



sec4dev

26C7q6A

So Happy Together

Making the Promise of DevSecOps a Reality



Hacker/Researcher/Advocate

BISO*

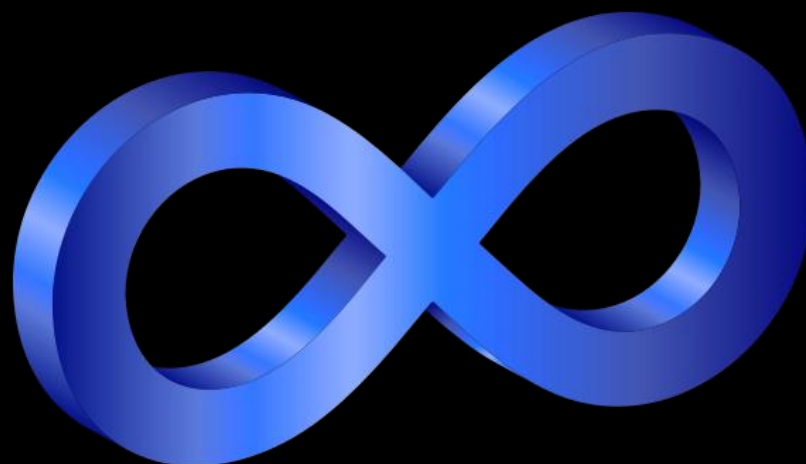
S&P Global
Ratings

10 Years Dev/16 Years Sec

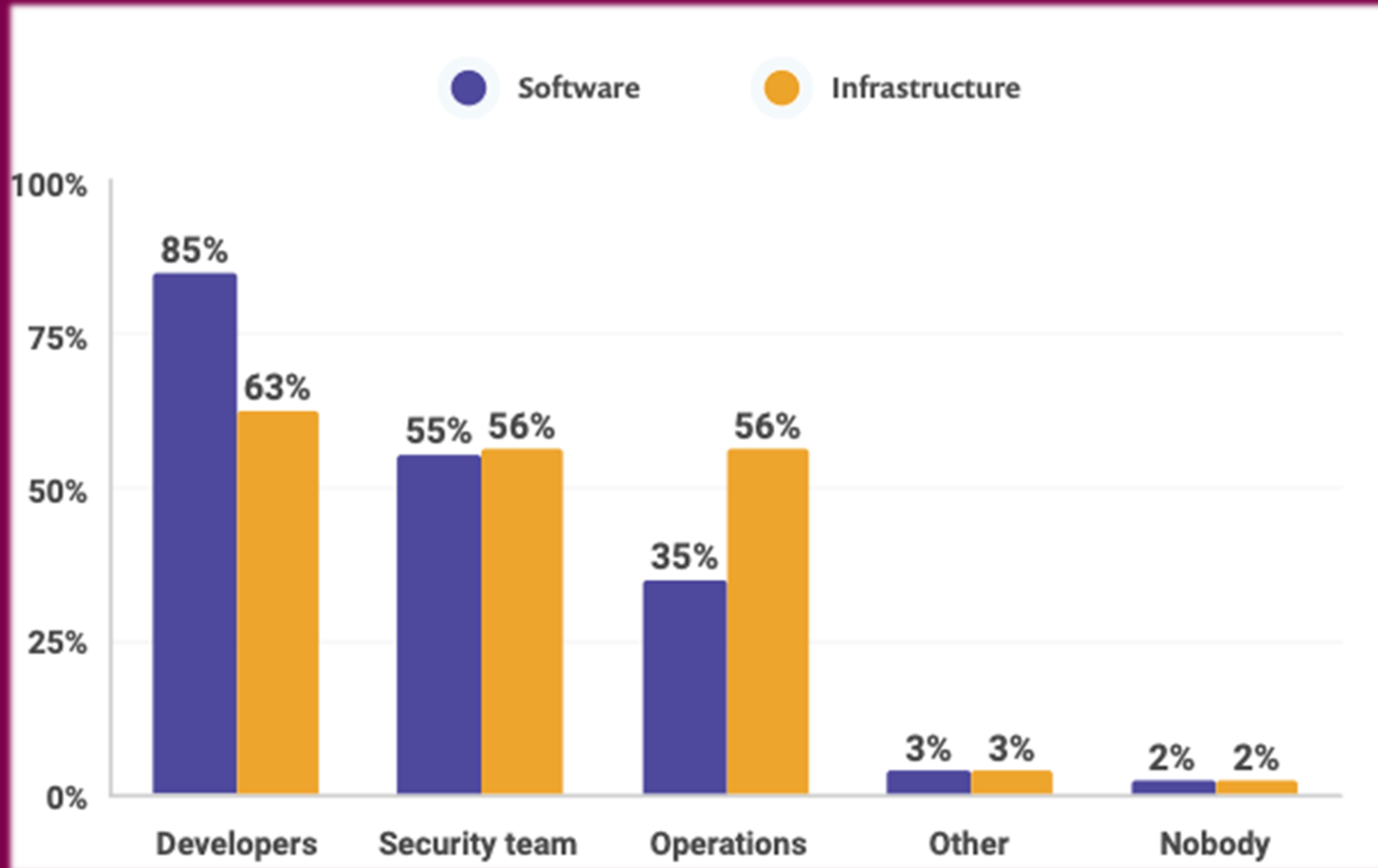
Author/Blogger/Podcaster

*What is a BISO?

