

Security is Everybody's Job!

Akira Brand

Developer Relations
Bright Security



Unspecified

SOFTWARE CO



Intellibus



VONAGE



frontegg

Yum!

**DIGITAL +
TECHNOLOGY**

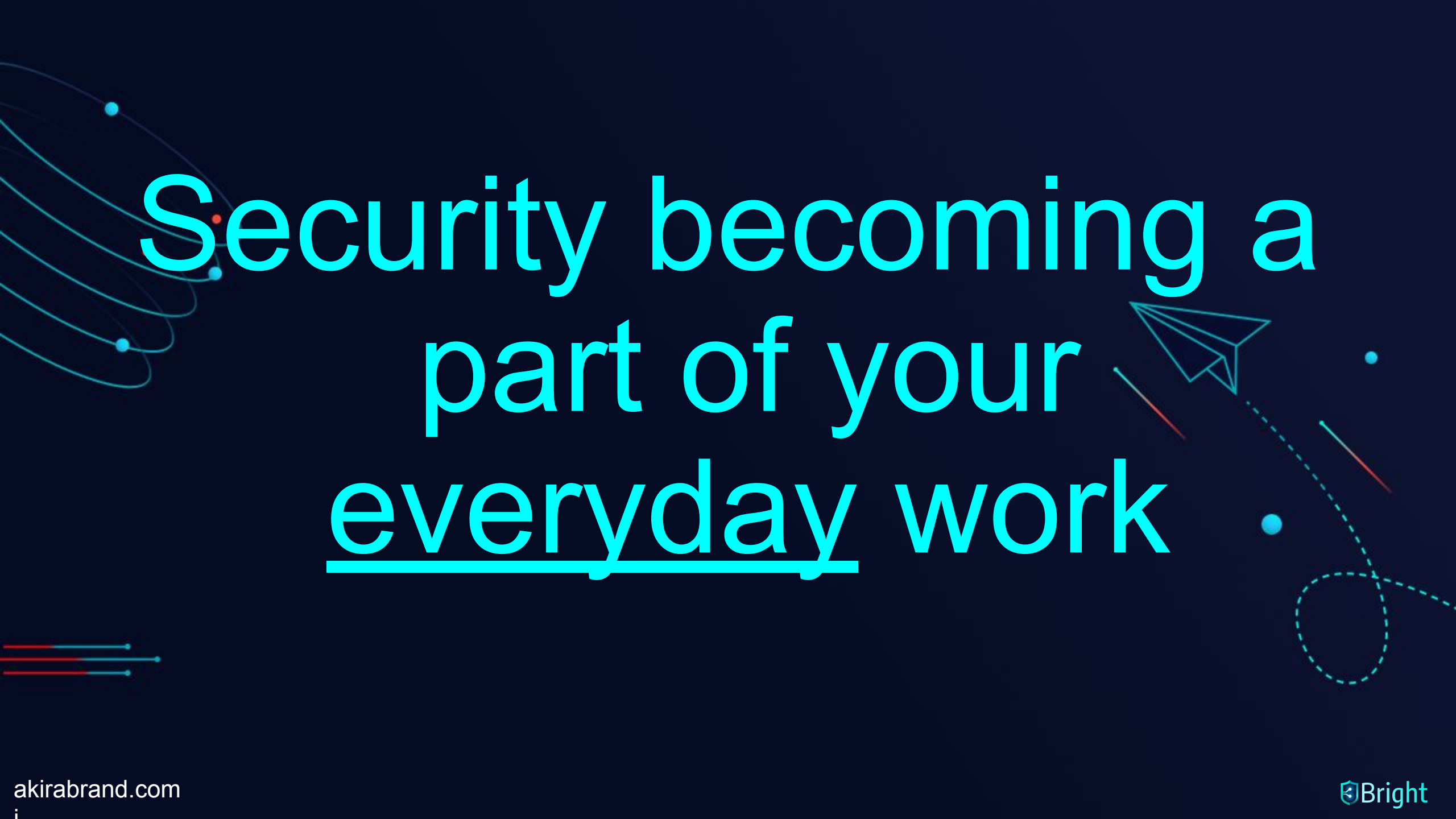
THANK YOU





A few questions
for you...



