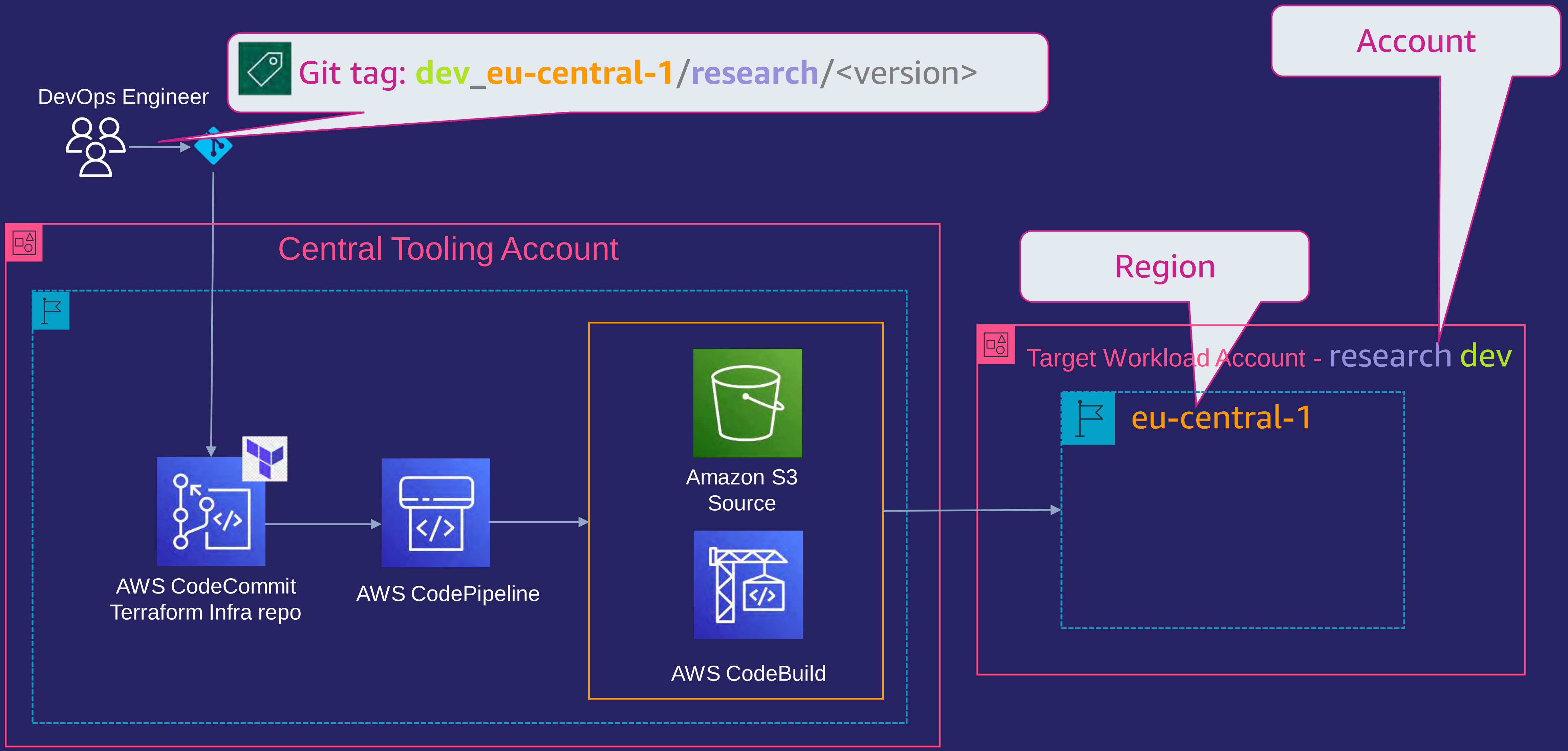
dev_eu-central-1/research/1.0

dev_ap-southeast-1/risk/1.0

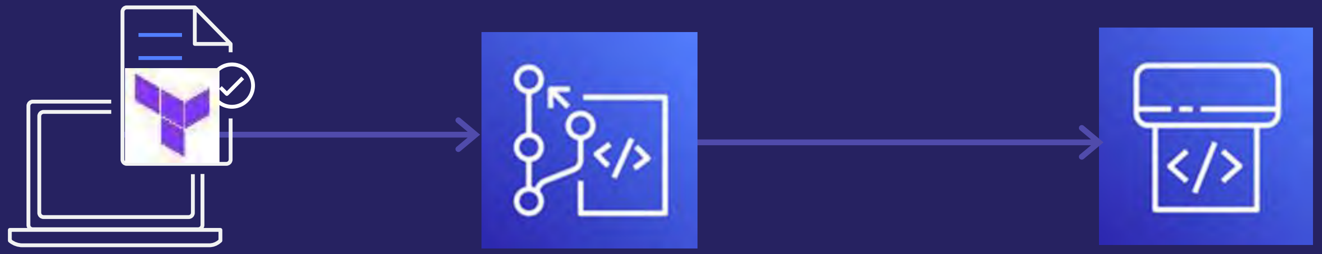
dev_global/research/1.0

DevOps Engineer

MULTI REGION TERRAFORM DEPLOYMENTS WITH TERRAFORM BUILT CI/CD ON AWS



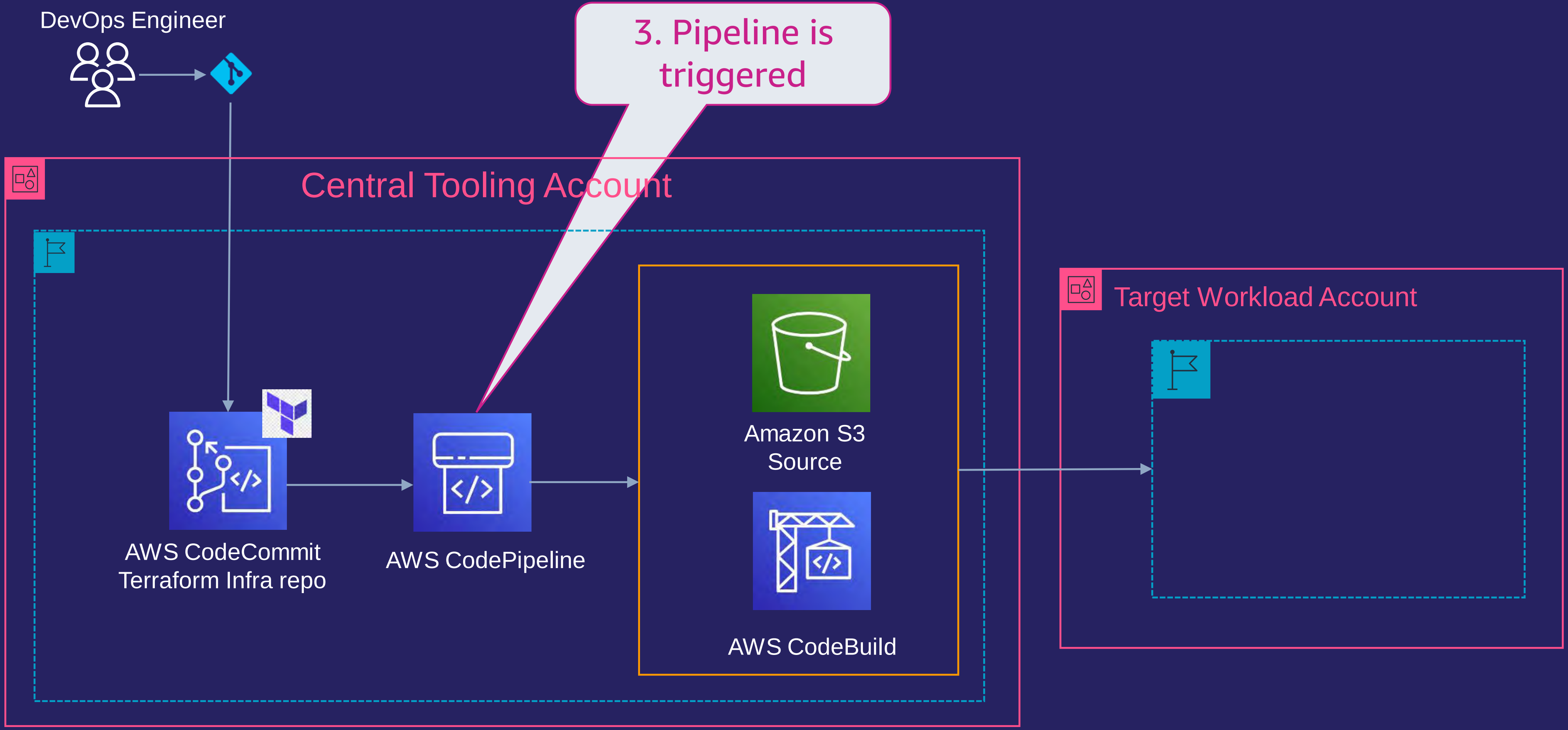
Terraform deployment workflow



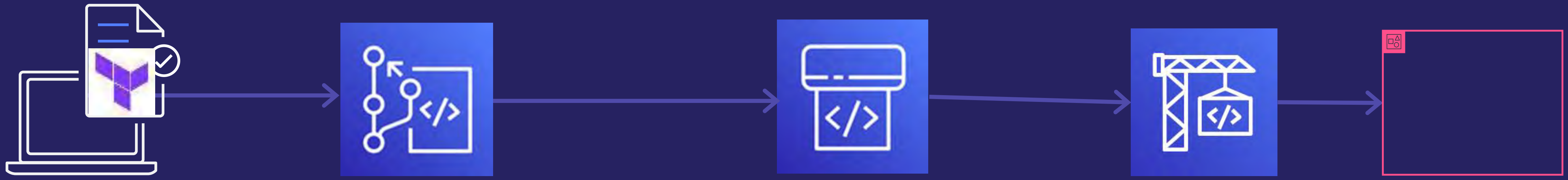
1. Infra as Code

2. Git Tag

3. Triggers Pipeline


DevOps Engineer
3. Pipeline is triggered
Central Tooling Account
Amazon S3 Source
AWS CodeBuild
AWS CodeCommit Terraform Infra repo
AWS CodePipeline
Target Workload Account

