DevSecOps; More Than Just Pipelines

Tanya Janca

Community and Education

@Semgrep

- She Hacks -

PURPLE

What are we going to talk about today?

The fact that DevOps is not just Pipelines

What are we going to talk about today?

DevSecOps

=

AppSec + DevOps

What are we going to talk about today?

AppSec Program Goals
that work with DevOps
OUTSIDE THE PIPELINE

About me

Tanya Janca

- Community and Education at Semgrep!
- Founder @ We Hack Purple
- AKA @SheHacksPurple
- Author: **Alice and Bob Learn Application Security**
- 25 years in tech, Sec + Dev
- Advisor: Nord VPN, Aiya Corp, Cloud Defense
- Blogger, Podcaster, Streamer, Nerd at Large

What *is* DevOps?

What is CI/CD?

Continuous Integration

Continuous Delivery

Continuous Deployment

Why CI/CD?

Trunk Based Development – Less Risk

Automation – Speed and Accuracy

Integration – Less Errors

What is Application Security?

It’s every and any thing that you do to ensure your software is secure.

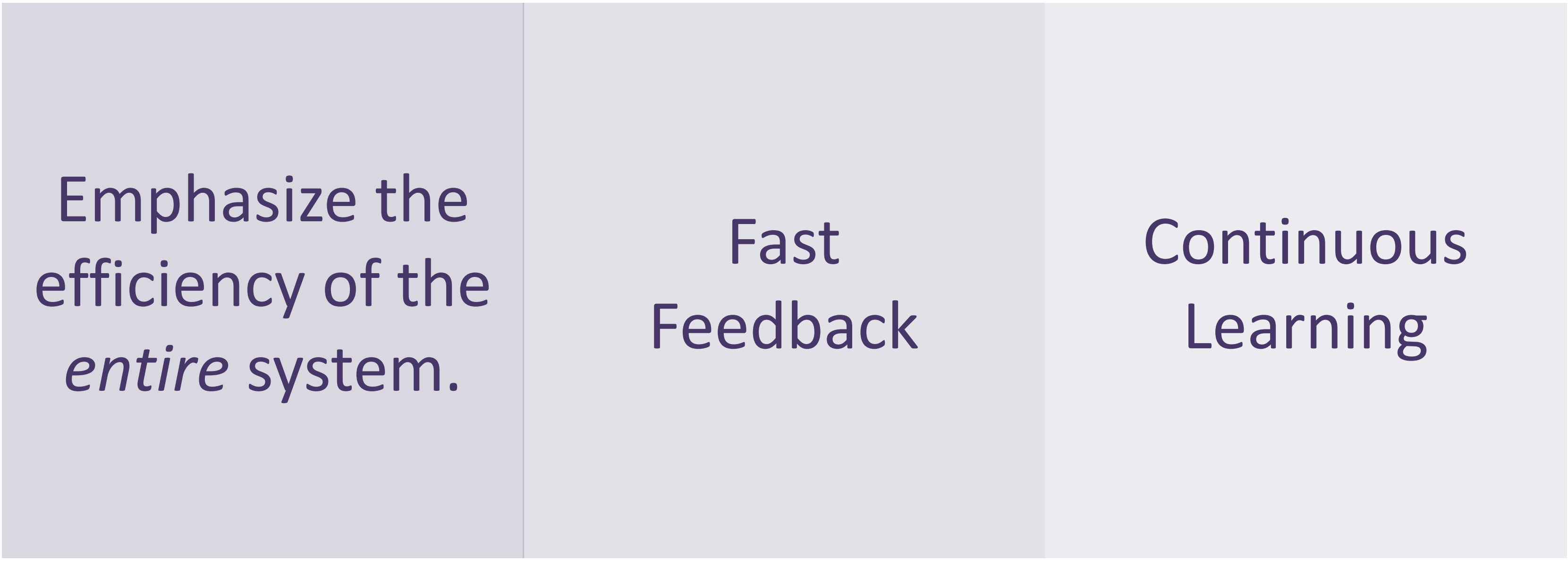
-Me

What is DevSecOps?

Application Security, adjusted for a DevOps Environment.