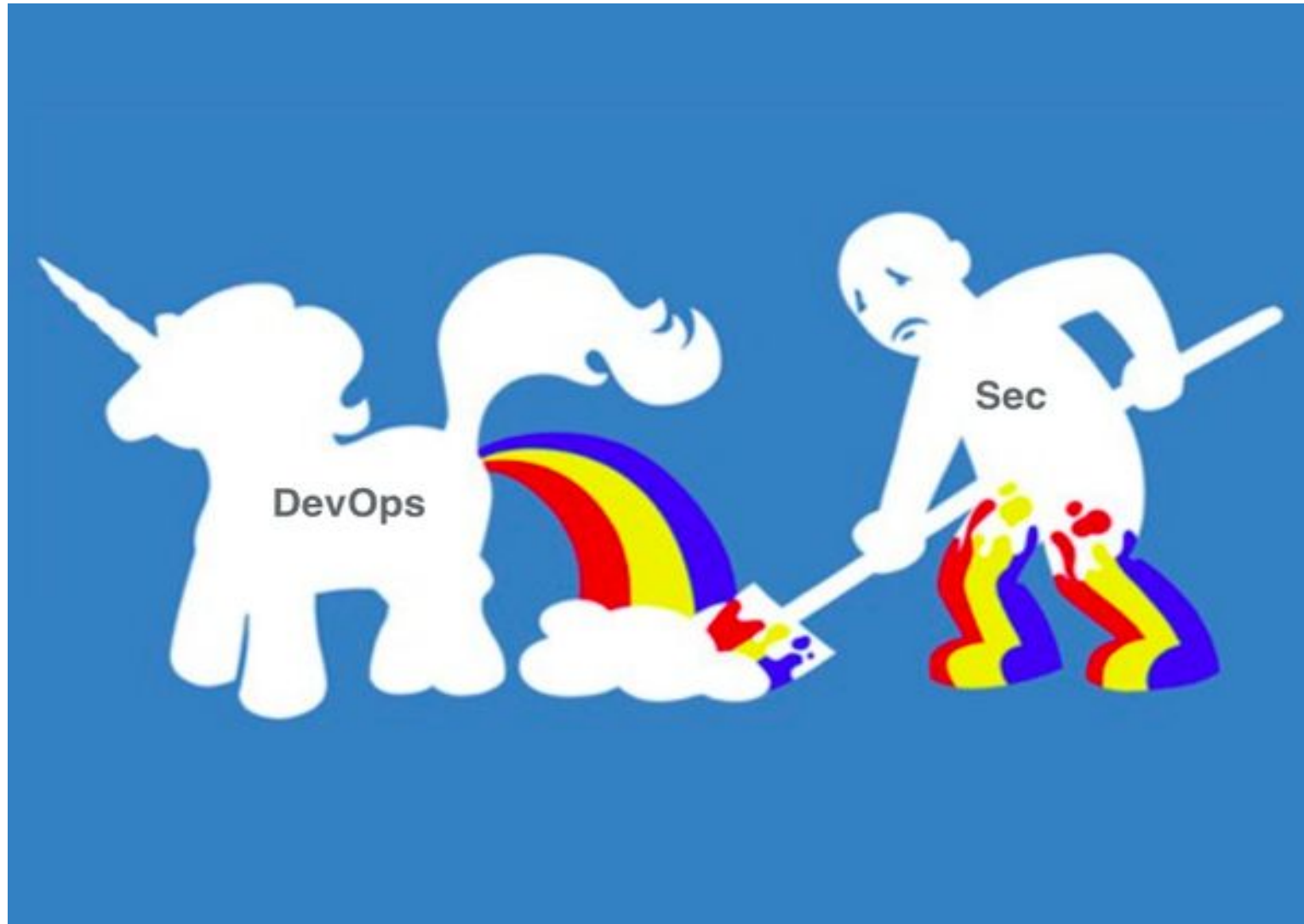


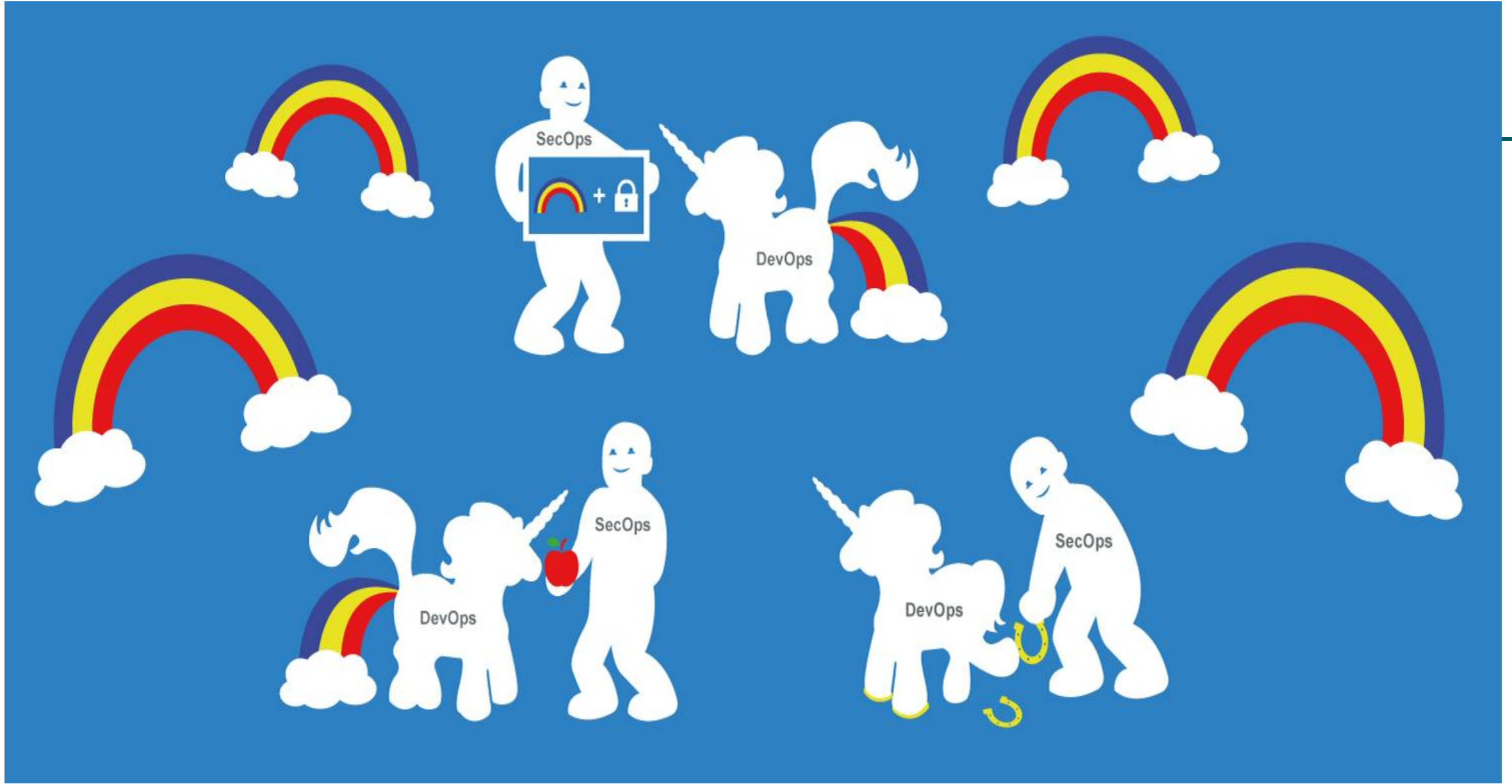
Security becoming a
part of your
everyday work