<https://alyssasec.com/2020/12/what-is-a-business-information-security-officer>



Who is responsible for security?



SOURCE: Snyk State of Open Source Security 2020 - <https://snyk.io/open-source-security/>

WHAT'S IN YOUR SOFTWARE?

```

), window.confirm(vp.themes.
a"}).fadeOut(350, function()
, e.trigger("themes:update")
enshotCheck: function(a) (var
ick .close-full-overlay">vi
review"), render: function()
ter.navigate(c.router.baselin
. $el.addClass("iframe-ready"
.removeClass("iframe-ready")
rigger("preview:close"), this
, this.$el.toggleClass("calle
view-device", c), this.toggle
.attr("aria-pressed", !0)).An
s("disabled") || (vp.update(a
)))))}}), c.view.Themesvp.$el
)

```

```

<project xmlns="http://maven.apache.org/POM/4.0.0" xm
xsi:schemaLocation="http://maven.apache.org/POM/4.0
<modelVersion>4.0.0</modelVersion>
<groupId>com.yourorganization</groupId>
<artifactId>my-application1</artifactId>
<packaging>jar</packaging>
<version>1.0-SNAPSHOT</version>
<name>my-application1</name>
<url>http://maven.apache.org</url>
<dependencies>
  <dependency>
    <groupId>junit</groupId>
    <artifactId>junit</artifactId>
    <version>3.8.1</version>
    <scope>test</scope>
  </dependency>

```

280 Original Lines of Code

8 Dependencies (89 Sub-Dependencies)

2.4M Total Lines of Code

What about those ops teams?



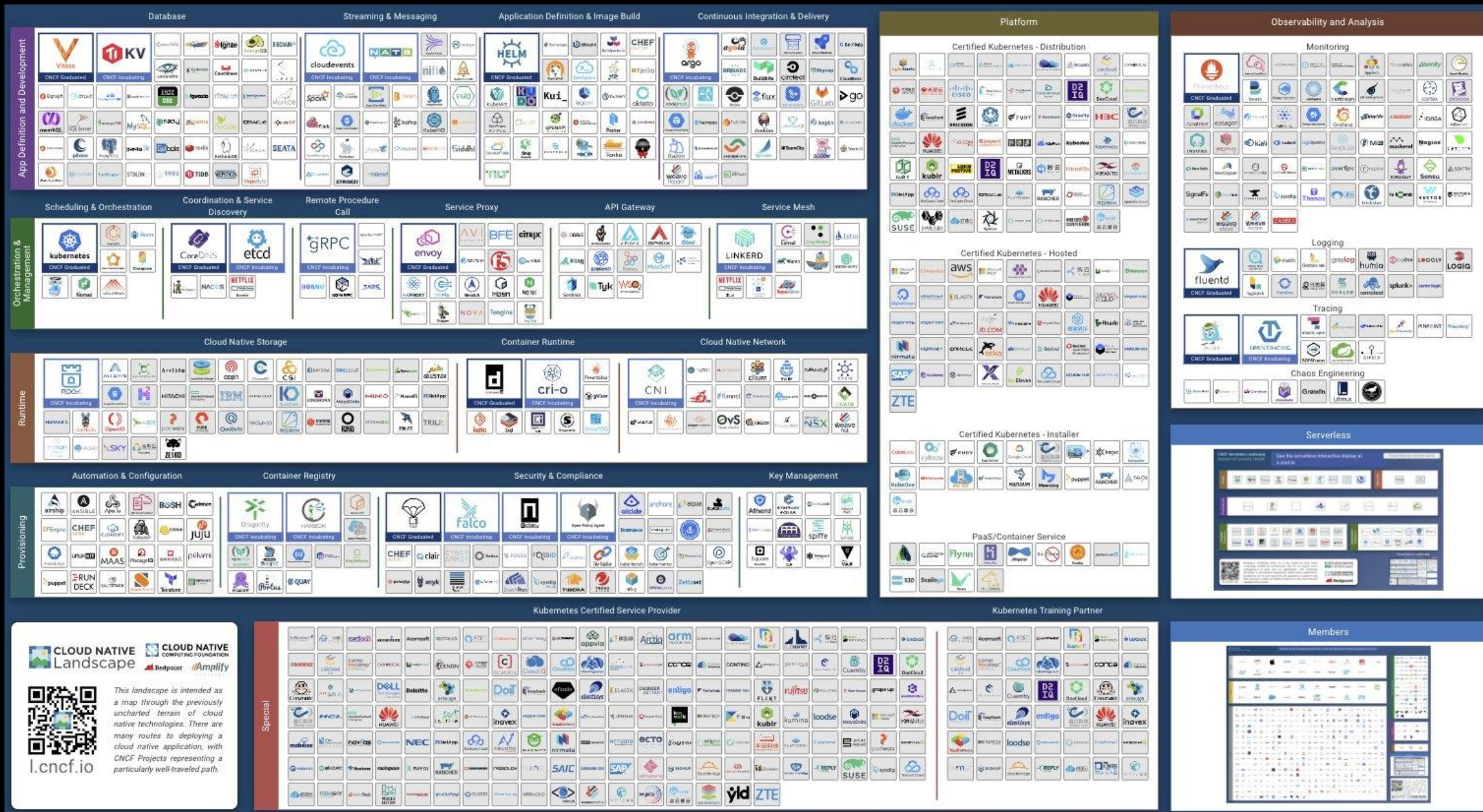
Kelsey Hightower ✓ @kelseyhightower · 17h