Terraform deployment workflow



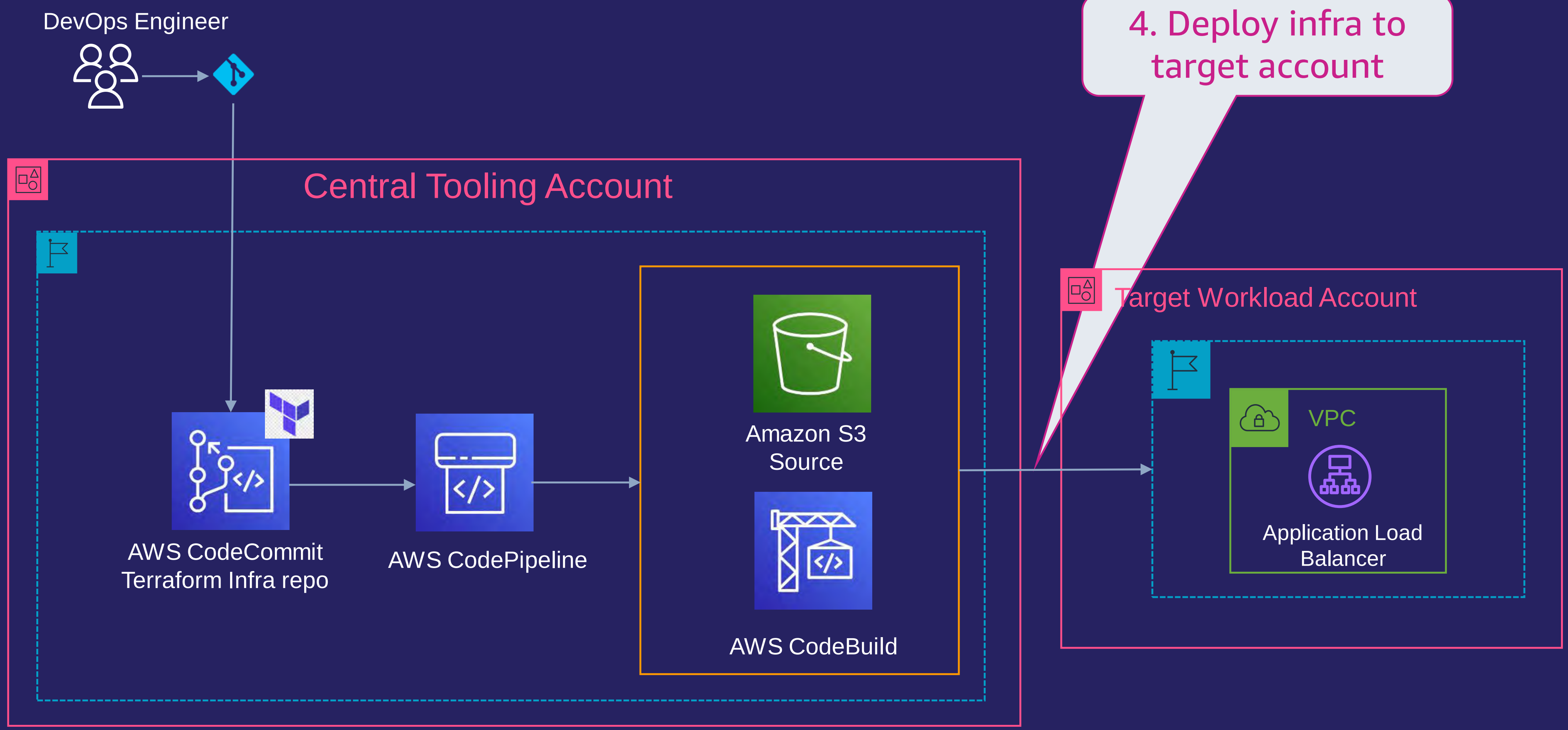
1 Infra as Code

2 Git Tag

3 Triggers Pipeline

4 Deploys into target account

MULTI REGION TERRAFORM DEPLOYMENTS WITH TERRAFORM BUILT CI/CD ON AWS



Multi-region Terraform Deployments: Core Infrastructure Pipeline

Pipeline stages

1 Source

2 IaC Lint

3 IaC Security Scan

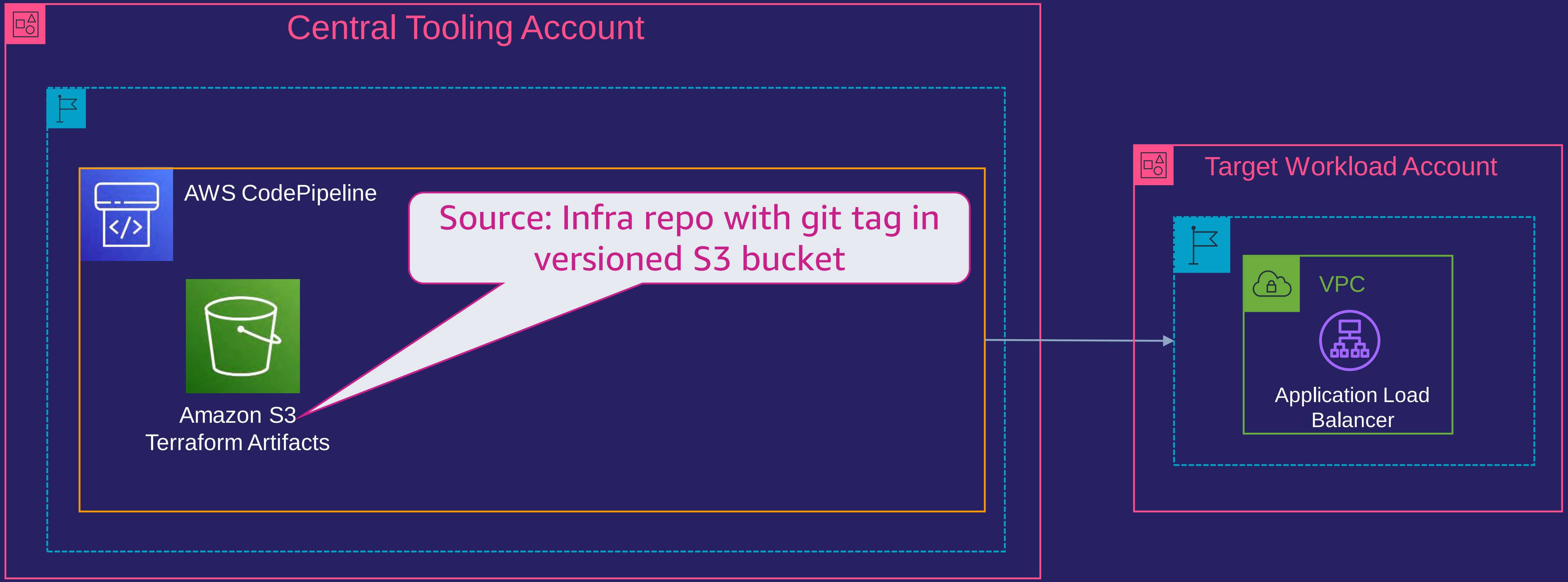
4 IaC Build

Pipeline stages