-Imran A. Mohammed

The Three Ways of DevOps

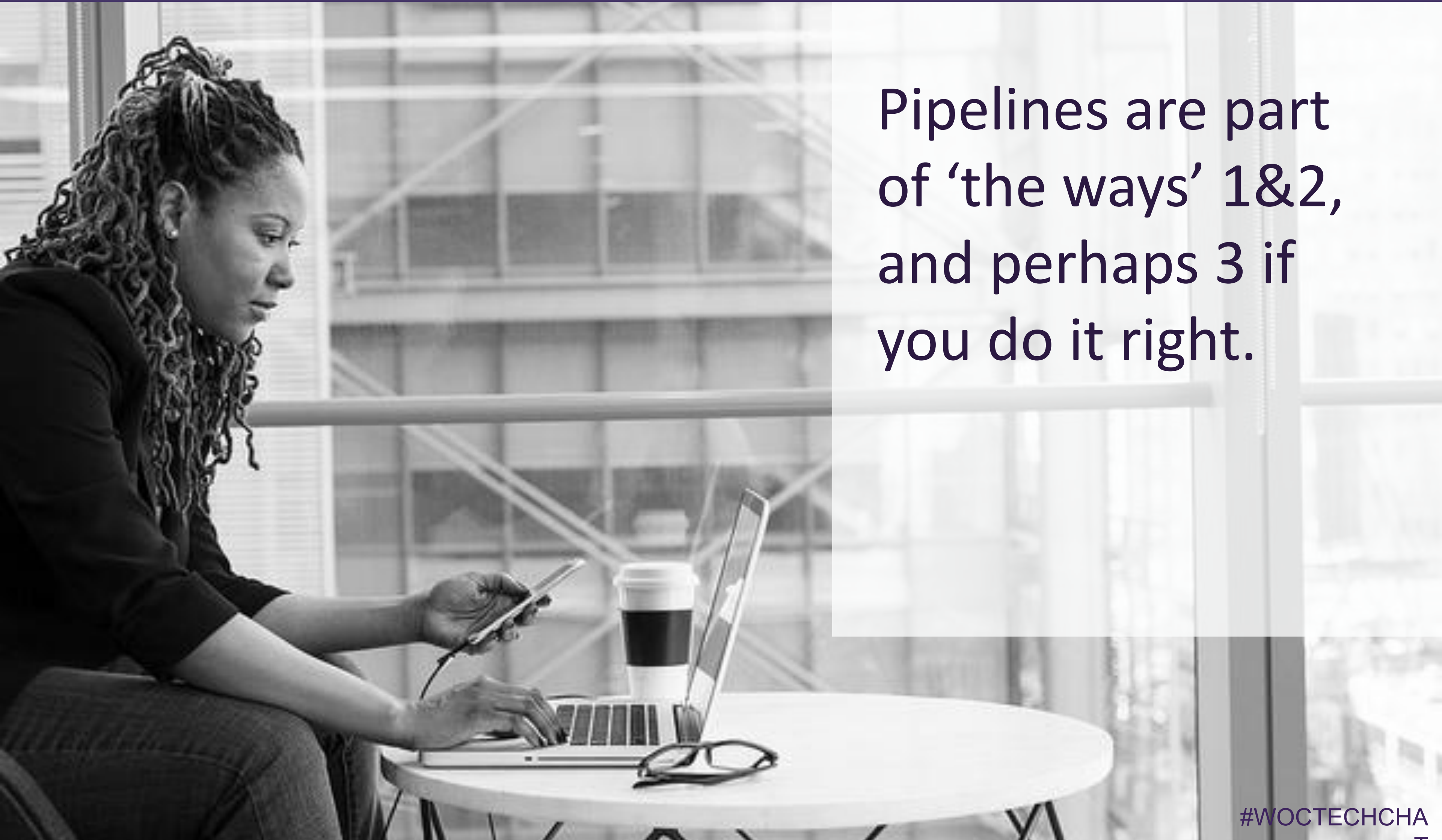


Emphasize the efficiency of the *entire* system.

Fast Feedback

Continuous Learning

But what about Pipelines?



Pipelines are part of ‘the ways’ 1&2, and perhaps 3 if you do it right.

