Make Security Sprint Along

DevSecOps Is a Thing

~# whoami

↳ Current
  ↳ Penetration Tester
  ↳ Team Leader
↳ Experience
  ↳ 2 years Software Developer
  ↳ >8 years Linux System Engineer
  ↳ 1½ years Information Security Management

```
~# more goals.txt

Integrate security into DevOps workflow

Bring security team up to speed with DevOps

Security + DevOps = <3
```
goals.txt {END}
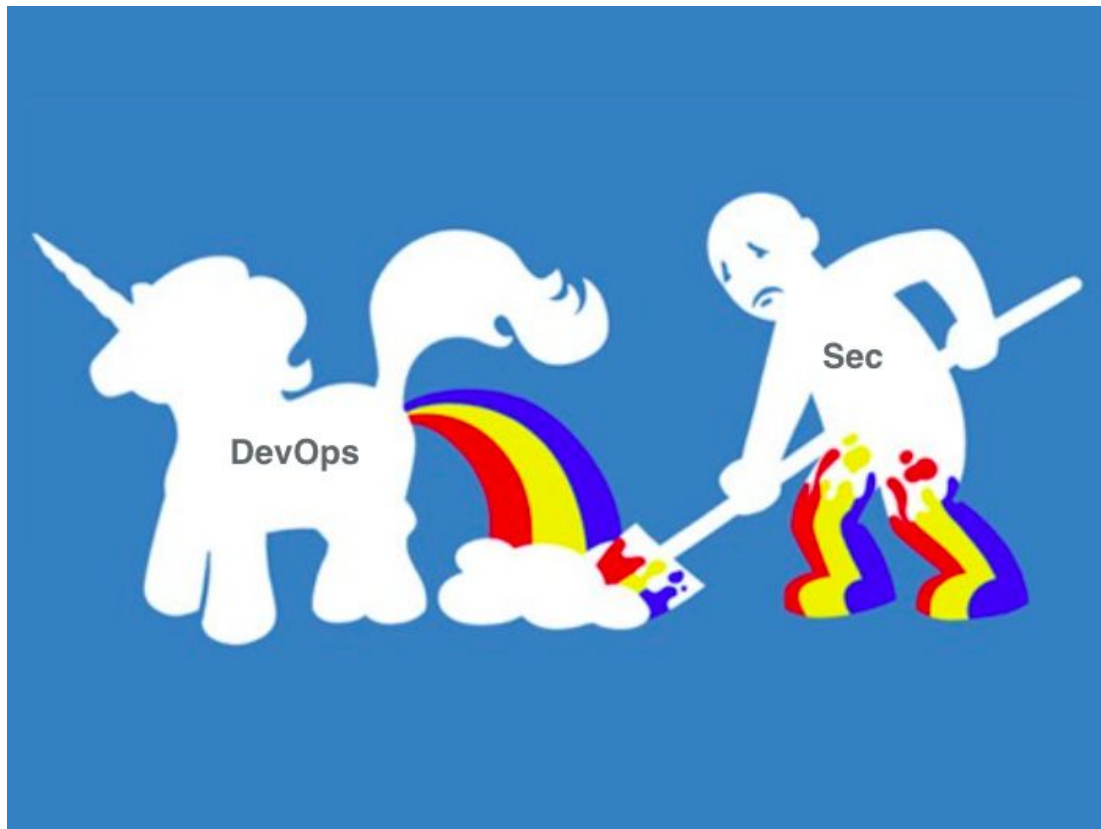
```
~# more agenda.txt

⟹ State of the Teams

    ⟹ AppSec

        ⟹ DevOps

            ⟹ Integrating Security

                ⟹ Wrap Up

agenda.txt {END}
```

How Security sees DevOps[1]

[1]https://twitter.com/petecheslock/status/595617204273618944

How Security sees DevOps[2]
[2] Also some twitter.