1

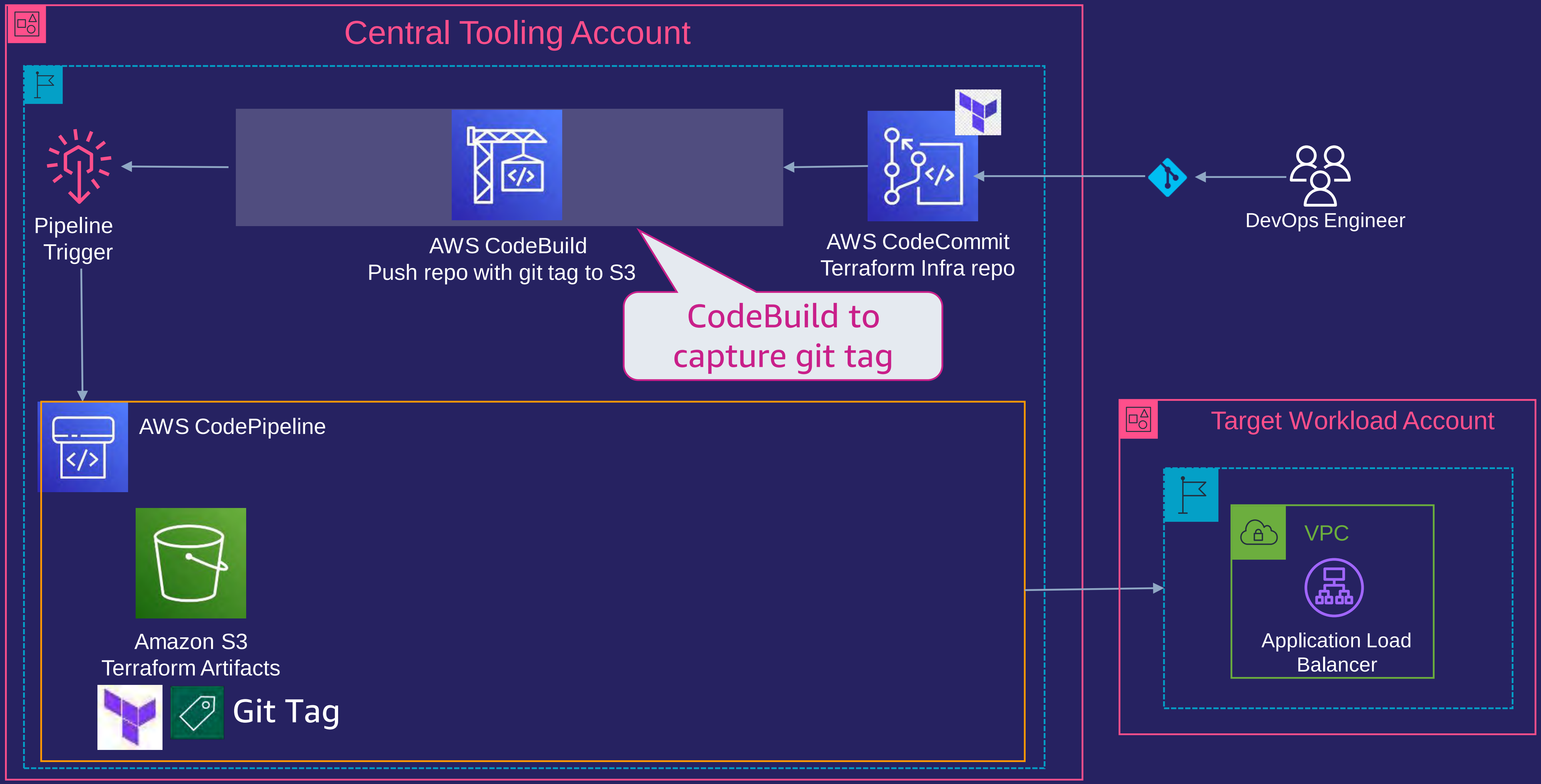
Source

Pipeline: source stage



Source: Infra repo with git tag in versioned S3 bucket

MULTI REGION TERRAFORM DEPLOYMENTS WITH TERRAFORM BUILT CI/CD ON AWS



Pipeline stages

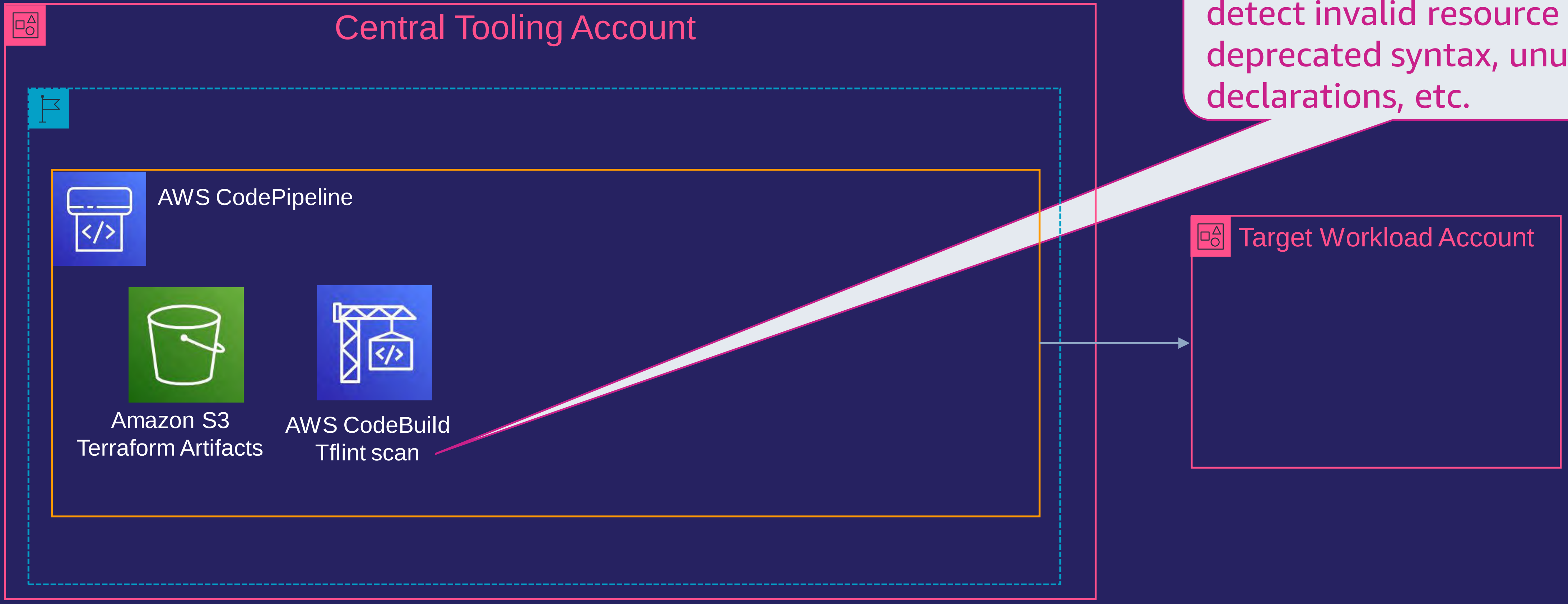
1

Source

2

IaC Lint

Pipeline: IaC linting stage



Improve Code Quality to detect invalid resource types, deprecated syntax, unused declarations, etc.

