AWS re:Invent

SEC302-R

DevSecOps: Integrating security into pipelines

Nathan Case
Security Strategist
Amazon Web Services

Jonathan VanKim
Senior Specialist Solutions Architect
Amazon Web Services

AWS re:Invent

aws

Agenda

What is DevOps?

What about DevSecOps?

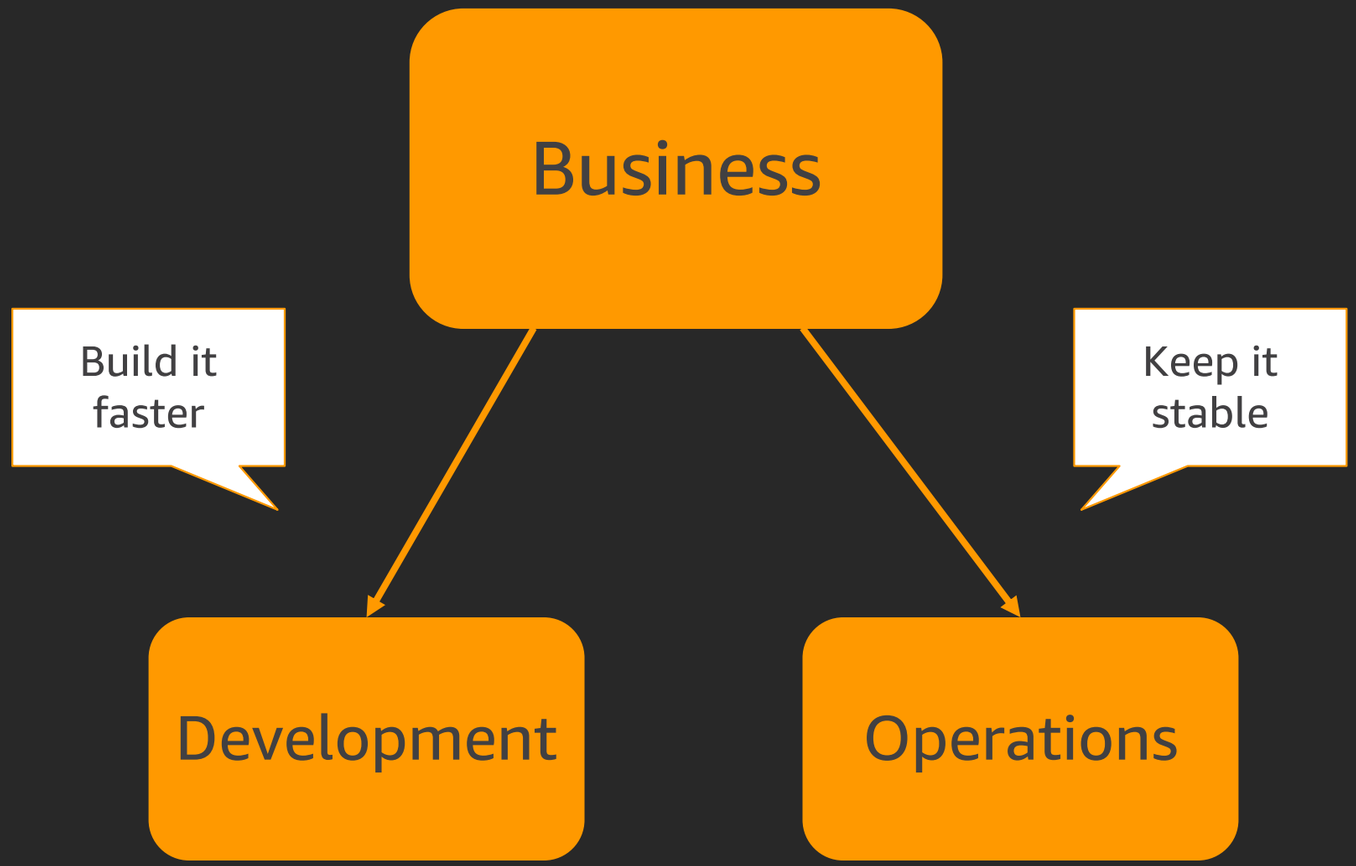
