RSAConference2019
San Francisco | March 4–8 | Moscone Center

BETTER.

SESSION ID: STR-R03

Security Learns to Sprint: DevSecOps

Tanya Janca

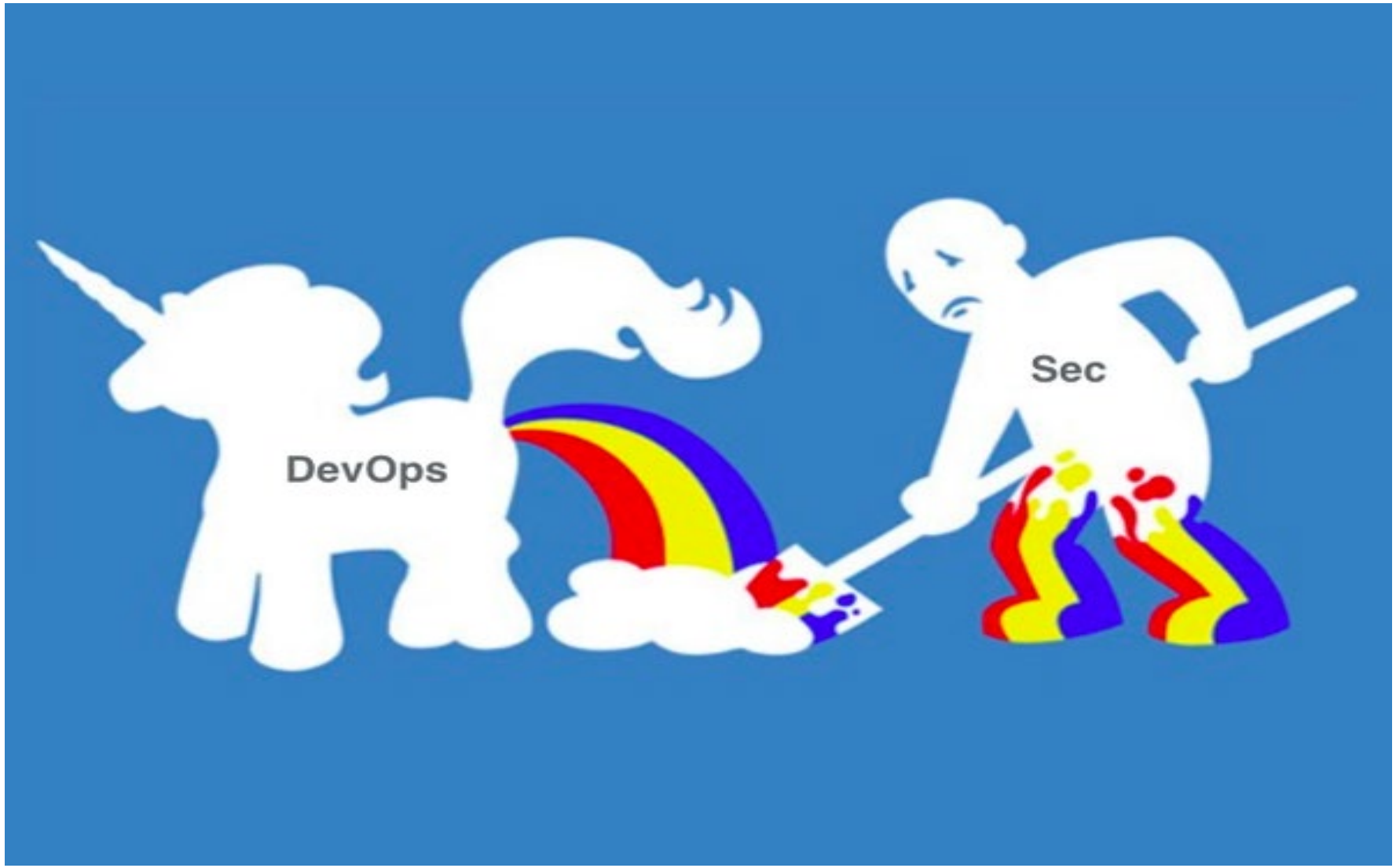
Senior Cloud Developer Advocate
Microsoft
@SheHacksPurple

What are we going to talk about today?