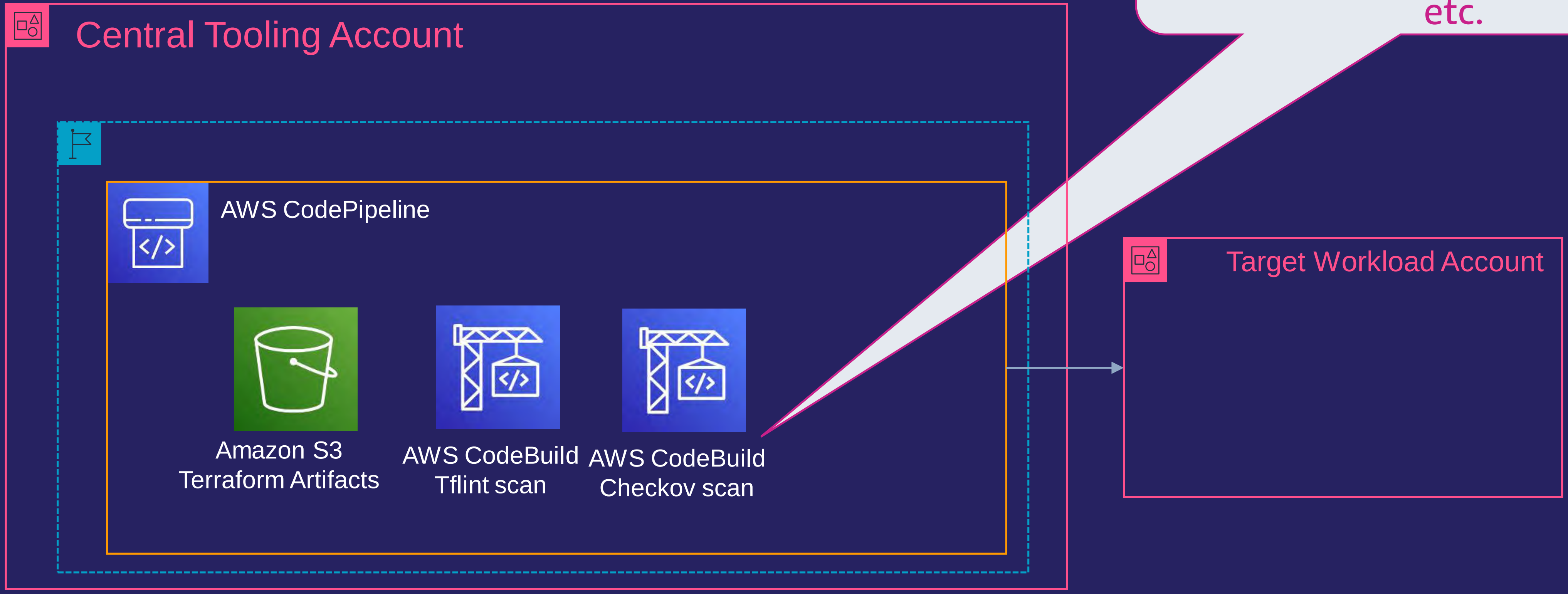
Pipeline stages

1 Source

2 IaC Lint

3 IaC Security Scan

Pipeline: IaC security scan stage



Identify security related issues like publicly accessible S3 buckets, or a security group open to the world, etc.

