



Security in a DevOps Environment

PRESENTED BY:

Shain Singh, Security Architect [APCJ]

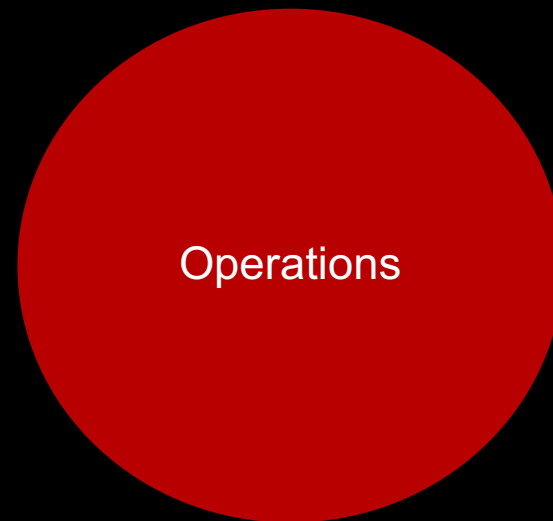
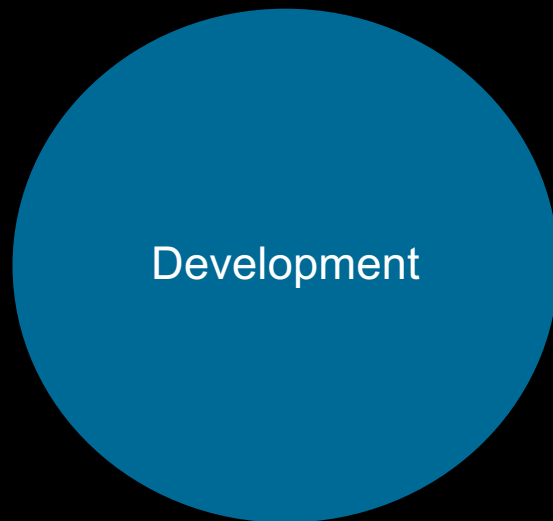
Refresher

In Super-NetOps Class 1 and 2 we covered:

- Foundations of Automation & Orchestration
- Automation & Orchestration of F5 technology using declarative and imperative API's
- Continuous Delivery & Deployment
- DevOps Methodologies
- Infrastructure & Code
- Building an F5 toolchain

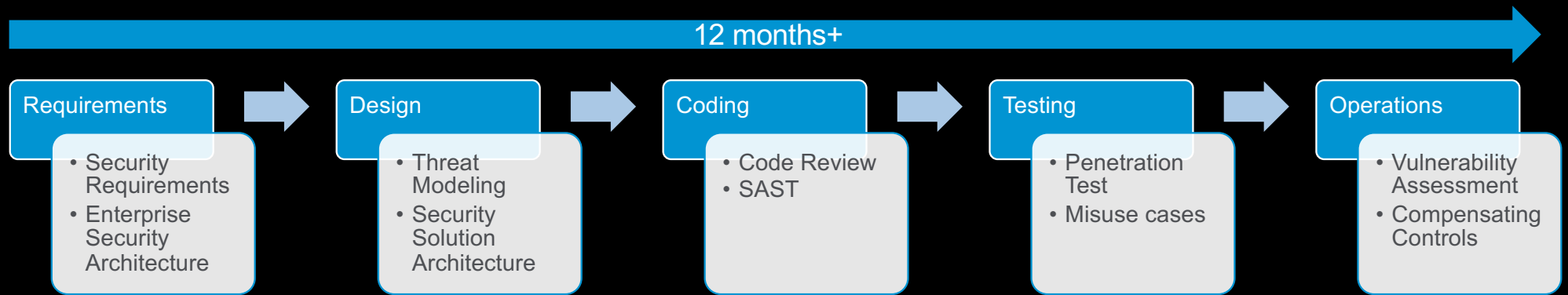


Organizations are Transforming



Adopting DevOps & Continuous Integration processes

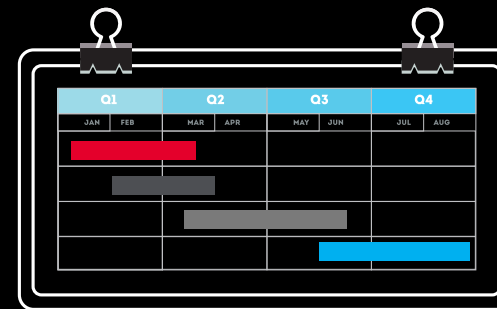
Security in the Waterfall AppDev SDLC



800-64: Security Considerations in the SLDC
<https://csrc.nist.gov/publications/detail/sp/800-64/rev-2/final>

