#DEVOPSEC - KILLING THE BUZZ?

HELLO!

i'm a security consultant at NCC Group.

you can find me:

- on twitter as @rossja
- pretty much everywhere else as algorythm

A SPECIAL NOTE ABOUT THIS PRESENTATION!

anytime i include a "buzzword" in a slide...

i will also include this:

AGENDA

setting the stage

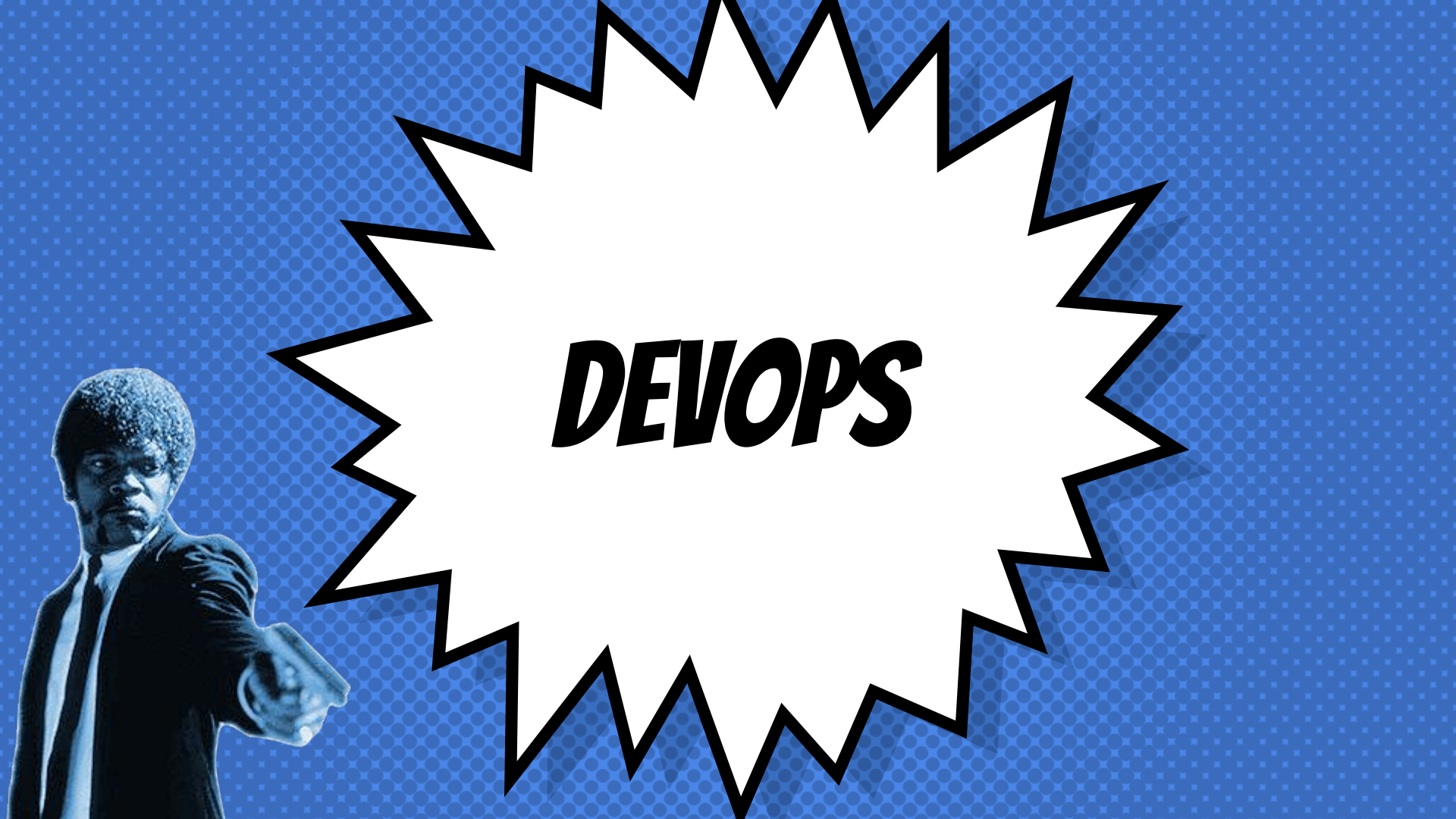
- blue team
- red team
- fight!