Pipeline stages

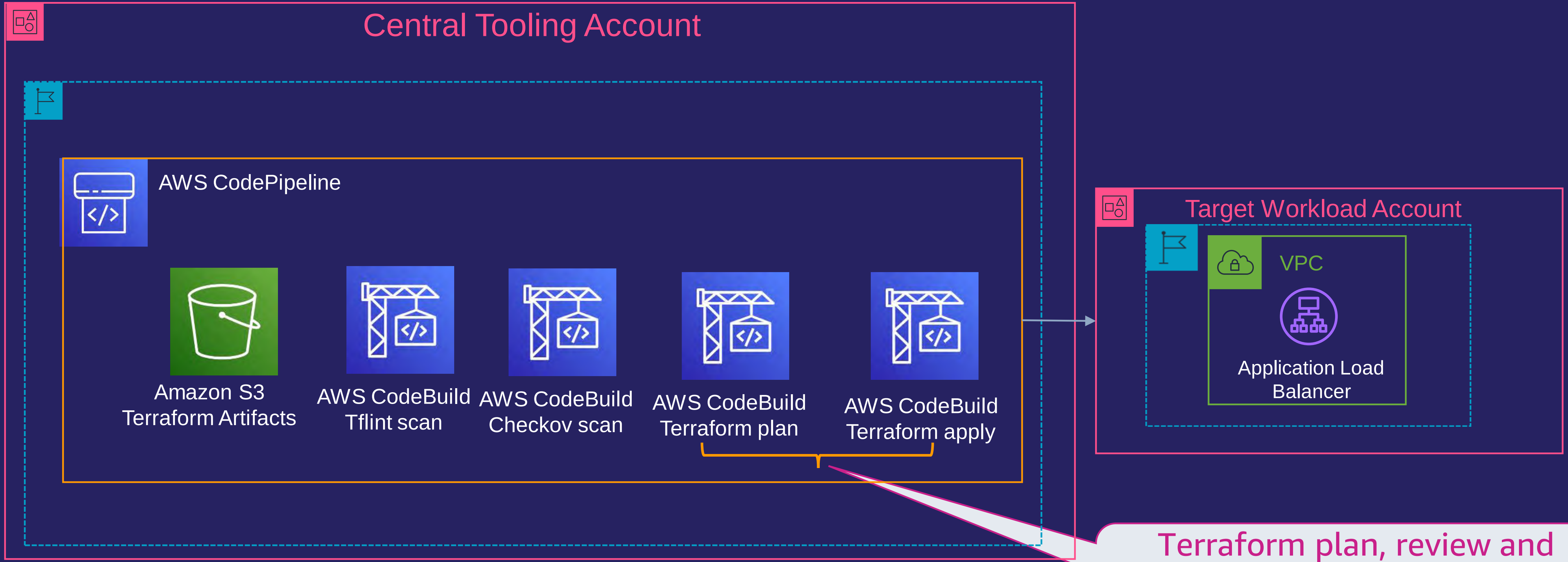
1 Source

2 IaC Lint

3 IaC Security Scan

4 IaC Build

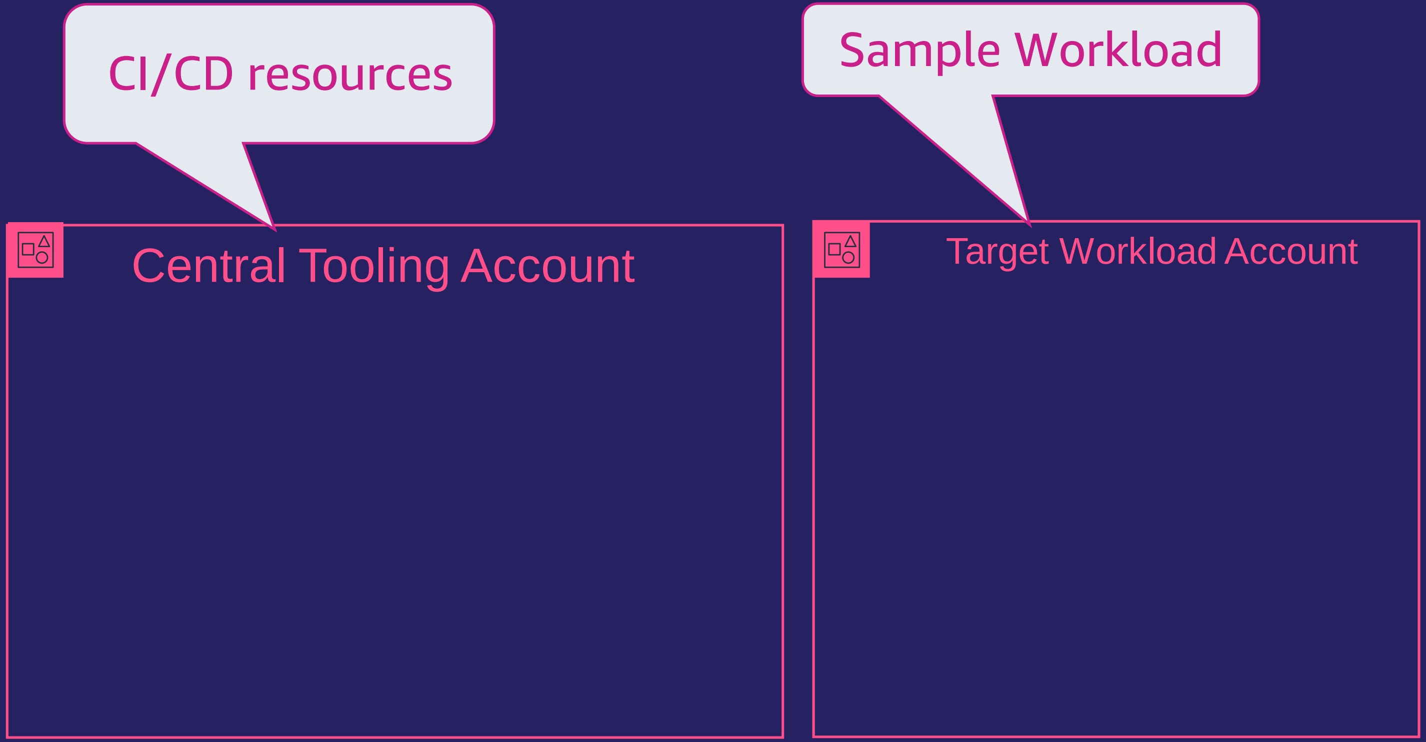
Pipeline: IaC build stage



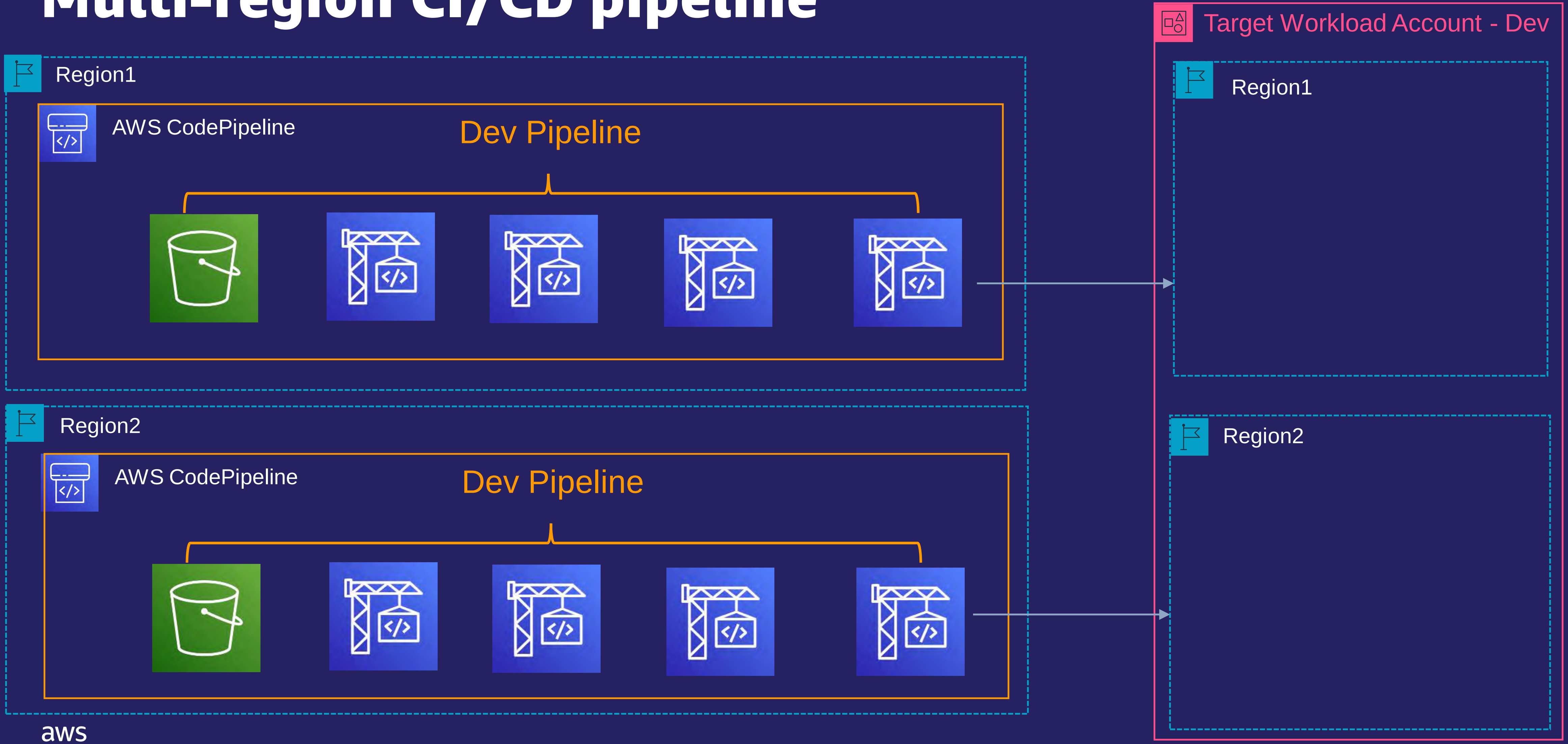
Terraform plan, review and approve the plan and apply to deploy resources