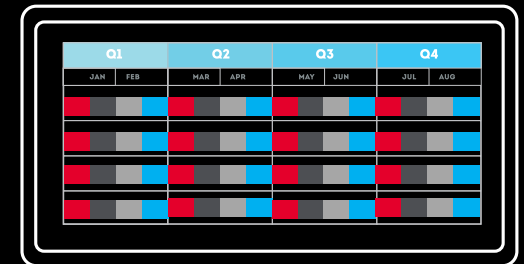
DevOps, Agile breaks traditional AppSec

- Cycle time for Application development is getting shorter – being developed and released faster than ever before using agile, iterative methods.
- Traditional models for application security **can't scale to the speed of delivery required by agile teams**



Traditional waterfall

Agile DevOps



Applications are exposed to significant security risks

- Injections
- Credential Stuffing
- Deserialisation Attacks
- Transport layer attacks
- Man in the browser malware
- Denial of Service attacks



F5 Labs Application Protection Report

https://interact.f5.com/2018ALLFNetOpsMeetsDevOpsTheStateofNetworkAutomation_DownloadBookPage.html

Deliver more frequent releases to get new capabilities to market faster

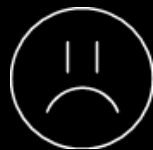
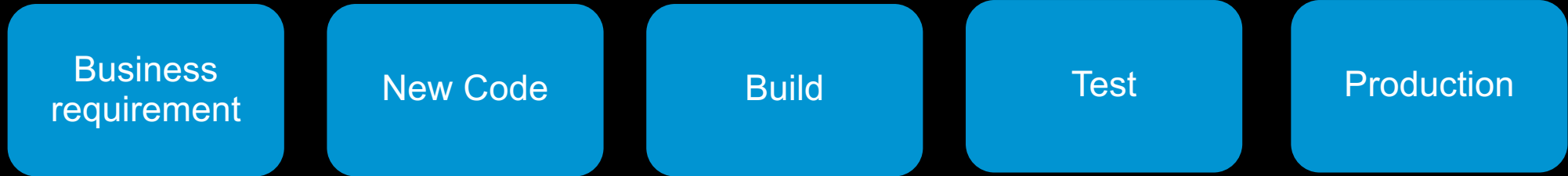
app

app

app



It's all about speed



Find out about an application code change or feature release late in the development process



IT Security
(Traditional)

It's all about speed

Business
requirement

New Code

Build

Test

Production



IT Security
(Traditional)

Something got blocked – Inconsistency between development environment and production.
Delays in resolution awaiting SecOps response – no rollback

Business Perception: Security is preventing business/breaking the app

In digital led businesses, the

SPEED TO MARKET

**trumps traditional security and
operational processes.**

Security is important but must adapt.

