

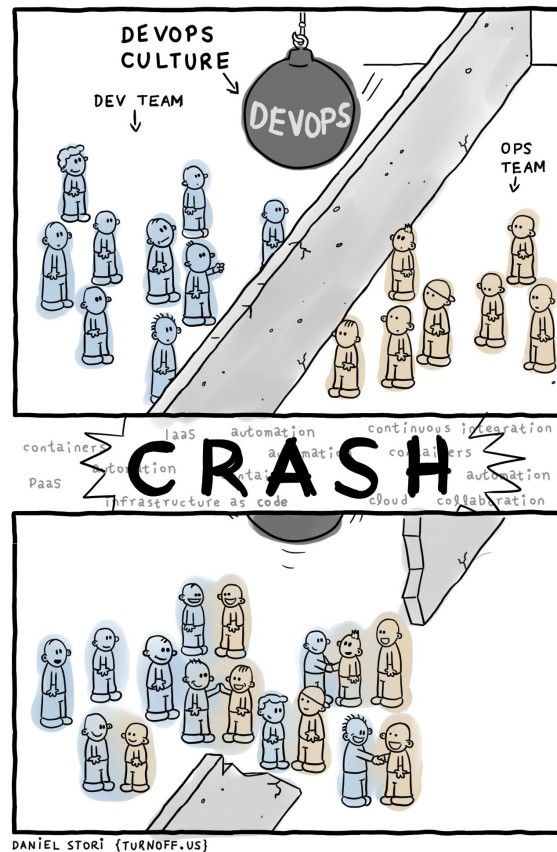
DevOps = Velocity + Security

DevOps er samansafn af menningu,
ferlum, og tólum,
með markmiðið að koma út
breytingum hratt, en á öruggan máta

Menning

Menning er einn mikilvægasti hluti DevOps

- Ábyrgð dreifist á fleiri
 - Allir sem eru að vinna með kerfið bera ábyrgð á árangri þess
- Breytt samskipti
 - Opnari samtöl og meiri samvinna milli teyma
 - Þegar allir eru ábyrgir fyrir sama markmiði, þá er meira traust



Ferlar

- Kóði skilar sér hratt í production umhverfi
 - Helst samdægurs
- Auðvelt og fljótlegt að bakka með kóða, þegar þess þarf
- Stillingar eru notaðar til að rúlla hlutum út og til baka
- “ClickOps” lágmarkað, allt skilgreint í kóða

```
if (  
    Math.random() < conf.useNewStuffFrac  
) {  
    // new stuff  
} else {  
    // old stuff  
}
```

Alls ekki tæmandi listi!

“Hvernig get ég hjálpað til við að koma hlutum út hraðar”

Þegar hlutir fara úrskeiðis

Menning kemur skýrast fram undir þrýstingi

Mikilvægt að halda ámælislausar samræður um af hverju hlutir fóru úrskeiðis

Oftast fór fleiri en eitt atriði úrskeiðis

Action Items mikilvæg

Five Whys

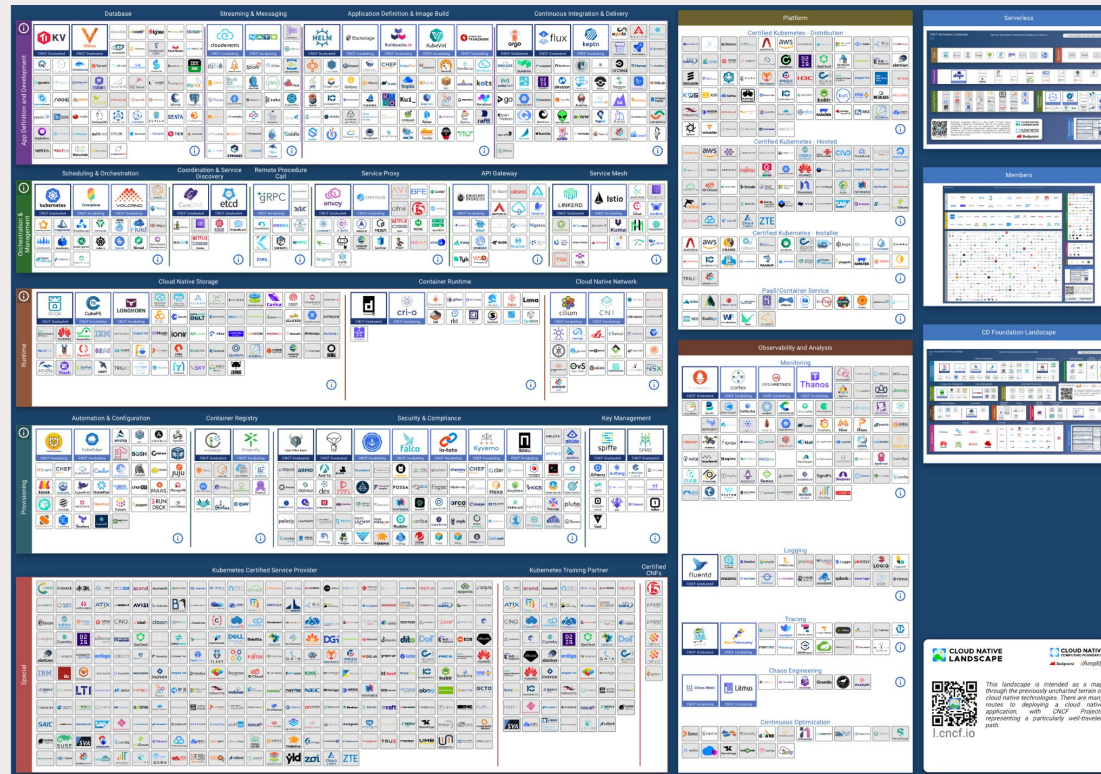
Why did it take so long to fix?

