Alyssa MILLER

So Happy Together

Making the Promise of DevSecOps a Reality

Hacker/Researcher

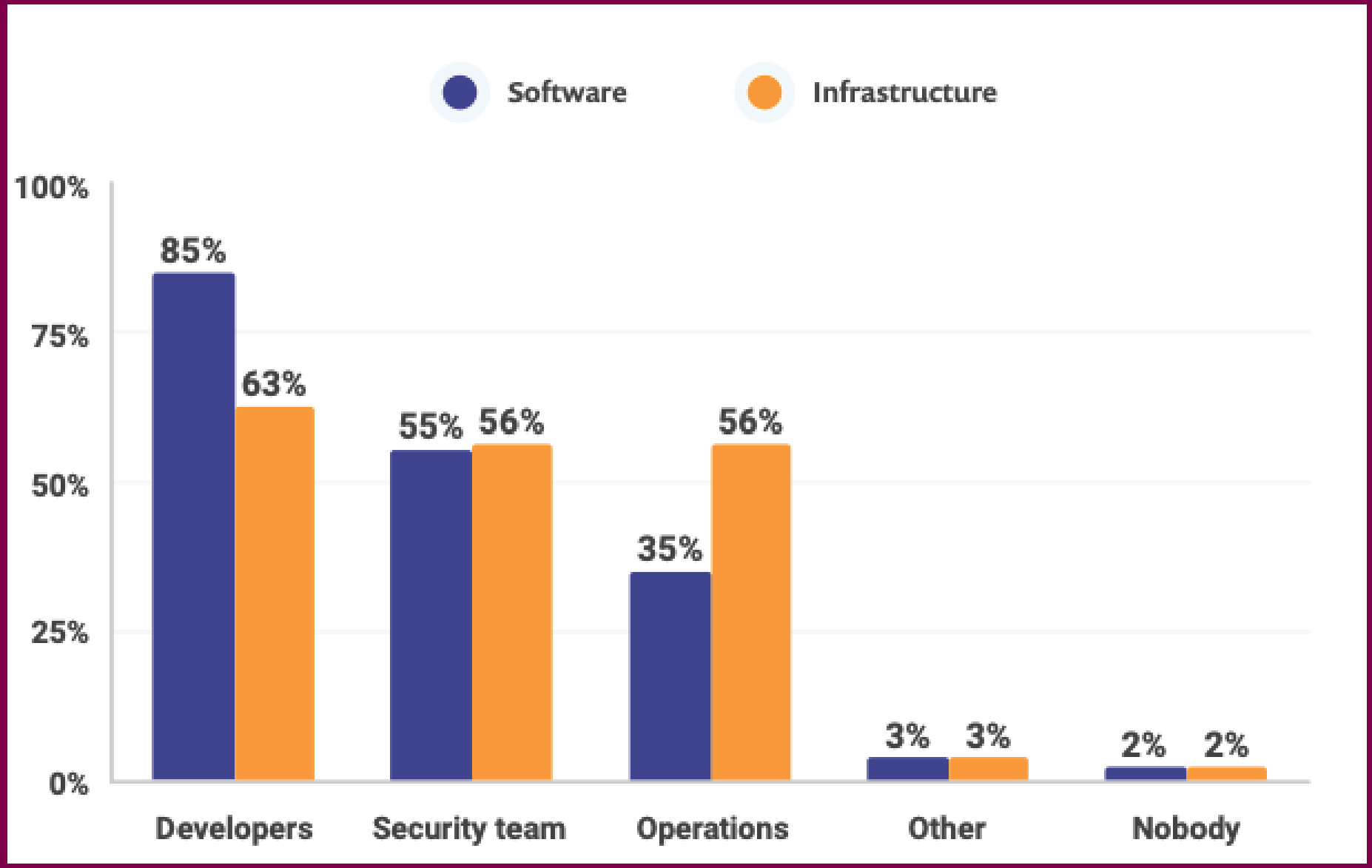
Security Advocate

Former Developer

Co-Host: Uncommon Journey

snyk

Who is responsible for security?



The reality of Modern Development…

```java
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(0.50D)));
			repository.save(new Item("Milk", new Double(1.09D)));