If you put *everything* in the pipeline your devs will not want to be friends with you anymore.

And you will fail at AppSec. :-/

An Application Security Program

GOALS

@SheHacksPurpl

Inventory

You can't protect it if you don't know you have it.

Inventory

- Internet domain scraping
- Network agents on servers tracking your assets
- NMAP all the things
- Scan for open port 443 and 80
- Cloud PaaS and IaaS dashboards
- Code Repo scraping

If you don’t know about it, it’s not very likely it’s in a pipeline.

Finding Bugs

- written code
- running code
- 3rd party code

Finding Bugs – Old Guard

- manual code review
- SAST outside the pipeline
- DAST run manually
- manual review of 3rd party

Components

- PenTester at the end

Finding Bugs – New Guard

- testing in real time, as apps are used – IAST
- scanning 3rd party components in the pipeline, on check-in, *and* your rep
weekly or daily
- DAST automated scheduled scans

Knowledge

To fix the bugs you have found.

Knowledge

This is the 3rd way, through and through - Continuous learning.

Using vulnerability management tools to learn your weaknesses and address them in a more strategic/big picture way, is the essence of the third way.

Security champions program, for scaling these efforts.

No pipeline required.

Education

REPORTING SERVICES
Host Integrity Monitoring
High Performance Web Sites
Foundations of ASP.NET AJAX
The Design and Implementation of the FreeBSD

Developer Education

REPORTING SERVICES
Host Integrity Monitoring
High Performance Web Sites
Foundations of ASP.NET AJAX
The Design and Implementation of the FreeBSD

Developer Education

- Education and reference materials for developers about security.
- Advocacy program
- Security champion program
- Lunch and learns
- Time reserved for learning each week, in their calendars so they *actually do it*

Host Integrity Monitoring
High Performance Web Sites
Foundations of ASP.NET AJAX

Give Developers Security Tools

- DAST and/or SAST
- Negative Unit Tests
- Code Repo Scanning
- IDE tools and hooks
- SCA

Talk about pushing left!

Secure-SDLC

One or more security activities in every phase of the SDLC.

Secure-SDLC

- Have a set of standardized security requirements for software projects
- Have a secure coding guideline, teach them the guideline, have reference materials and code samples if possible
- Review and respect secure design

principles when in design phase(s)

- Threat modelling – design phase
- PenTest in testing phase
- The possibilities are endless!