How DevOps see Security[3]

[3]https://www.flickr.com/photos/philwolff/3788258352

Enterprise DevOps[4]

[4]https://twitter.com/pczarkowski/status/1006208448101535745?s=19
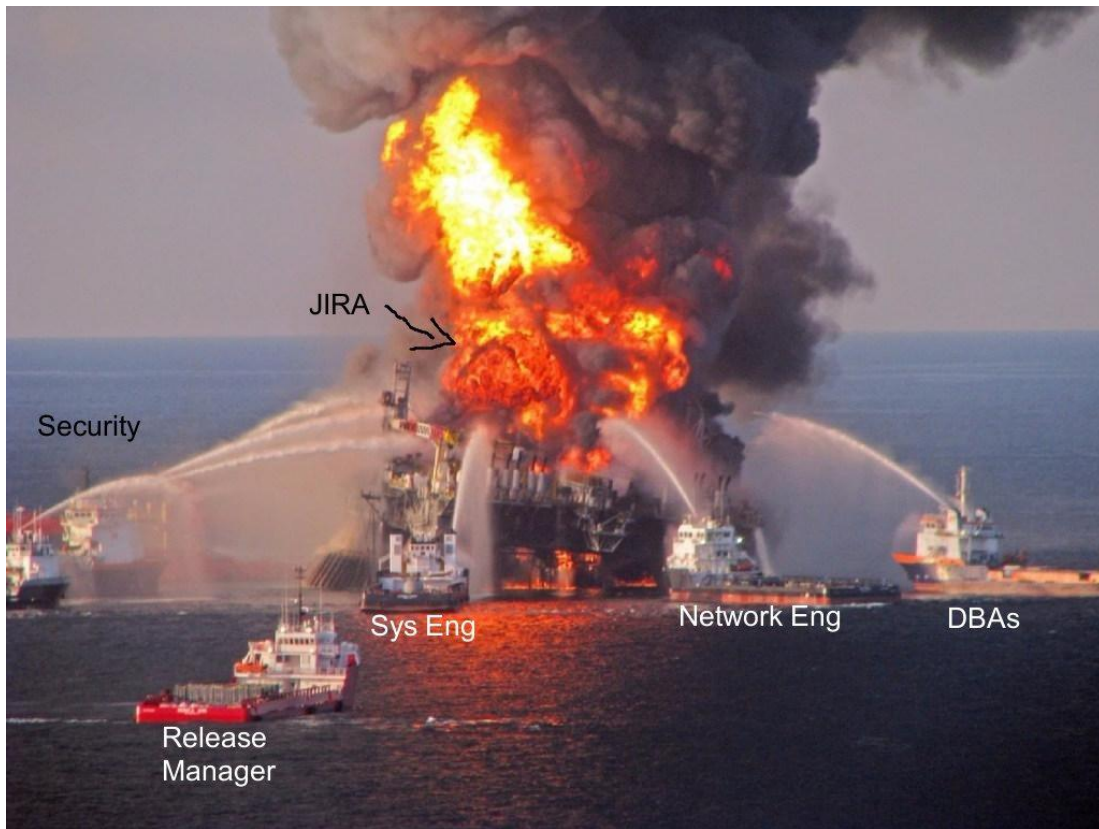
This is how it should be![5]

[5]me

AppSec

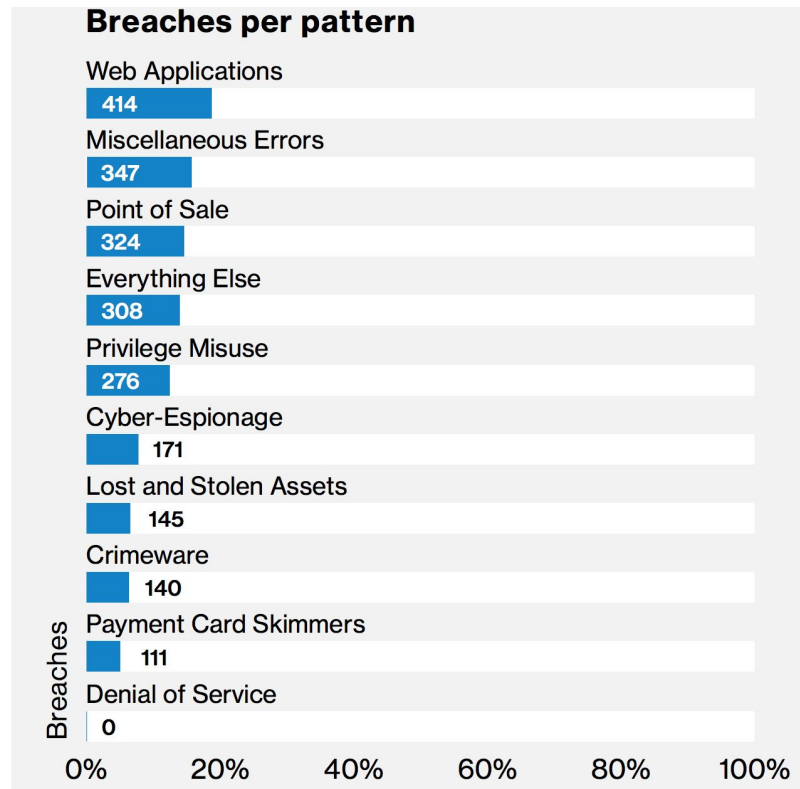"Application Security is the art (or is that battle?) of making an application secure"