			repository.save(new Item("Bread", new Double(1.5D)));
			repository.save(new Item("Sausages", new Double(4.99D)));
			repository.save(new Item("Beer", new Double(5.99D)));

			// 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);
			};
	};
}
```

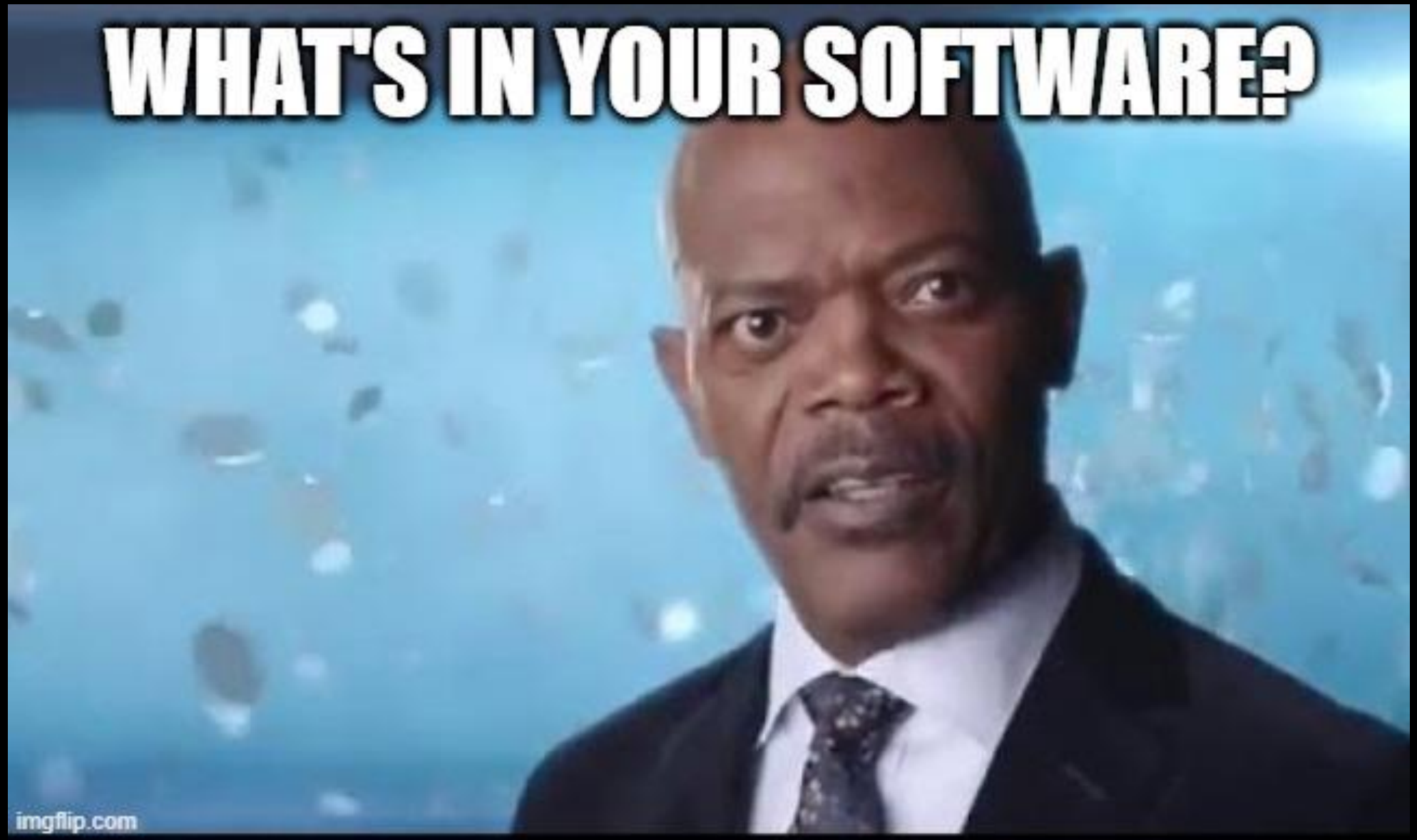
```xml
<dependency>
	<groupId>org.springframework.boot</groupId>
	<artifactId>spring-boot-starter-data-jpa</artifactId>
</dependency>