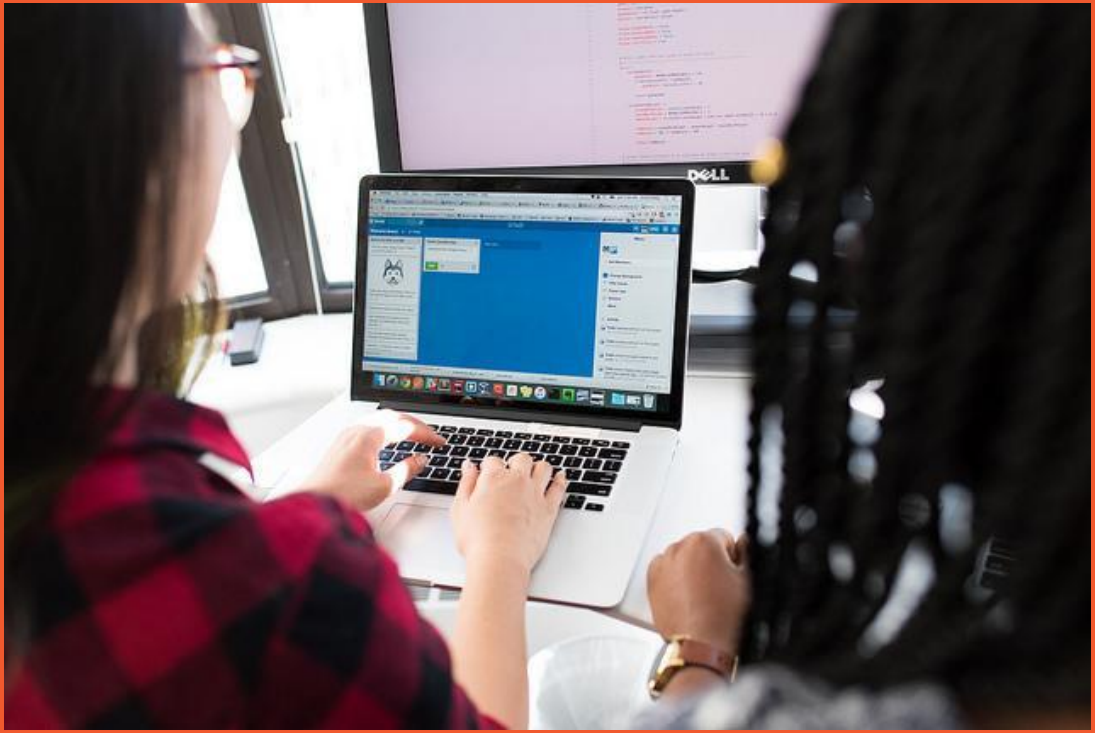
Secure-SDLC

- Assigning an AppSec resource to the project team (partnership model)
- PenTesters operate outside the pipeline
- Chaos Engineering /Red Team exercises happen outside the pipeline
- Monitoring, alerting, logging – outside pipeline
- Incident Response – no pipeline
- Security Sprints

Tools (outside the pipeline)

A big goal for AppSec programs is to implement useful and effective tooling.

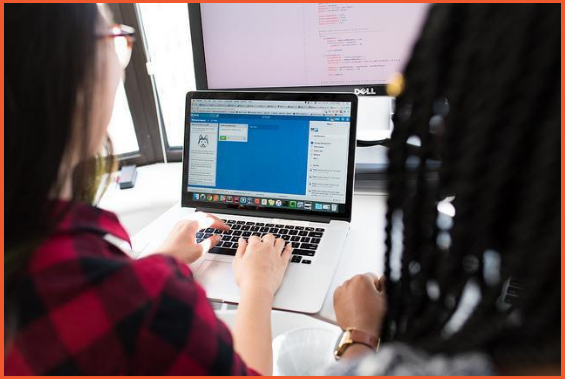
- Accurate results
- Good coverage
- Valuable feedback



Tools (outside the pipeline)

Not all tools should go in the pipeline!

- False positives (and broken builds) makes devs cranky
- Long pipeline times can result in your tool being turned off
- Continuous scanning can be more accurate
  - DNS based
  - Agent based
  - Code Repo Scans
- Asynchronous pipeline options



Incident Response

Wanted: a trained incident response team that understands AppSec.

Does Not Require a Pipeline!

Incident Response

- Create an incident response process and circulate it widely
- Give access to your inventory doc
- Access to repos
- Access to tools
- Blameless postmortems
- Training, once a year

Incident Response

Bonus: implementing tools to prevent and/or detect application security incidents (can be homemade), providing job-specific security training to all of IT.

including what to do during an incident.

Metrics

Continuously improve your program based on metrics, experimentation and feedback from any and all stakeholders.

All feedback is important.

Metrics

Every 3 months review all of your tool output, post mortem findings, information from stakeholders

Metrics

Experiment to find better ways to reach your goals.

POC new tools and approaches on just one project, instead of all

Metrics

Visit other AppSec shops to learn from them, if possible.

Follow industry leaders in this area to learn more

Attend conferences and sit in on talks,

like this one

Metrics

Form relationships with other areas of IT and the business, in efforts to work better together.

Summary

AppSec Program Goals

AppSec is not one tool or tactic

DevOps is not just pipelines

Resources

Awesome Books

- The DevOps Handbook
- The Phoenix Project
- Accelerate
- The Unicorn Project
- Alice and Bob Learn Application Security

Semgrep Newsletter!

Wicked Content, Fun Events!

https://bit.ly/semgrepnewsletter

Join the community!!!!!

Join the We Hack Purple Community for FREE

Community.WeHackPurple.com

Meet like-minded people and nerd out!

#CyberMentoringMonday

Every Monday!

Resources: ME!

@SheHacksPurple - everywhere

https://SheHacksPurple.ca

YouTube.com/SheHacksPurple

https://Newsletter.SheHacksPurple.ca

Thank You!

- She Hacks -

PURPLE

Tanya Janca

SheHacksPurple.ca