Security is EVERYBODY'S job!



How *some* security people see DevOps





Otherwise known as...

DEVSECOPS



Akira Brand

- Developer Relations @ Bright Security
- Co-host, Application Security Weekly podcast
- Community Manager, Artists who Code
- WeHackPurple host & contributor
- Former Opera Singer

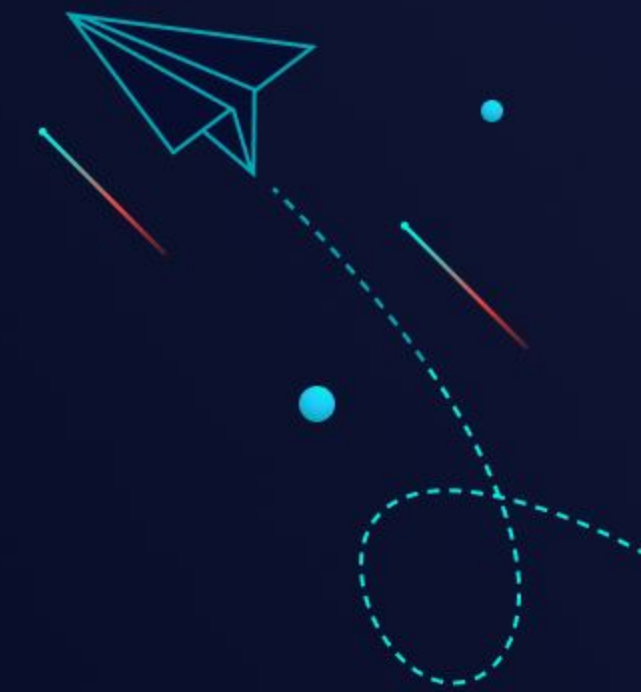




Let's do
this!



What is Application Security?



“It’s any and every activity that you perform to ensure that your software is secure.”

-Tanya Janca

This includes...

- Threat modeling!
- Hiring a pentester!
- Running a DAST or SAST tool against your code!
- Secure code review!
- Software composition analysis!
- And MORE!