Multi-region Terraform Deployments: Core Infrastructure Pipeline Considerations

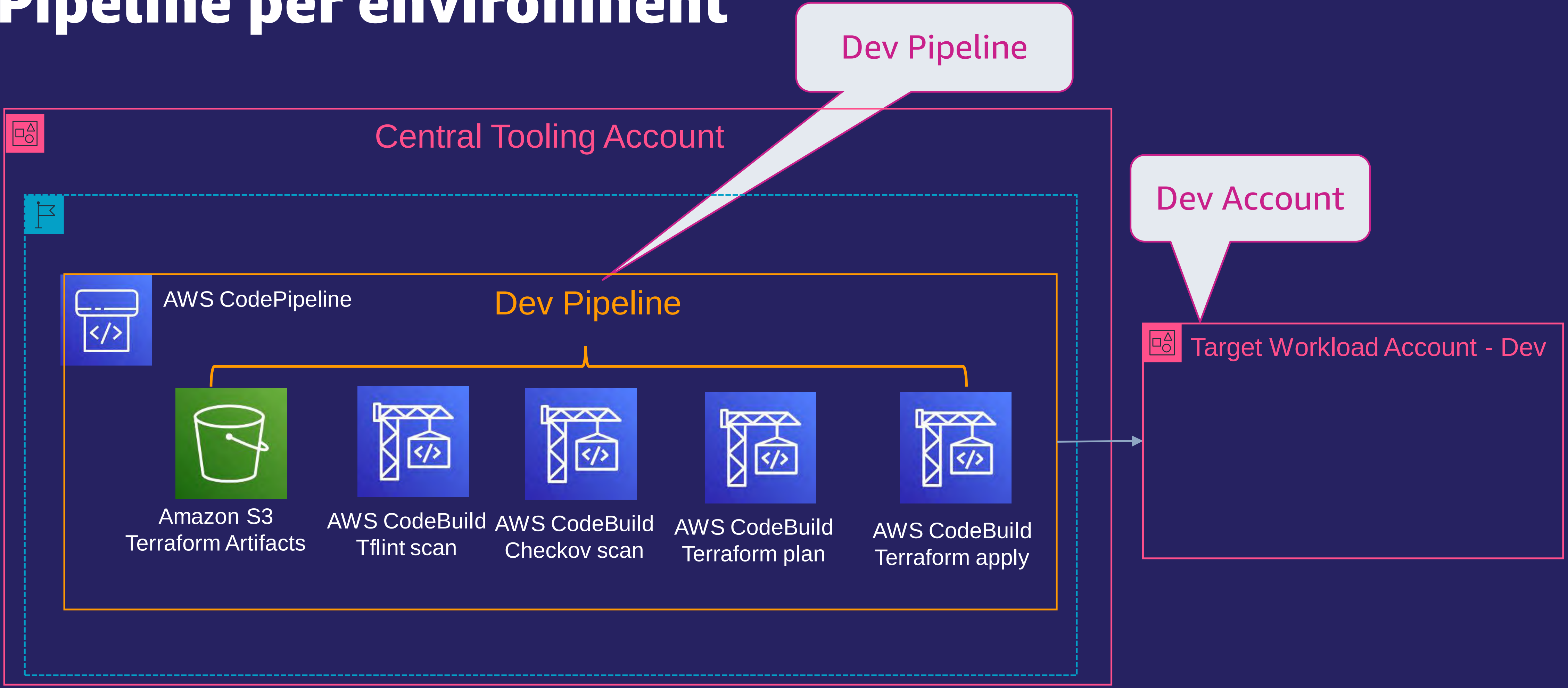
Multi-account structure



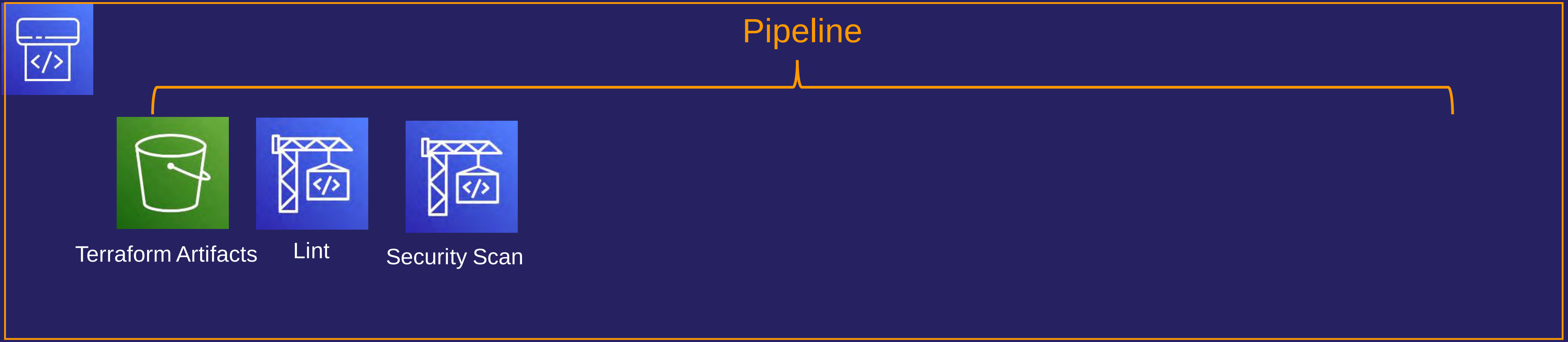
Multi-region CI/CD pipeline



Pipeline per environment



Shift security left in SDLC: Include security scanning early in the pipeline

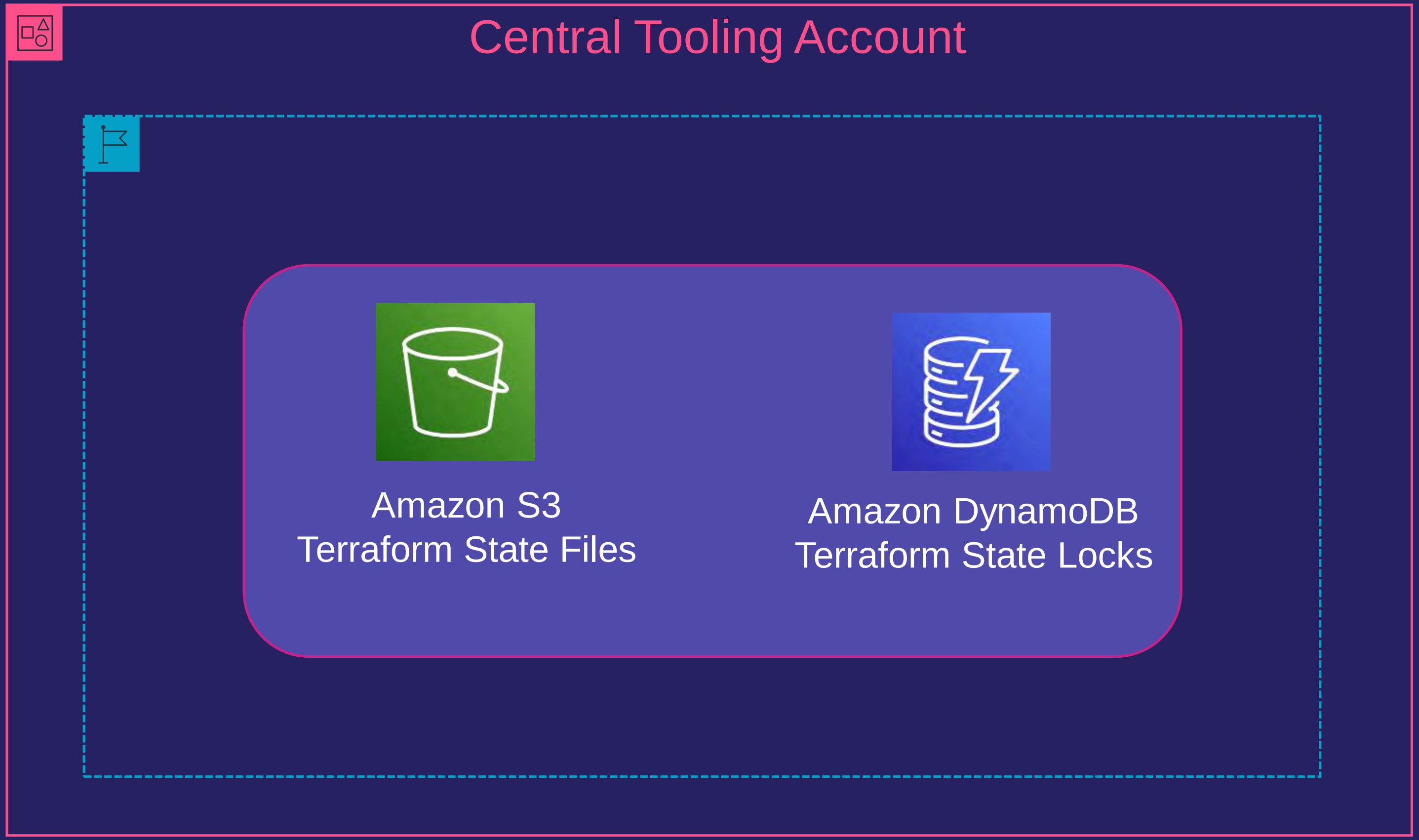


Make the pipeline the authoritative source for deployments.