– Tanya Jance
  Senior Cloud Developer Advocate

~# cat AppSec.txt | column

↳ WebApplications account for ~18% (n=2,216) of breaches in 2018[6]
↳ 23.244 WebApplications compromised as a mean to attack something else[6]

[6]https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

Breaches per pattern

| Pattern	Breaches
Web Applications	414
Miscellaneous Errors	347
Point of Sale	324
Everything Else	308
Privilege Misuse	276
Cyber-Espionage	171
Lost and Stolen Assets	145
Crimeware	140
Payment Card Skimmers	111
Denial of Service	0

~# display education.png

Very little to no AppSec courses i[n]
higher education.

Biggest techn. uni in AT:

- ↳ 2 courses
- ↳ ~25% AppSec each
- ↳ 1.5/180 ECTS
- ↳ if elected

DevOps
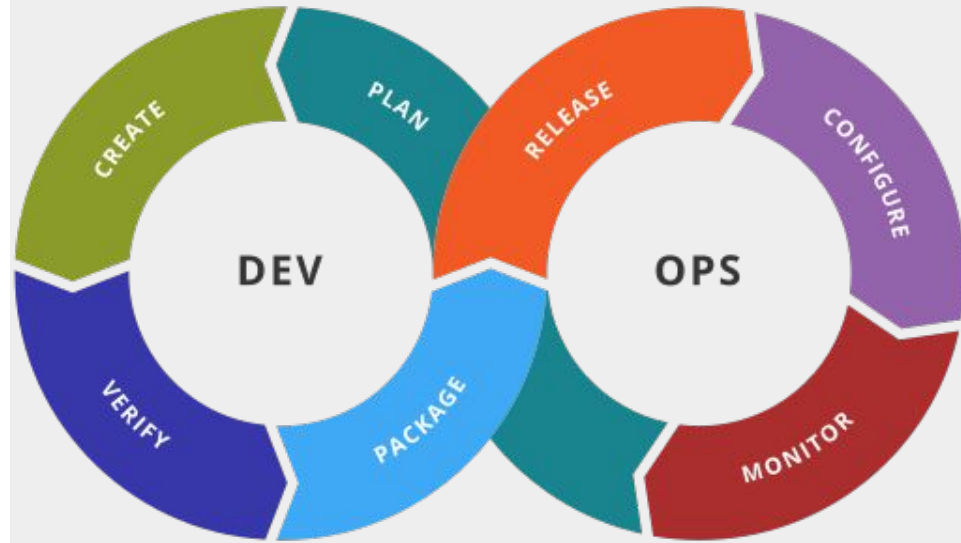
~# cat speed.txt | column

Decrease time from implementation
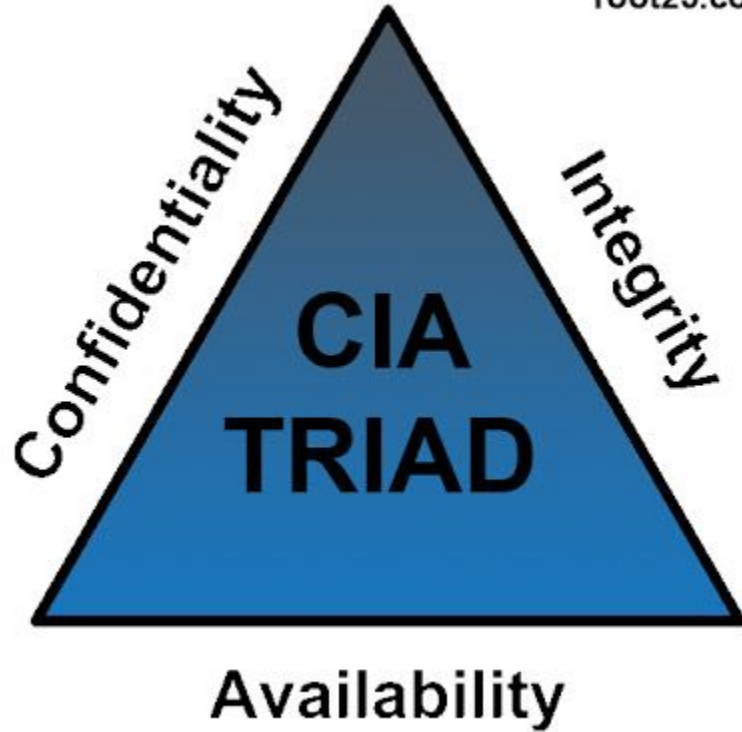to deployment.

Security fixes can be fixed NOW.

```
~# cat reliability.txt | column
```

Low Failure Rates   Security win: Availability

~# display cia.png

```
~# cat market.txt | column
```

Nobody wins, if we don't ship

Security can't win, if we do not ship.

Integrating Security

