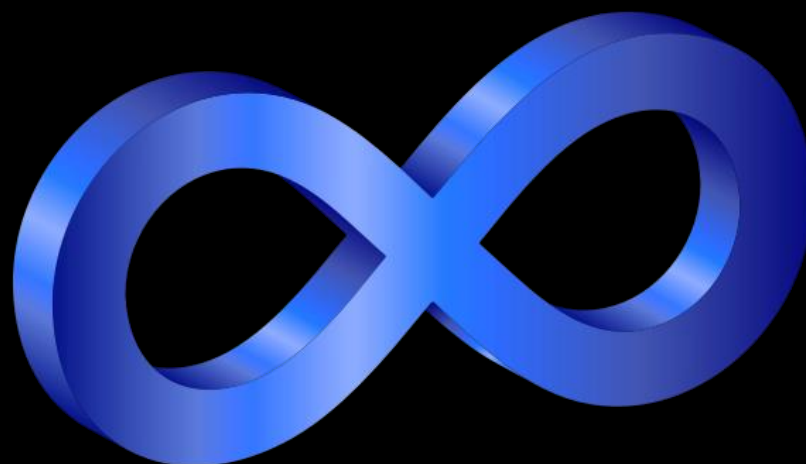




So Happy Together

Making the Promise of DevSecOps a Reality





Hacker/Researcher

Security Advocate

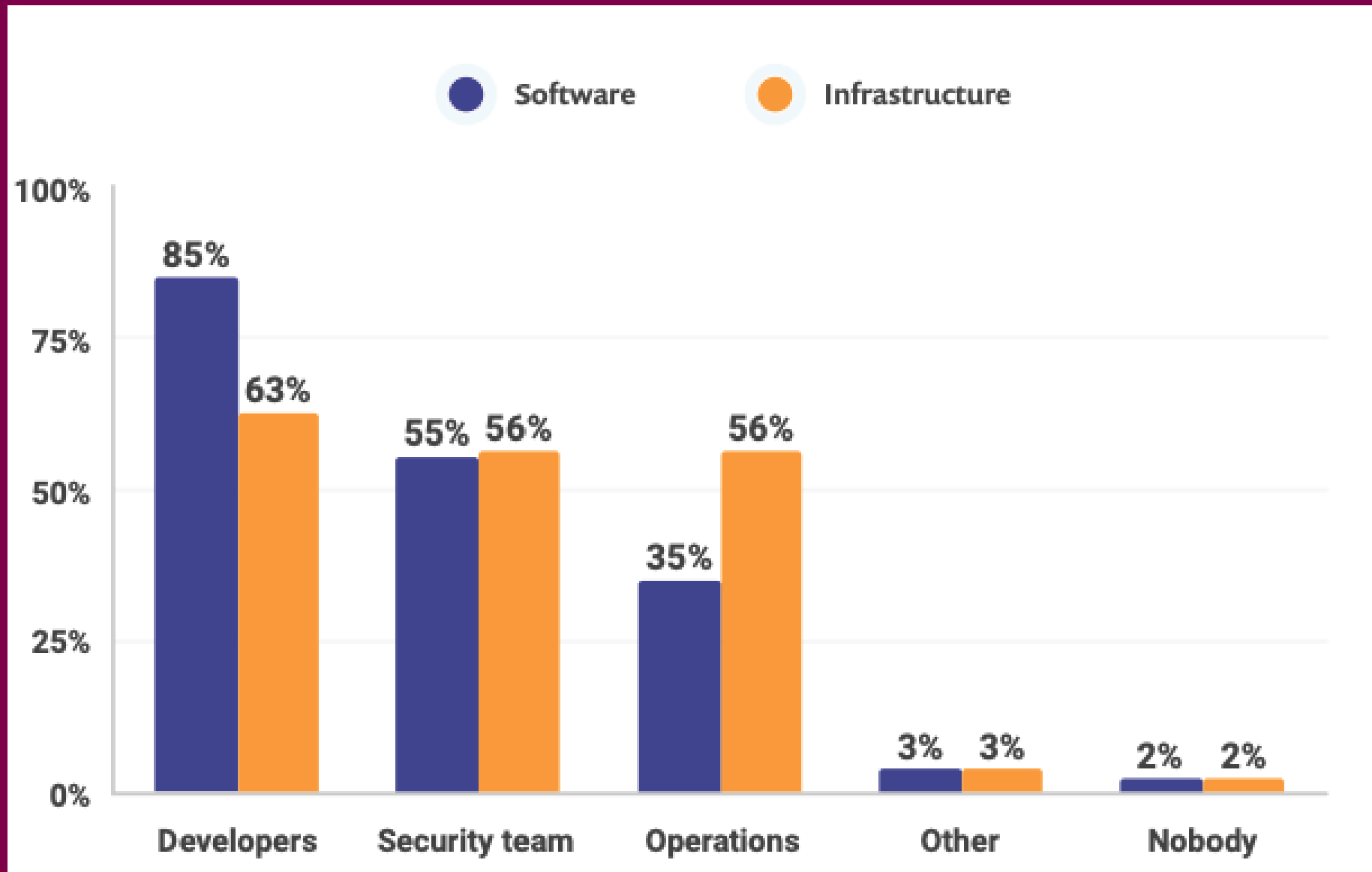
Former Developer

Co-Host: Uncommon Journey



snyk

Who is responsible for security?