Security of the pipeline

Security in the pipeline

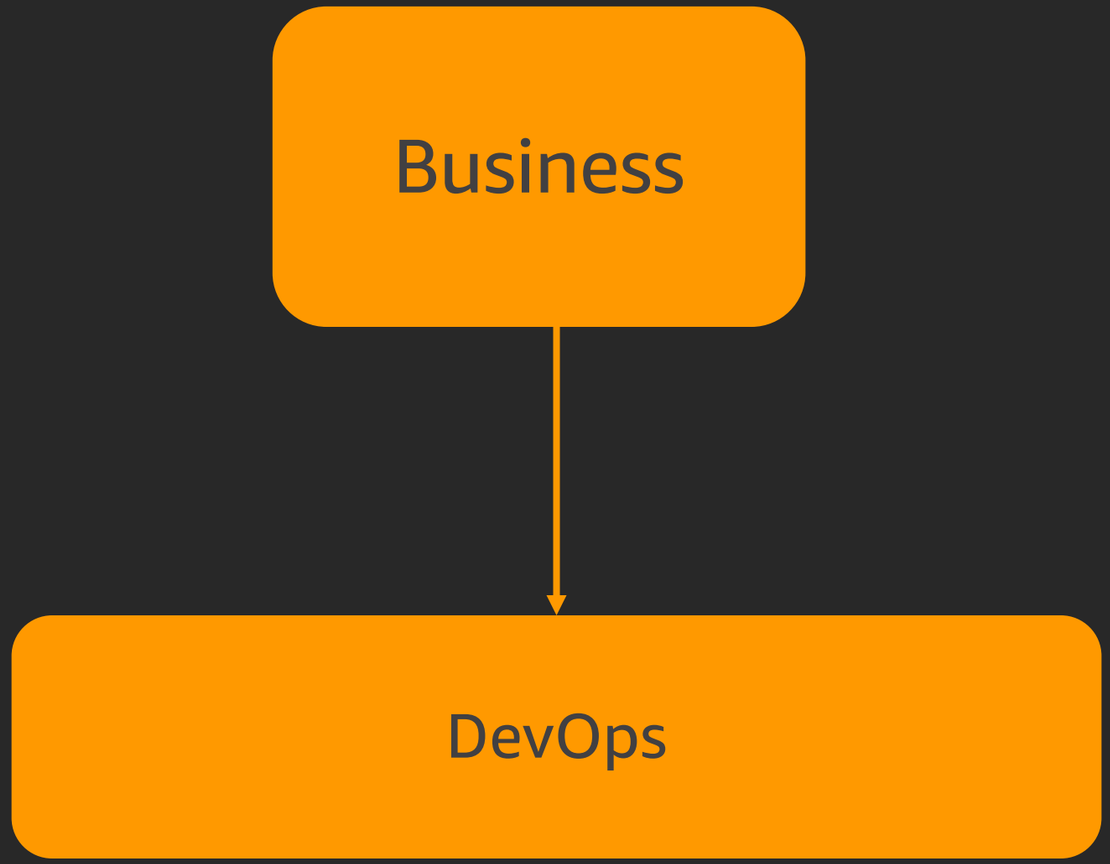
Enforcement of the pipeline

Lab

Competing forces

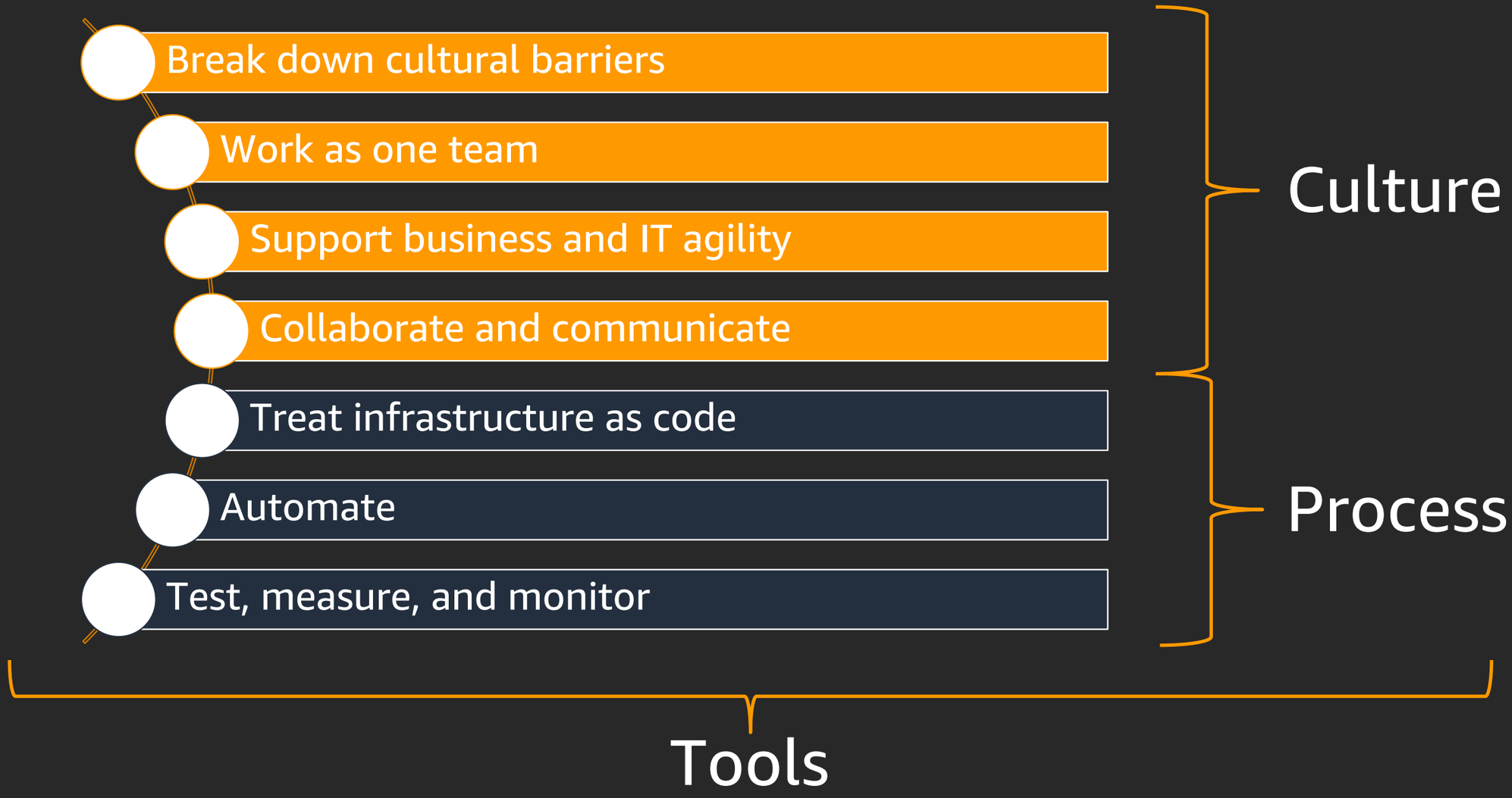


Competing forces

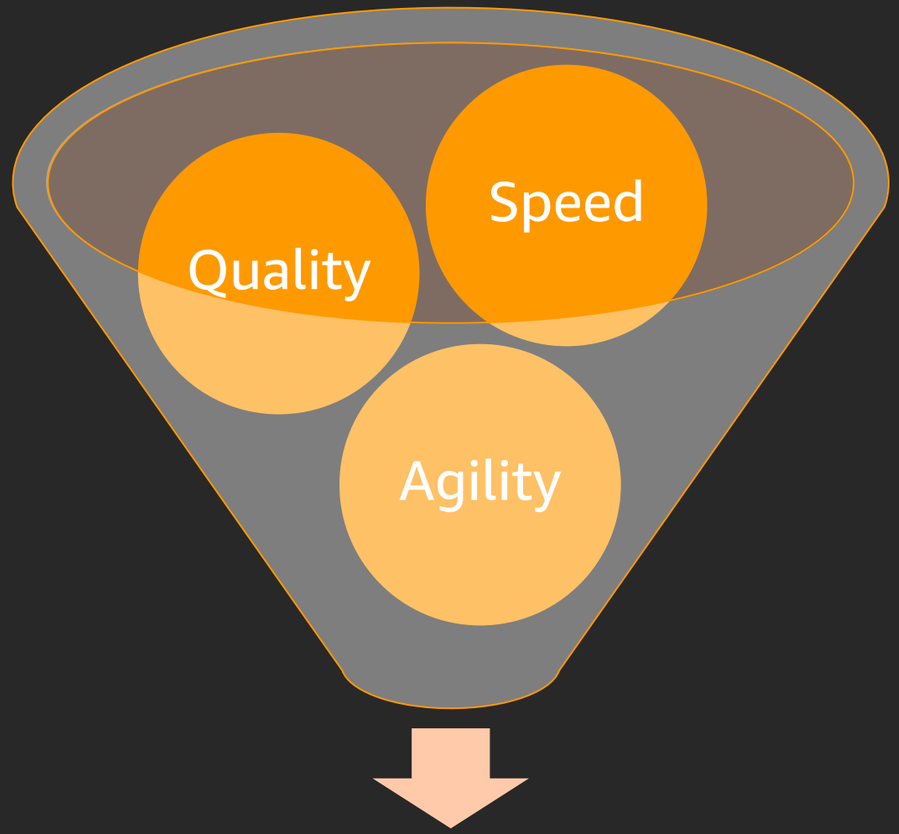


What is DevOps?

What is DevOps?



Why adopt DevOps?