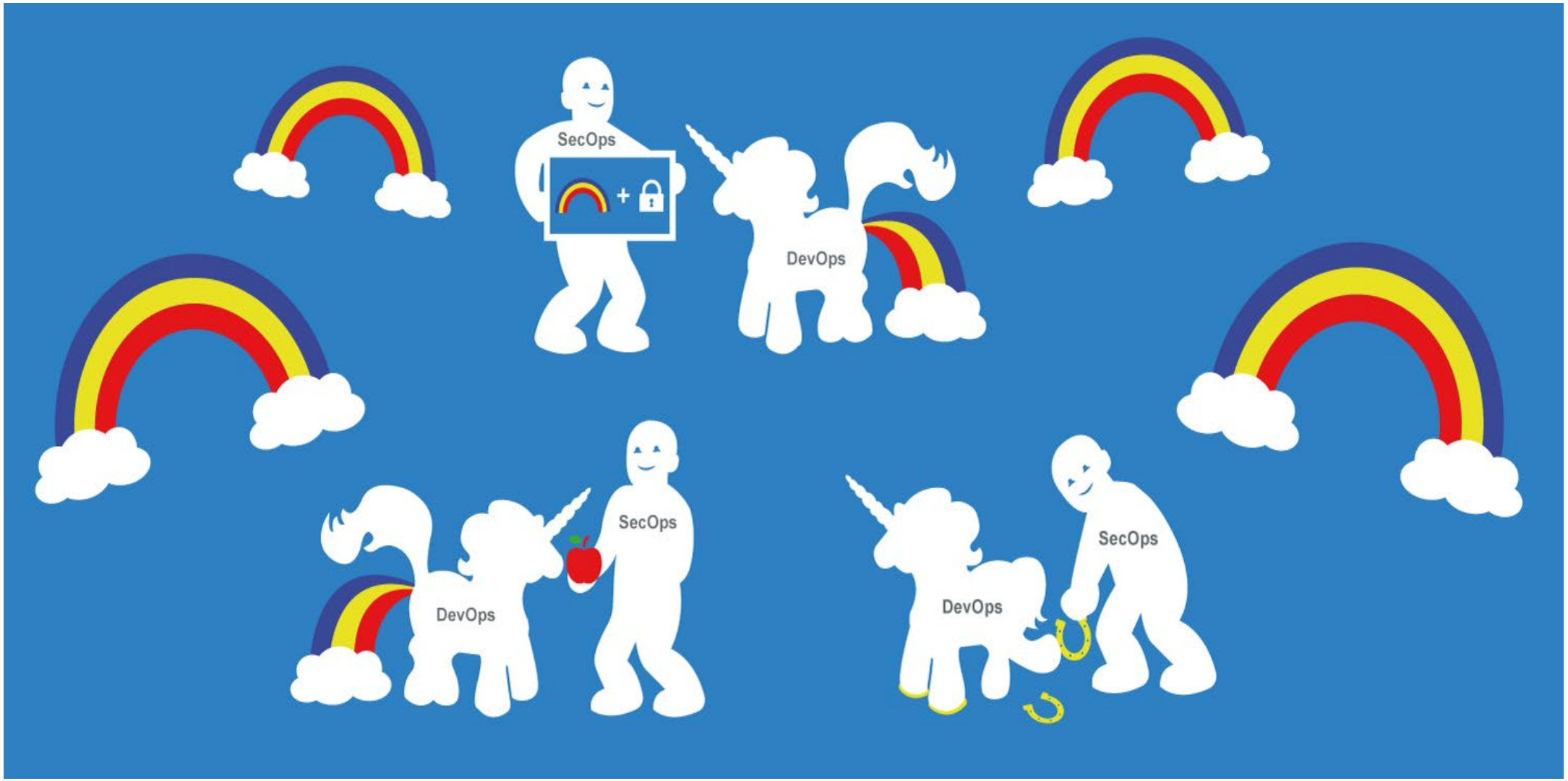
What are we going to talk about today?

What are we going to talk about today?

How ***some*** security people see DevOps



How I see DevOps: DevSecOps



This is me.

This is me.

I’m a Senior Cloud Developer Advocate at:

What does **THAT** mean?

This is me.

I'm a Senior Cloud Developer Advocate

I help developers use our products more securely.

I work to make security features easier to use.

I do security research and share it with the community.

I provide feedback from the community to internal teams, so they can make our products more secure.

Security research, such as this presentation, OWASP DevSlop, and much more.

This is me.

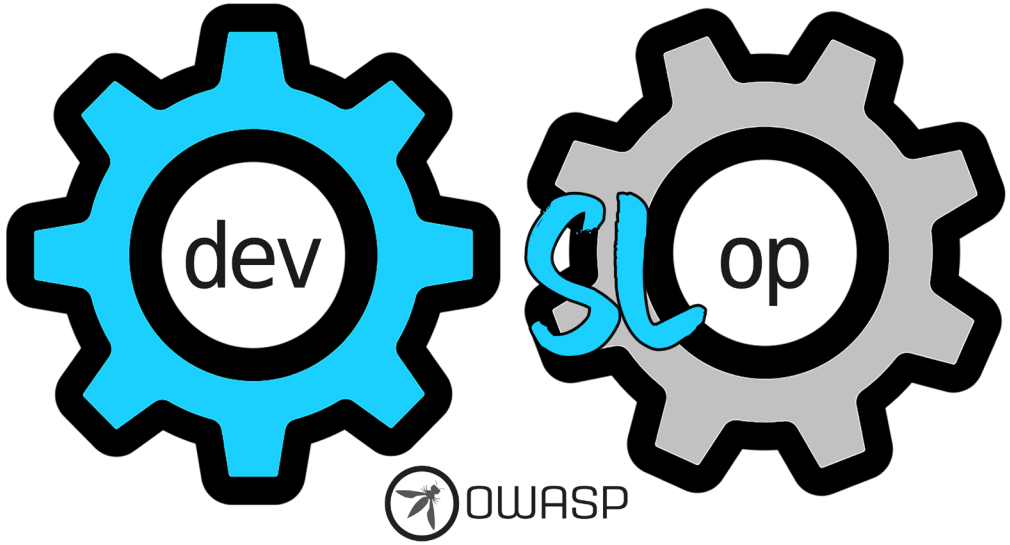
Application Security Evangelist

This is me.