The reality of Modern Development...

```
import org.snyk.groceries.domain.Item;
import org.snyk.groceries.repository.ItemRepository;
import org.springframework.boot.CommandLineRunner;
import org.springframework.boot.SpringApplication;
import org.springframework.boot.autoconfigure.SpringBootApplication;
import org.springframework.context.annotation.Bean;
import org.springframework.web.bind.annotation.RestController;

@SpringBootApplication
@RestController
public class SpringGoofApplication {

    public static void main(String[] args) {
        SpringApplication.run(SpringGoofApplication.class, args);
    }

    @Bean
    public CommandLineRunner demo(ItemRepository repository) {
        return (args) -> {
            // save a few of items to the grocery list
            repository.save(new Item("Beans", new Double(0.500)));
            repository.save(new Item("Milk", new Double(1.090)));
            repository.save(new Item("Bread", new Double(1.50)));
            repository.save(new Item("Sausages", new Double(4.990)));
            repository.save(new Item("Beer", new Double(5.990)));

            // fetch all items on the grocery list
            System.out.println("Items found with findAll():");
            System.out.println("-----");
            for (Item item : repository.findAll()) {
                System.out.println(item.toString());
            }
            System.out.println("");

            // fetch items by name
            System.out.println("Item found with findByName('Bread'):");
            System.out.println("-----");
            repository.findByName("Bread").forEach(System.out::println);
        };
    }
}
```

```
<dependency>
    <groupId>org.springframework.boot</groupId>
    <artifactId>spring-boot-starter-data-jpa</artifactId>
</dependency>
<dependency>
    <groupId>org.springframework.boot</groupId>
    <artifactId>spring-boot-starter-data-rest</artifactId>
</dependency>
<dependency>
    <groupId>org.springframework.boot</groupId>
    <artifactId>spring-boot-starter-hateoas</artifactId>
</dependency>
<dependency>
    <groupId>org.springframework.boot</groupId>
    <artifactId>spring-boot-starter-jdbc</artifactId>
</dependency>
<dependency>
    <groupId>org.springframework.boot</groupId>
    <artifactId>spring-boot-starter-web</artifactId>
</dependency>
<dependency>
    <groupId>org.springframework.data</groupId>
    <artifactId>spring-data-rest-hal-browser</artifactId>
</dependency>
<dependency>
    <groupId>com.h2database</groupId>
    <artifactId>h2</artifactId>
    <scope>runtime</scope>
</dependency>
```