So you want to roll your own application platform. All you need is:

Linux
Docker
Kubernetes
Istio
Prometheus
Fluentd
Grafana
Jaeger
Harbor
Open Policy Agent
Vault
Spinnaker and Jenkins

Oh, almost forgot, you're also going to need servers, people, and glue. Bring lots of glue.

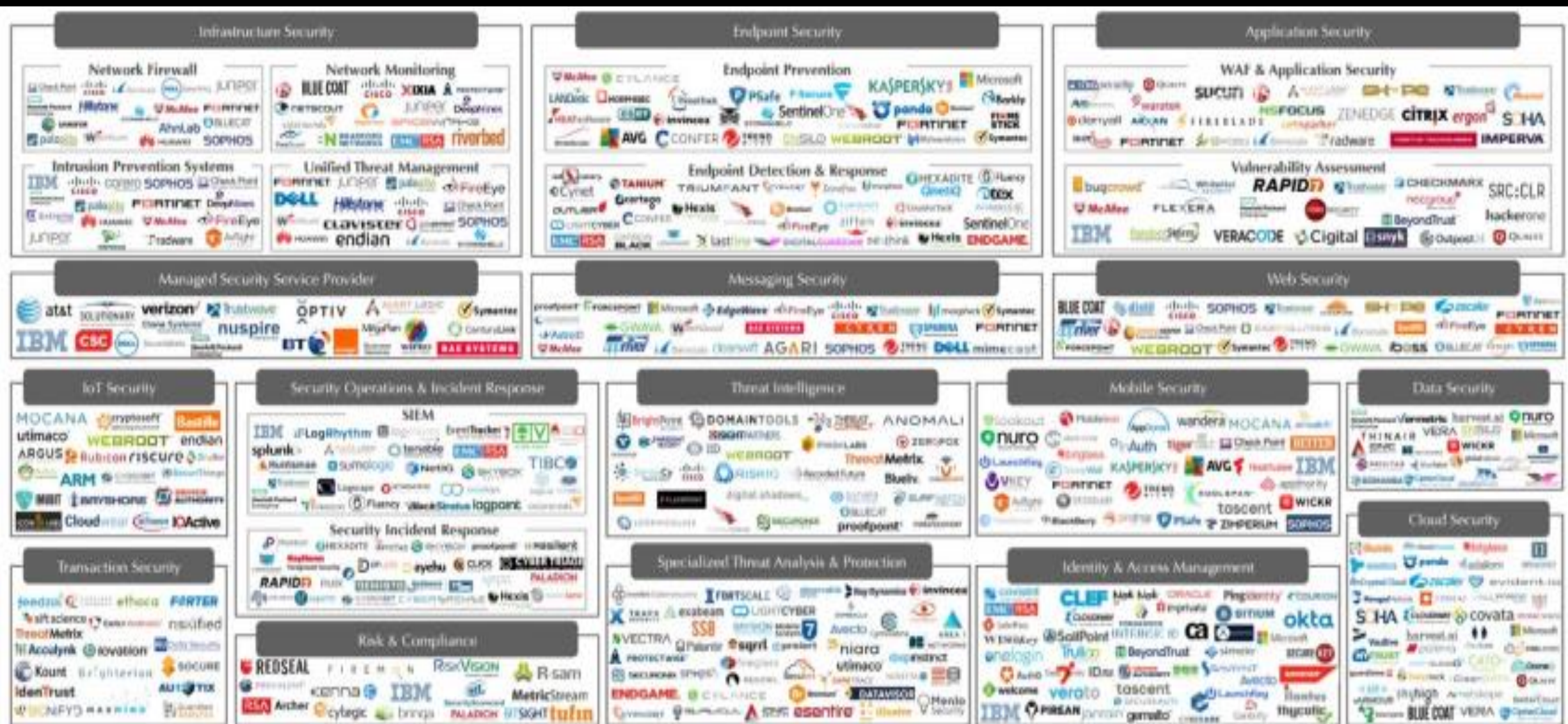
Cloud Native??



Security to the Rescue?