Application Security Evangelist

This is me.

I'm *obsessed* with OWASP! **Open Web Application Security Project**



An international non-profit that operates chapters, projects and conferences all over the globe, in efforts to help everyone create more secure software.

This is me.

Founder and Leader of **WIST Ottawa!**

Women In Security and Technology

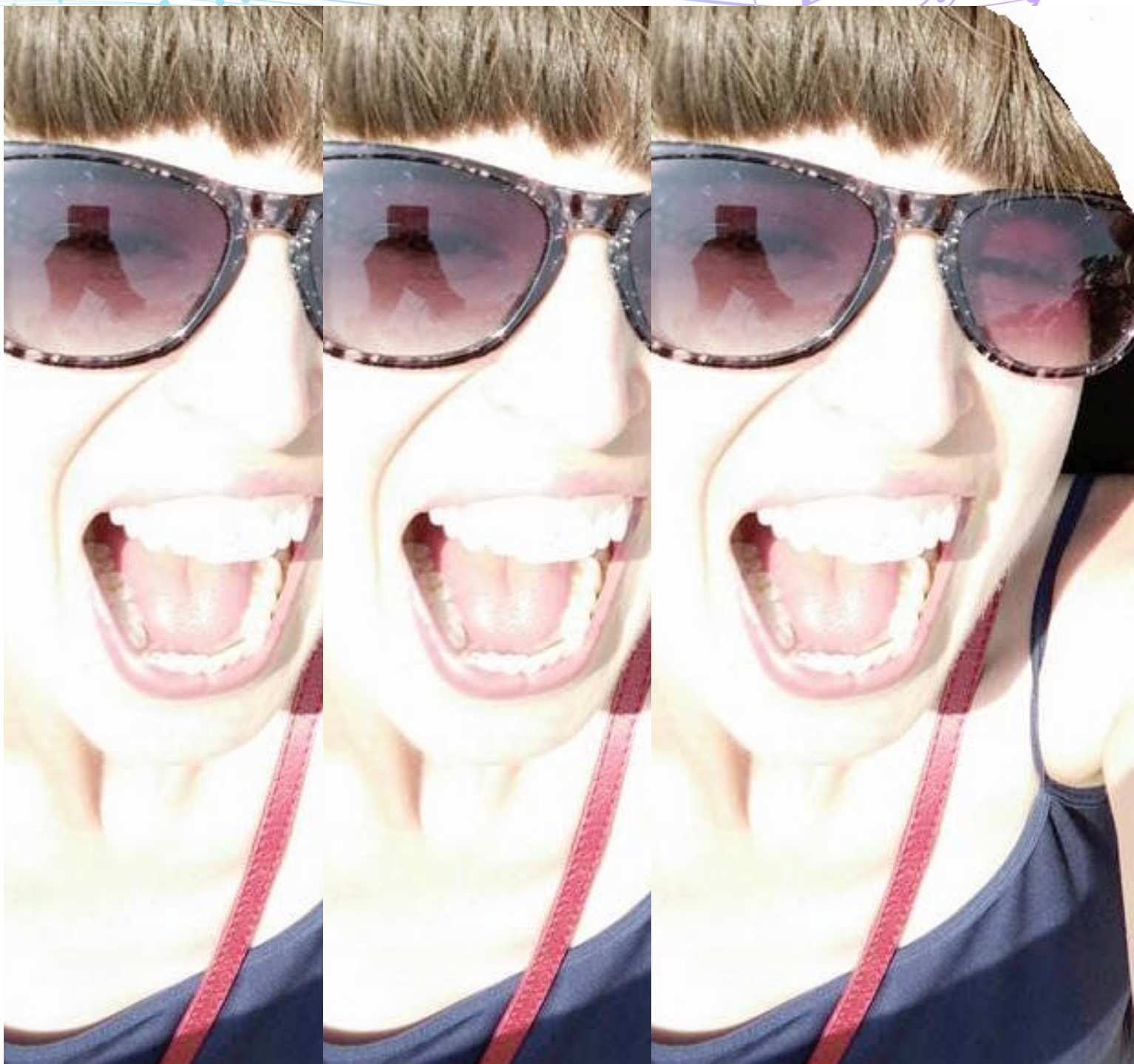
This is me.

Software Developer

(since the late 90’s)

That’s over 20 years!

AHHHHHHHHHHHH!



This is me.

Goal: to change the way we make software so that the easiest way to do something is also the most secure way.

Let’s do this.

RSAConference2019

Introduction: Application Security

What IS AppSec?