7

direct
dependencies

59

transitive
dependencies

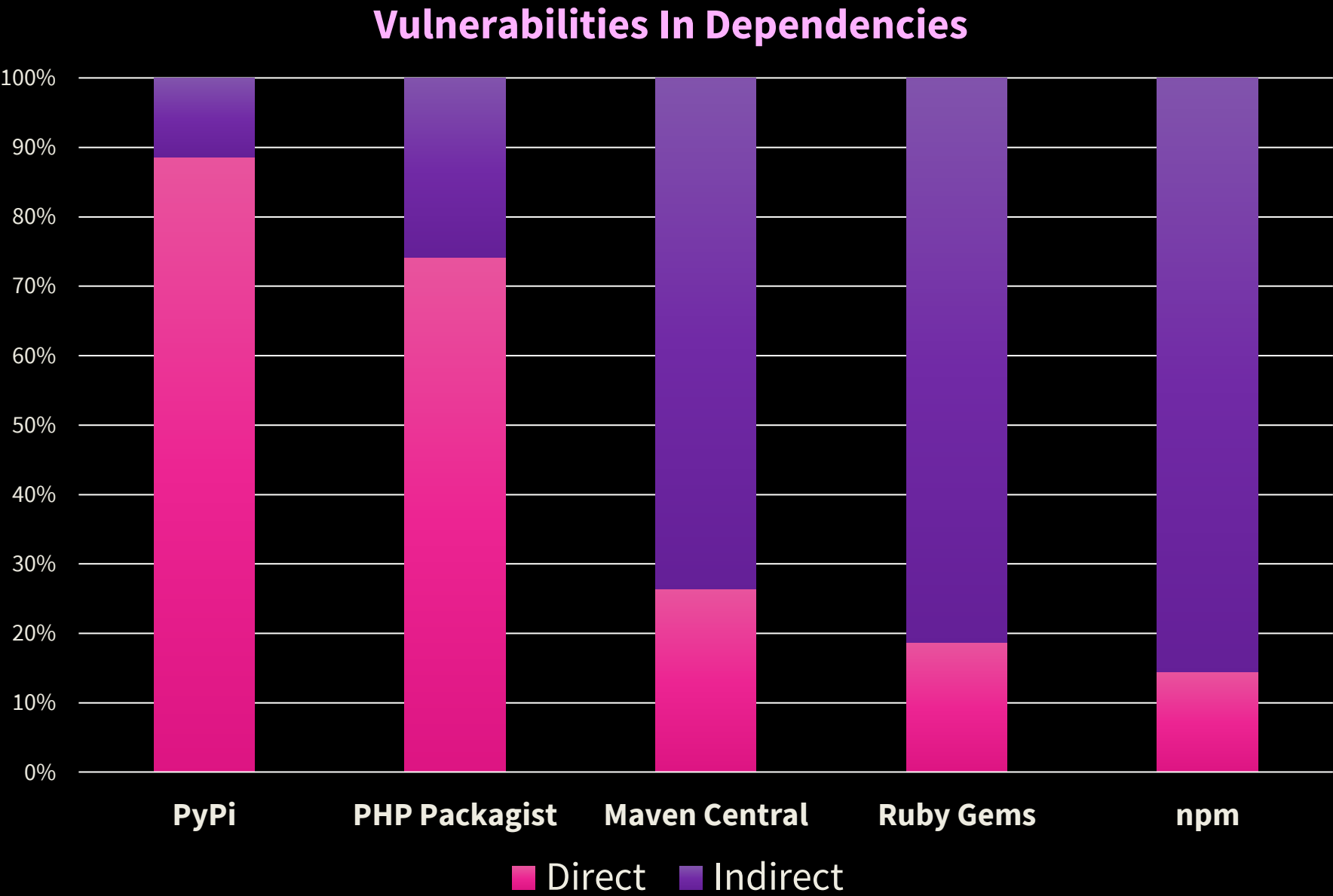
713,348

Lines of code

80 Lines of Code | 3 java files

WHAT'S IN YOUR SOFTWARE?

Security of Dependencies...



What about those ops teams?



Kelsey Hightower ✓ @kelseyhightower · 17h

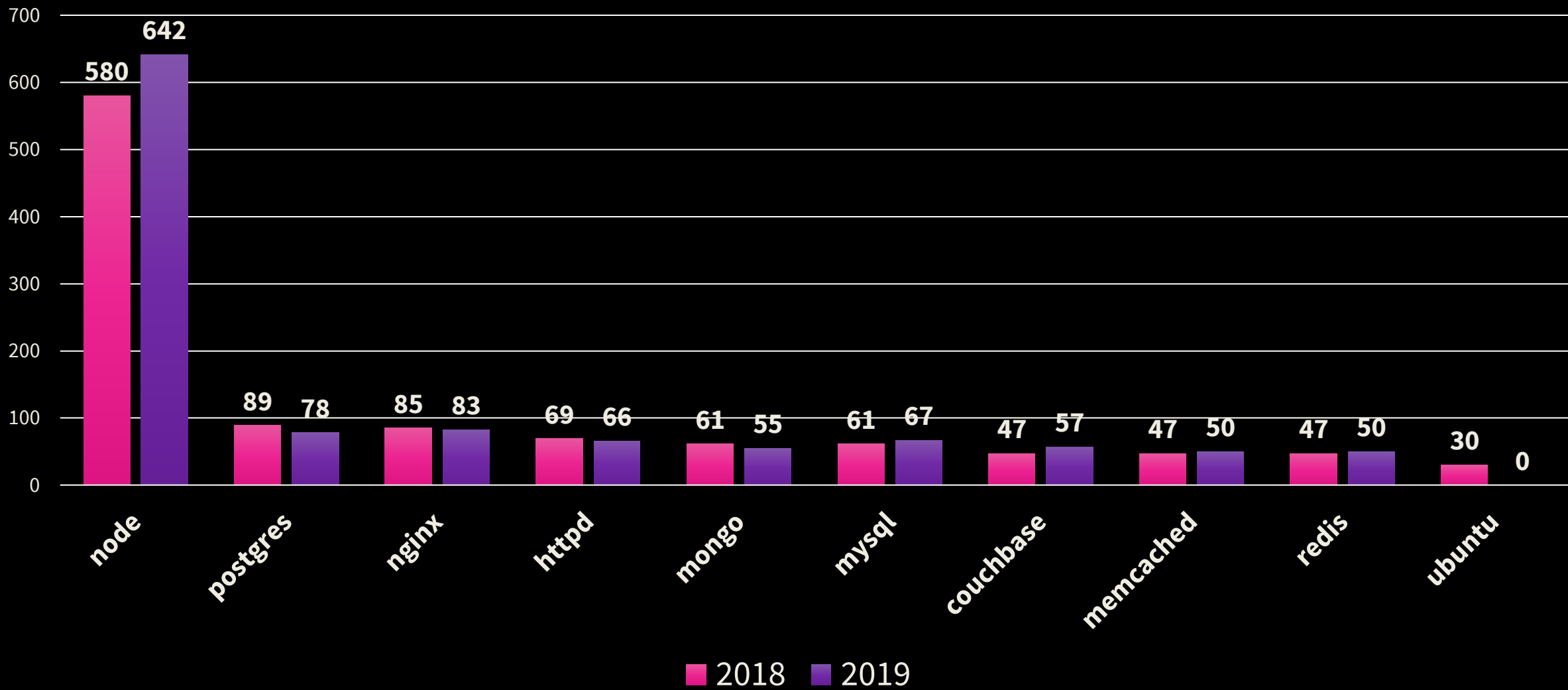
So you want to roll your own application platform. All you need is:

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

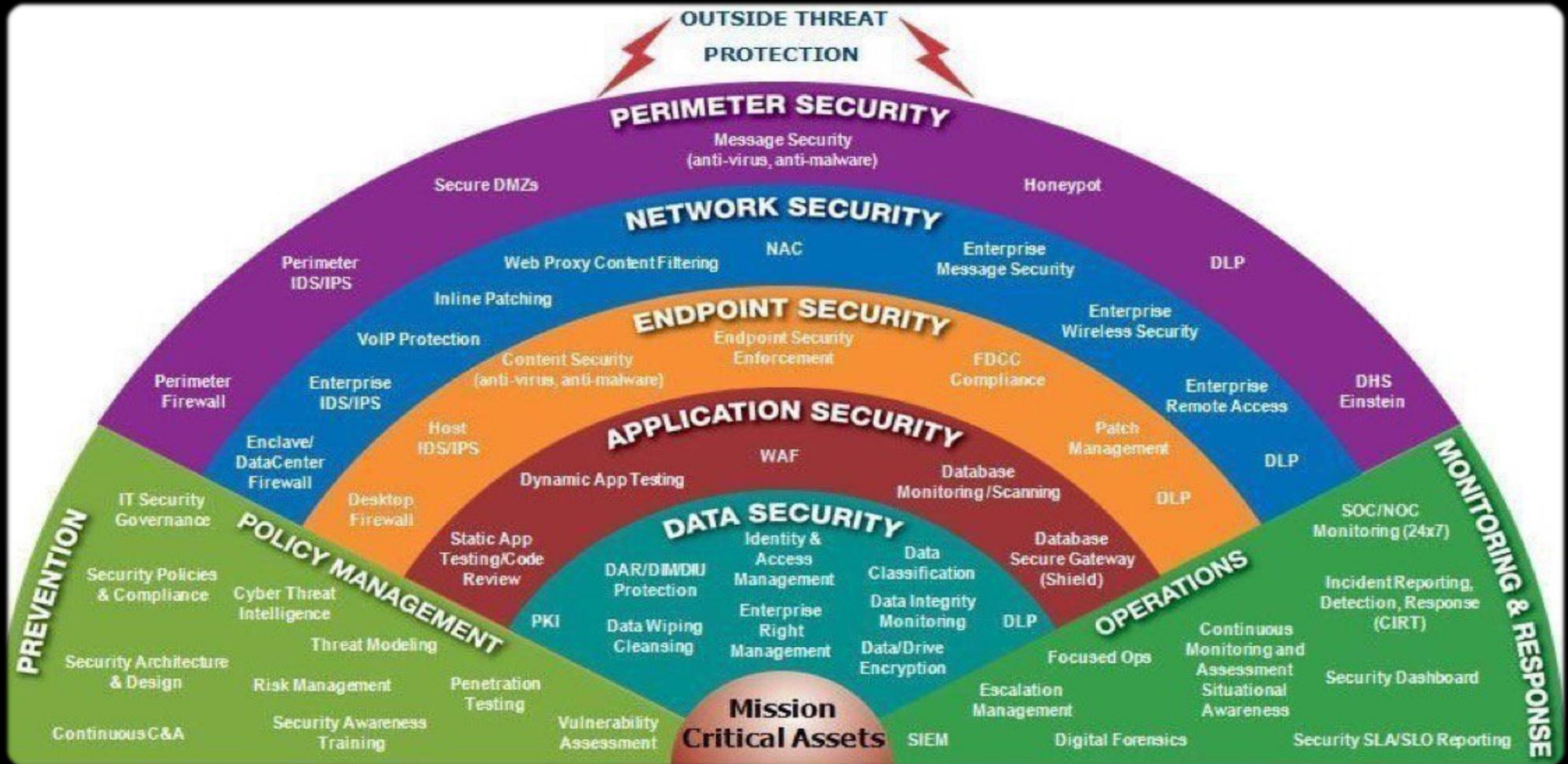
Oh, almost forgot, you're also going to need servers, people, and glue. Bring lots of glue.

About those docker images...