Cultural Shift

FROM

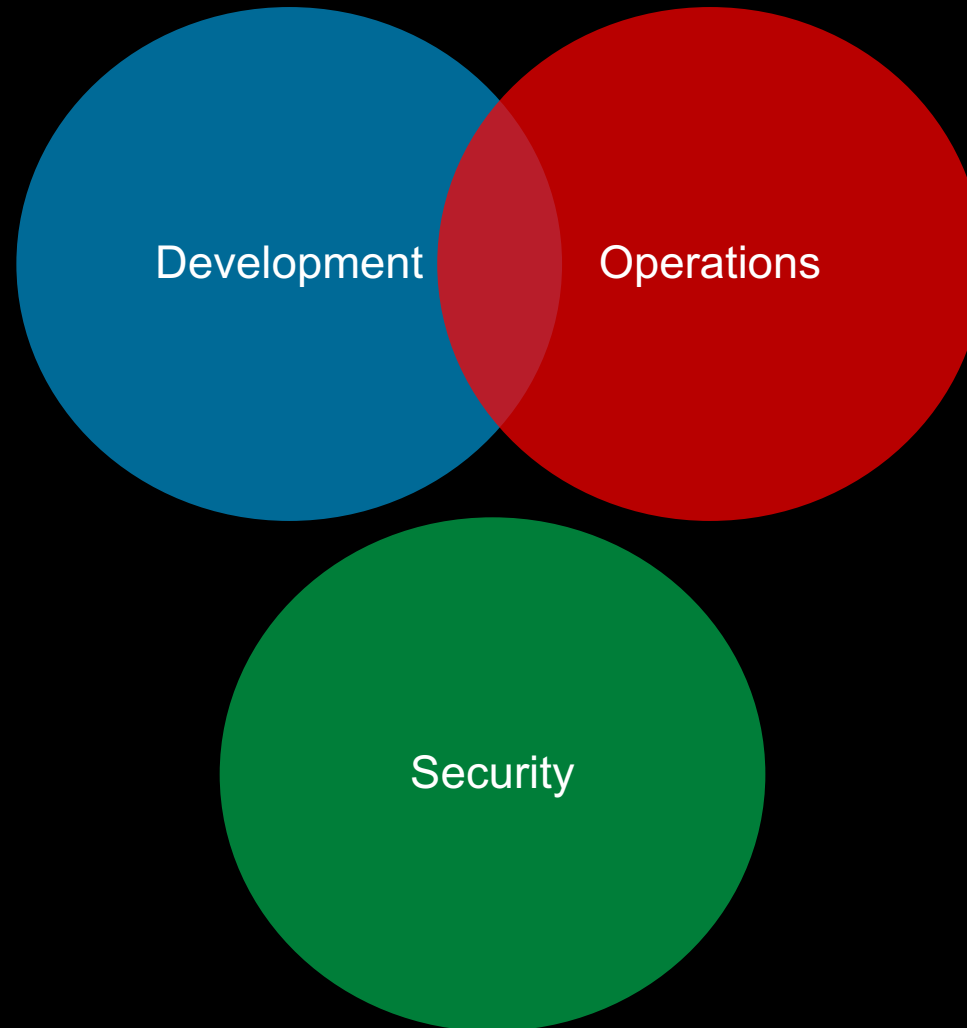


TO

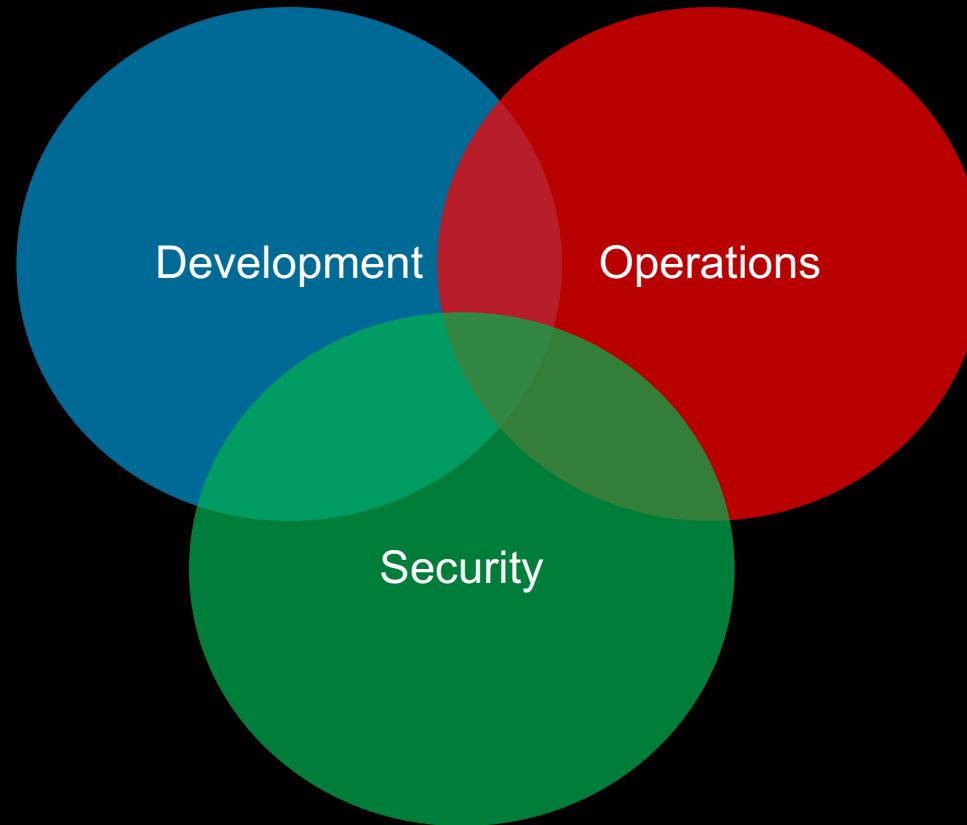
A shift away from the
“gatekeeper” mentality.