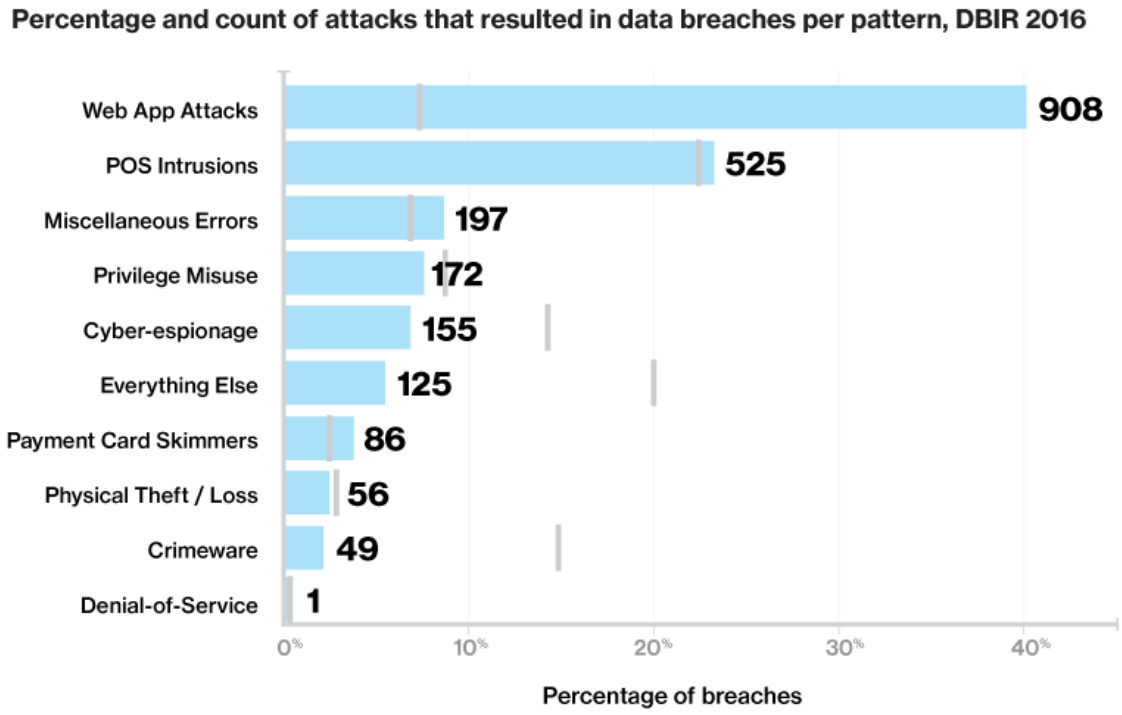
"It's any and every activity that you perform to ensure that your software is secure."

-Me

Poor AppSec is a Problem!

Poor AppSec Causes 29-40%~ of Breaches!

Verizon Data Breach Investigation Report (DBIR) for 2017 and 2016.



Application Security 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

Waterfall Never Worked Well

And the accompanying security model was much, much worse.

What IS DevSecOps?

"Performing AppSec in a DevOps culture."