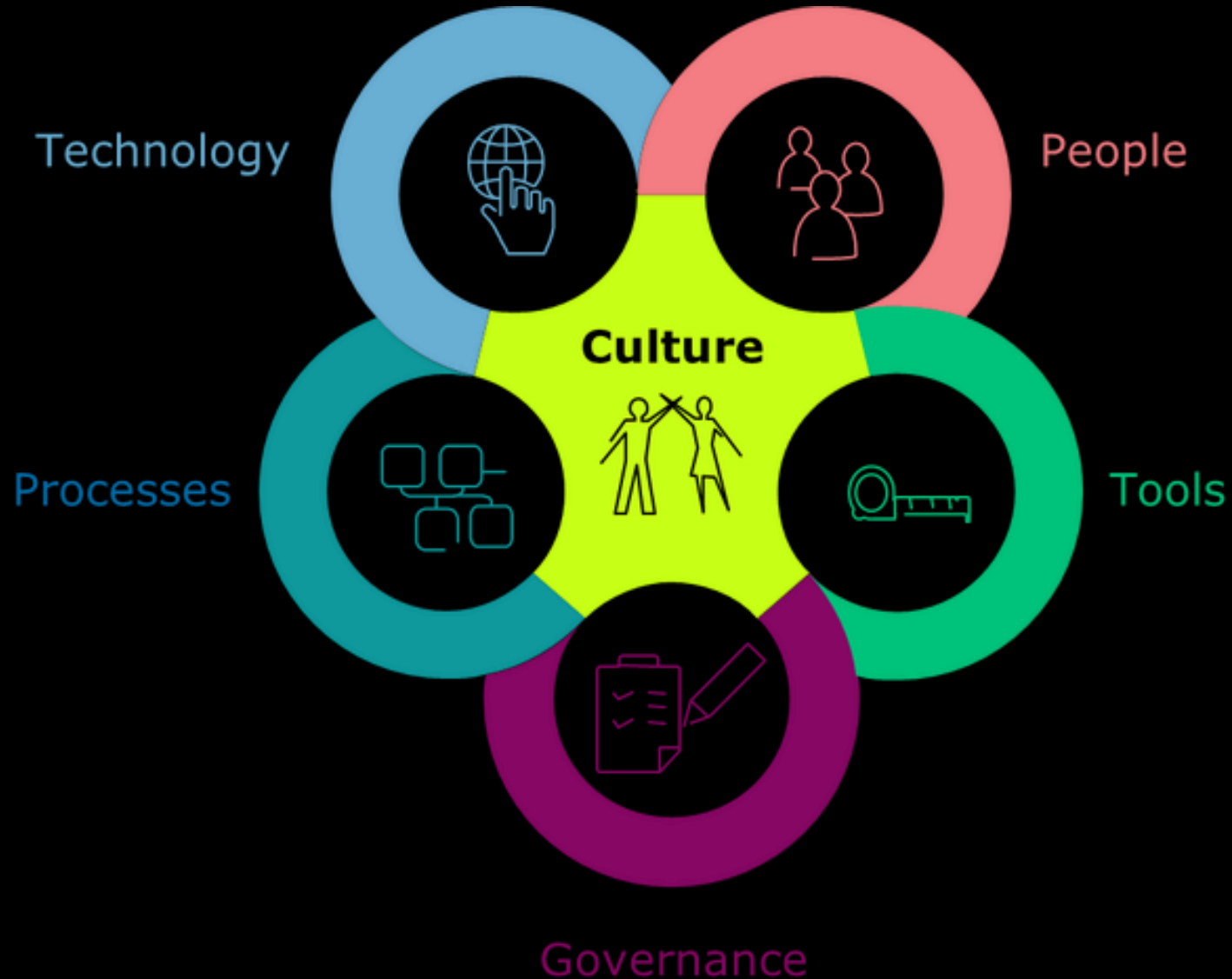
Vulnerabilities in Official DockerHub Images



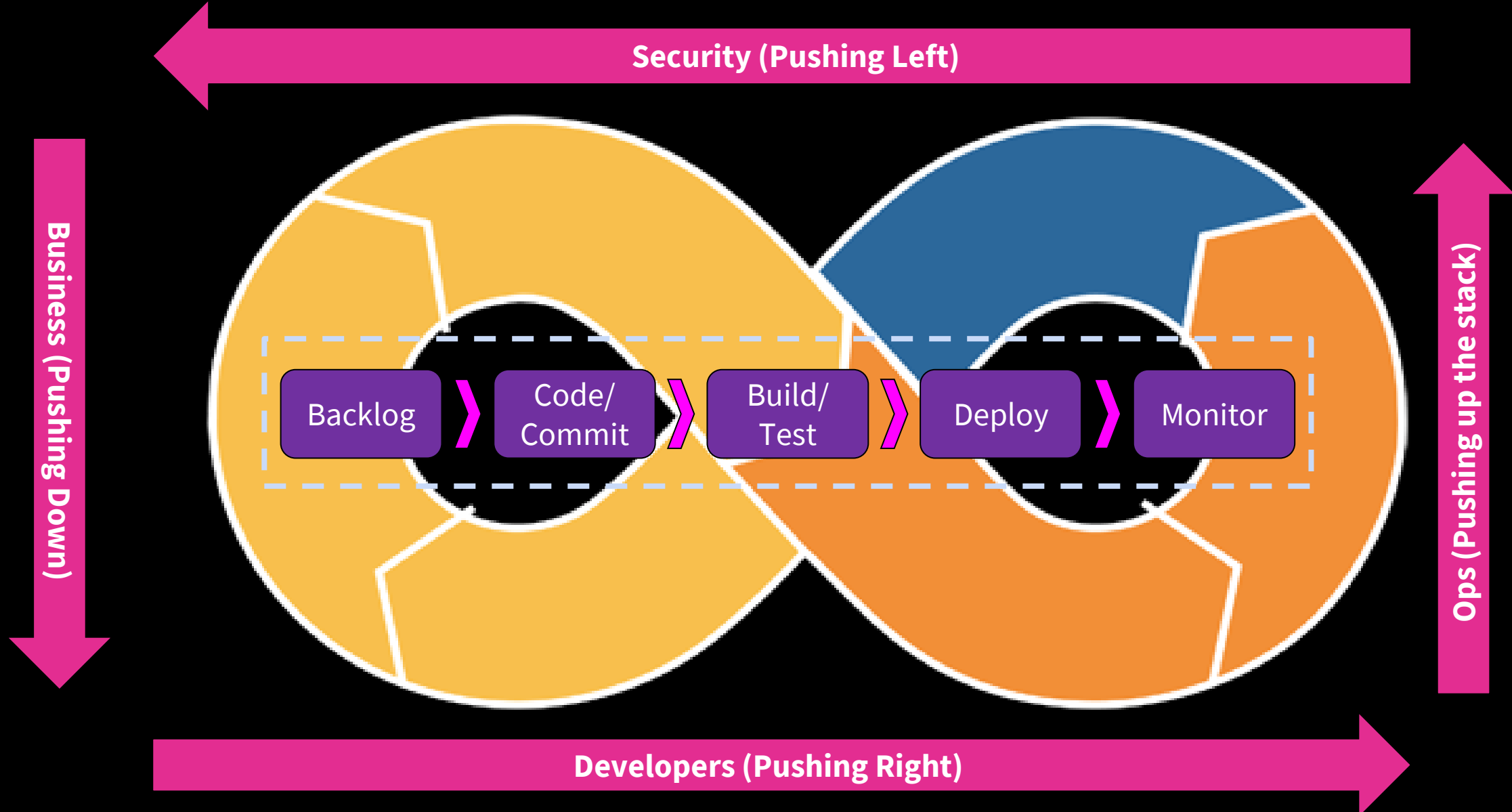
But that's why we have a security team right?