Faster time to value

What is a pipeline?

- Build automation
- Continuous integration
  - Deployment automation
- Test automation
- Service orchestration

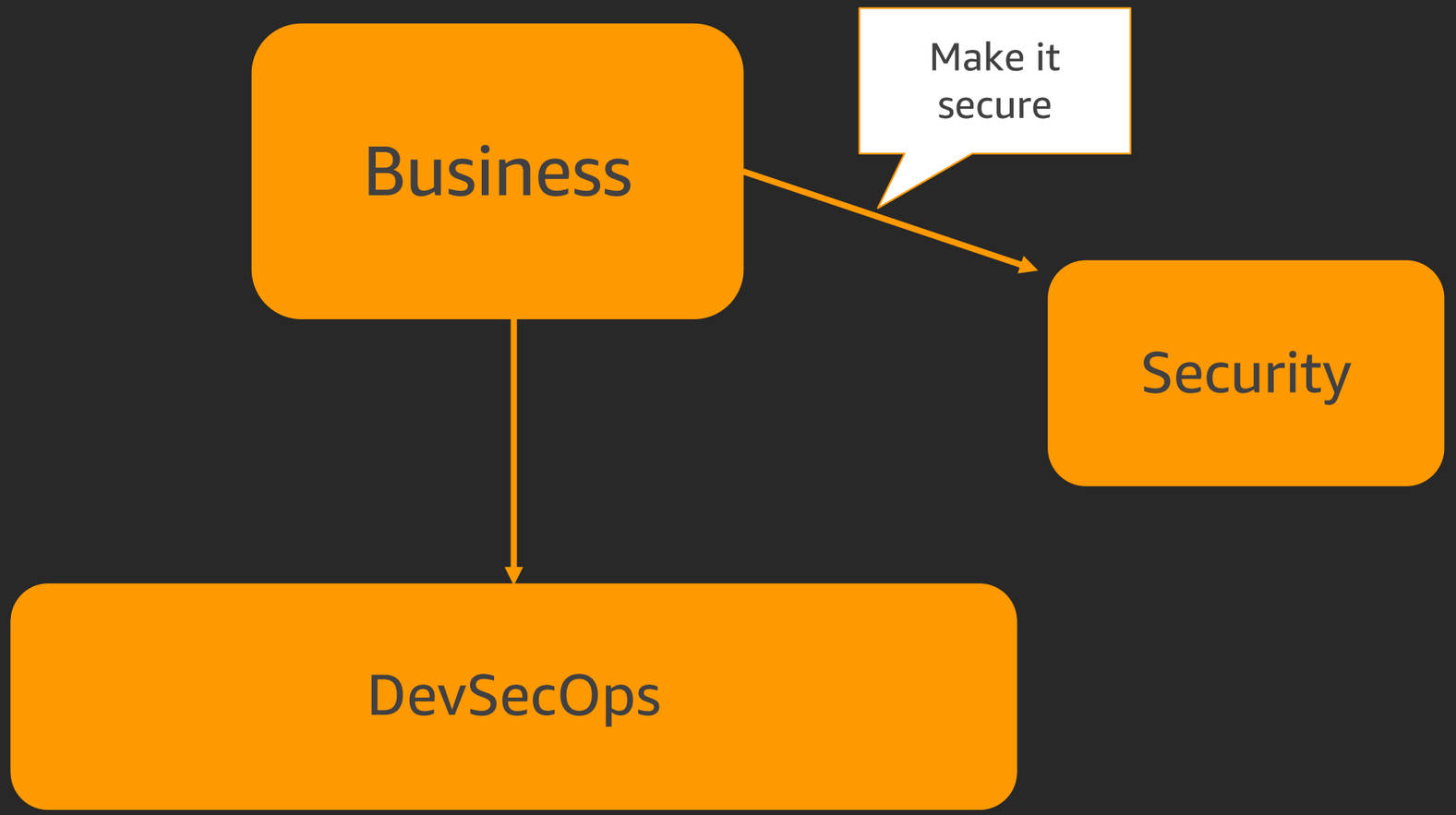
Promotion process in continuous deployment

Continuous Delivery

Continuous Deployment

What about DevSecOps?