<dependency>
	<groupId>org.springframework.boot</groupId>
	<artifactId>spring-boot-starter-data-rest</artifactId>
</dependency>
<dependency>
	<groupId>org.springframework.boot</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

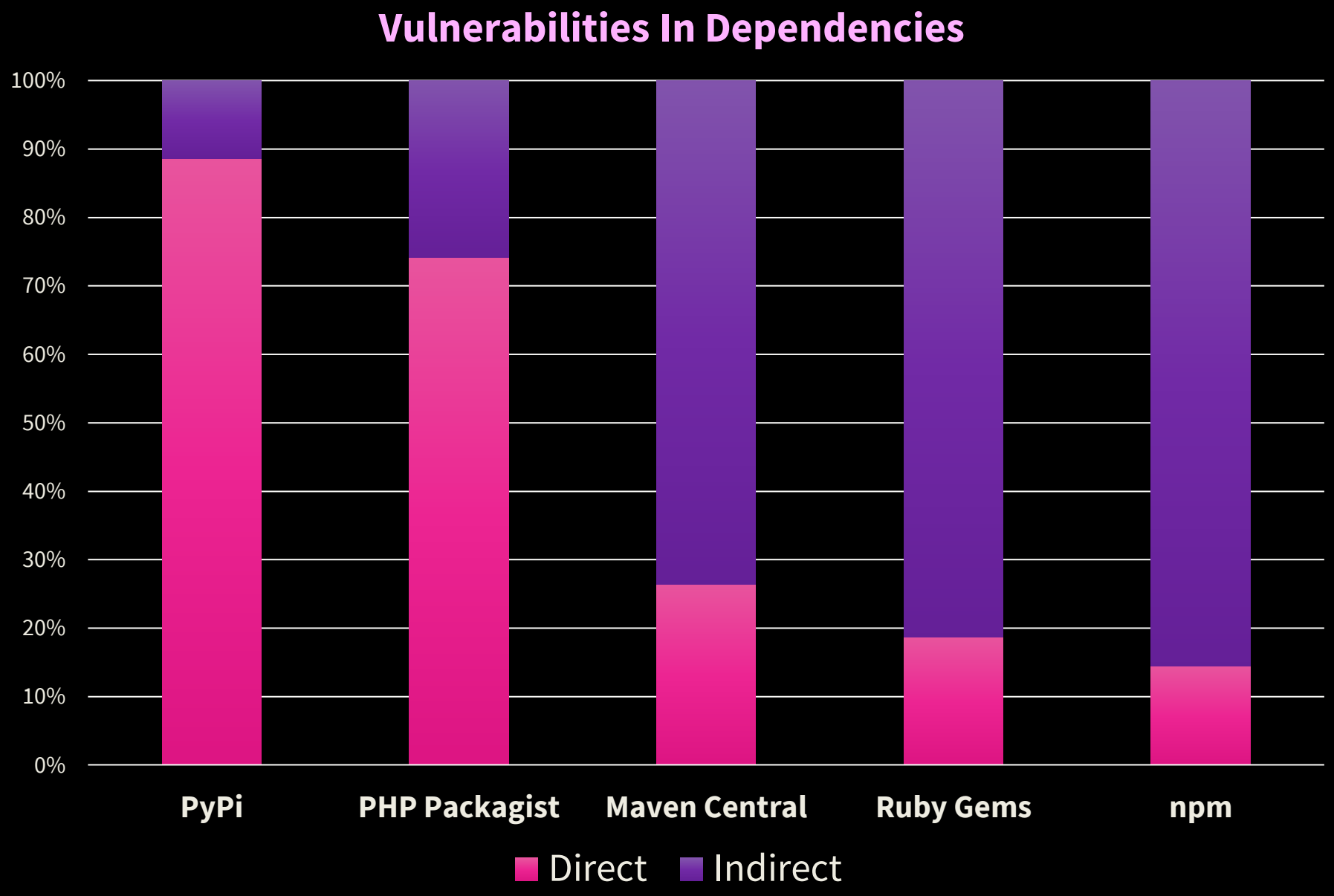
59 transitive dependencies

713,348 Lines of code

80 Lines of Code | 3 java files

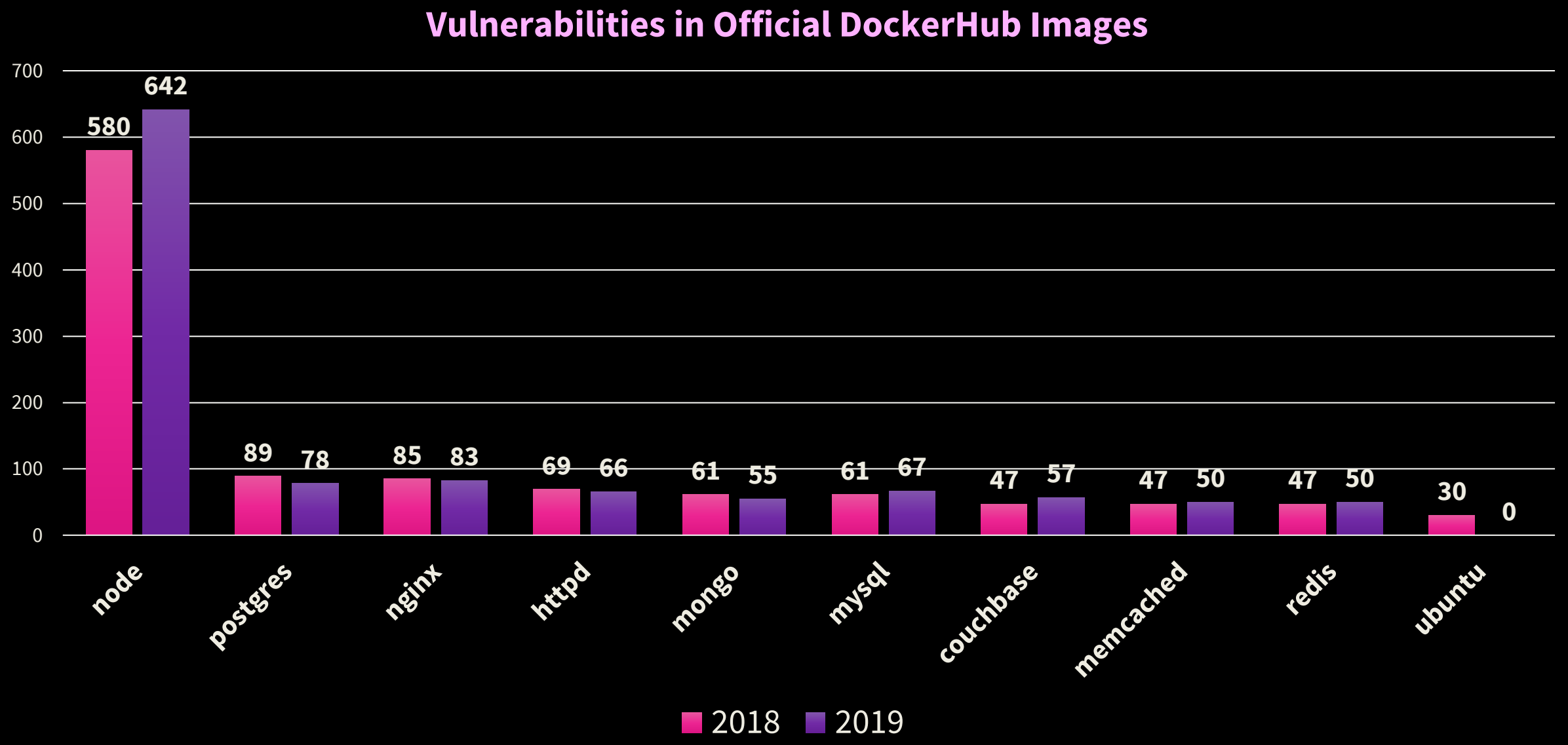

WHAT'S IN YOUR SOFTWARE?