- Imran A Mohammed

RSAConference2019

DevOps

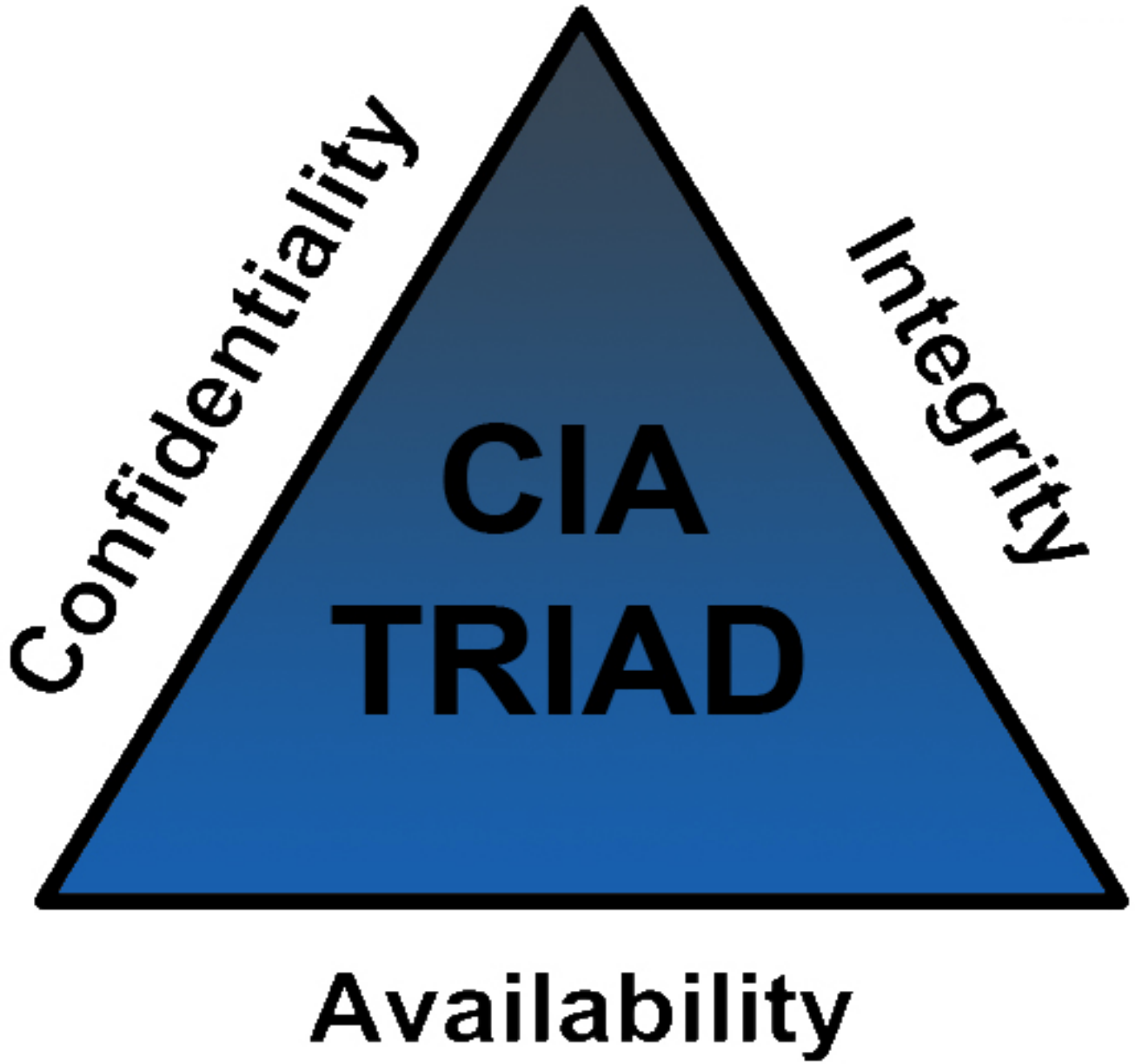
The Main Goals

Improved Deployment Frequency

Security emergencies can be fixed NOW.

Lower Failure Rates

Resiliency


Confidentiality
Integrity
CIA
TRIAD
Availability

Lower Failure Rates

Resiliency = Confidentiality
Integrity
Availability

Faster Time to Market

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

RSAConference2019

"DevOps is the best thing to happen to Application Security since OWASP."

-Tanya Janca

RSAConference2019

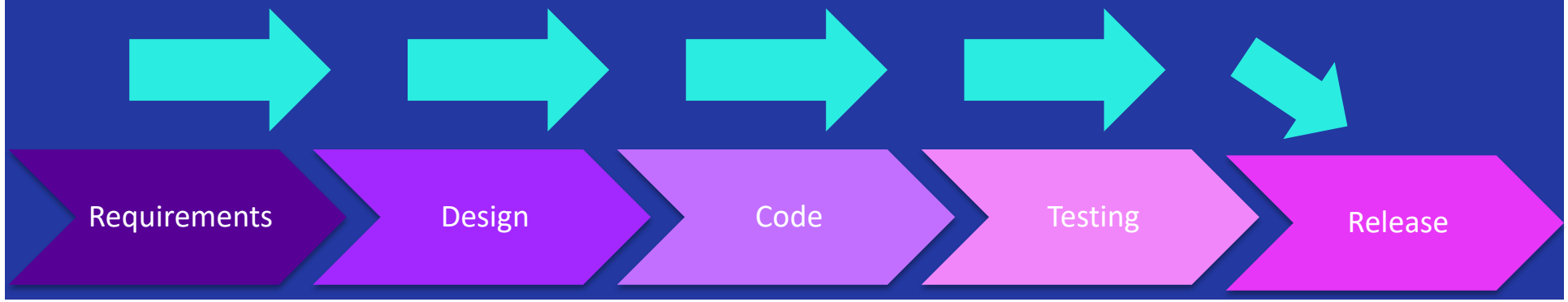
DevOps

The Three Ways

Emphasize the efficiency of the *entire* system.

Left -> Right = speed

Emphasize the efficiency of the *entire* system.



What does this mean for Dev & Ops?

What does this mean for Dev & Ops?

The "Photo" Slide, #1

- Assisting in tuning SAST and DAST tools
- Reusing known good code
- Using up-to-date images
- Using the Security Pipeline
- Making negative unit tests
- Severe security bugs break the build
- We cannot do it without them on board

What does this mean for Security?

What does this mean for Security?

What does this mean for Security?

The “Photo” Slide, #2

- Ensure Dev & Ops are not waiting on you
- Tuning security tools so they do not produce false positives
- Breaking security activities into smaller pieces so that they fit into the “sprints”
- Make processes that ***work*** , and match pace
- Providing secure templates and code samples that a known-secure (sec code library)

What does this mean for Security?

Create a parallel security pipeline.

For more in-depth testing.

What does this mean for Security?

What does this mean for Security?