In a DevOps mentality,
security is everybody’s
responsibility.

Breaking Down the Silos



Building Collaboration



Increasing collaboration and feedback between SecOps and DevOps.

DevSecOps Principles



**Breaking down
the silos**



**Nurturing
security
champions**



**Making the
secure path the
easy path**



Shifting Left



**Continuous
Testing/Test
automation**

The Pipeline

Build

Test

Package

Deploy

Verify

Rollback

CI

CD



Security Shifting left

Business requirement

New Code

Build

Test

Production



Security Shifting Left

Cost and Impact

The earlier that security requirements can be addressed in the Software Development Life Cycle, the less the cost and impact. To address this, security needs to shift left. Many of the low-hanging software vulnerabilities can be addressed by providing secure coding practices and skills to developers and by building tools such as static and interactive code analysis into the pipeline.

- It's always faster, cheaper to address application vulnerabilities as early in the SDLC as possible.
- Security awareness training for developers can reduce vulnerabilities being introduced into code.
- By building testing SAST/DAST etc. into the pipeline you can capture low hanging vulnerabilities, continuously improve.
- However, targeting "perfect security" - identifying and resolving all vulnerabilities before release - is incompatible with DevOps cadence.
- Advanced WAF can be built as a compensating control using automation driven by the developer's pipeline to guard against unidentified and advanced threats to the application.

Test Automation

Automation is the key to controlling vulnerabilities and advanced threats to web applications within the DevOps environment. Security organizations can focus on creating automated tests to ensure security controls are effective and that security services can be consumed without friction by DevOps teams.

Test automation is key to the DevOps effort. By building and automating test cases at all stages of the pipeline - develop, acquire, build, release, and operate - we can test for vulnerabilities that are not introduced within code commits using static code analyzers. We can ensure that controls are in-place and effective and that security issues cause and attacks are appropriately handled or blocked.

© 2018 FS Networks

Test Automation

Build

Test

Package

Deploy

Verify

Rollback



Allows you to incorporate abuse-test cases and attempts to exploit system vulnerabilities in order to ensure that your infrastructure is identifying and blocking those attempts.



Summary



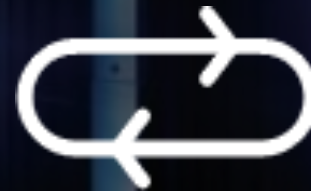
Breaking down
the silos



Shifting Left



Nurturing
security
champions



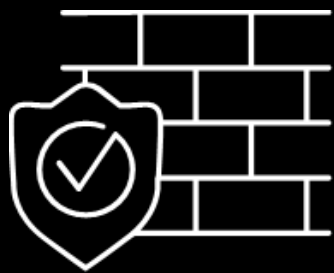
Continuous
Testing/Test
automation



Making the
secure path the
easy path

Building Advanced WAF into the CI/CD pipeline – Security as Code

Addressing every vulnerability at the release cadence required of today's DevOps teams is **impractical**.