Multi-region Terraform Deployments: Terraform Backend Config

Terraform state files and locks

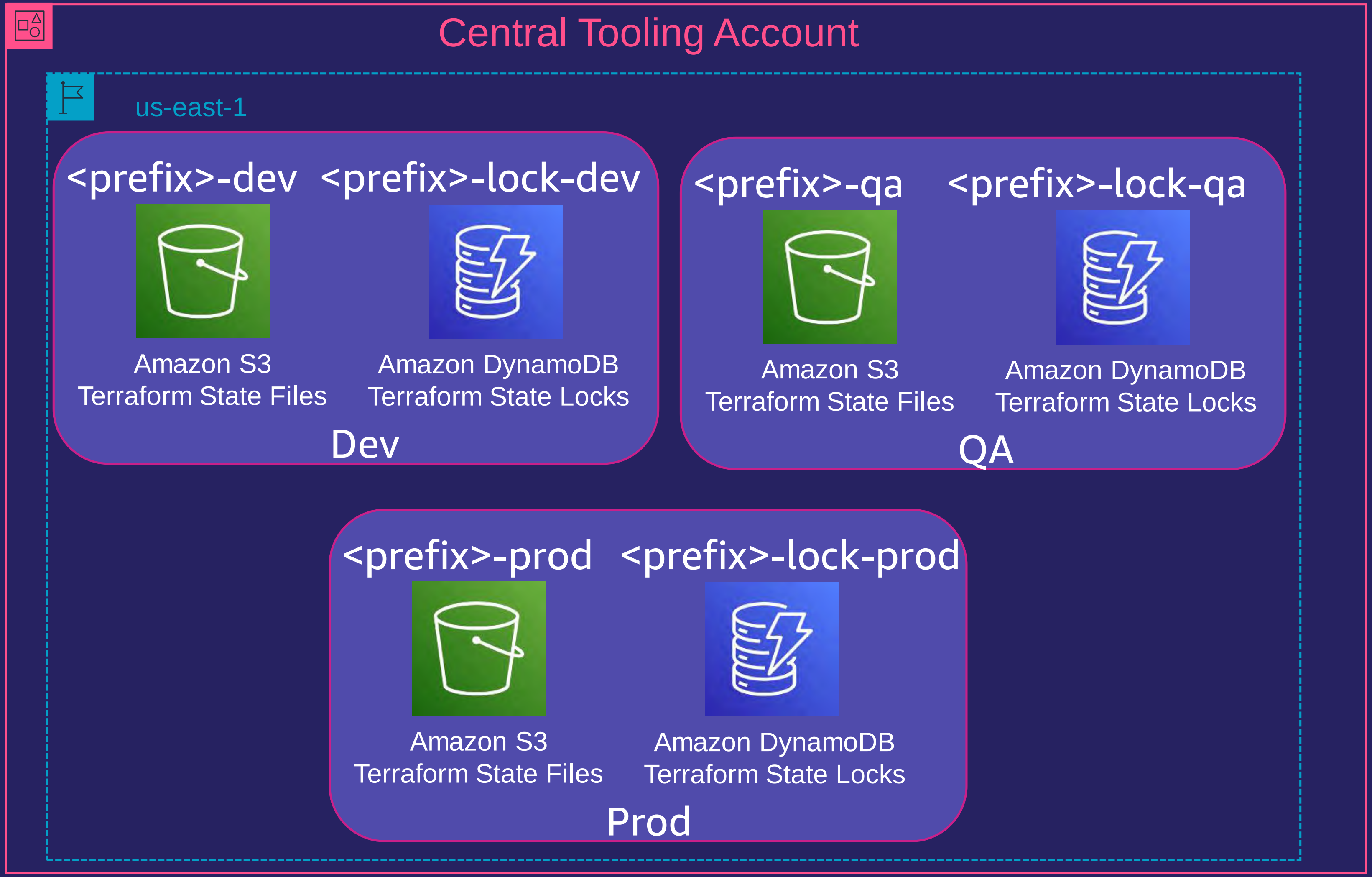
```
bucket=$prefix-$env

dynamodb_table=$prefix-lock-$env
```



Bucket and Amazon DynamoDB table

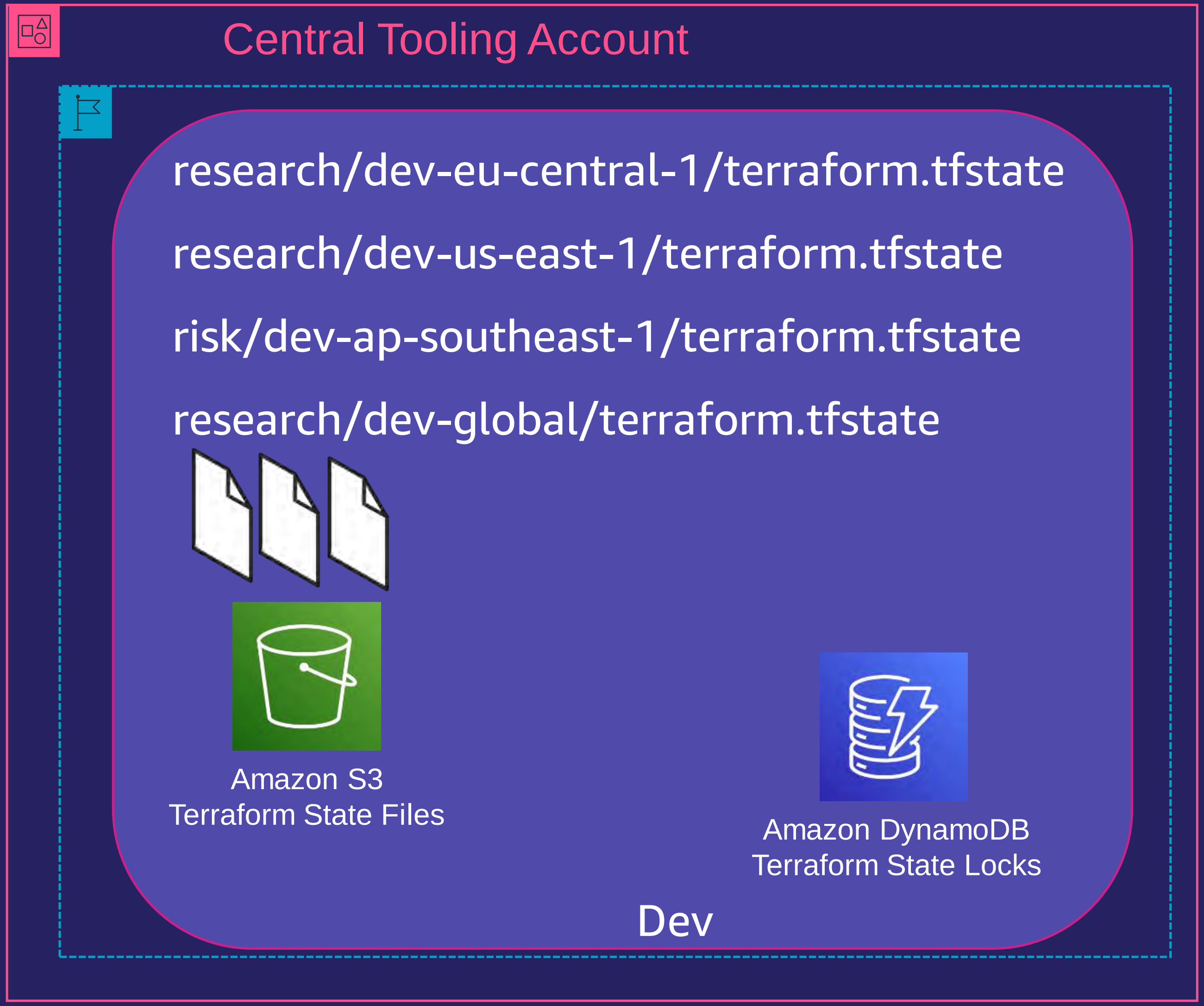
bucket=$prefix-$env”