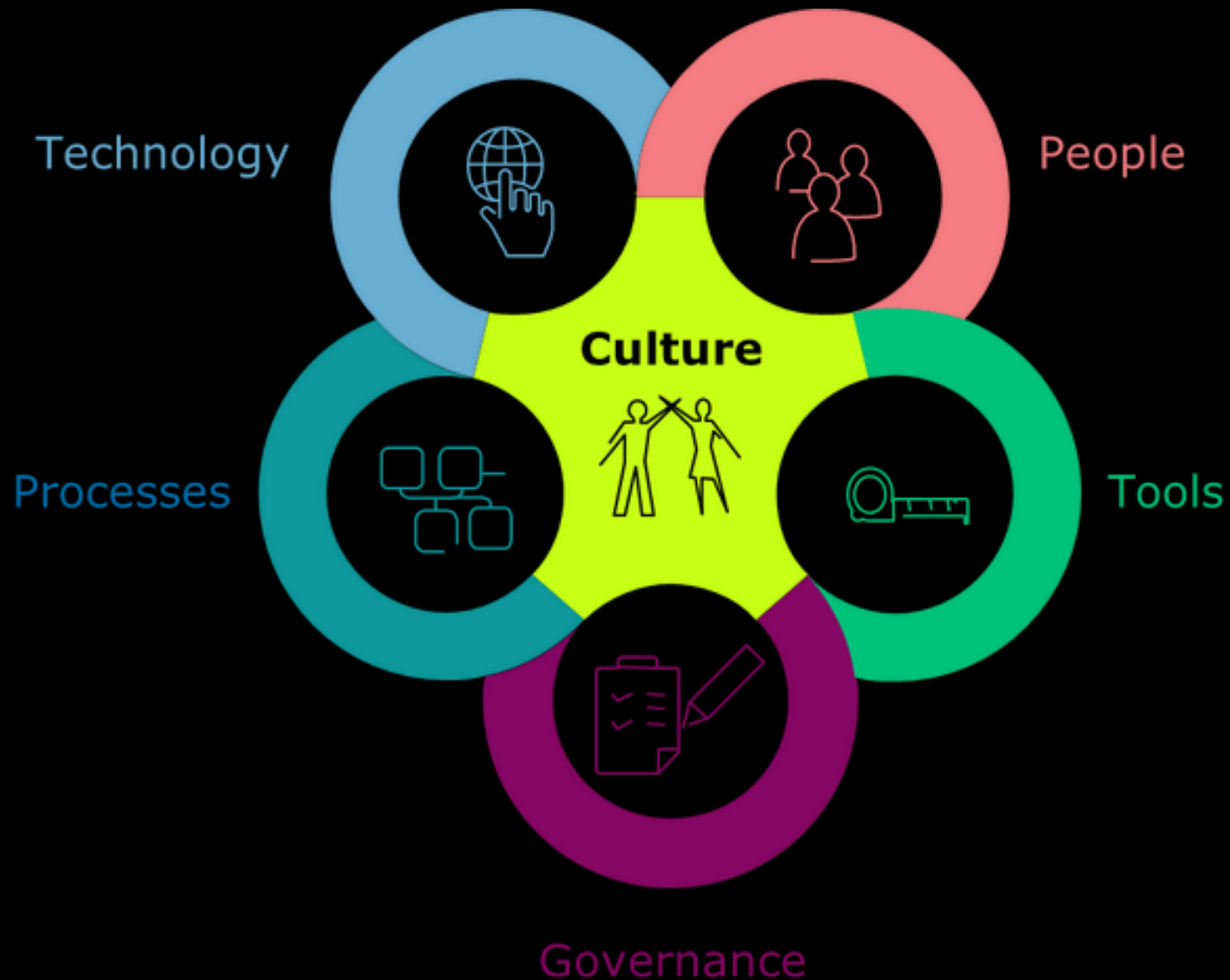


We'll secure you!