imgflip.com

Security of Dependencies…

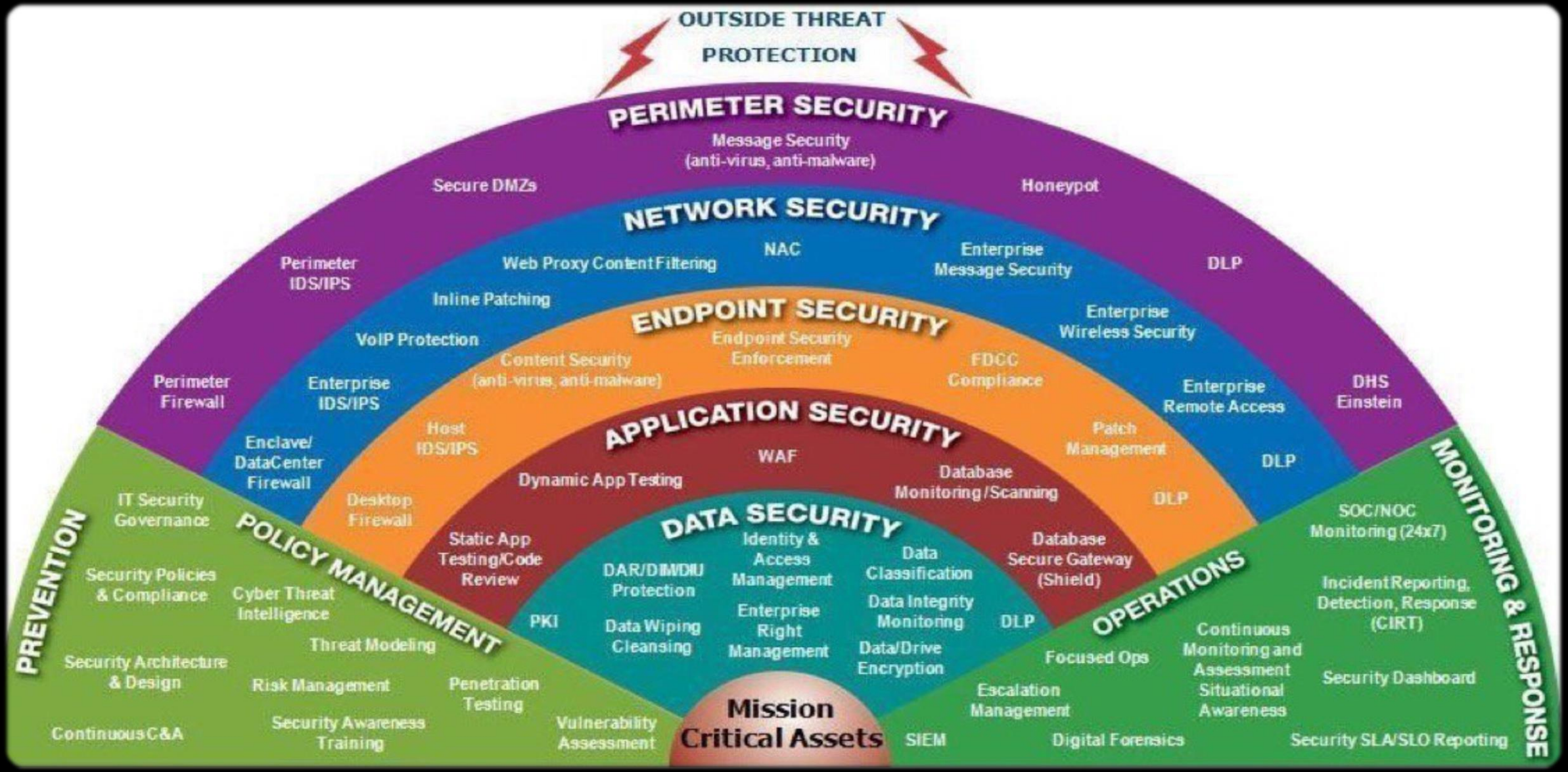


What about those ops teams?

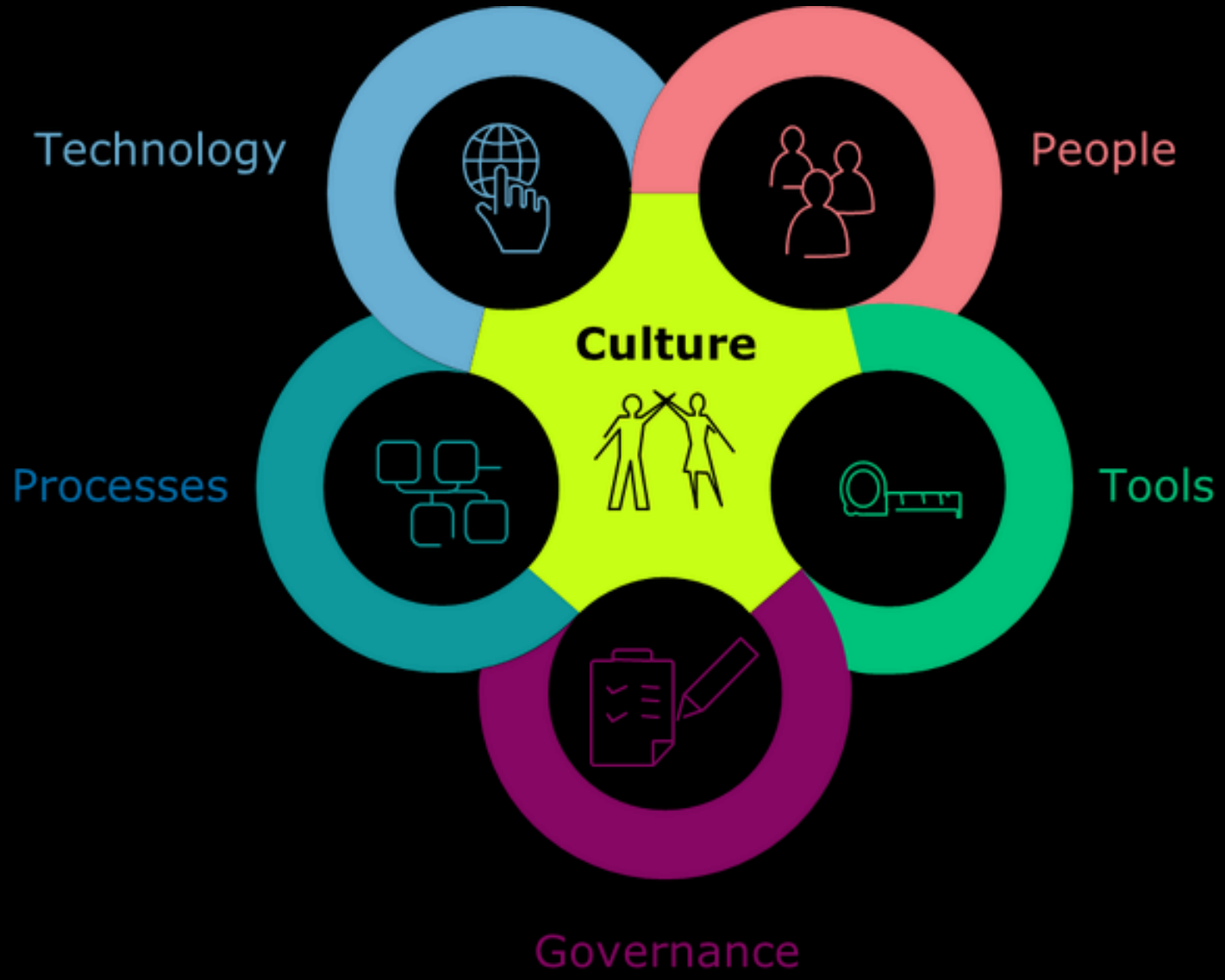
About those docker images...