tricks are for script kiddies

- techniques
- tools

wrapup


BLUE
TEAM


DEVOPS

STRESSES COMMUNICATIONS, COLLABORATION, INTEGRATION, AUTOMATION AND MEASUREMENT OF COOPERATION BETWEEN SOFTWARE DEVELOPERS AND OTHER IT PROFESSIONALS

DEVOPS GOALS?

1. rapid development
2. continuous deployment
3. quick scaling
4. instant rollback

DEVOPS METHODS?

continuous (delivery | deployment | measurement)

- orchestration & automation
- infrastructure as code
- feedback loops from users/production

virtualization

- cloud
- containers

revision control

- git (is anyone using anything else at this point?)

SO BASICALLY...
DEVOPS WANTS TO SET YOU FREE!


RED
TEAM


SECURITY

THE PROCESSES AND METHODOLOGIES INVOLVED WITH KEEPING INFORMATION CONFIDENTIAL, AVAILABLE, AND ASSURING ITS INTEGRITY.

SECURITY GOALS?

to “serve and protect”

- hosts & data
- the business
- end-users

"CONTINUOUS ANNOYMENT"?

policy

- creation
- enforcement

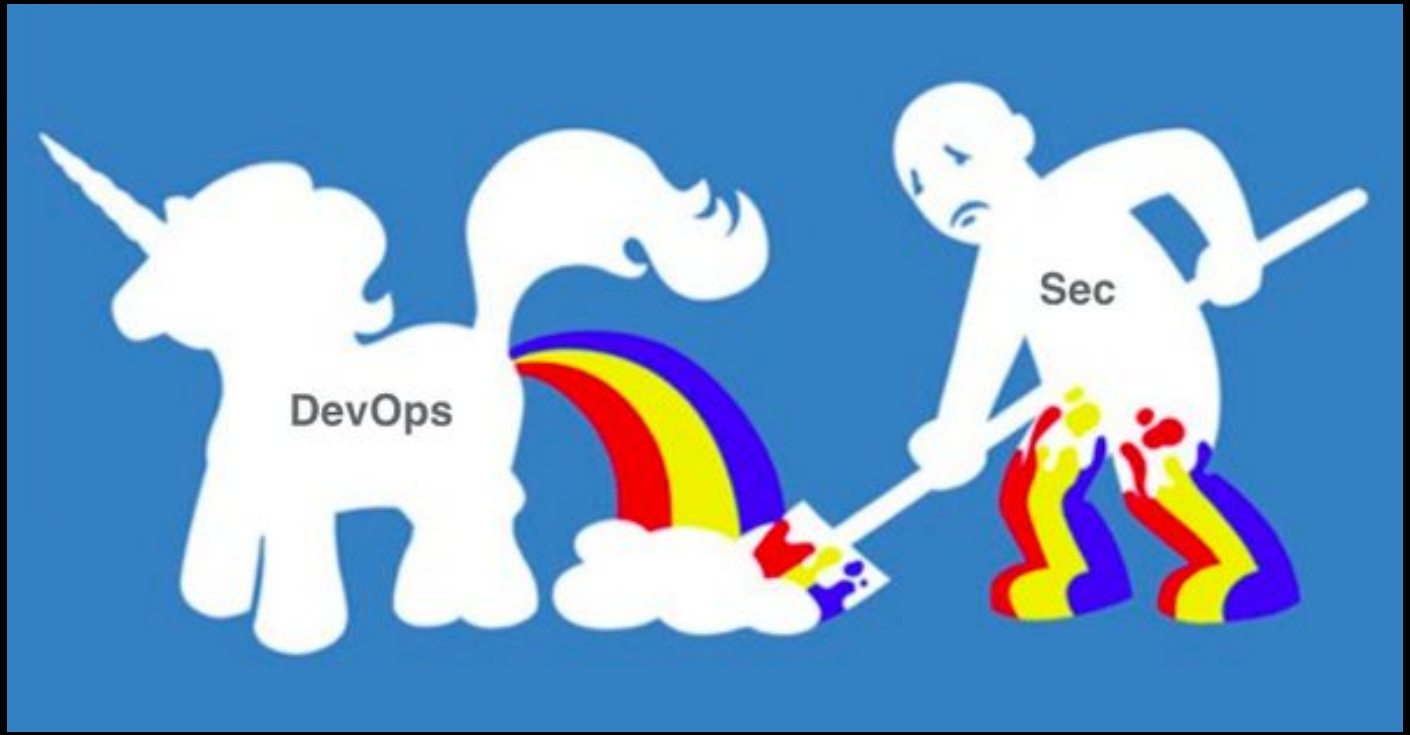
audit

- compliance testing
- log management & review

simulation

- penetration test
- phishing | social engineering

SO BASICALLY...
SECURITY WANTS TO BUST YOUR KNEECAPS!



THUS WE GET THIS.

DEVOPS SECURITY

can we even?


NO
AT

COMMON CONFLICTS

access control

devops:

- everyone can access everything so things get done

infosec:

- least-privilege, separation of duties

process flow

devops:

- rapid, constant update – often in prod

infosec:

- strict review, isolated env

culture / mindset

devops:

- we need to be able to do whatever we want...

infosec:

you can only do what we let you...

ULTIMATELY DIFFERENT GOALS?