How to integrate security into your development life cycle

Θ

I assume this is the number of dedicated FTE security people in your company

`~# display code.png`

Static and Dynamic Analyzers
for Security Testing

```
~# more sast.txt

    Scale well
↳ Often integrate into IDE

sast.txt {END}
```

~# more sast_tools.txt

↳ Highly Platform dependent!
↳ Cross Platform
    ↳ SonarQube
↳ Java
    ↳ FindSecBugs
    ↳ FindBugs
↳ Ruby
    ↳ Brakeman
↳ Python
    ↳ Bandit

`sast_tools.txt {END}`

~# more sast_selection.txt

↳ Must support your programming language
↳ Types of vulnerabilities detected? (OWASP Top 10; more?)
↳ Does it understand the Libraries you use?
↳ Require fully buildable set of source?
↳ Run against binaries or source?
↳ Can it be run continuously?
↳ License costs…

`sast_selection.txt {END}`

```
~# more dast.txt
```

↳ Scan for vulnerabilities like
    ↳ Cross-Site Scripting
    ↳ SQL Injection
    ↳ Command Injection
    ↳ ....
↳ Mostly Web Applications

`dast.txt {END}`

```
~# more dast_tools.txt
```

↳ Nikto
↳ OWASP ZAP
↳ Burp Suite
↳ ...

dast_tools.txt {END}
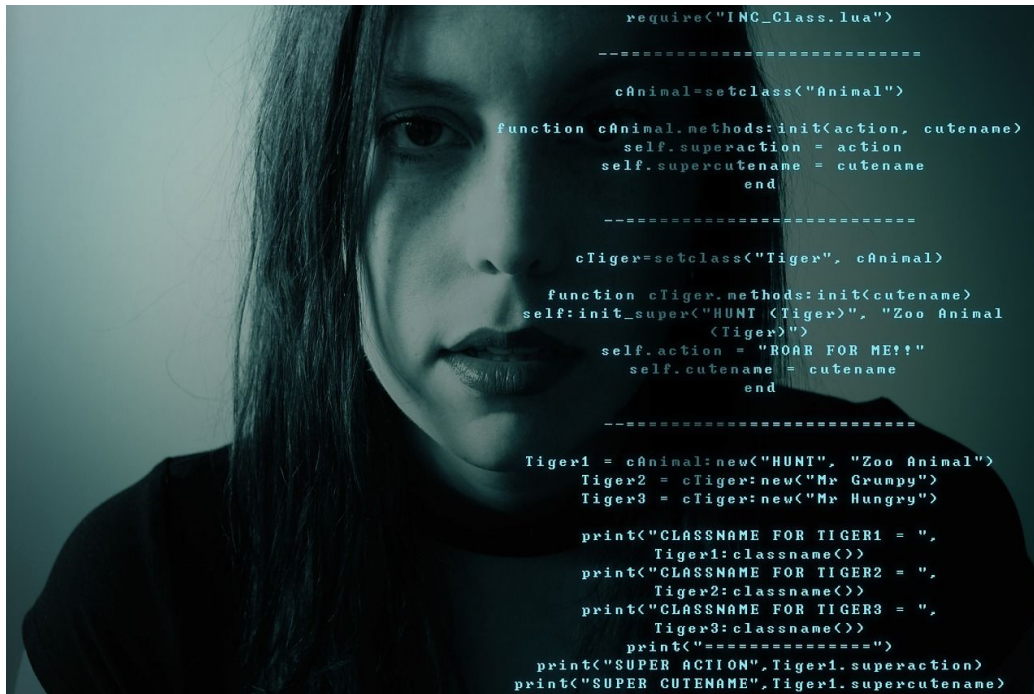
```
~# display approved.png
```