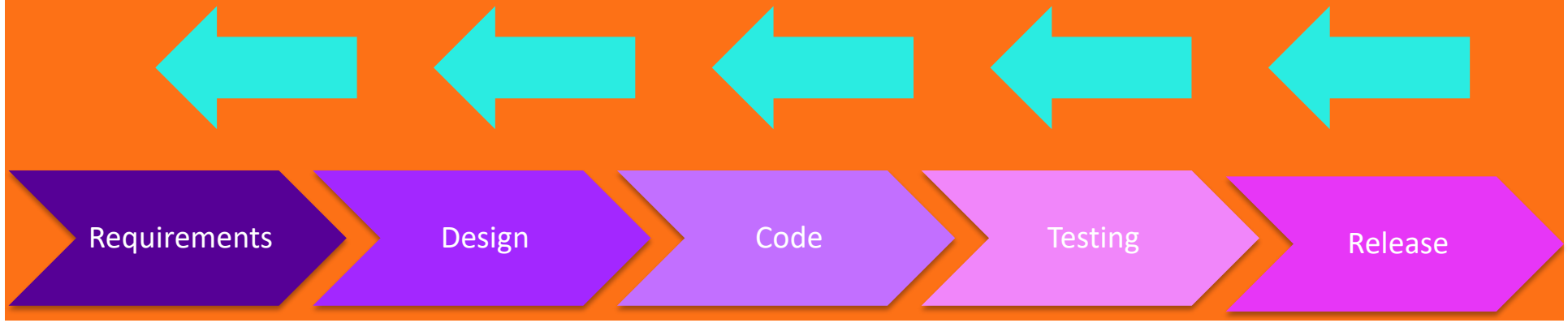
The “Photo” Slide, #3

- Create a security pipeline
- Buy licenses for dev and ops for sec tools
- This does not mean doing 100% of the work yourself, it means making it possible for Dev & Ops to perform security as part of their daily work.
- Writing your own tools and libraries, see RepoKid from Netflix
- Enable Dev and Ops, in every way you can.

Faster Feedback

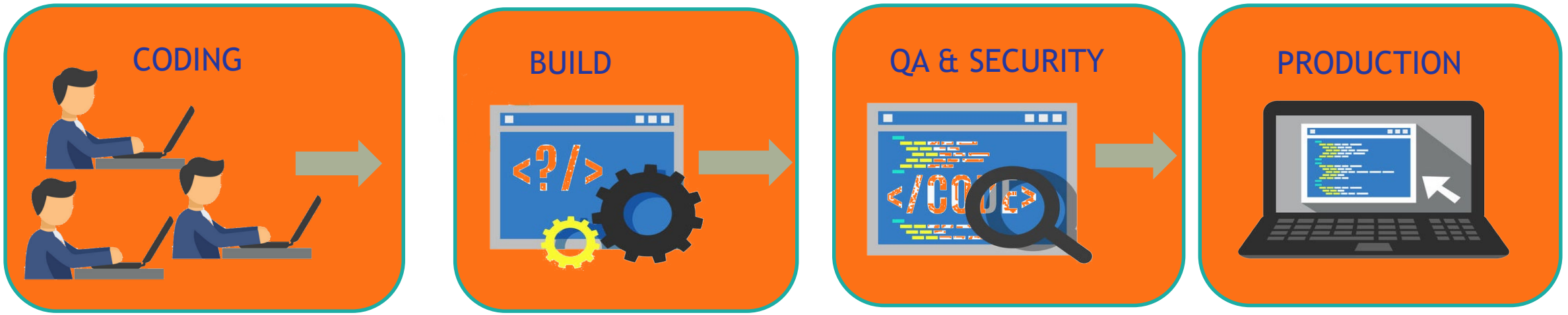
Right -> Left = Feedback

Faster Feedback = Pushing Left!



DevOps and the "Shift Left" principal

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



$80/defect	$240/defect	$960/defect	$7,600/defect

What does this mean for dev & ops?

Providing feedback to the security team about what they are concerned about.

The security team listening and taking action.

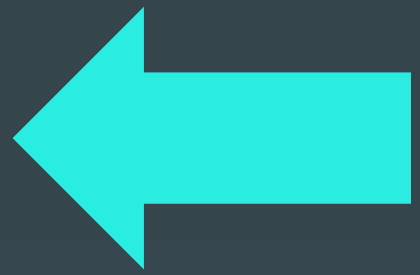
Participating in security activities.

What does this mean for Security?

Side Tangent: The SecDevOpronomicon

High ROI Security Engineering Tasks

- Build libraries / tools that are secure by default for dev teams
- E.g. Today, many web frameworks handle output encoding by default
  - Before that, devs had to manually add it everywhere, `h()` in Rails
- Potential areas to consider:
  - Managing secrets
  - Anything related to crypto
  - Authentication / authorization
  - SQL, file system access, shell exec()
  - E.g. `nonCryptographicallySecureMd5()`