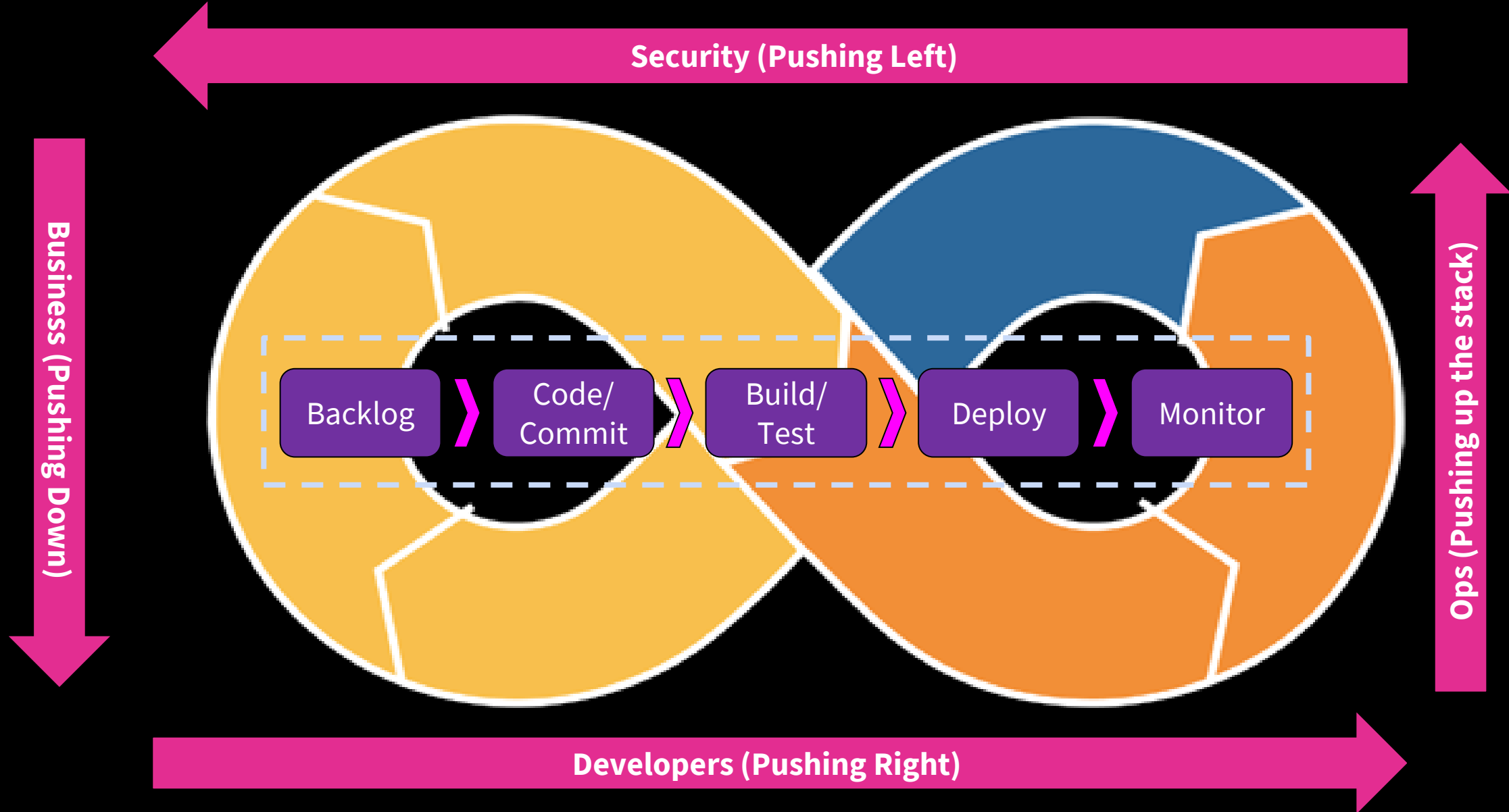


Source: Momentum Partners.