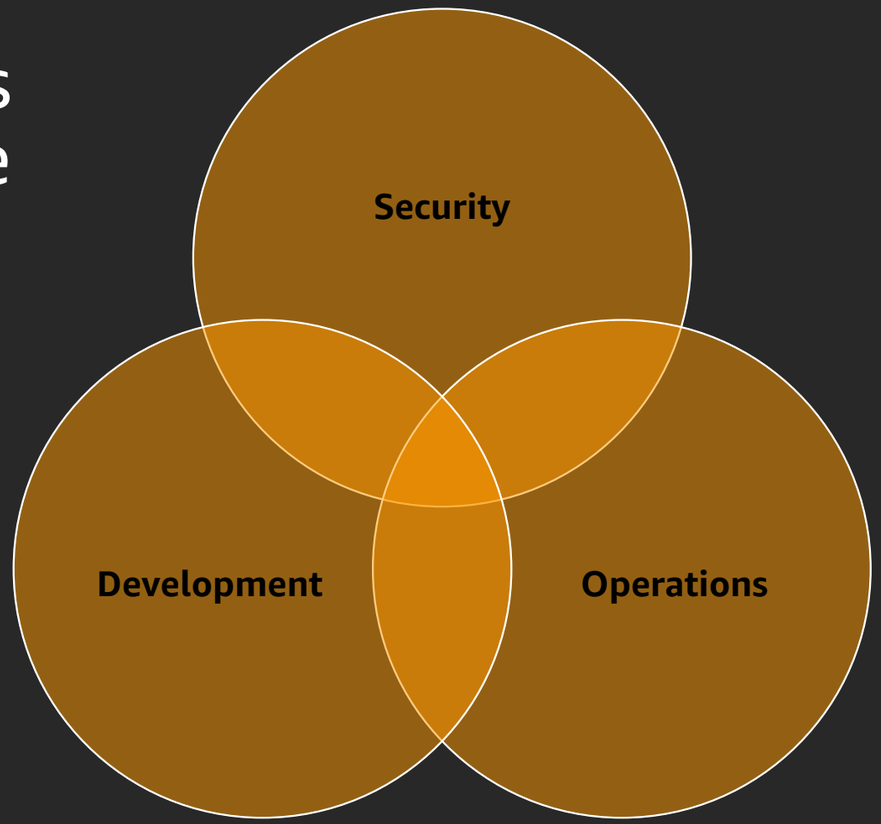
More competing forces



What is DevSecOps?

DevSecOps is the combination of cultural philosophies, practices, and tools that exploits the advances made in IT automation to achieve a state of production immutability, frequent delivery of business value, and automated enforcement of security policy

DevSecOps is achieved by integrating and automating the enforcement of preventive, detective, and responsive security controls into the pipeline



Three major components to DevSecOps

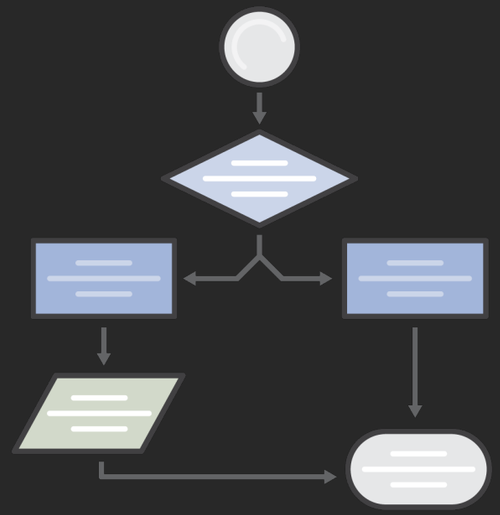
Security OF the pipeline

Security IN the pipeline

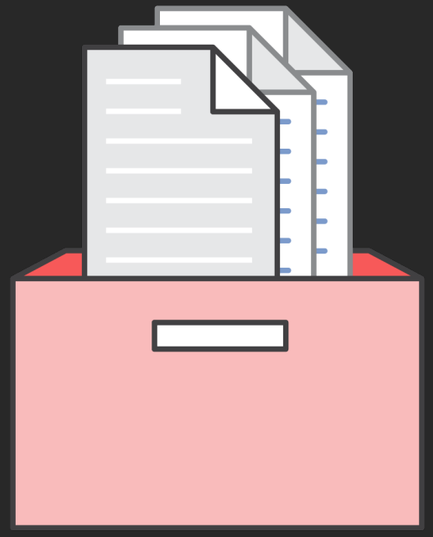
Enforcement of the pipeline

Governance and DevSecOps

Security governance is meant to support business objectives by defining policies & controls to manage risk



Framework

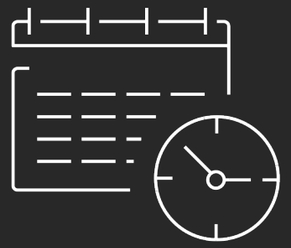


Policies

Business outcomes

Manage risks

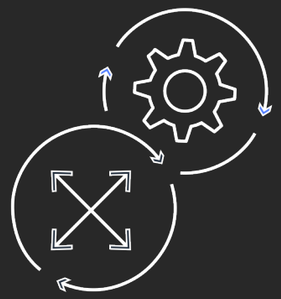
What is DevSecOps?