F5 Advanced Web
Application Firewall (WAF)



Application layer distributed
denial of service

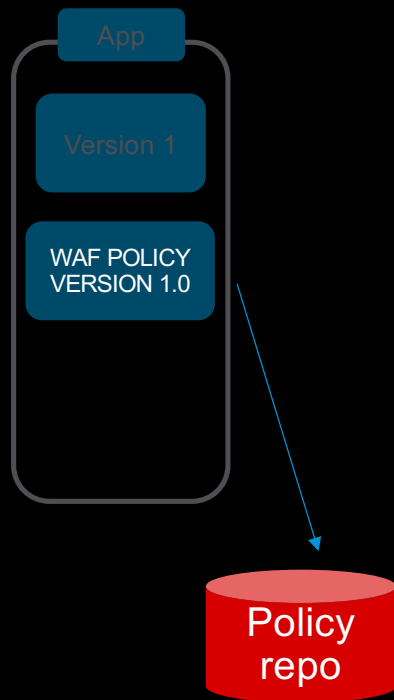
Credential stuffing

Man in the browser credential
stealing

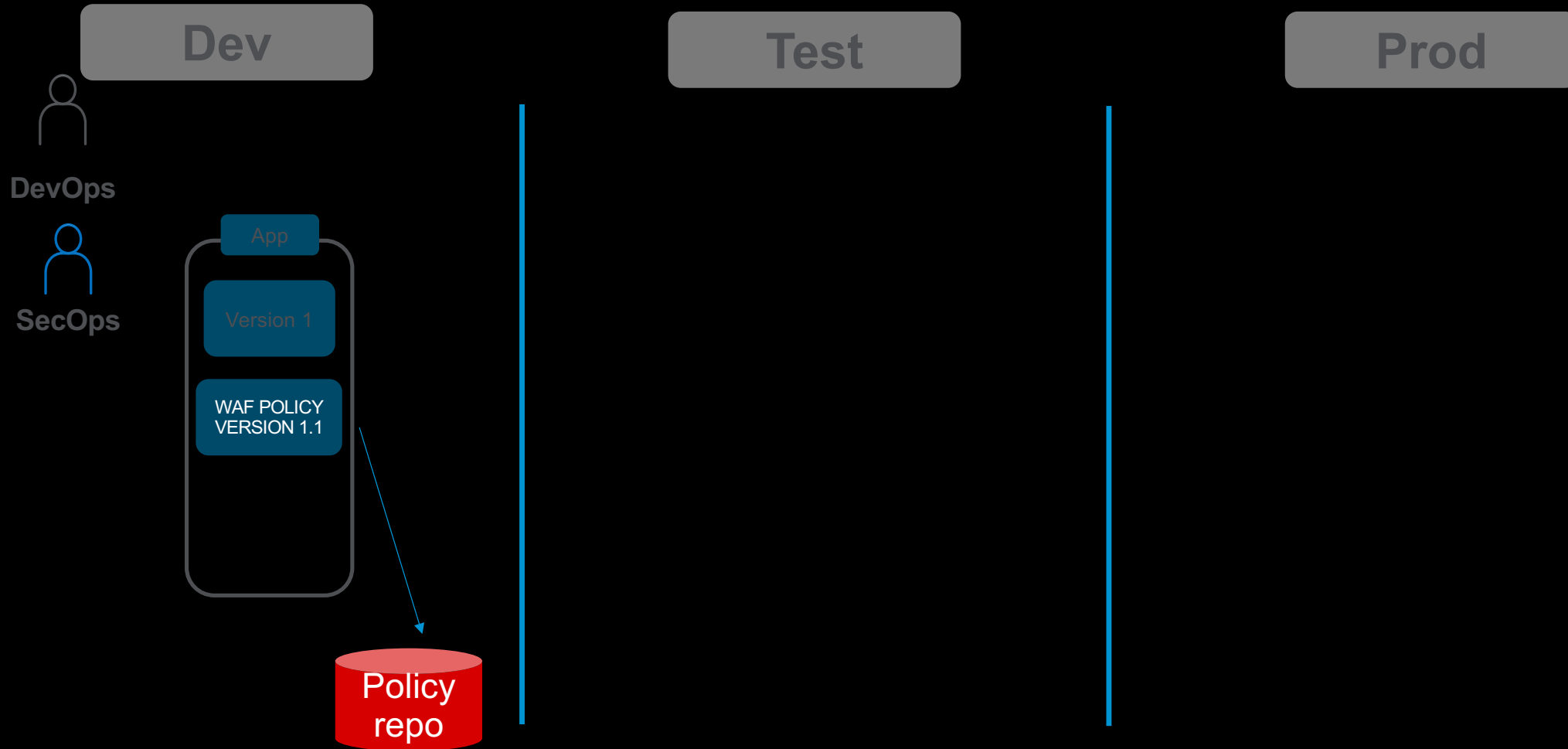
Creation of a policy template

Linux-high - CVE Vulnerabilities + Bot Protection