Clint Gibler - @clintgibler

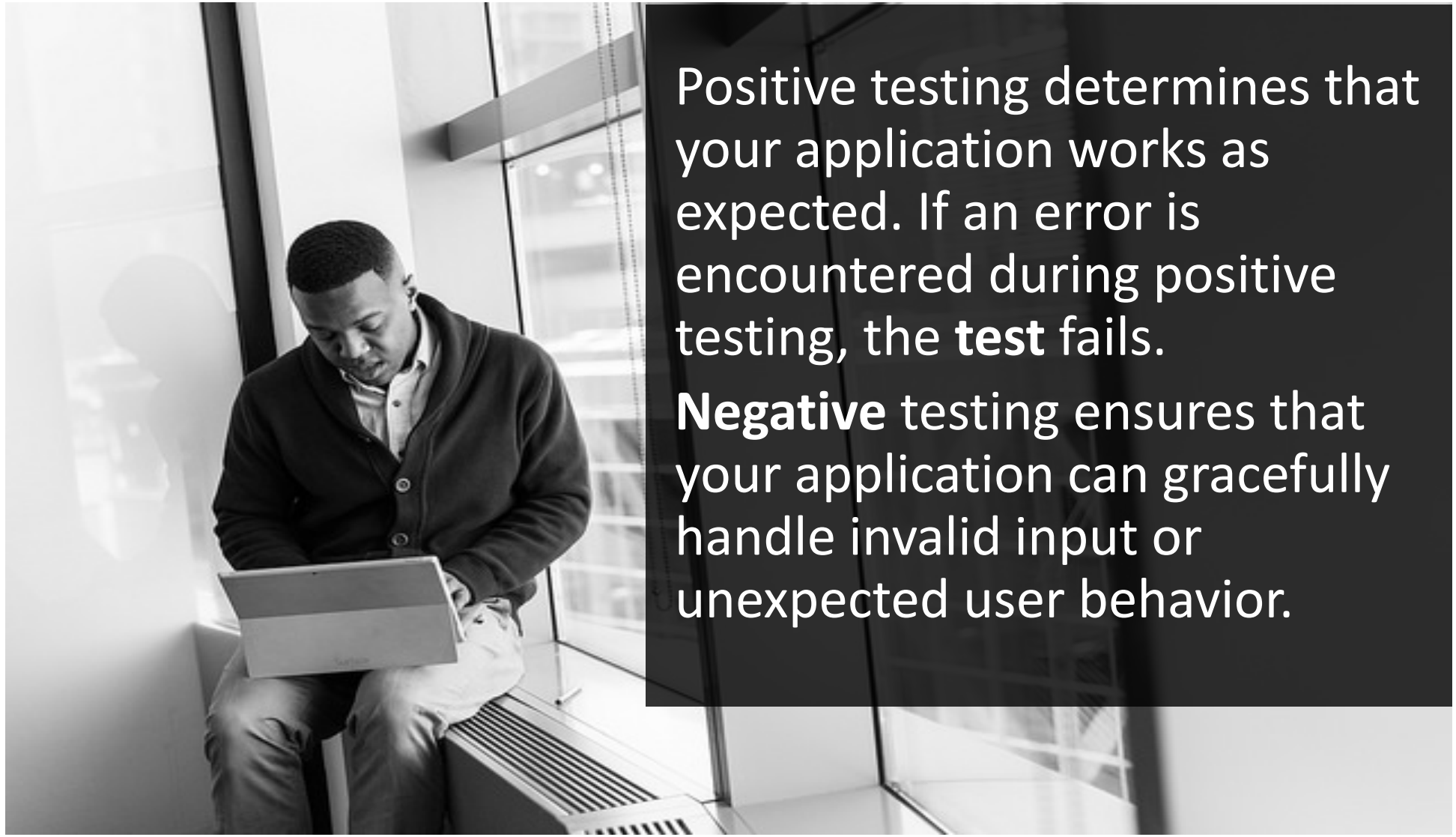
What else does this mean for Security?

What does this mean for Security?

The “Photo” Slide, #4

- Automate as much as humanly possible, then teach dev and ops to understand the results
- Tune the tools, so they don’t waste anyone’s time
- Add security into each phrase of the SDLC, including requirements and design
- Insist that the build breaks if a large security vulnerability is introduced, security is a part of quality
- Rename functions you want to phase out
- Check out Netflix’s RepoKid!

What does this mean for Security?



Positive testing determines that your application works as expected. If an error is encountered during positive testing, the **test** fails.

Negative testing ensures that your application can gracefully handle invalid input or unexpected user behavior.

What does this mean for Security?

Inviting Dev and Ops to participate in Security Activities.

Incidents

Threat Modelling

Security Sprints

Etc.

What does this mean for Security?

What does this mean for Security?

The “Photo” Slide, #5

- If a PenTest is done, check all apps for those vulns
- Use tools like OWASP DefectDojo to provide feedback on metrics and trends to Dev & Ops
- Invite Dev & Ops to participate in Security activities, for feedback and teaching
- Don’t be afraid to try new things and get creative, writing your own tools likely is to provide your best results.
- Add negative use cases as unit tests, not just positive use cases (Morgan Roman, **@Hackimedes**)

Continuous Learning

Full Circle

What does this mean for dev & ops?

What does this mean for Security?

What does this mean for Security?

What does this mean for Security?

The “Photo” Slide, #6

- Offer security training to Dev & Ops. Pay for it.
- Share information widely when you fix or find new security issues,
- Run Security Exercises or Incident Simulations
- Provide and analyze metrics from security testing, look for patterns or systemic issues
- Checkout Netflix Chaos Monkey
- Never forget that your focus is to enable Dev and Ops to get their jobs done, securely.

What does this mean for Security?

What does this mean for Security?

What does this mean for Security?

The “Photo” Slide, #7

- Share information widely when you fix something
- EVERYTHING goes into a knowledge base. **
- Ensure you perform blameless post mortems
- Talk about security incidents after they are over
- Teaching developers and ops what the output from security tools actually mean
- Create formal lessons and learning opportunities; lunch and learns, white papers, formal training, job shadowing

RSAConference2019

Security becoming *a part of* DevOps.

Culture Change!

Reinforce Culture Change

Celebrate Security Wins

Reinforce Culture Change

Work More Closely: Security + Dev + Ops

Reinforce Culture Change

No More Blaming

Reinforce Culture Change

Create Security Champions

Call To Action

Security's job is to enable Dev and Ops to do their jobs, securely.

Enabling
Teaching
Automation
Feedback

RSAConference2019

Conclusion

We got this.