Test early

Detective WITH responsive controls

Prioritize preventative



Automate, automate, automate

Security OF the pipeline

AWS Cloud Adoption Framework

1 Business

- Align business and IT needs
- Map IT investments to business results

2 People

- Prioritize cloud-based competencies
- Drive organizational readiness

3 Governance

- Manage cloud investments
- Measure business outcomes

4 Platform

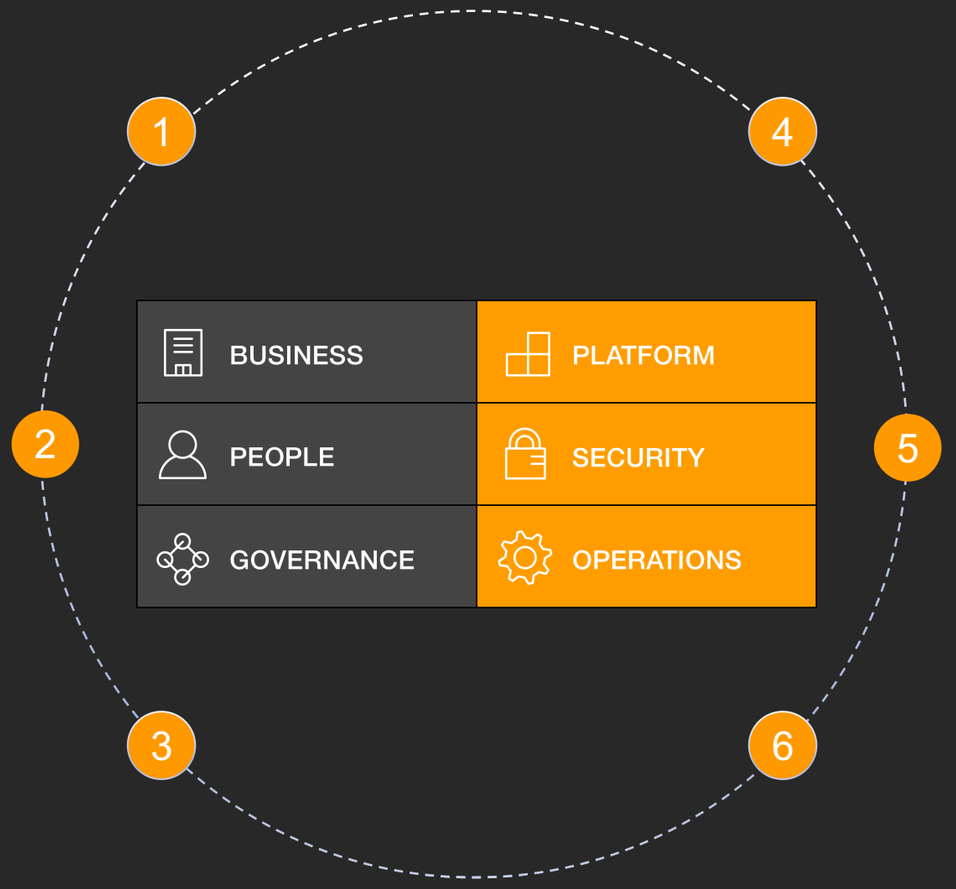
- Provision cloud applications and infrastructure
- Improve cloud services and solutions

5 Security

- Align security and compliance with current requirements
- Manage access and authorization

6 Operations

- Monitor and maintain system health and reliability
- Observe cloud best practices



Align with Cloud Adoption Framework

Identity and access management

Detective controls

Infrastructure controls

Data protection

Incident response

Some IAM risks for pipelines

- Anyone can run build jobs
- Consistent user management across build servers
- Pipeline role is too permissive
- Slave node adverse affects on masters

Enforcing least privilege between pipelines

- Pipeline can perform a specific job
- E.g., Jenkins/Spinnaker/AWS CodePipeline is a pipeline factory
- Pipelines can be limited to blast-radius-based functions
  - Pipeline factory
  - AMI factory
  - Artifact factory

Exercise: IAM for pipelines wrap-up

- Could you write a user story for the DevOps team managing the pipeline to implement?
  - If not, what is missing?
- What are the acceptance criteria for your user story?
- How would you validate your user story?

”As (user/role), I want to be able to (what)?”

Align with Cloud Adoption Framework

Identity and access management

Detective controls

Infrastructure controls

Data protection

Incident response

Detective controls for pipelines

- Who logged in?
- What code was committed and by whom?
- What jobs did they run?
- Did the jobs succeed/fail?
- Was static/dynamic analysis enforced?
- What were the results of the static/dynamic analysis?

Exercise: Detective controls

- What produces logs?
- How are logs produced?
- Where do logs go?
- How do I protect my logs?
- What are the items of interest in my logs?
- At what threshold are those items interesting?
- What should I do when thresholds are exceeded?

Detective controls wrap-up

- There are multiple consumers of logs produced by the pipeline
- Fast feedback to the log consumers is critical
- Results of static/dynamic tests are as important as any other audit trail

Align with Cloud Adoption Framework

Identity and access management

Detective controls

Infrastructure controls

Data protection

Incident response

Infrastructure security risks to pipelines

- Who has access to underlying infrastructure resources?
- How are pipelines patched and updated?
- How is least privilege between pipelines enforced?
- Are my pipelines deploying into approved AWS accounts?
- Does the pipeline align with organizational responsibility?

Infrastructure as code

Infrastructure as code is a practice whereby traditional infrastructure management techniques are supplemented and often replaced by using code-based tools and software development techniques

AWS resources

Operating system and host configuration

Application configuration

AWS CloudFormation

Amazon Virtual Private Cloud (Amazon VPC)
Amazon Elastic Compute Cloud (Amazon EC2)
AWS Identity and Access Management (IAM)
Amazon Relational Database Service (Amazon RDS)
Amazon Simple Storage Service (Amazon S3)
AWS CodePipeline
More

AWS Systems Manager/AWS Secrets Manager

Windows Registry
Linux Networking
OpenSSH
LDAP
Centralized logging
System metrics
Deployment agents
Host monitoring
More

AWS CodeDeploy

Application dependencies
Application configuration
Service registration
Management scripts
Database credentials
More

Infrastructure security for pipelines wrap-up

- The pipeline is a workload and needs to be treated with the same rigor as other critical infrastructure
- Build a pipeline factory to build pipelines from known good configurations
- Deploy workloads into known good environments

Align with the Cloud Adoption Framework

Identity and access management

Detective controls

Infrastructure controls

Data protection

Incident response

Data protection risks for pipelines

- Who can change/commit code?
- How is production data prevented from being introduced into non-prod environments?
- How is artifact integrity maintained?