Problem: *Exists*

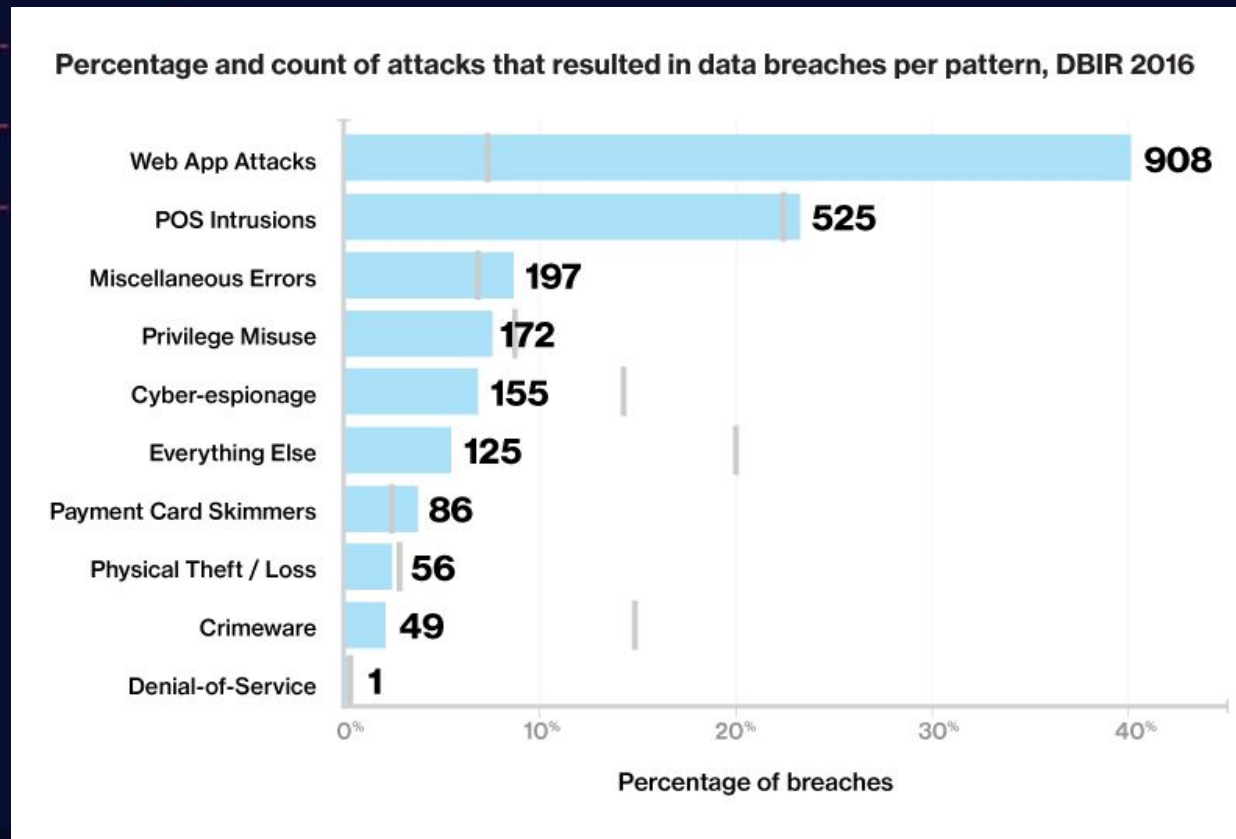
Hacker in a movie: *types
bdnceikanekirjbsk*

The problem:



Poor AppSec is a problem!

Poor AppSec Causes ~29-40% of Breaches!



Application Security Is Missing!



AppSec is not covered in most post-secondary Comp-Sci and Soft-Eng programs

And when it is, it's often an after thought

Security is Outnumbered!



Security is Outnumbered!

Dev | Ops | Sec

100 / 10 / 1




Solution?

DevSecOps



What is DevSecOps?





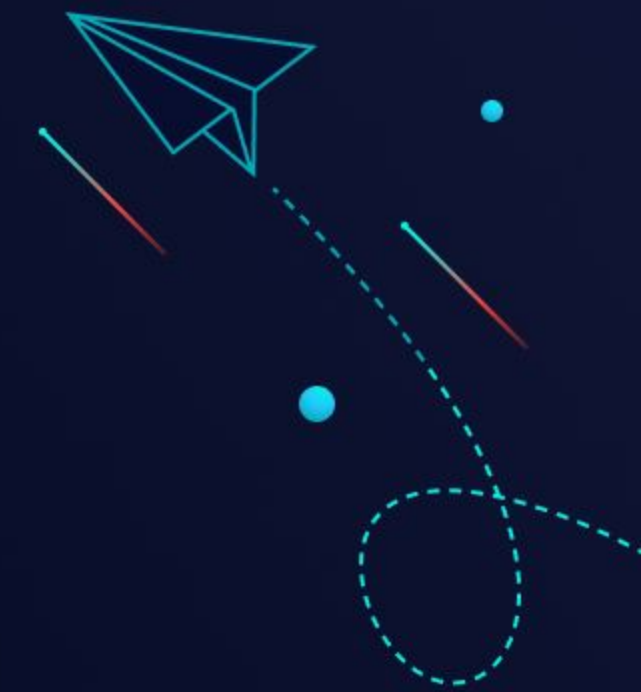
"AppSec in a DevOps Environment"



-Imran A. Mohammed



AppSec +
DevOps =
DevSecOps

Integrating DevOps and Security





What are the goals of
DevOps, and are they the
same goals as security?