What we learned today

AppSec + DevOps = DevSecOps

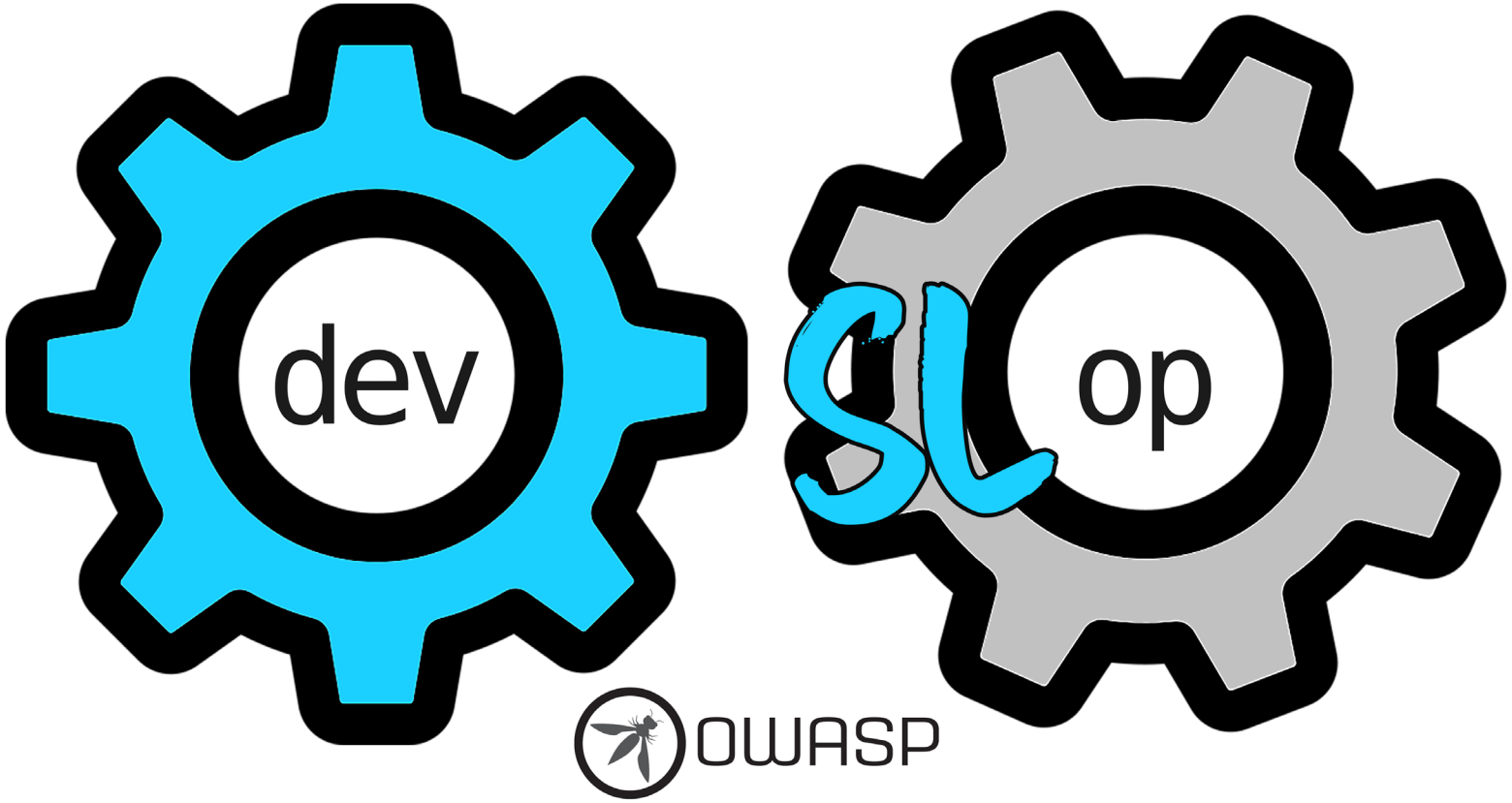
- Speeding Up Security Activities
- Faster Security Feedback
- Security Learning Opportunities

Prioritization of Security Throughout the SDLC

Apply What You Have Learned Today

- Next week you should:
  - Add security verification to CI/CD Pipelines
  - Critical security bugs break the build
- In the first three months following this presentation you should:
  - Create Negative Unit Tests from existing positive unit tests
  - Lessons on top 3 security bugs
  - High security bugs break the build
- Within six months you should:
  - Regular lessons on AppSec, including a security exercise or simulation
  - Improvements of security processes for speed and removal of obstacles
  - Creation of parallel security pipeline
  - Medium security bugs break the build

Resources: OWASP DevSlop Has Your Back!



DevSlop.co

https://www.owasp.org/index.php/OWASP_DevSlop_Project

Resources


The Microsoft
DevOps Journey
https://stories.visualstudio.com/

Resources


Links for Getting Started in Application Security
https://aka.ms/GettingStartedWithAppSec

Resources


Security is
Everybody's Job!
Learn Dev and Ops' View of
DevSecOps in the Companion Talk

RSAConference2019

Thank you

https://aka.ms/learn-to-sprint-RSA

Tanya Janca

@SheHacksPurple