Use only up-to-date and approved images

~# display unit_tests.png

Make negative unit-tests

~# display ci.png

Severe security bugs break the build

Security

Fit activities in a sprint

~# display dependency_mgmt.png

↳ Retire.js
↳ Snyk.io
↳ OWASP dependency check
↳ ...

```
~# more vuln_mgmt.txt
```

↳ Start managing early
↳ Easier to convince management

For example: DefectDojo

`vuln_mgmt.txt {END}`

```
~# more security_builtin.txt
```

↳ Logging of security events
↳ Monitoring of said events
↳ Make APIs for security mechanisms
↳ Collect metrics

`security_builtin.txt {END}`
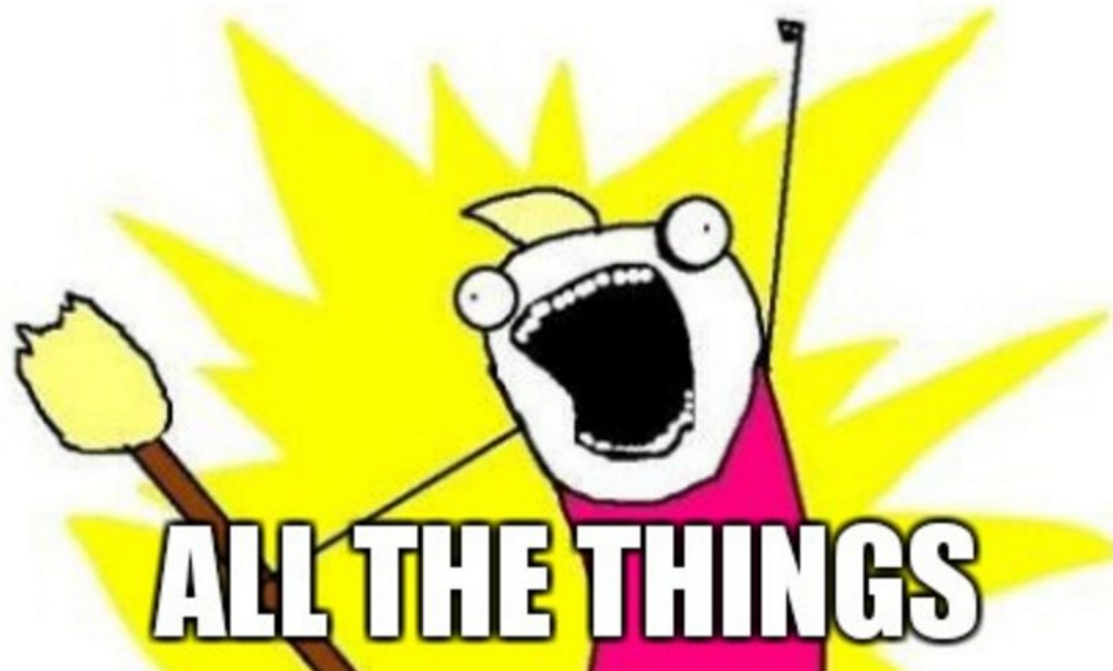
Wrap up

Last key messages.

Me, Ex-Ops Guy

~# more wrap_up.txt

↳ No "throwing over the wall"
　　↳ Neither to security
　　↳ nor from
↳ There is no perfect time
↳ Start now
↳ Demand training
　　↳ You got reports rights?

`wrap_up.txt {END}`

```
~# sleep 2; clear; display last_pic.png
```

AUTOMATE ALL THE THINGS

```
~# more last_slide.txt
```

Thank you for your attention!

Questions?

```
last_slide.txt {END}
```