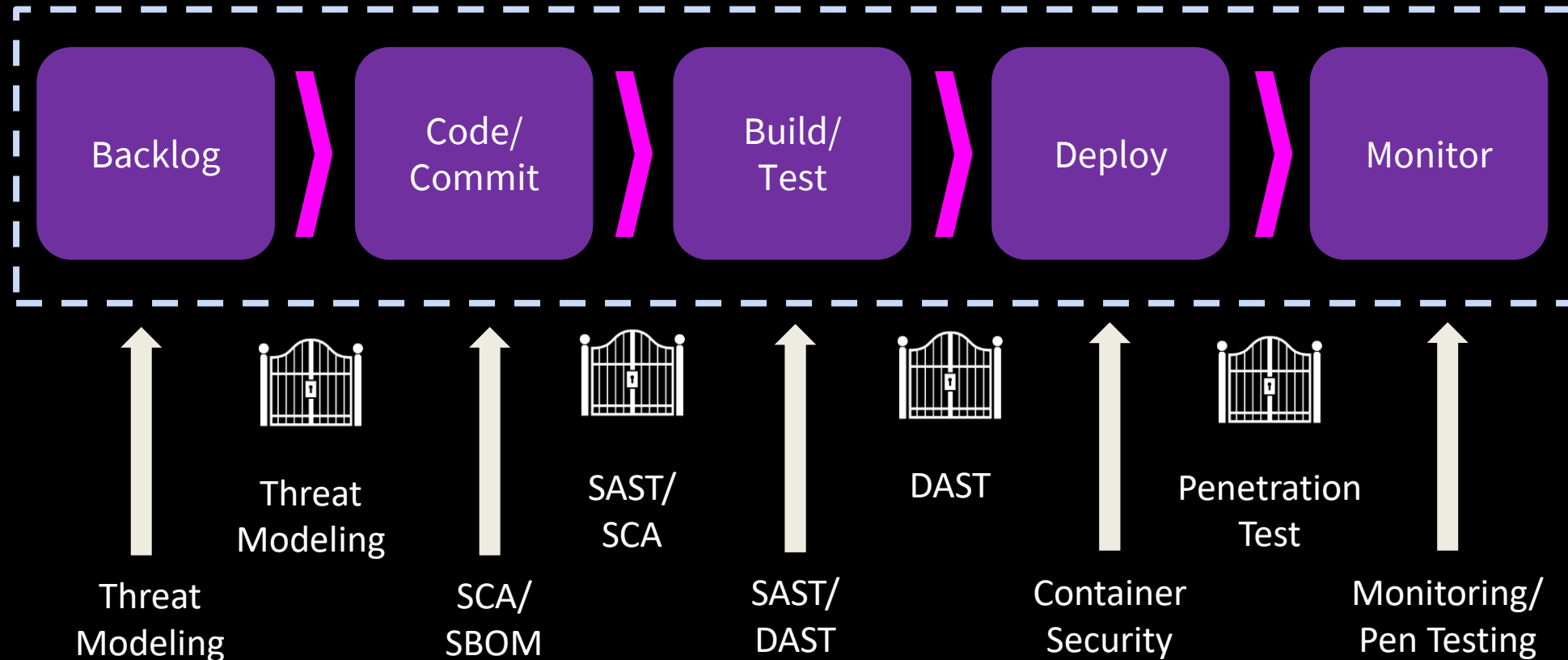
Welcome to DevSecOps

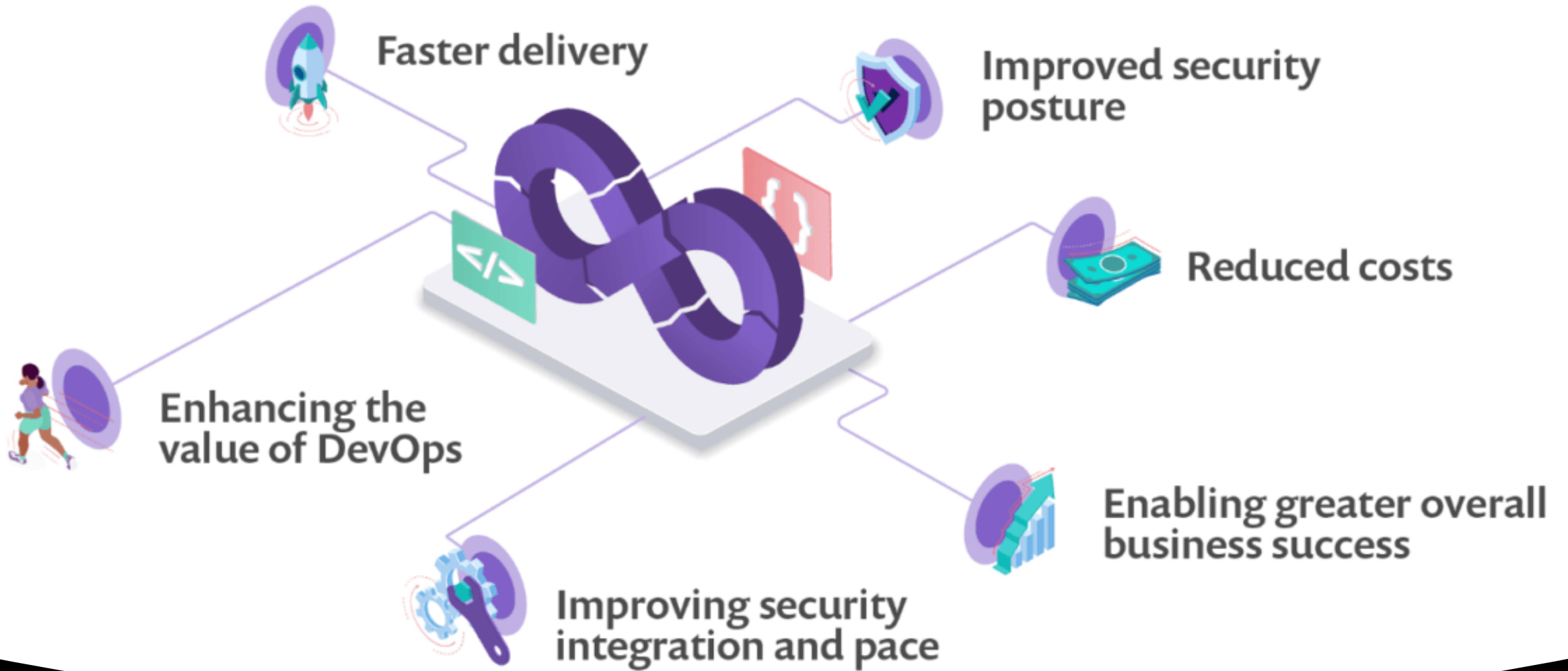