First Goal of DevOps

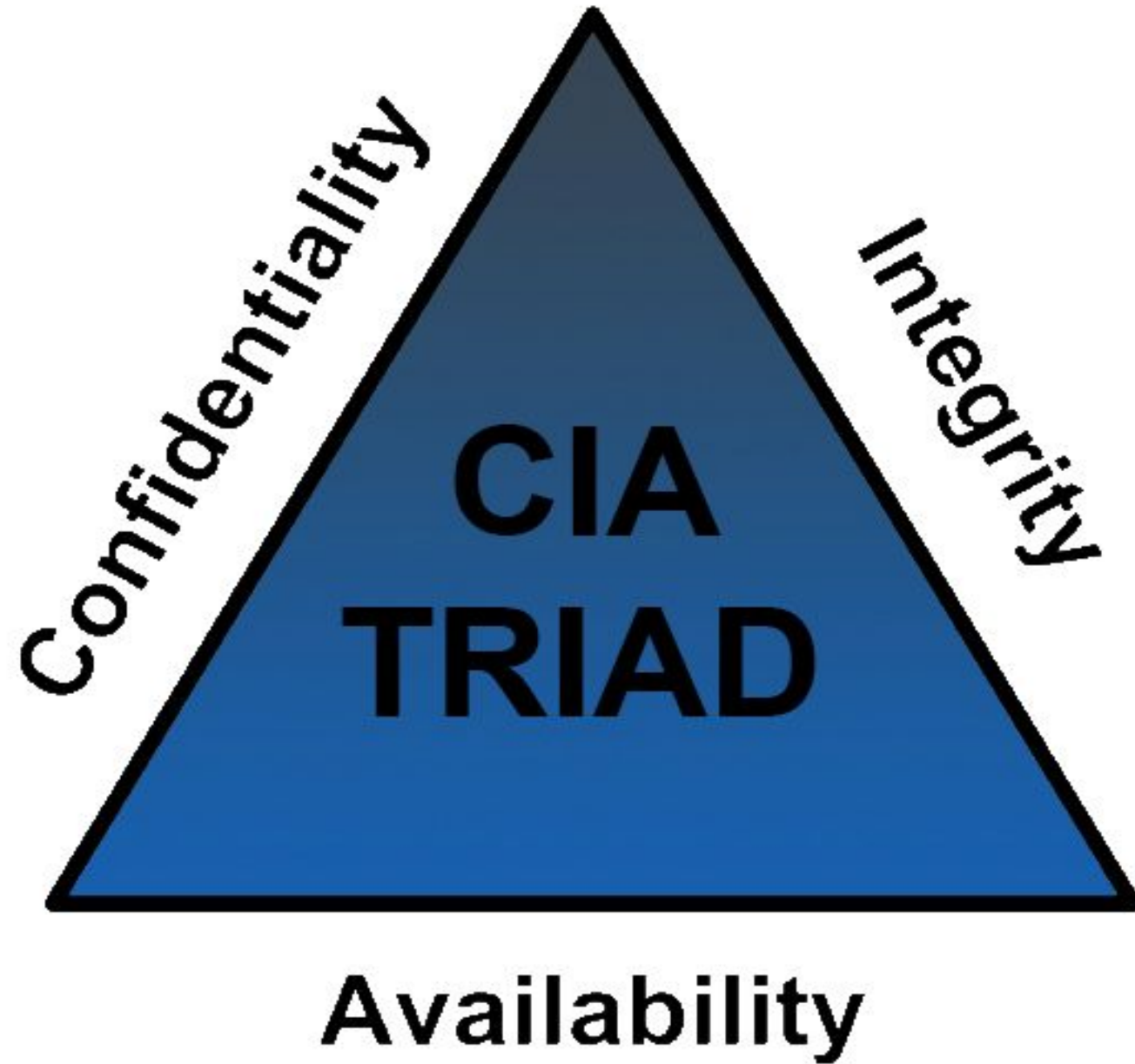
Improved Deployment
Frequency

Huzzah, I can fix security bugs quickly!

Second Goal of DevOps

Lower Failure Rates

= Availability



Less Failure Rates =
Better Availability

Third Goal of DevOps

Faster Time to Market



Security doesn't win if
the business doesn't win



DevOps

The Three Ways



The Three Ways of DevOps

Emphasize the efficiency of the *entire* system.

**Fast
Feedback**

**Continuous
Learning**

The First Way of DevOps

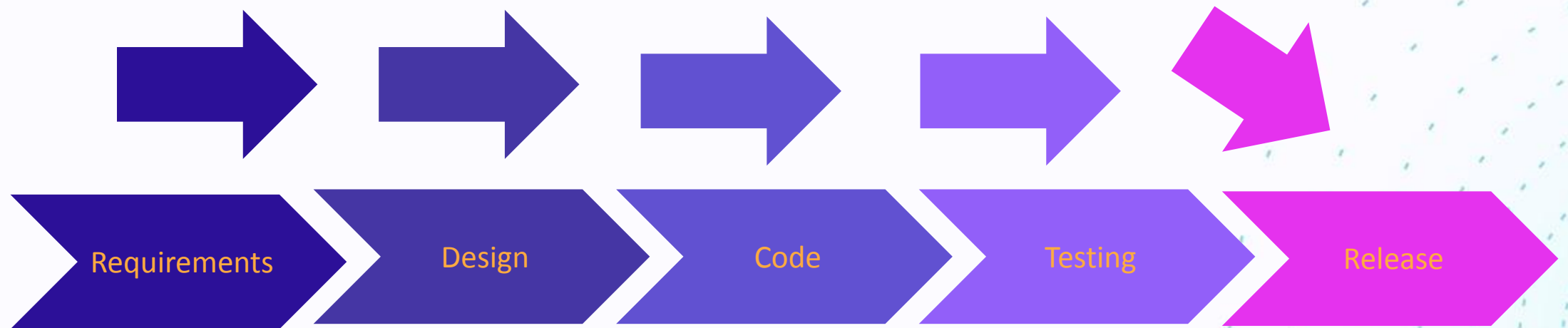
Emphasize the efficiency of the *entire* system

not just your part!