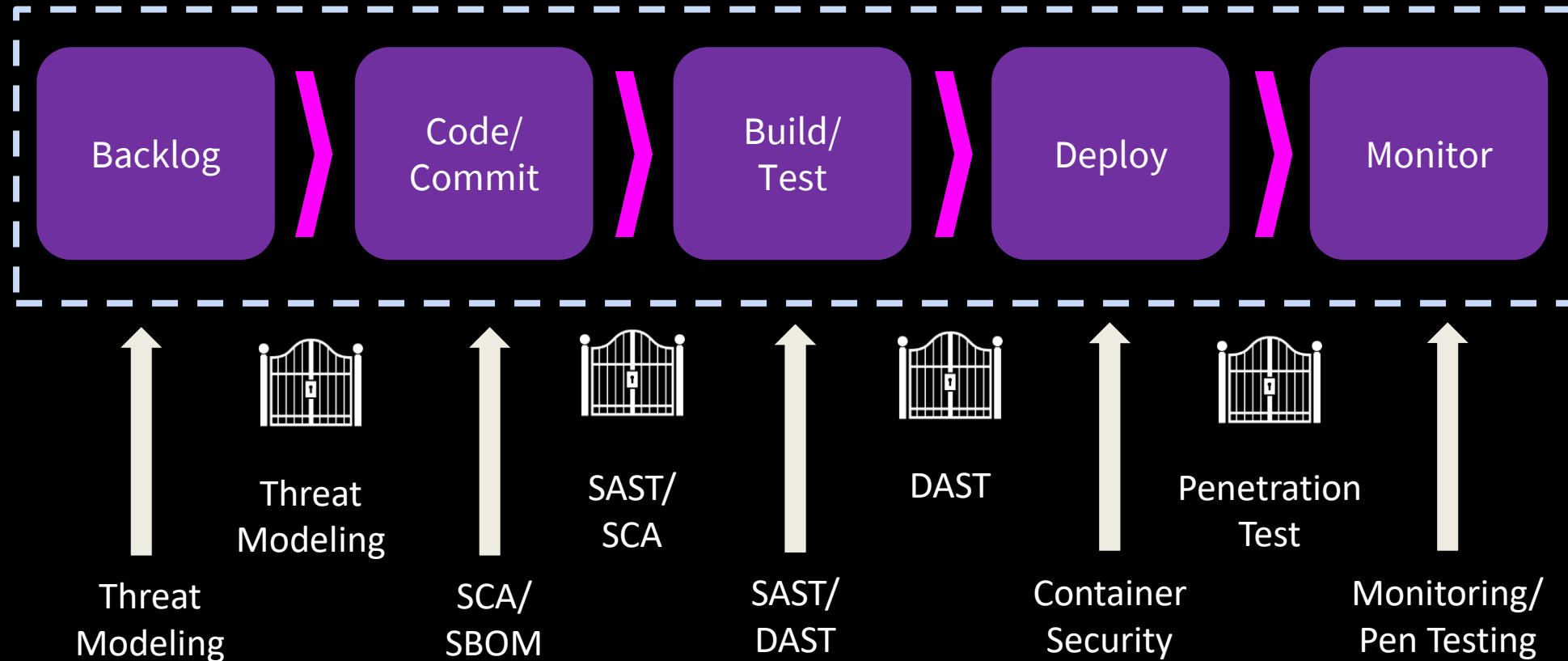
Welcome to DevSecOps



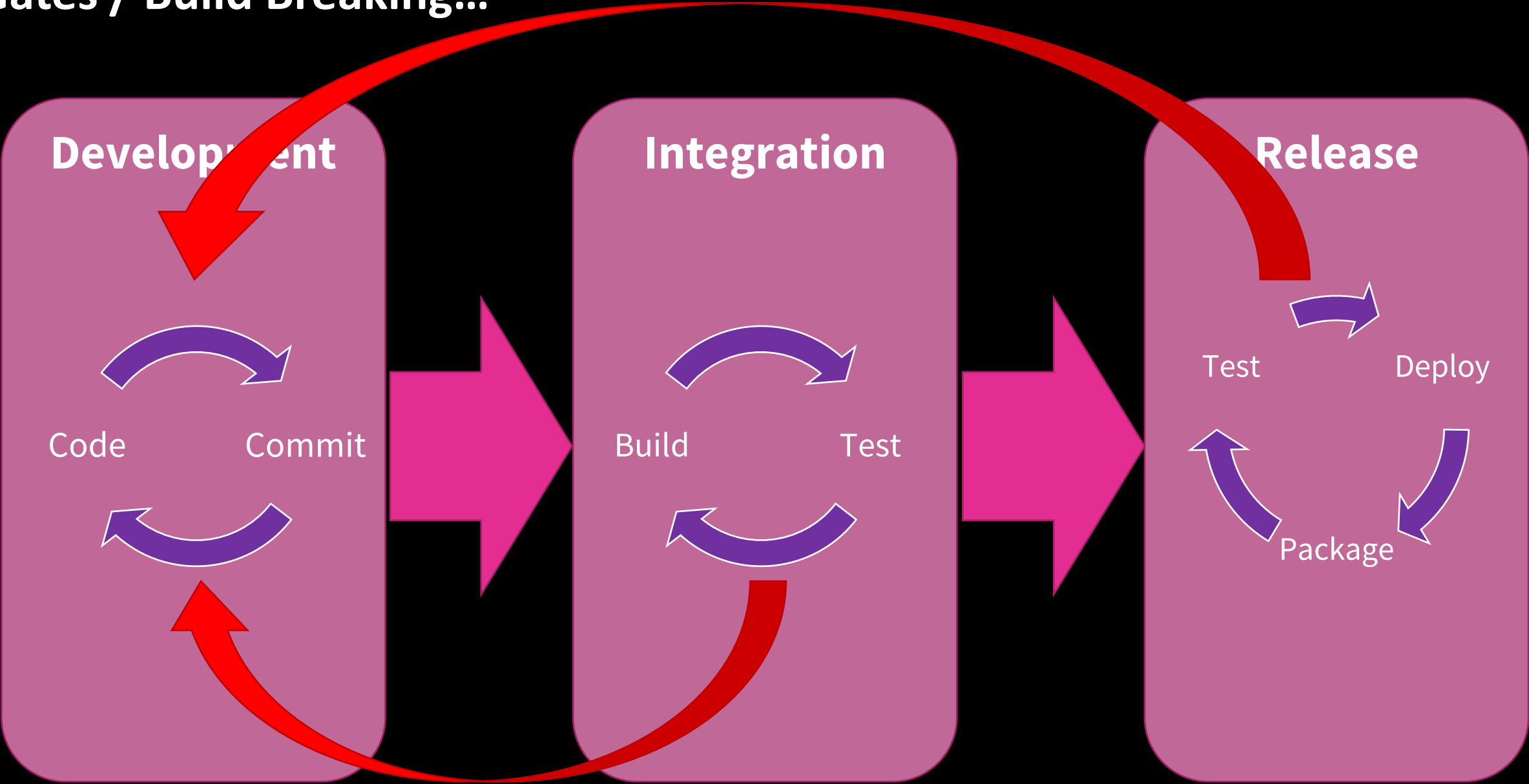
The motion of today's DevSecOps Pipeline...