- It took a long time to find the root cause of the problem
- Why?
- People were unfamiliar with the system
 - **AI: Improve documentation around the system**

Why didn't it alert sooner?

- The error rate was under the monitor thresholds for very long
 - Why?
 - It paged regularly in the past where it was just noise
 - **AI: Make the monitor composite and tune thresholds**
 - Why did we change the monitor instead of fixing the problem?
 - ...

...



Tól



Tól



Tól



Of mörg tól



DevOps “Tool Sprawl”

Mikilvægt að halda hlutum nokkurn veginn eins

Skilgreina góð mynstur, og fara eftir þeim

Hafa einhverja skilgreiningu á

“svona lítur kerfi út hjá okkur”



Velocity = Security

Velocity = Security



DevOps = Security

Öryggi, Stöðugleiki, Hraði,
Þróun, <allt annað>

Menningarlegt öryggi

Öryggi kerfisins á ábyrgð allra

Hluti af þróunarferlinu frá upphafi

Forðast ásakanir – engum að kenna

- Opnar á betri samskipti um öryggi

Öryggisteymi ættu að vinna í að gera öryggisteymi óþarft

- Efla spennu fyrir öryggi
- Dreifa þekkingu



CommitStrip.com

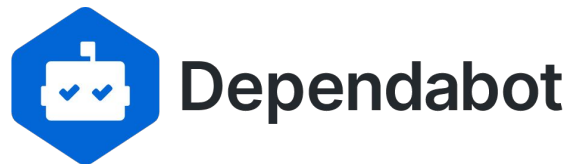
Öryggi sem hluti af CI

Eitthvað af hlutum öryggis má sjálfvirknivæða

Hægt að nota tól til að benda á mögulega öryggisgalla

- Tólin benda á staði þar sem code reviewer þarf að fara vel yfir!

Linting, Static Code Analysis, Dependency analysis



Öryggi sem hluti af mynstrum

Skýrt hvernig er best að gera hluti á öruggan hátt,
“secure by default”

- Auðveldasta leiðin ætti alltaf að vera örugg
- Á að vera augljóst þegar hlutir gætu verið óöryggir

Mynstur eru “secure by default”

- Enginn “default” aðgangur, kerfi verða að skilgreina þann aðgang sem þau þurfa
- Netöryggi byggt inn

```
const data = "blabla"

UNSAFE_directlyQueryDatabase(
  `SELECT * FROM data WHERE name LIKE "${data}%"`
)
```

laC = Öryggi



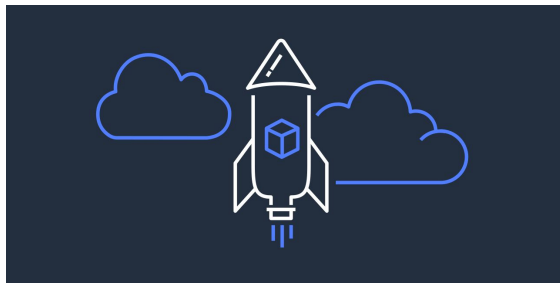
Auðvelt að endurskoða kerfi sem eru skilgreind í kóða

Manneskjur þurfa takmarkaðan/engan aðgang til að geta breytt kerfum, breytingar gerast sjálfkrafa

Kubernetes öryggi

Taka allt sem er óþarft úr image-inu

- [distroless](#)



kubearmor



cilium

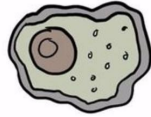


clair

[NSA/CISA Kubernetes Hardening Guide](#)

EVOLUTION of OPERATIONS

OPS



- PRIMORDIAL, PROTOZOIC
- BORN IN THE SWAMPS OF PERL
- OPERATES IN A SINGLE-CELL SILO
- SURPRISINGLY RESILIENT

DEVOPS



- A CROSS-FUNCTIONAL MARVEL
- VASTLY INCREASED AGILITY
- SECRETLY JUST A BUNCH OF SINGLE CELLS THAT HAVE LEARNED NOT TO KILL EACH OTHER

DEVSECOPS



- MORE ADVANCED, MORE PARANOID
- SECURITY IS AUTOMATED RIGHT INTO ITS DNA
- KNOWS THAT SHARED RESPONSIBILITY IS THE ONLY ESCAPE FROM FOSSILIZATION

DEVSECMLOPS



- WHAT EVEN IS THIS?
- IS IT A FISH WITH FEET?
- WE SHOULD PROBABLY LEAVE IT ALONE FOR A FEW MILLION YEARS AND SEE WHAT HAPPENS

TRICERATOPS



- DOES NOT CARE ABOUT YOUR ORG STRUCTURE
- VULNERABLE ONLY TO DIRECT METEOR STRIKES
- WHAT WERE WE TALKING ABOUT, AGAIN?

@acloudguru



Takk