dev – build cool things

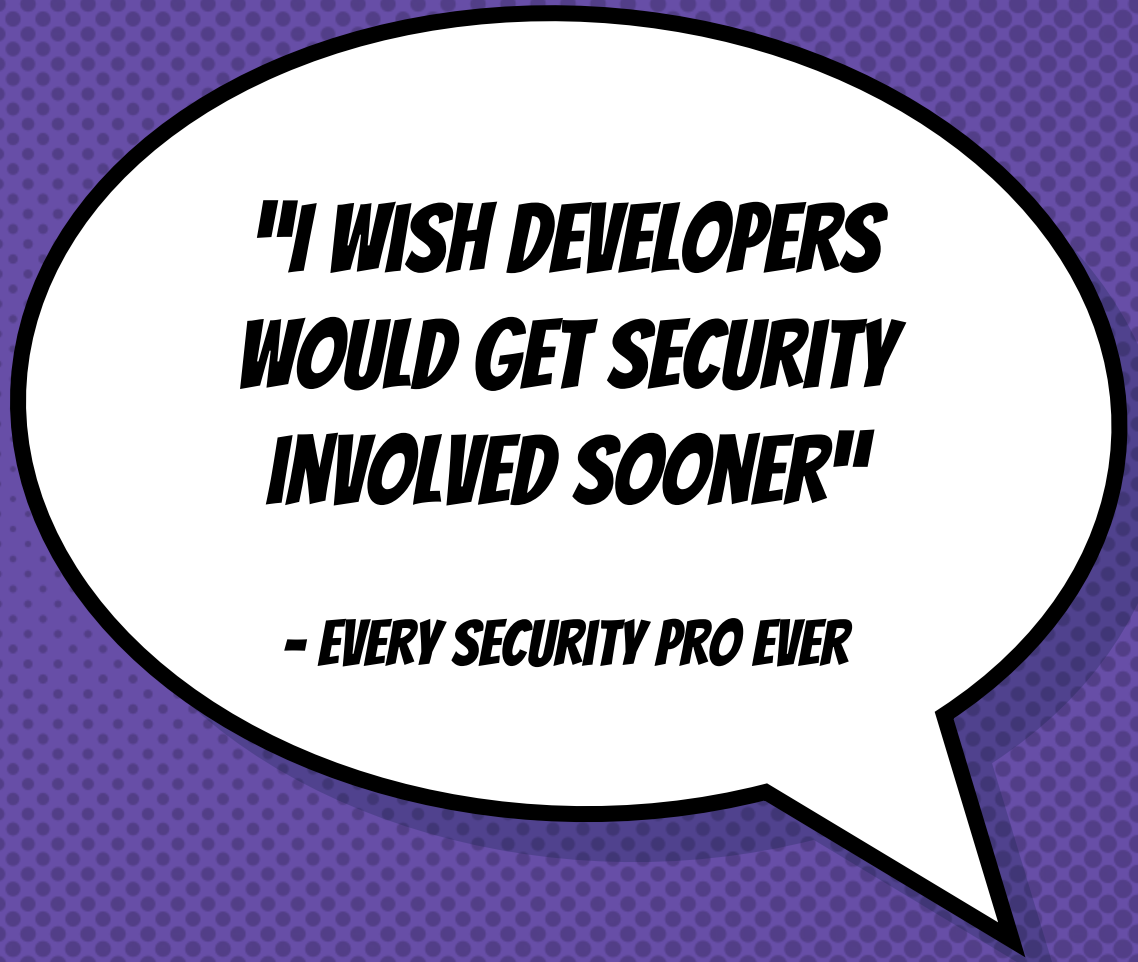
ops – run cool things

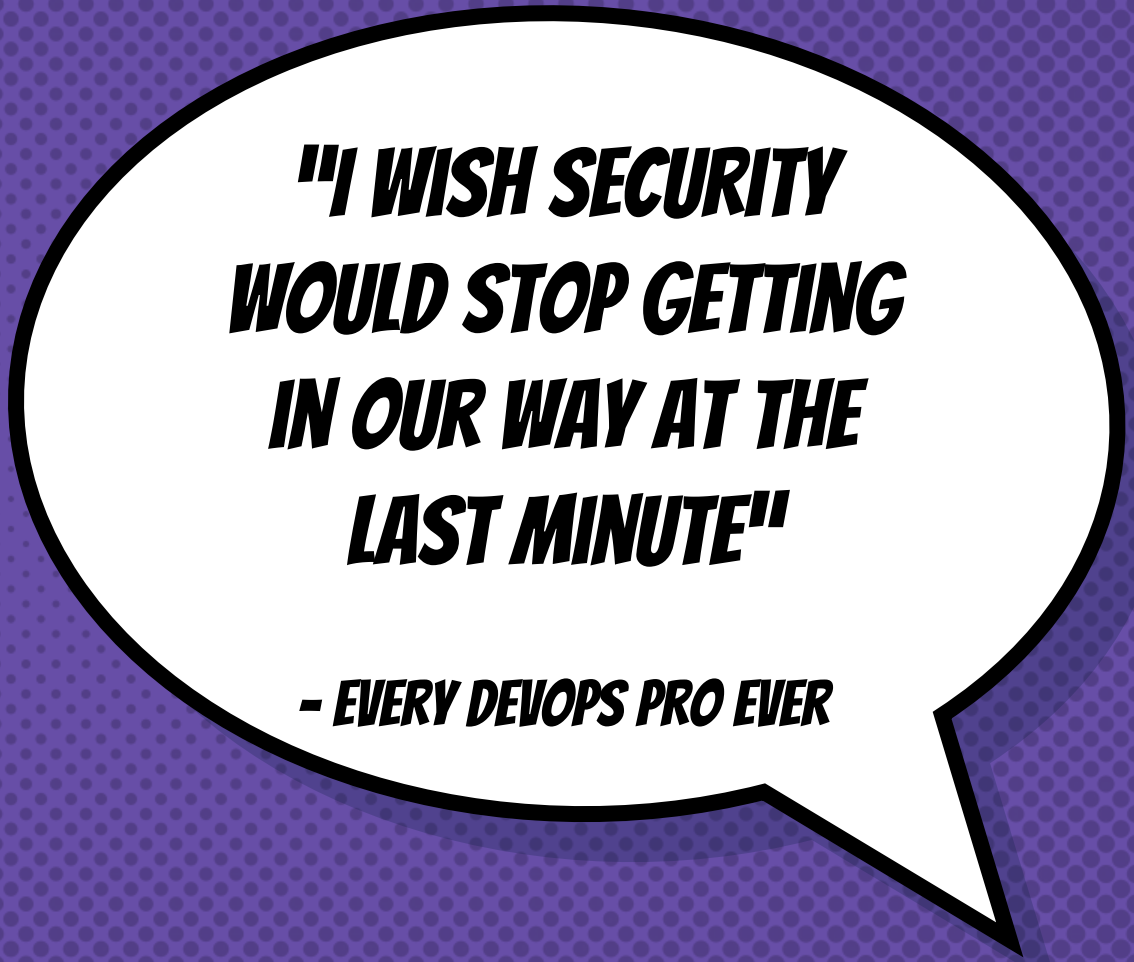
sec – break all the things

nod to @codesoda


HUMAN SACRIFICE, DOGS AND CATS LIVING TOGETHER...
MASS HYSTERIA!


GET OVER
IT & MOVE
ON


"I WISH DEVELOPERS WOULD GET SECURITY INVOLVED SOONER"
- EVERY SECURITY PRO EVER


"I WISH SECURITY WOULD STOP GETTING IN OUR WAY AT THE LAST MINUTE"
- EVERY DEVOPS PRO EVER


GOOD NEWS
EVERYONE!!!


DEVOPSEC
IS A
THING!

ALSO KNOWN AS...

(look how friendly it is!) ---->>

DEV & OPS & SEC WORK TOGETHER IN ALL PHASES

- design
- development
- deployment
- maintenance

image taken shamelessly from
https://newrelic.com/devops/lifecycle

How does this help security?

continuous security delivery

- use the pipeline to meet compliance & audit objectives
- CD/CI lends itself well to rapid patching

continuous monitoring

- use feedback loops from prod to feed 'attack-driven defense'

improves security awareness

- everyone is involved

SOME SUGGESTIONS:

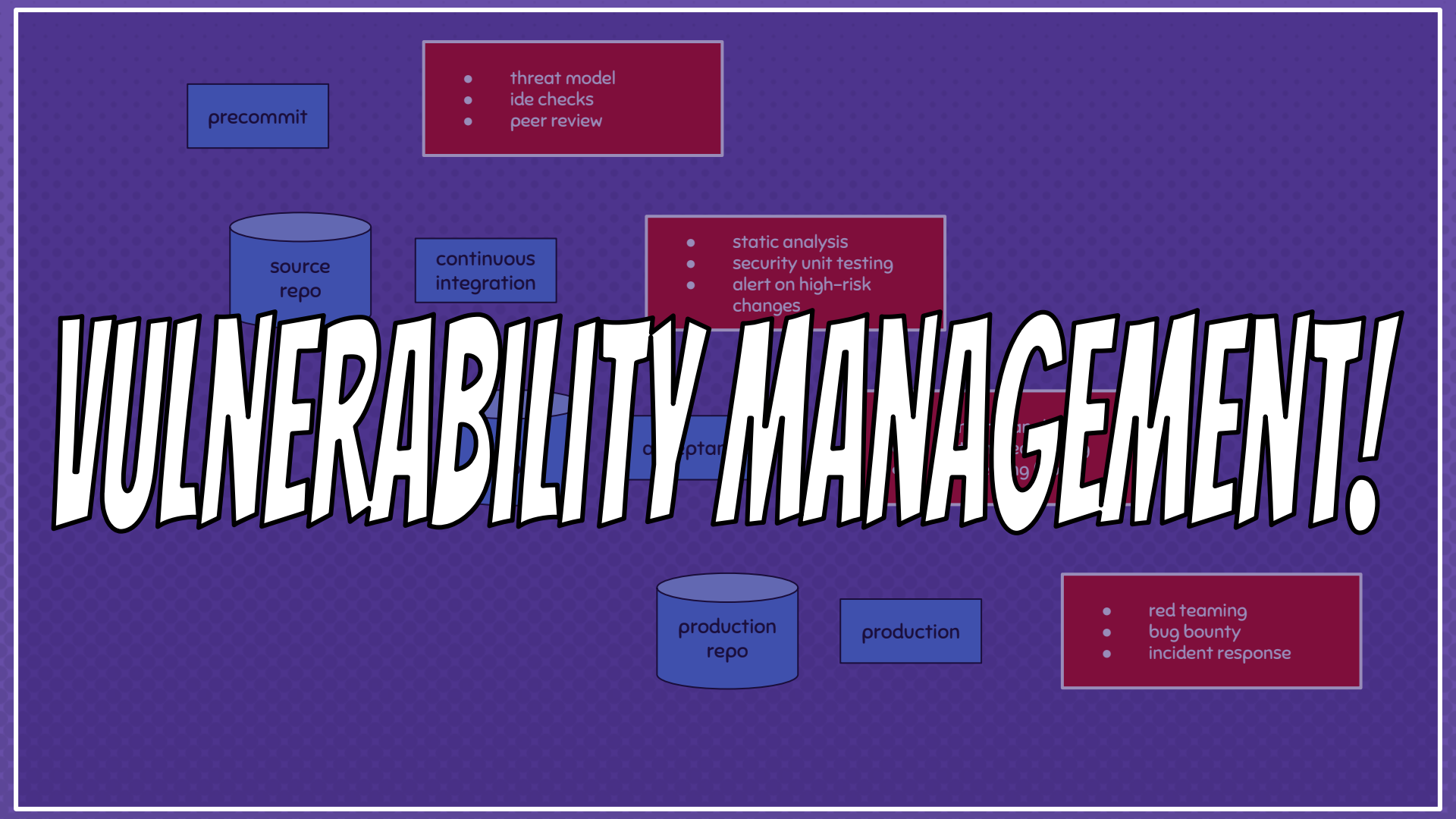
- inject code analysis tools into the dev process
  - enforce fixes prior to deployment
- automate attacks against pre-prod code
  - prevent vulnerable code from reaching prod
- implement “compliance as code” strategies

COMPLIANCE AS CODE?

make security part of the pipeline

- × setup requires time and effort
- × may involve learning new ways of working
- × it is worth it (really...)

THE DEVOPSEC CYCLE


precommit
threat model
ide checks
peer review
source repo
continuous integration
static analysis
security unit testing
alert on high-risk changes
VULNERABILITY MANAGEMENT!
production repo
production
red teaming
bug bounty
incident response


PRECOMMIT

PRECOMMIT TOOLS

- OWASP Proactive Controls (shift security left!)

code peer review tools:

- Gerrit
- Phabricator
- Atlassian Crucible


COMMIT

COMMIT TOOLS

chef vault

keywhiz

lib/deps checkers:

- OWASP Dependency Check
- Retire.js
- Bundler Audit
- SourceClear (commercial)

ACCEPTANCE

Acceptance Tools

- hardening.io
- dynamic scanning tools (nessus, etc.)
- OWASP ZAP
- Jenkins ZAP plugin
- Mittn
- Gauntlt
- BDD-Security


PRODUCTION

PRODUCTION TOOLS

ansible | chef | puppet | salt | docker

dynamic scanning tools (nessus, etc.)

bugcrowd

simian army

aws inspector

scout2 (NCC Group tool)

NEXT-GEN WAF

Some interesting new devopsec tech is coming out in the WAF market
(like SignalSciences)

Chaim will be talking more about WAF stuff in his talk, up next.


WRAPUP

DEVOPS + SECURITY IS COOL

integrating the two requires culture shift
there will be lots to work out
it can be awesome when it's done right
look to industry leaders like AWS/Netflix

SAY DEVOPSEC ONE MORE TIME...