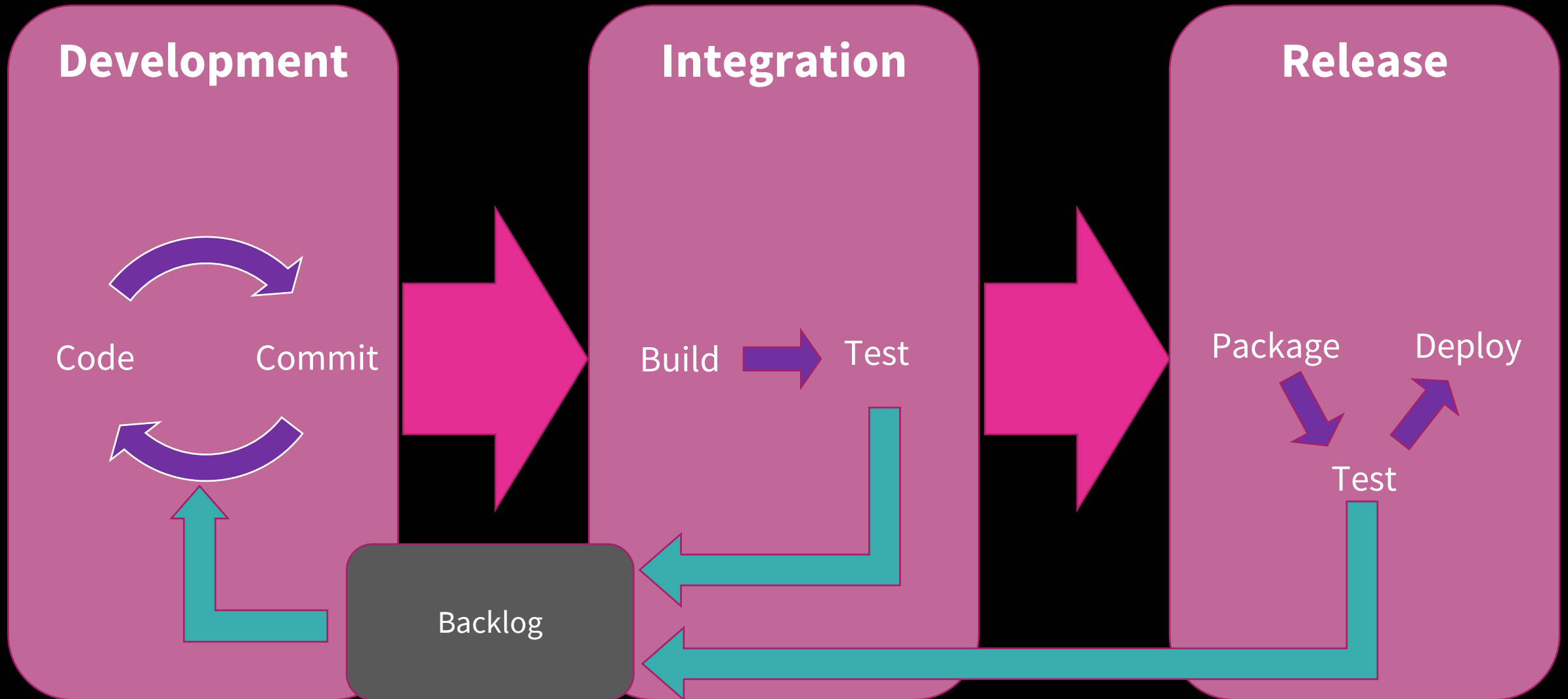
Frictionless enablement...



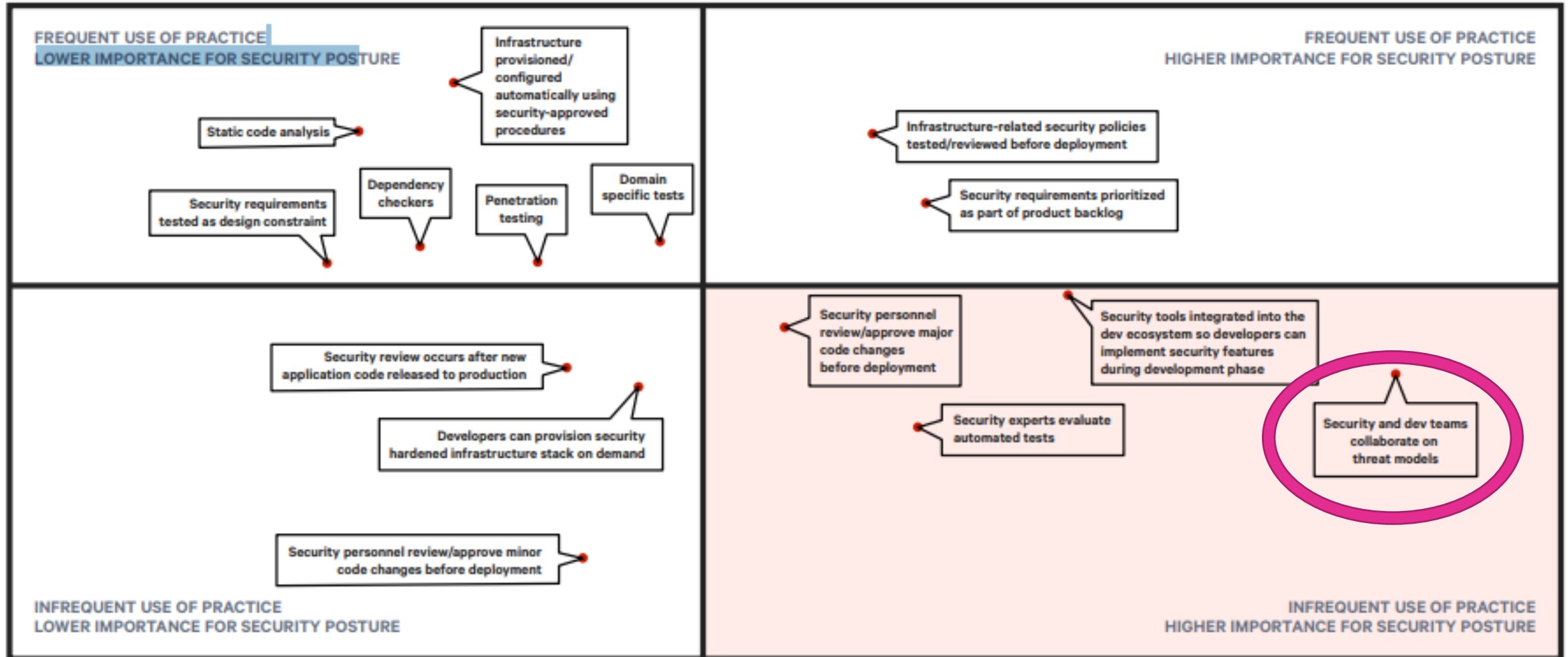
Gates / Build Breaking...