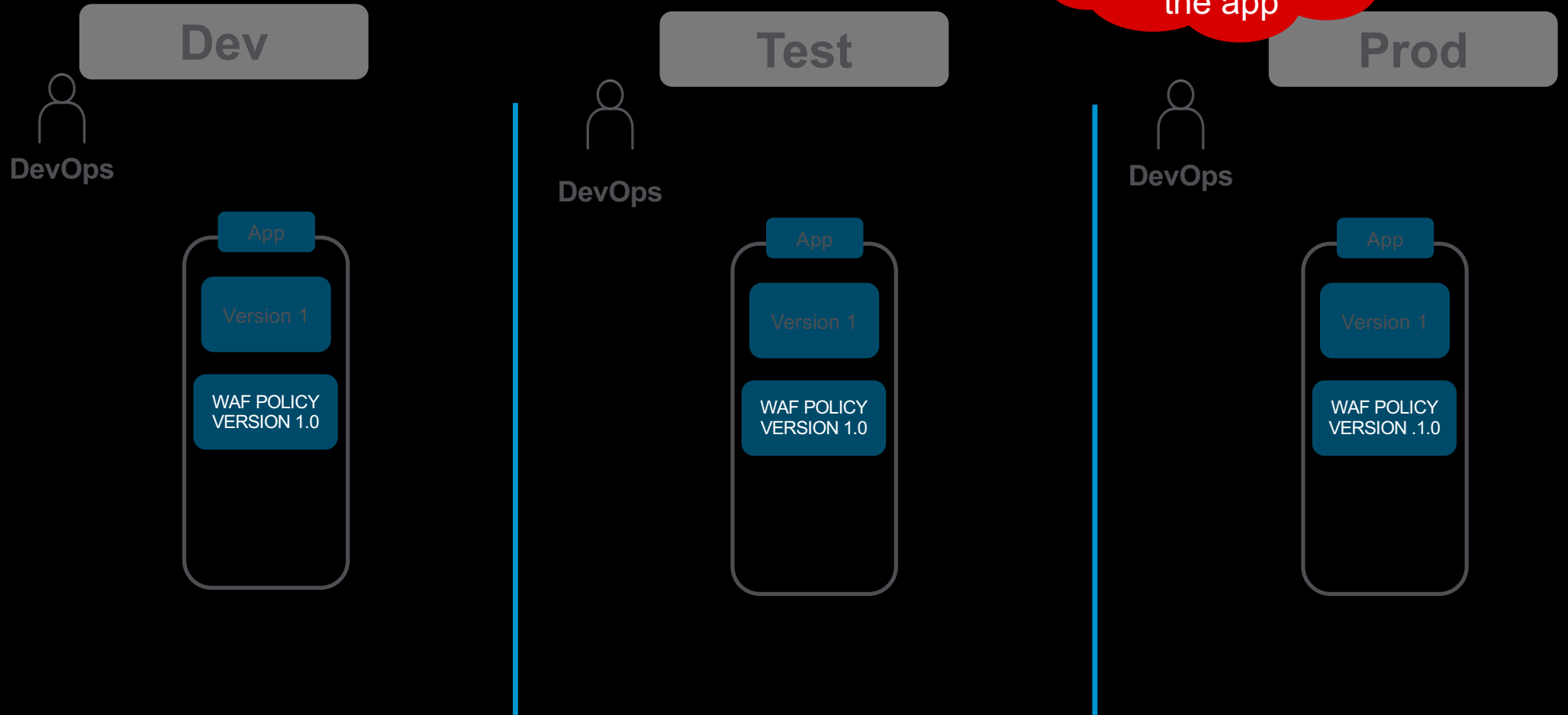

SecOps



Deployment of a policy to DEV



Deployment of a policy to DEV



Benefits

SecOps:

1. **Focus on security** not on button pushing
2. Not involved in rollbacks
3. Enables faster adoption of **advanced security features**.