dynamodb_table=$prefix-lock-$env

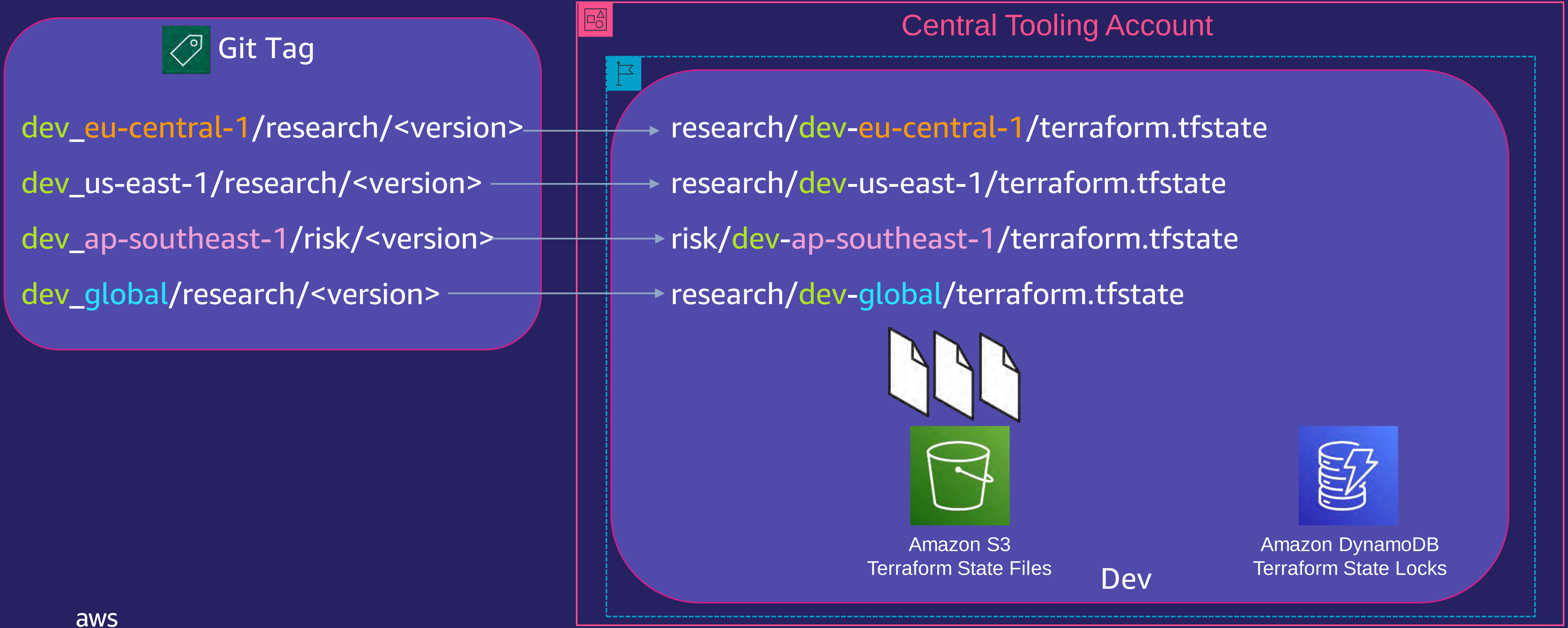


Amazon S3 key

key=$team/$env-$deployment-scope/terraform.tfstate


Central Tooling Account
research/dev-eu-central-1/terraform.tfstate
research/dev-us-east-1/terraform.tfstate
risk/dev-ap-southeast-1/terraform.tfstate
research/dev-global/terraform.tfstate
Amazon S3
Terraform State Files
Amazon DynamoDB
Terraform State Locks
Dev

Git Tag example



Git Tag

dev_eu-central-1/research/<version> → research/dev-eu-central-1/terraform.tfstate

dev_us-east-1/research/<version> → research/dev-us-east-1/terraform.tfstate

dev_ap-southeast-1/risk/<version> → risk/dev-ap-southeast-1/terraform.tfstate

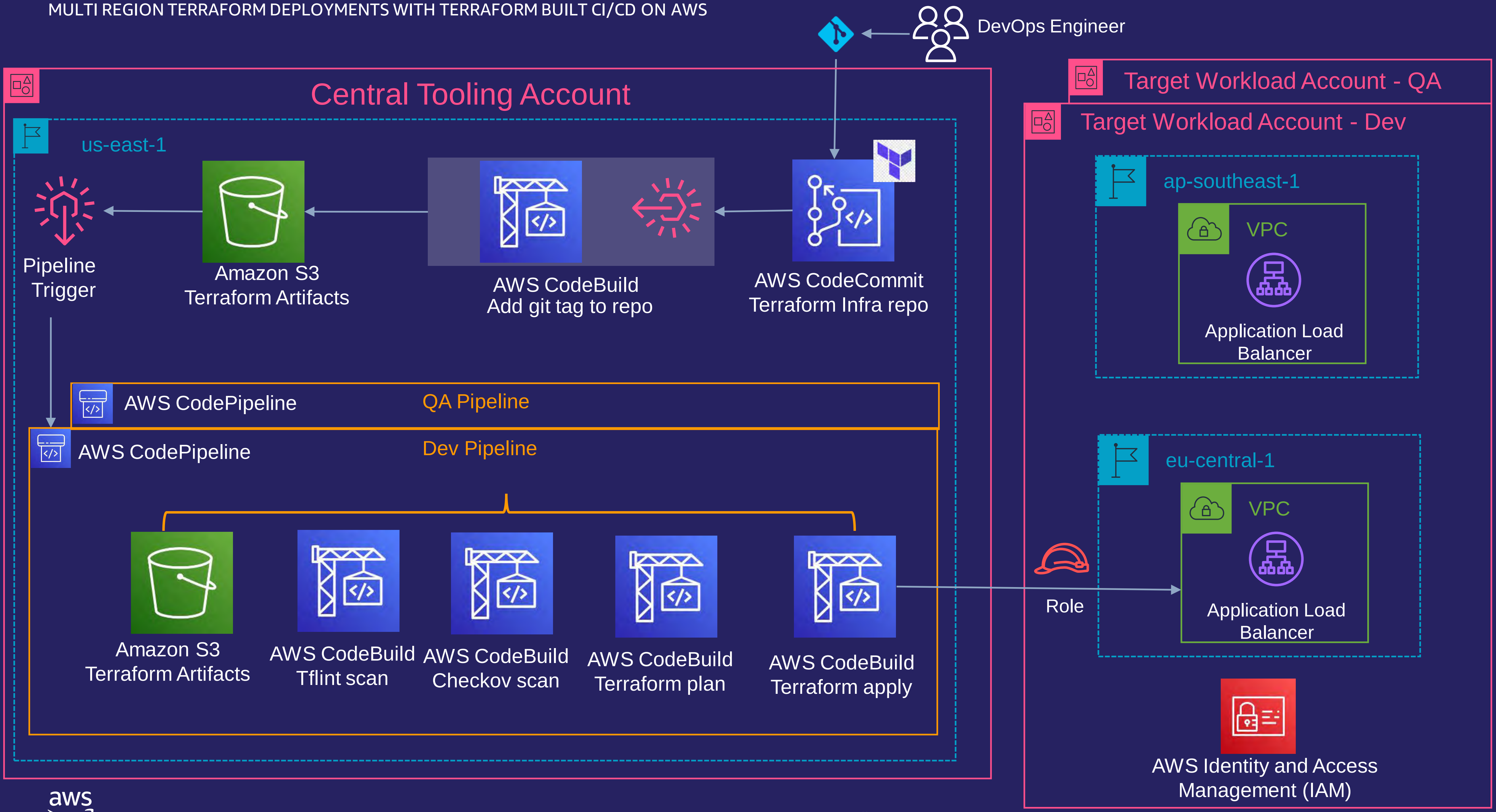
dev_global/research/<version> → research/dev-global/terraform.tfstate

Central Tooling Account

Multi-region Terraform Deployments: Demo and Terraform Code Structure

Multi-region Terraform Deployments: Putting all together

MULTI REGION TERRAFORM DEPLOYMENTS WITH TERRAFORM BUILT CI/CD ON AWS



aws

Key takeaways

Leveraging the pipeline as the single source of truth.

Structure IaC and architect pipeline to maximize reusability and consistency.

Shift left for security.

Thank you!