The motion of today's DevSecOps Pipeline...

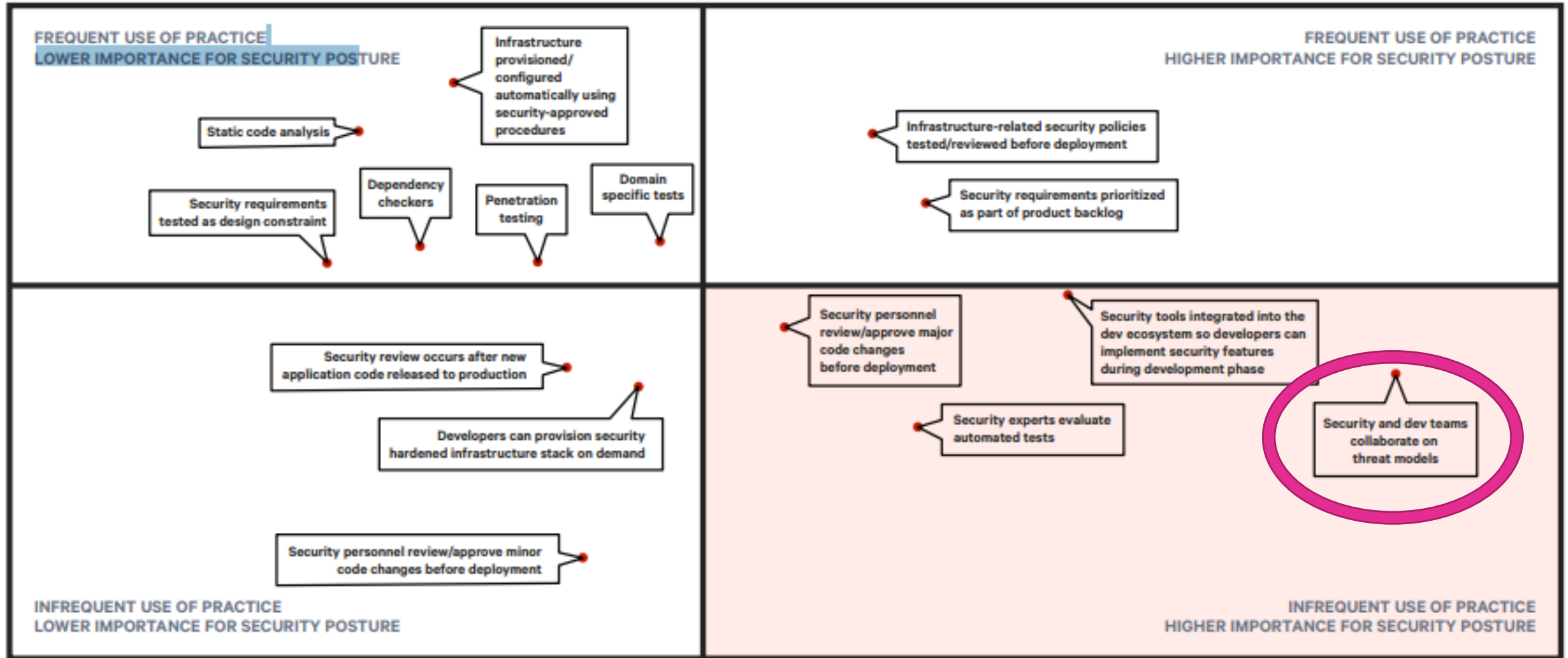


Frictionless enablement...