Top data protection best practices

- Control access and permissions to the code repository
- Trigger builds automatically (time based or event based)
- Use tokenization or dummy data in non-production environments
- Categorize data and enforce restrictions through pipeline
  - For example, pipeline is configured to build the Dev environment but is not allowed to pull production data from repo

Data protection for pipelines wrap-up

- Control access and permissions to source repository: artifacts are critical data for your pipeline
- Build pipelines that are environment aware (e.g., prod vs. non-prod)
- Build artifact handlers to validate integrity across pipelines and environments

Align with the Cloud Adoption Framework

Identity and access management

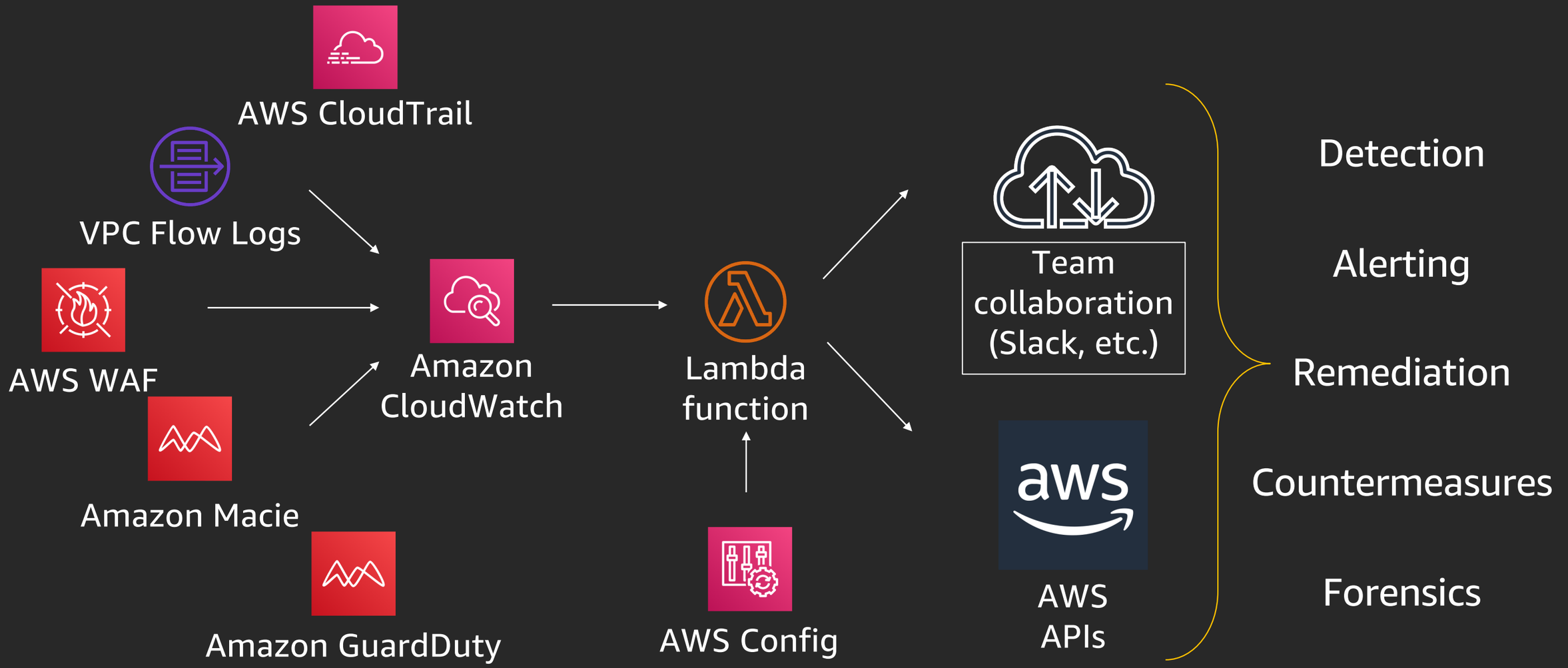
Detective controls

Infrastructure controls

Data protection

Incident response

Pattern for automated remediation



Align with the Cloud Adoption Framework

Identity and access management

Detective controls

Infrastructure controls

Data protection

Incident response

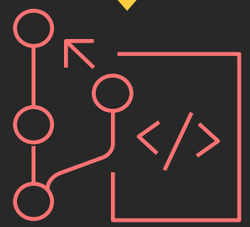
Security IN the pipeline

Pipeline as a workload

- Securing the application starts with securing the pipeline
- The CI/CD pipeline is a workload
- Its purpose is to integrate and deliver other workloads
- It has users, supporting infrastructure, application, data components, etc.
- Those components are typically managed as code