DevOps (Tools team) :

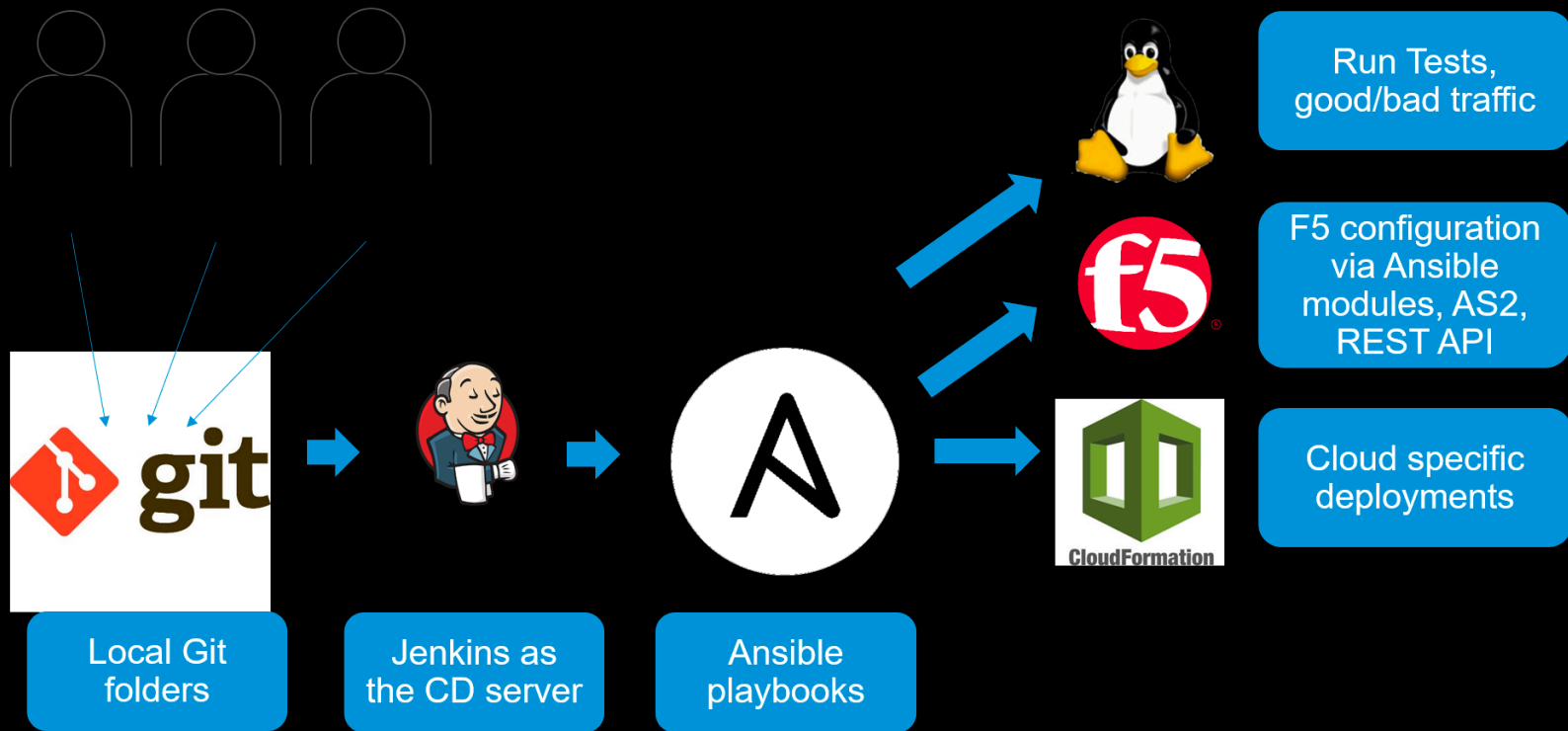
1. Clear **visible changes**
2. Changes are part of the pipeline – enables **continuous improvement of the deployment**
3. Enables advanced deployments – blue/green , canary - **increases reliability**

App owner:

1. Security policy is deployed early in development and enables **faster time to market**.
2. Choses what are the features that make sense for him and have '**control over his destiny**'

Lab

- Managing AppSec as code via a CI/CD pipeline





SOLUTIONS FOR AN APPLICATION WORLD