The outcomes of putting the First Way into practice include never passing a known defect to downstream work centers...and always seeking to achieve profound understanding of the system...

-Gene Kim, The DevOps Handbook

Left → Right = Speed



What does this mean for security teams?



What does this mean for security teams?

- Security cannot break the build unless it's absolutely necessary; true emergency
- Tune our tools and replace shoddy ones
- Work with the QA team to get .har files to test only what is absolutely necessary
- Fit our work into the sprint cycles of devs

What does this mean for dev & ops?



What does this mean for dev and ops?

- Give feedback to the security team - what works and what does not?
- Hate a tool? Tell us!
- Put security bugs into your bug tracker
- Create a secure code library - reusable code that is tested and secure
- Use up-to date and patched Docker images
- Set up regular, automated scans for VMs and containers



How can dev and ops help?

- Help the AppSec team tune web proxy scanners such as Zap, Bright, SonarCube...
- Ensuring your libraries and other 3rd party components are secure by adding OWASP Dependency check or track, Retire.js, Black Duck, Snyk, (more!) to your pipeline.
- If the AppSec team creates a long-running security pipeline for you, please use it!

**Help the
AppSec Team
tune their
tools.**

**For their sake,
and yours.**

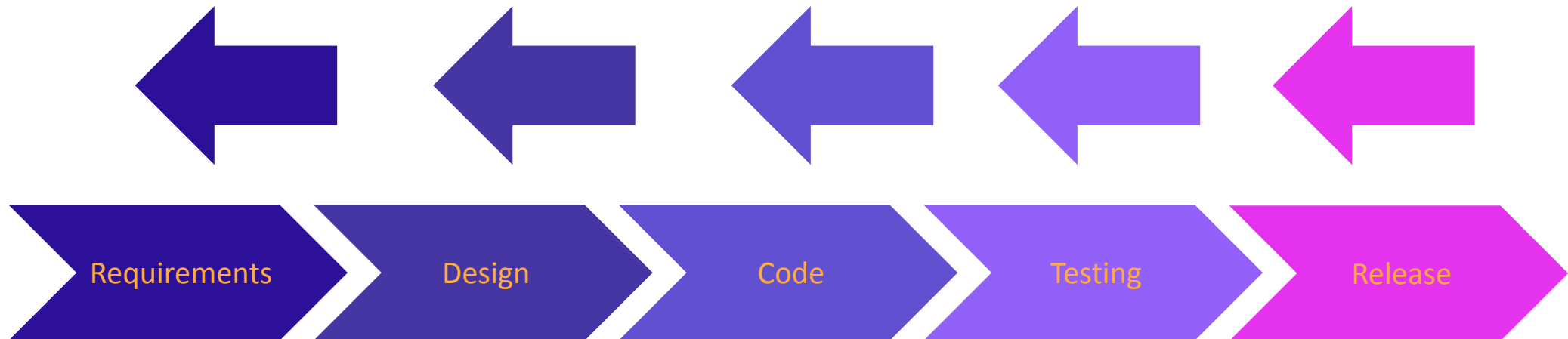


The Second Way of DevOps

Fast Feedback!