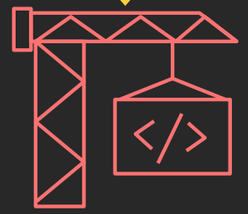
Security IN the pipeline

Code analysis



Code

Dependencies



Build

Vulnerability scan

Test

Hash verification

Deploy

Automated

Monitor

Security IN the pipeline

Static analysis

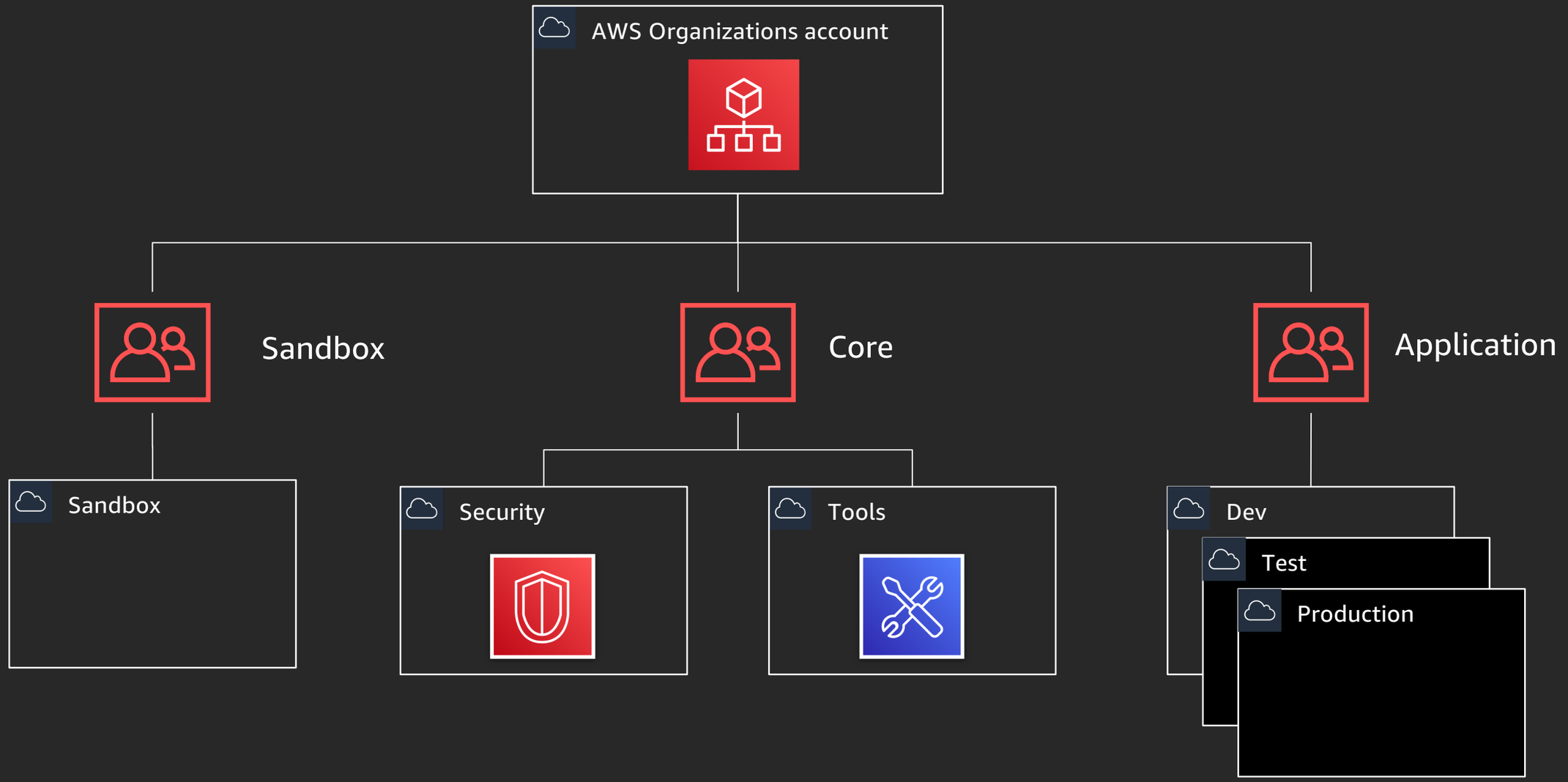
- Infrastructure as code
- Security as code

Dynamic analysis

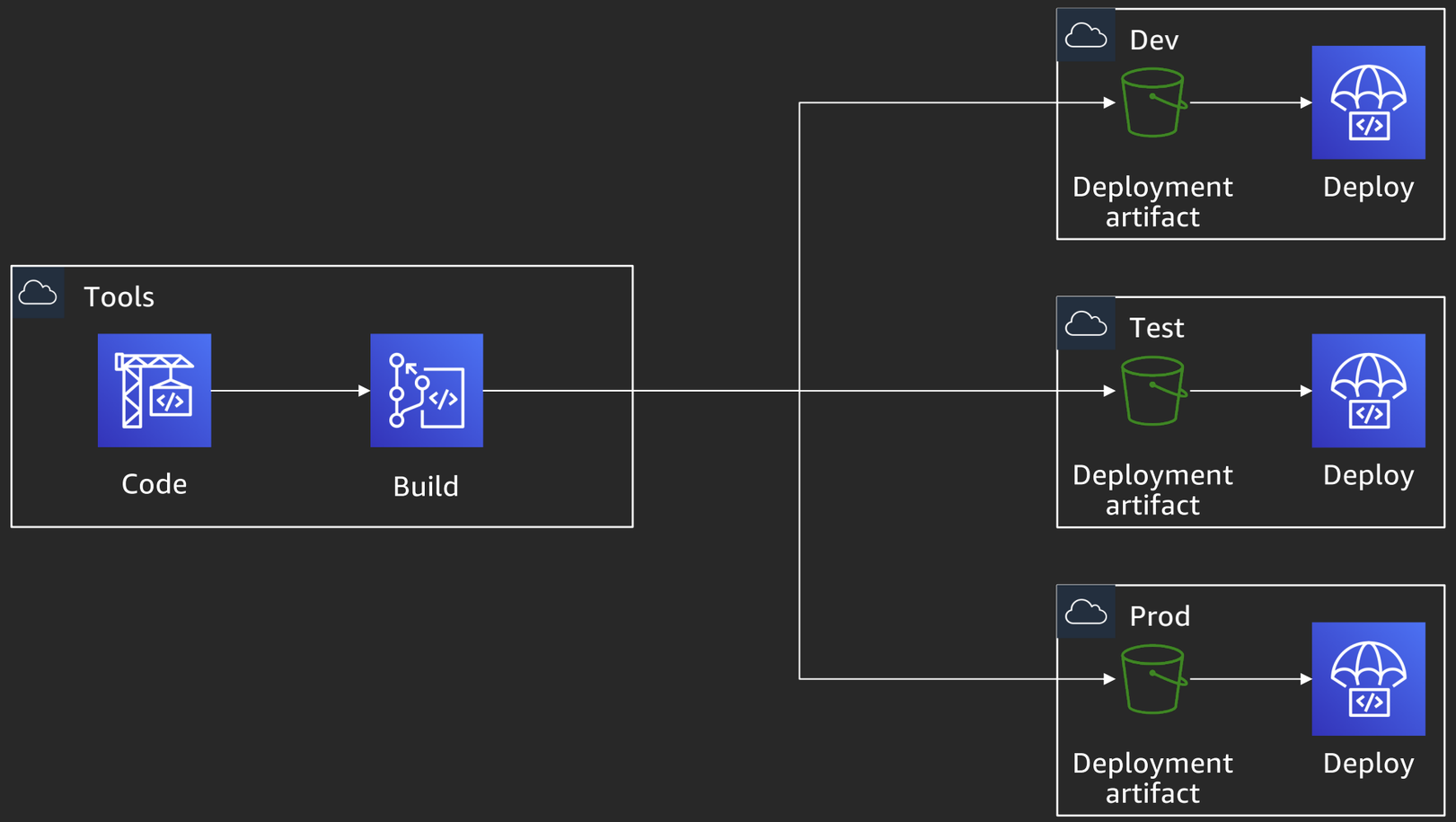
- Unit tests
- Integration tests
- System tests