Getting to a True CI/CD...



- FREQUENCY OF PRACTICE +



- IMPORTANCE OF PRACTICE FOR STRENGTHENING SECURITY POSTURE +

Source: <https://puppet.com/resources/report/state-of-devops-report/>
Puppet/Circle-CI 2019 State of DevOps Report

Think Differently...

Traffic Jam Chauffeur

Car Trust Boundary

Vehicle Data Store

Damage

Reproc

Exploit

Affecte

Discov

Detect

ConFoo Van

CIS board

Story Map by Easy Agile

+ Create Epic

Quick filters

Sprint swimlanes

Backlog

Navigation

Car Statistics

Phone Integration

Play Media

Fatigue Management

Sprint 1

The 'Young Professional' Driver / Install maps so that I can navigate to places easier

The 'Young Professional' Driver / Touch Screen to navigate easily

The 'Young Professional' Driver / Apple CarPlay Integration so that I can safely send and receive calls, texts and emails from my iOS device while driving

The 'Young Adult' Passenger / Allow Wifi Hotspot to support up to 5 devices

The 'Sunday' Driver / Enable 'Tourist Mode Assist' when travelling outside of standard travel radius

Sprint 2

The 'Sunday' Driver / Showcase local landmarks if travelling outside of standard travel radius

The 'Young Professional' Driver / Wear and Tear Report so that I can take preventative action to preserve the life of the car if needed

The 'Family' Driver / Microphone so that I can make phone calls safely while I'm driving

The 'Family' Driver / Graphical User Interface for easier use of media while driving

The 'Young Professional' Driver / Android Auto Integration so that I can safely send and receive calls, texts and emails while driving

Sprint 1

The 'Family' Driver / 'Hot Cues' to make ...

Sprint 2

The 'Young Professional' Driver / Custom...

The 'Family' Driver / A 'Favourites' Cont...

The 'Sunday' Driver / Engine Temperatu...

The 'Young Professional' Driver / Amaz...

The 'Sunday' Driver / Show designated '...

The 'Family' Driver / Object Detection fo...

The 'Family' Driver / Safe Volume Adjus...

The 'Young Professional' Driver / Aux C...

The 'Young Professional' Driver / Do No...

The 'Family' Driver / Time/Distance to m...

The 'Young Adult' Passenger / Spotify In...

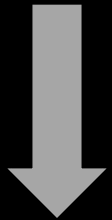
Install Improperly

Bribe P

arget to Combo



Threat Information



Plan

**Security
Requirements**

Build

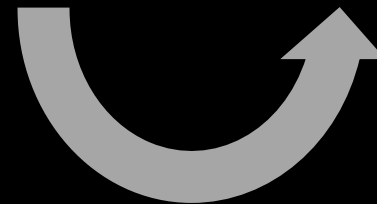
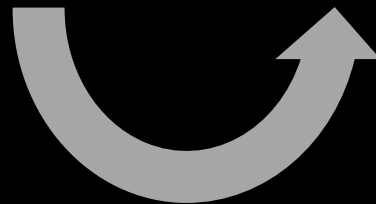
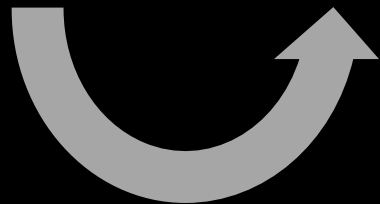
**Security
Controls**

Test

Test Cases

Deploy

Monitoring



Build the empathy and culture...

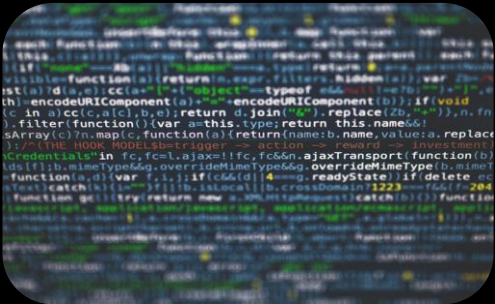


Walk-a-Mile In Their Shoes

Job shadow / Dev, Sec, and Ops / Build empathy

Meet Them Where They Live

Provide Resources and Tooling in the Pipeline



Pave the Road

Tool Selection / Accountable Trust

Mutual Engagement

Connect Daily Activities Across Disciplines



“ Coming together is the beginning.
Keeping together is progress.
Working together is success. ”

— Henry Ford





@AlyssaM_Infosec



/in/alyssam-infosec



<https://alyssasec.com>

Thank You



Alyssa

MILLER



sec4dev

26C7q6A

WIGTER