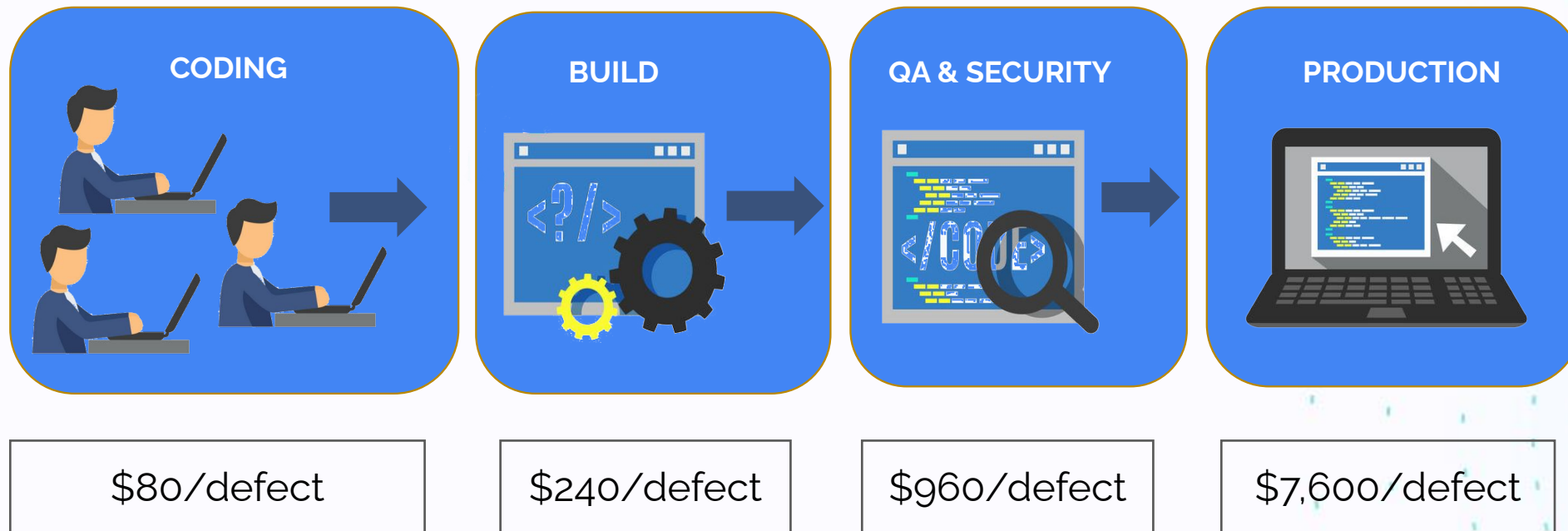
Faster Feedback

Right → Left = Feedback
= Pushing Left!



DevOps and the “Shift Left” principle

Fixing costs of quality & security issues rises significantly as the development cycle advances - Ponemon Institute



What does this mean for developers?

Telling the security team what you are concerned about.

Feedback goes both ways.



What does this mean for ops?

Participating in Security Activities

Incidents

Threat Modelling

Security Sprints

Etc



What does this mean for dev *and* ops?

- Fast feedback loops = fixing security bugs quickly
- Breaking the build *if* you introduce security issues
- Adding security sprints to your project timeline
- Threat modelling activities - do them!
- Participating in incident response, if need be
- Learning to use security tools
- Security becoming part of the definition of quality

The Third Way of DevOps

Continuous Learning & Improvement

Outcomes of the third way



Allocating time for the improvement of daily work

Creating rituals that reward the team for taking risks

Introducing faults into the system to increase resilience.



What does this mean for Security?



What does this mean for security?

- Every moment possible should be a teachable moment
- Allocate time for the improvement of daily security work for Dev and Ops
- Create rituals that reward the team for taking risk
- Celebrate success!
- Introduce faults into the system to allow for greater resilience

What does this mean for developers?



What does this mean for developers?

- Accept security training if offered
- Teach and train yourself on security
- Share information widely when you fix security issues

What does this mean for ops?



What else does this mean for dev and ops?

- Sometimes security teams do whiteboarding/security requirements, please come!
- Ask the security team for metrics - you can crunch that data in Excel and see the top 3 problems, etc.
- Whenever you do a postmortem, please make it blameless

And Last, but Not Least...

Culture Change!

Security becoming *a part of* DevOps.

Reinforce Culture Change



Celebrate
security wins.

Reinforce Culture Change



Work more closely: Security + Dev + Ops

Reinforce Culture Change

No more
blaming!

Reinforce Culture Change

Be a Security
Champion!





I do solemnly swear...



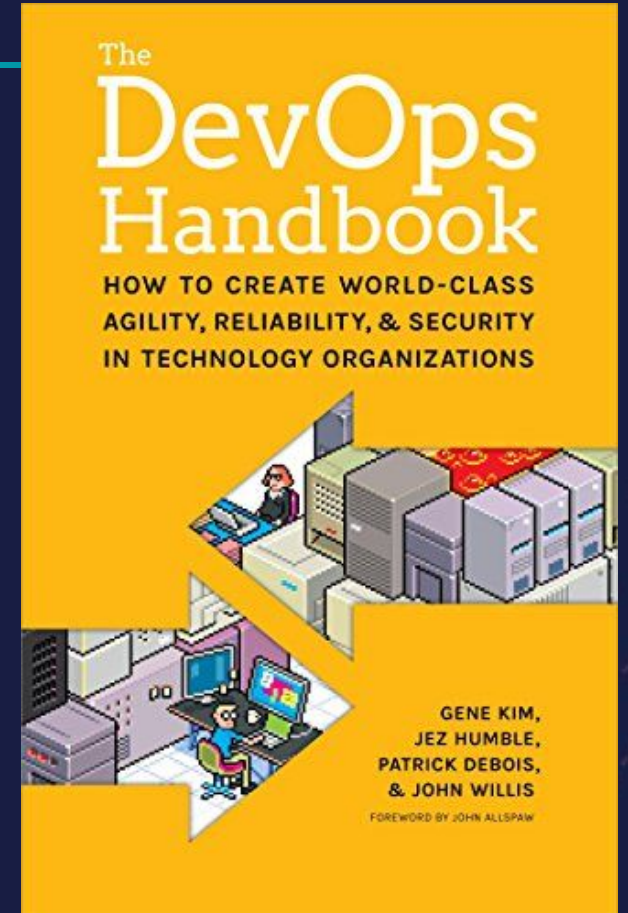
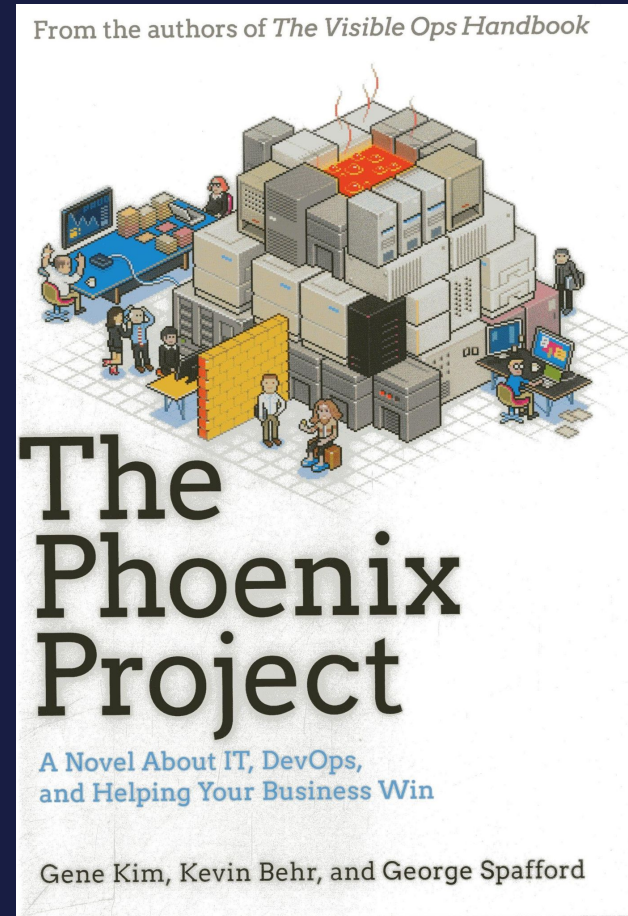
RESOURCES