- 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 Vane

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...

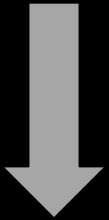
Install Improperly

Bribe P

arget to Combo



Threat Information



Plan

**Security
Requirements**

Build

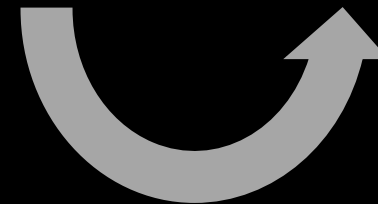
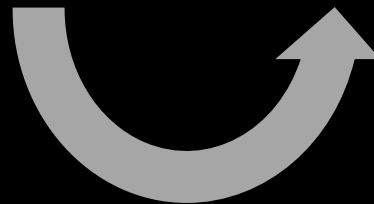
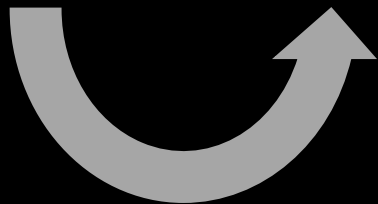
**Security
Controls**

Test

Test Cases

Deploy

Monitoring



Build the empathy and culture...



Walk-a-Mile In Their Shoes

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

Mutual Engagement

Connect Daily Activities Across Disciplines

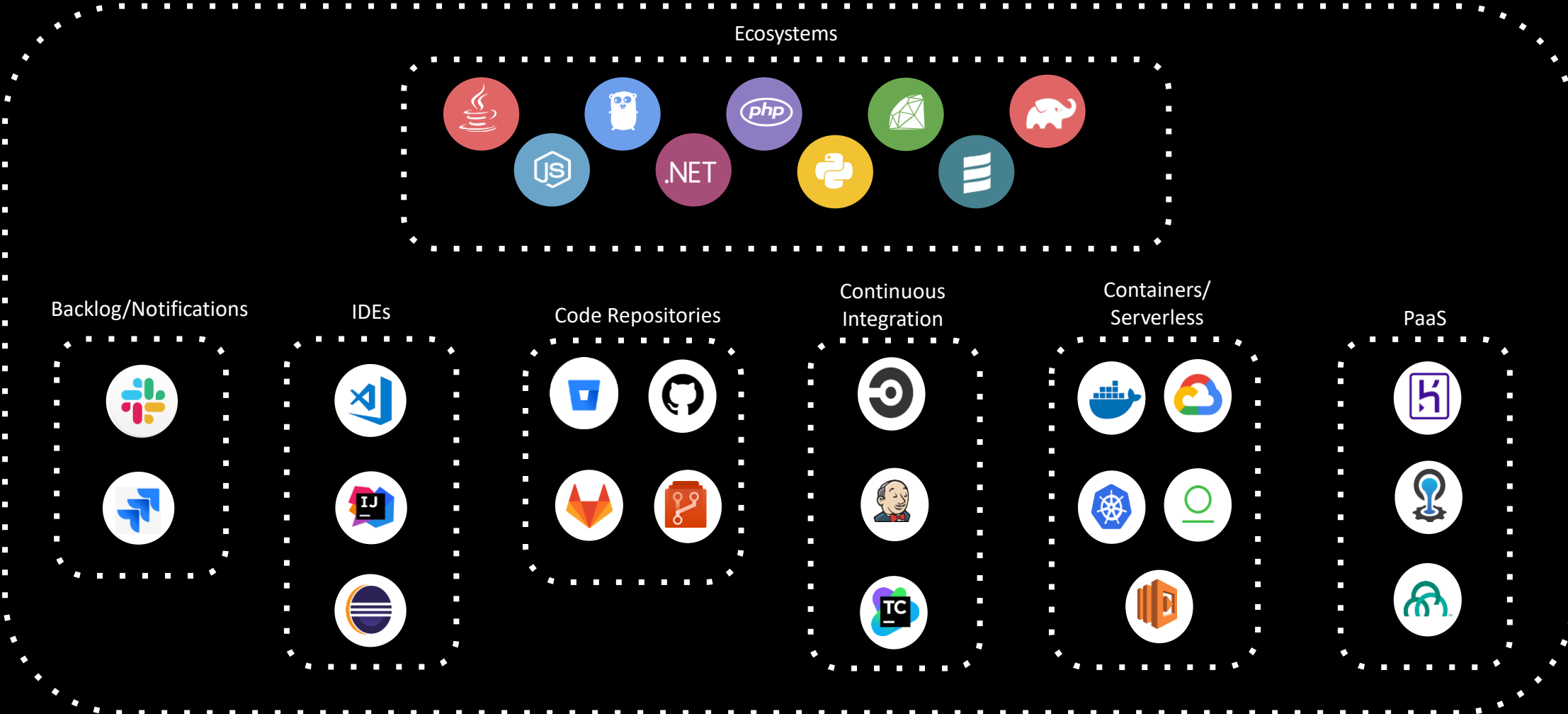


Pave the Road

Tool Selection / Accountable Trust

Meet them where they live...

DevSecOps Pipeline



“ 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



snyk

гнлк

Alyssa

MILLER

МІГГЕР

ALL
THINGS
OPEN 20
20

ВЕРУ 30
30