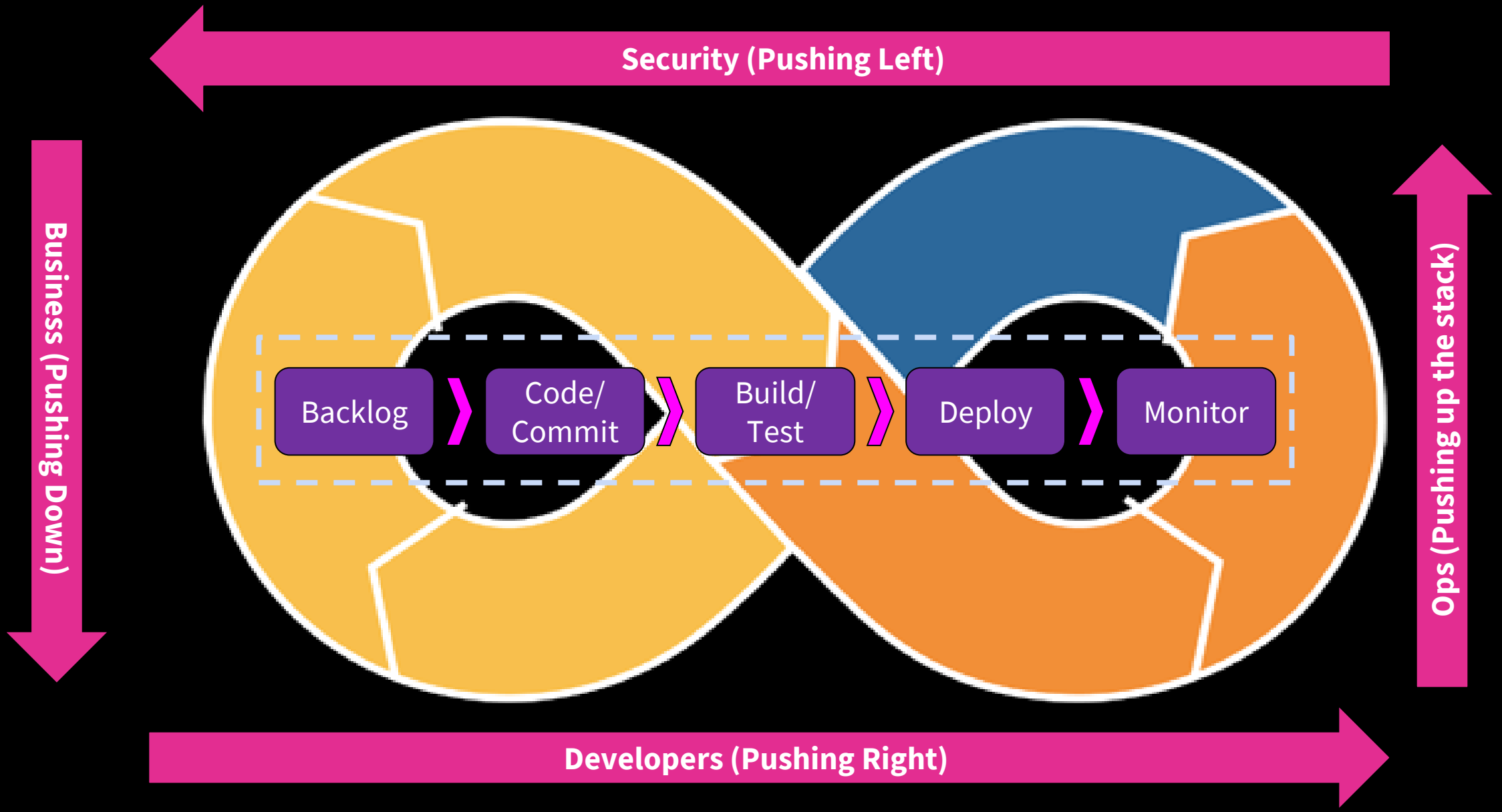
But that's why we have a security team right?



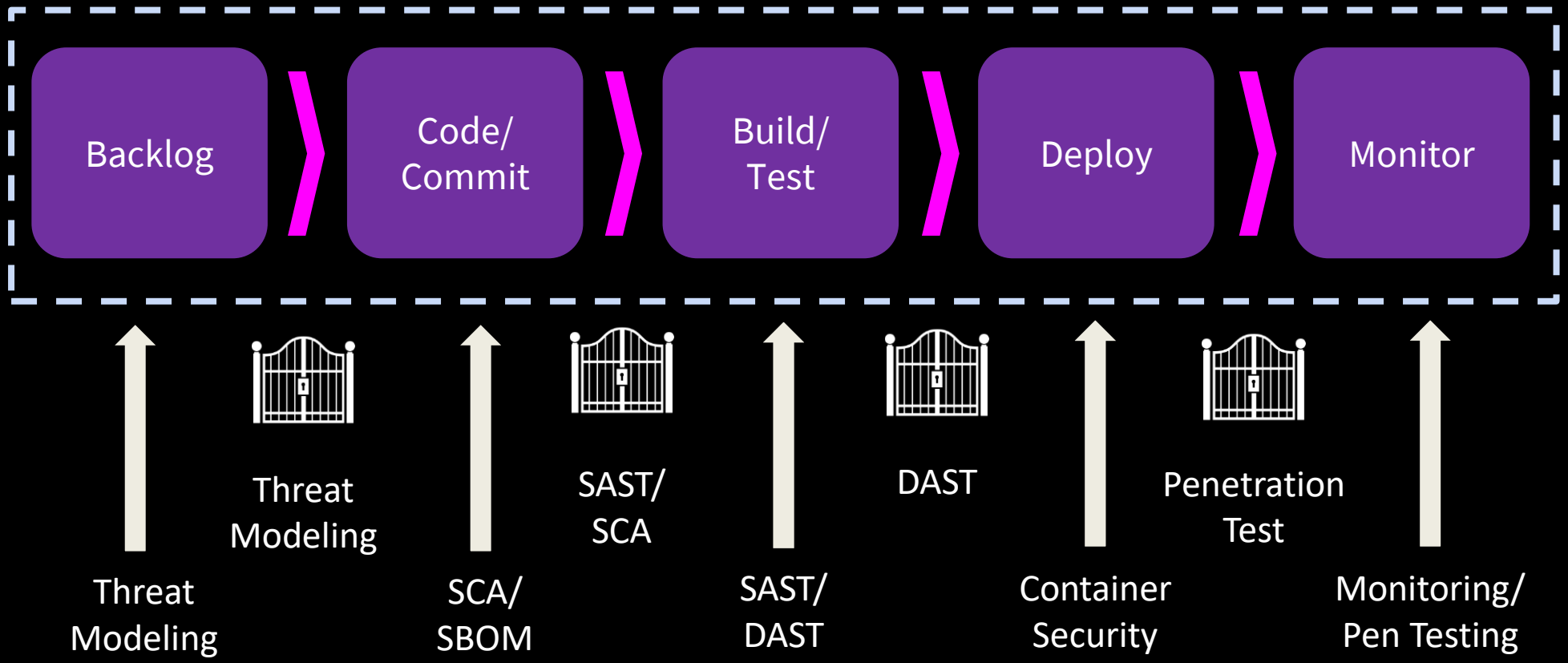
Welcome to DevSecOps



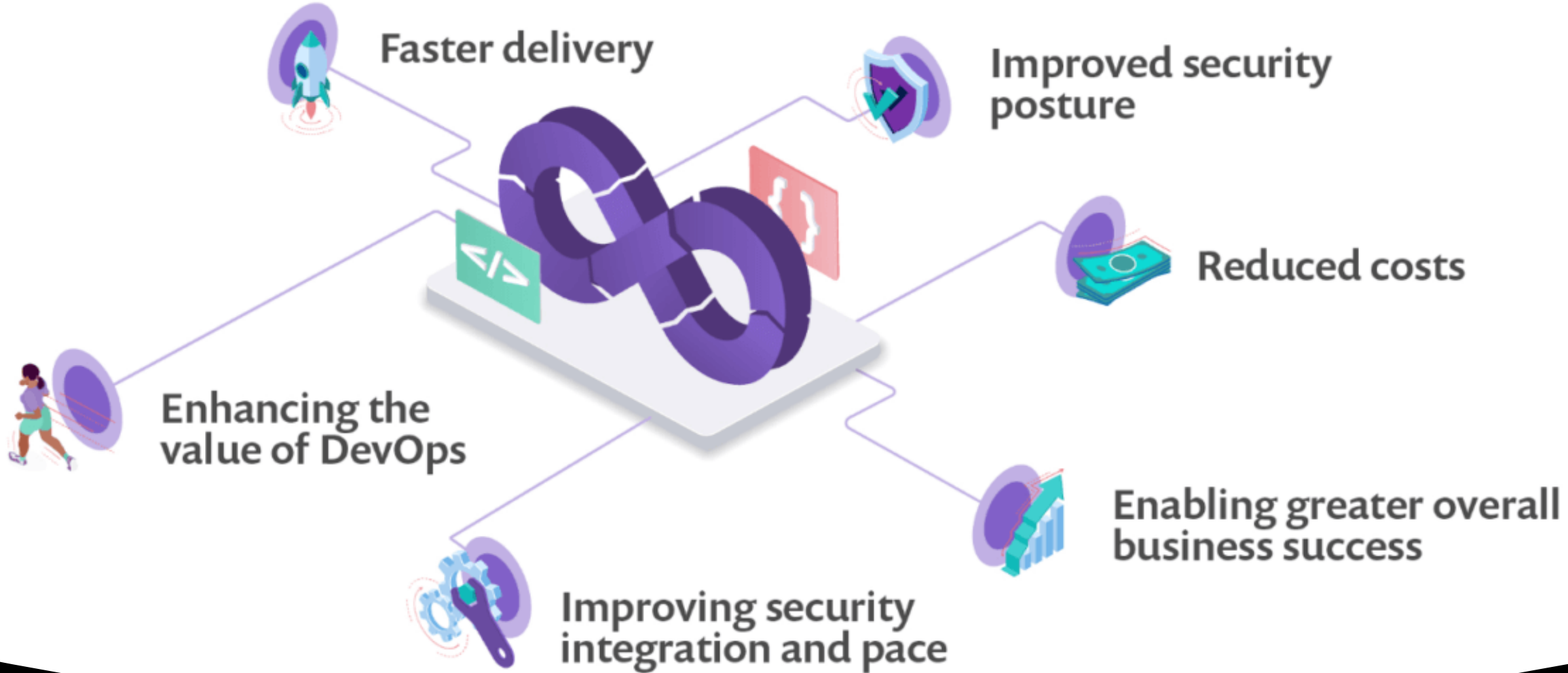