Enforcement of the pipeline

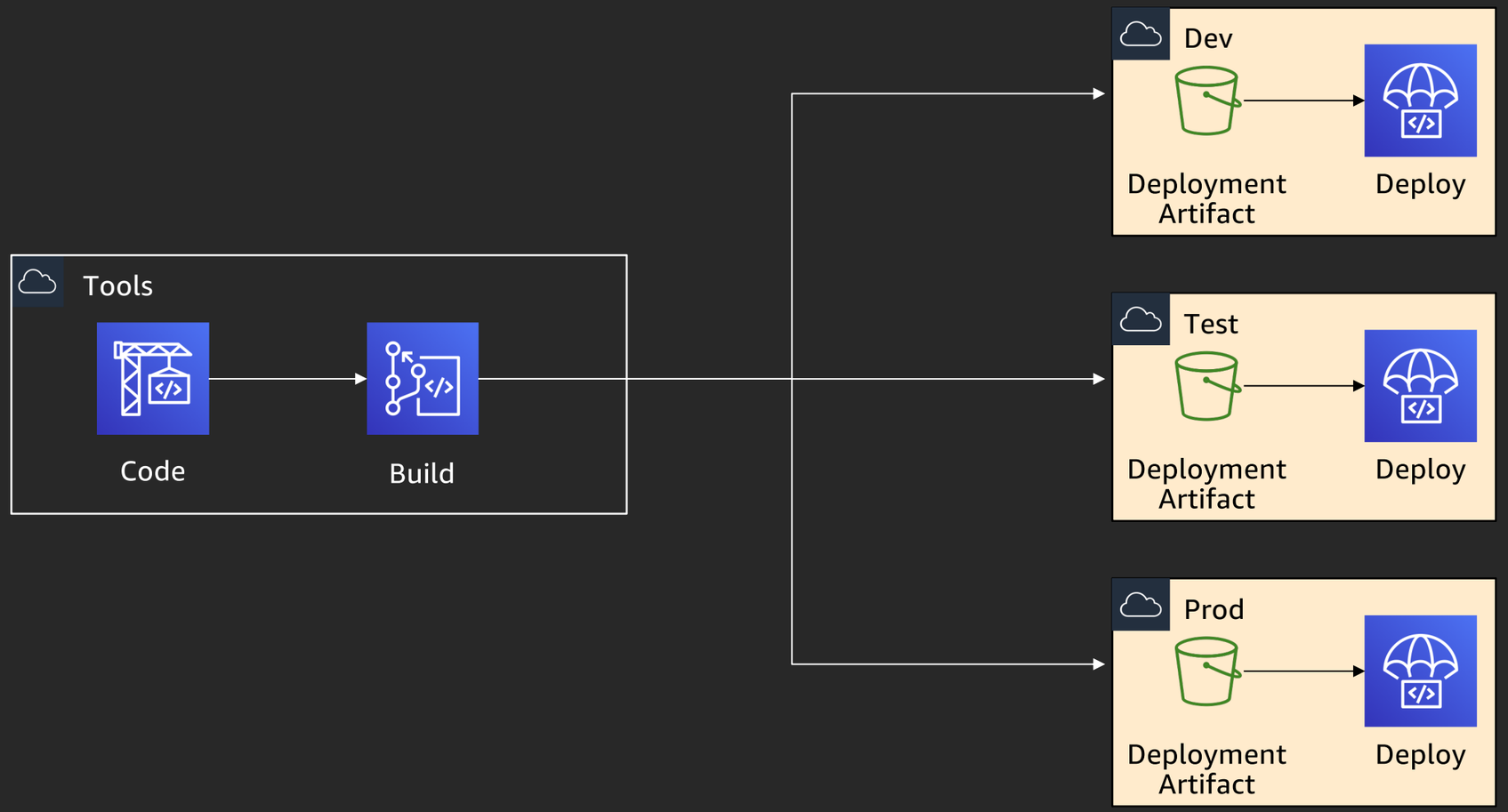
Separation of duty – Multi-account strategy



Separation of duty – Multi-account strategy



No more humans in productions



Three major components to DevSecOps

Security OF the pipeline

Security IN the pipeline

Enforcement of the pipeline

DevSecOps benefits

- Confidence validated against corporate security policies
- Consistency and repeatability of security validation
- Match the business pace of innovation
- Security at scale

Lab time

Lab time

- Download the lab bundle here: https://devops.awssecworkshops.com
- Join/create a group of 4 and come up here for a temp account
- Once you have an account, go to https://dashboard.eventengine.run/login, and enter your code

Learn security with AWS Training and Certification

Resources created by the experts at AWS to help you build and validate cloud security skills

30+ free digital courses cover topics related to cloud security, including Introduction to Amazon GuardDuty and Deep Dive on Container Security

Classroom offerings, like AWS Security Engineering on AWS, feature AWS expert instructors and hands-on activities

Validate expertise with the **AWS Certified Security - Specialty** exam

Visit aws.amazon.com/training/paths-specialty/

aws training and certification

Thank you!

AWS re:Invent

aws

Please complete the session survey in the mobile app.