Rad DevOps Books

The DevOps Handbook

The Phoenix Project





 **Me!**
theakirati@gmail.com

 **Bright Blog and Docs –**
www.brightsec.com/blog

 **"Secure Coding Course"**
from We Hack Purple - FREEEE!

 **MANY THANKS to Tanya**
Janca (@shehackspurple)

Join the community!

Join the We Hack Purple Community for FREE!!

community.wehackpurple.com

Meet like-minded people and nerd out!



I co-host a podcast!

Application Security Weekly

scmagazine.com/podcast-show/application-security-weekly



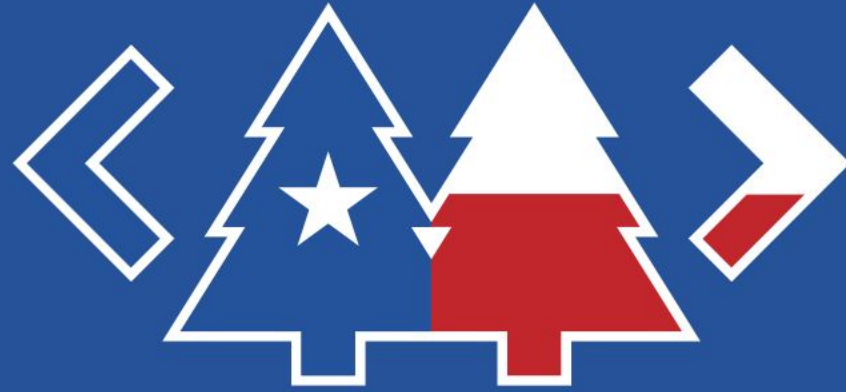


**Let's
connect!**

[linkedin.com/in/akirabrand](https://www.linkedin.com/in/akirabrand)

theakirati@gmail.com

www.akirabrand.com



2024

January 29th - February 1st





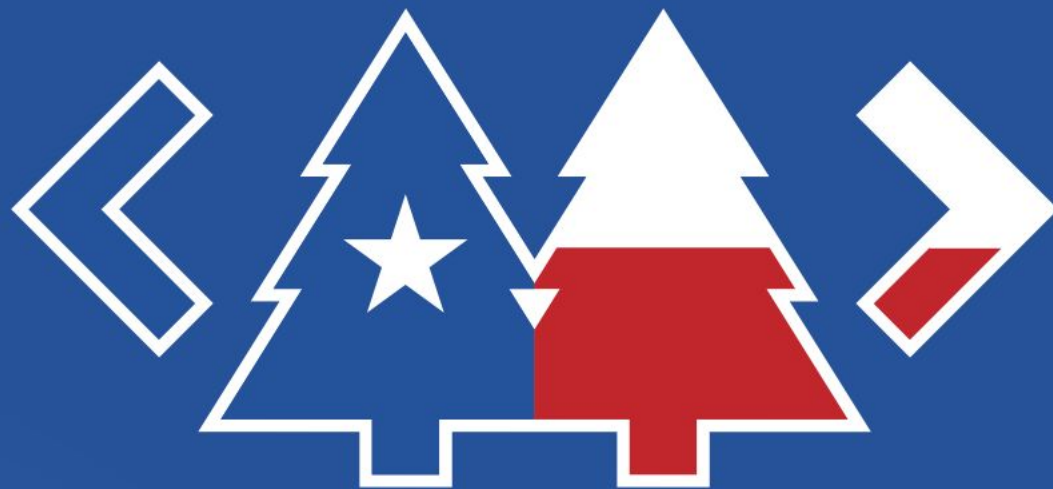
Security is now a
part of DevOps.



DevSecOps!

THANK YOU!





THAT CONFERENCE