The motion of today's DevSecOps Pipeline…

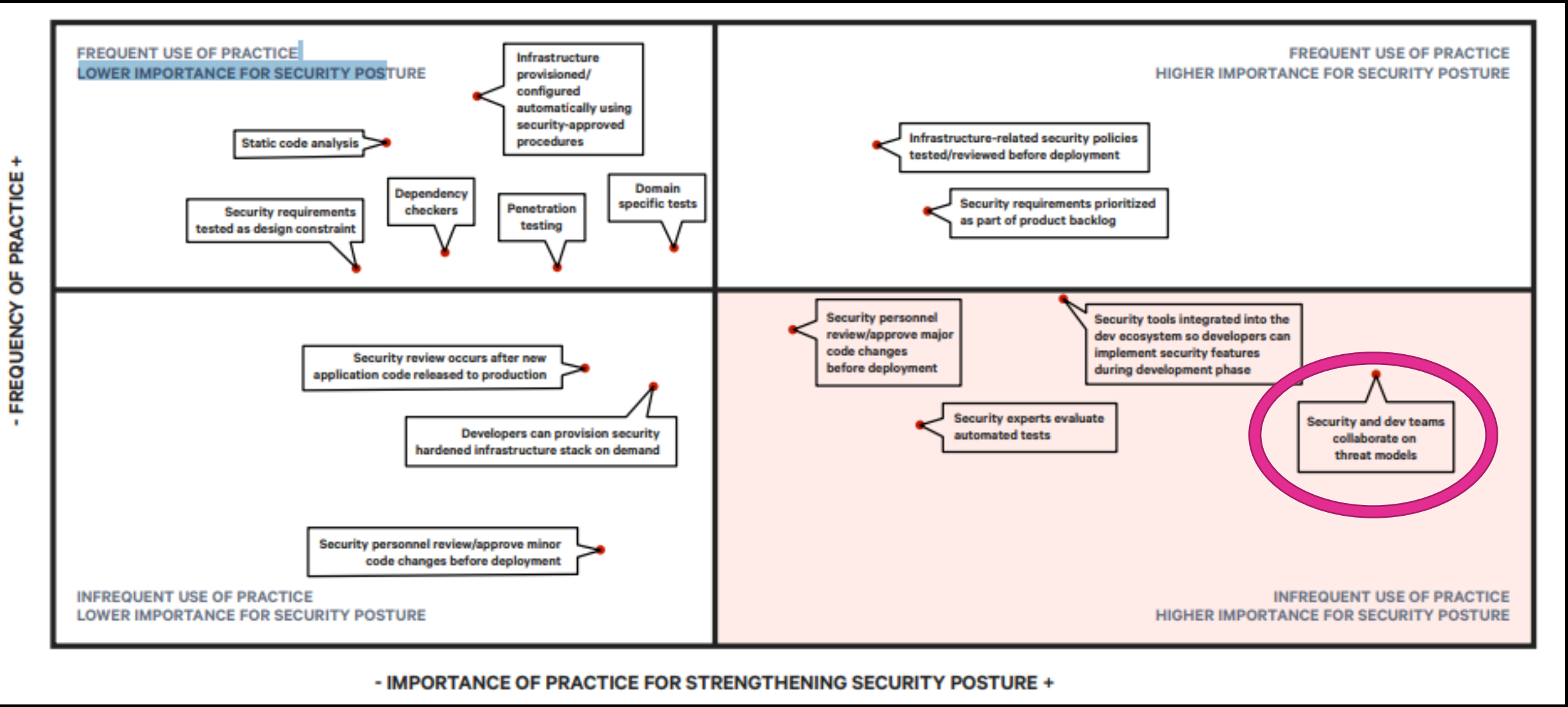


Frictionless enablement...



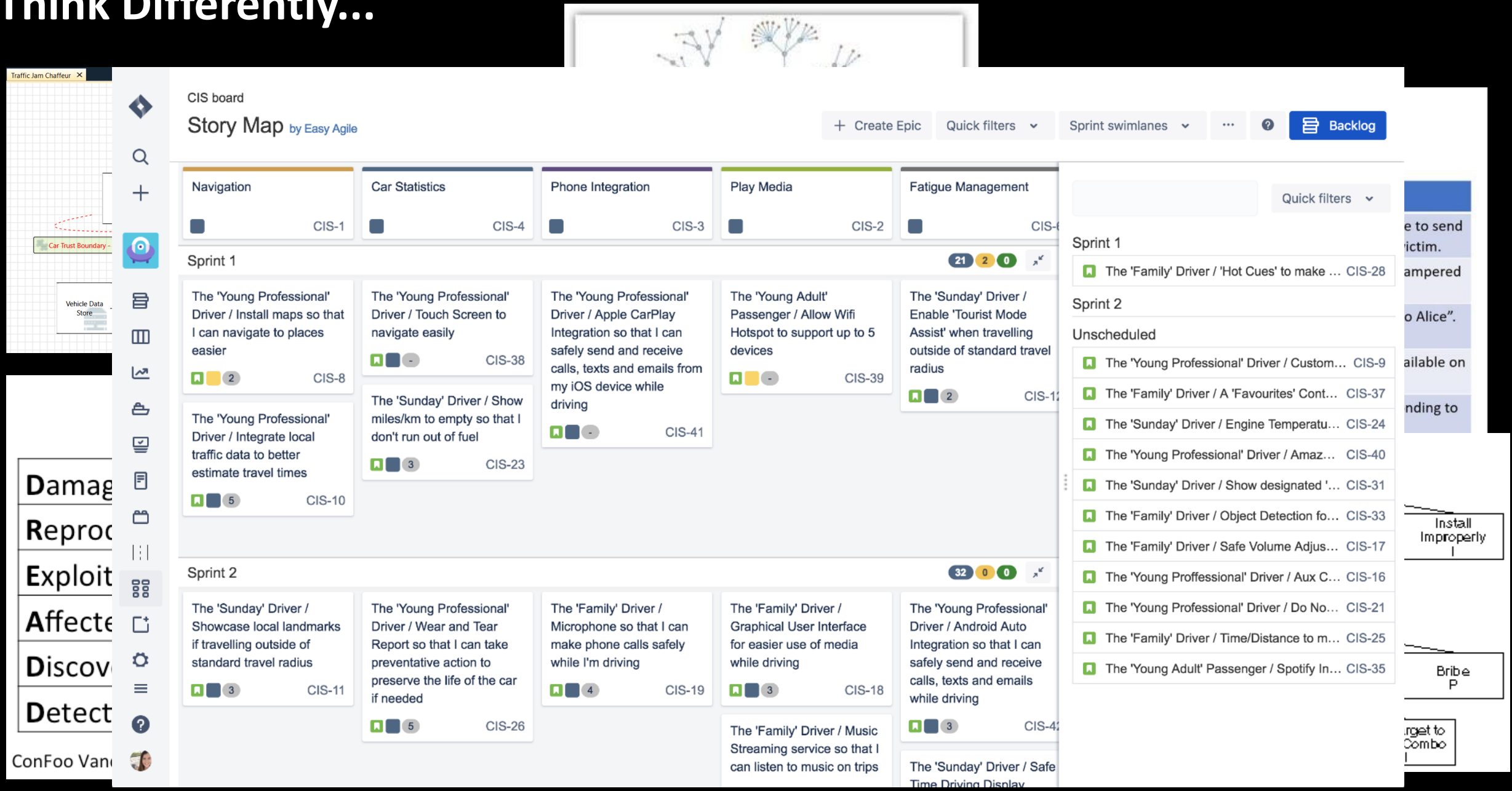
snyk


Faster delivery
Improved security posture
Reduced costs
Enabling greater overall business success
Improving security integration and pace
Enhancing the value of DevOps



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

Think Differently...



Threat Information

Plan

Security Requirements

Build

Security Controls

Test

Test Cases

Deploy

Monitoring

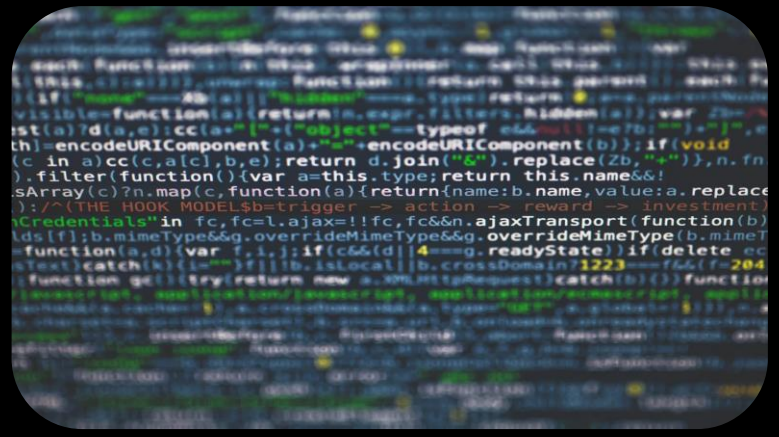
Build the empathy and culture…

Walk-a-Mile In Their Shoes

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

Mutual Engagement

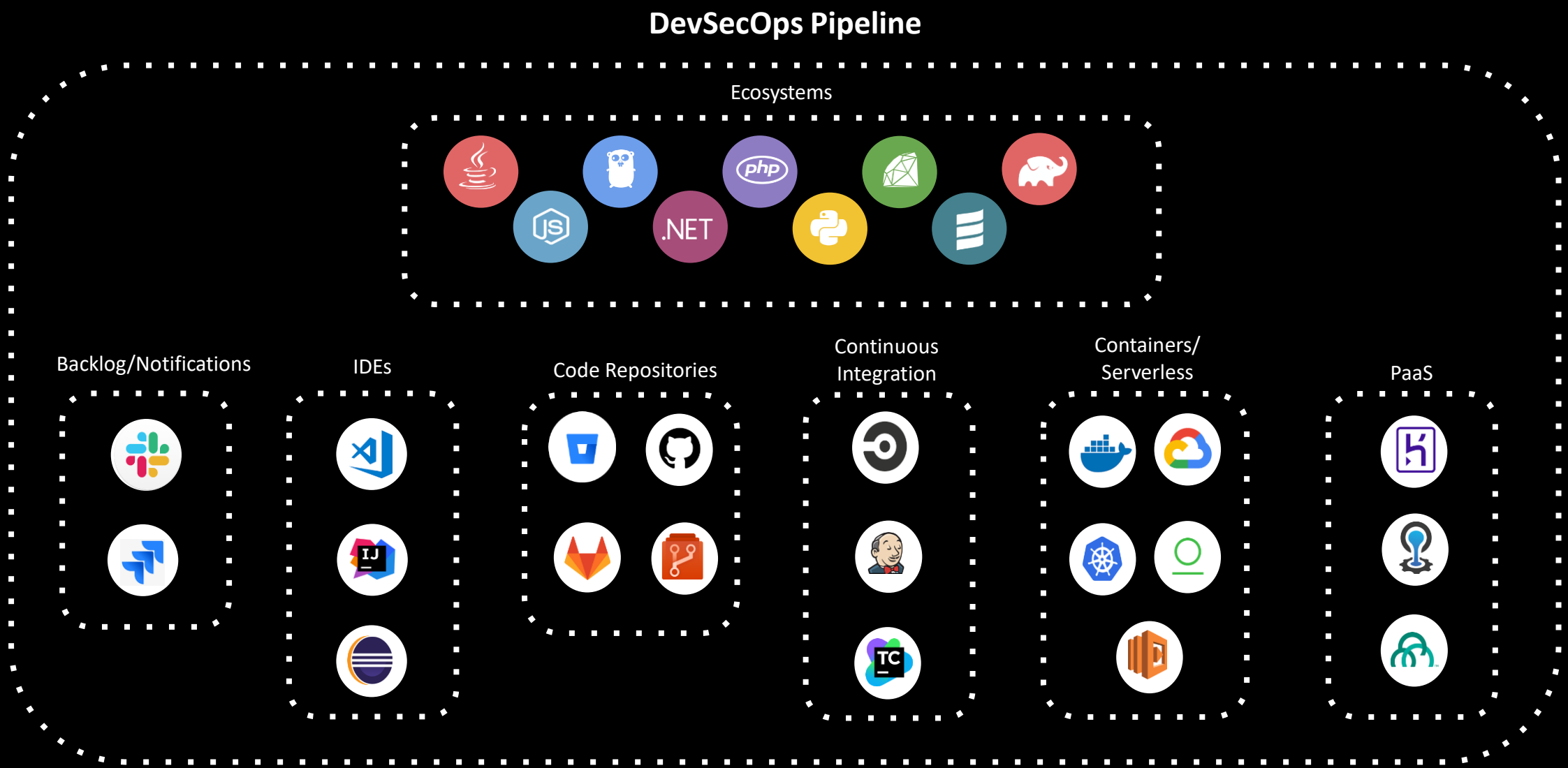
Connect Daily Activities Across Disciplines



Pave the Road

Tool Selection / Accountable Trust

Meet them where they live...



“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