TOWARDS

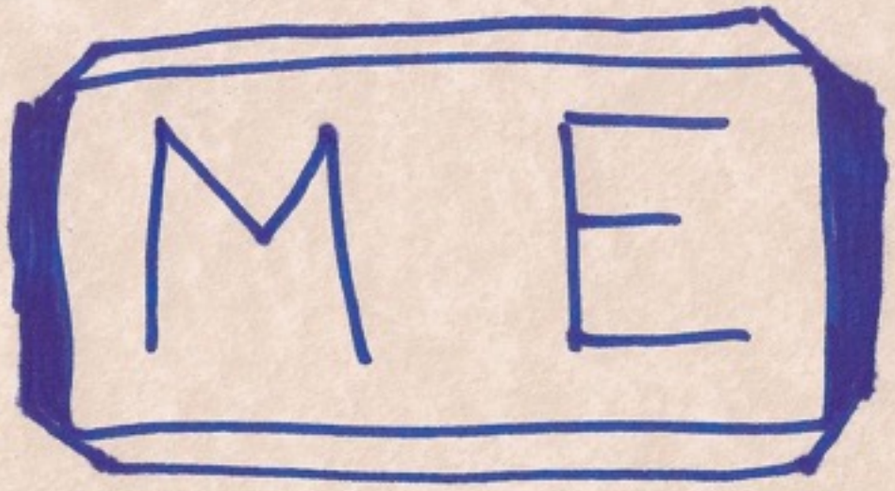
SECURING

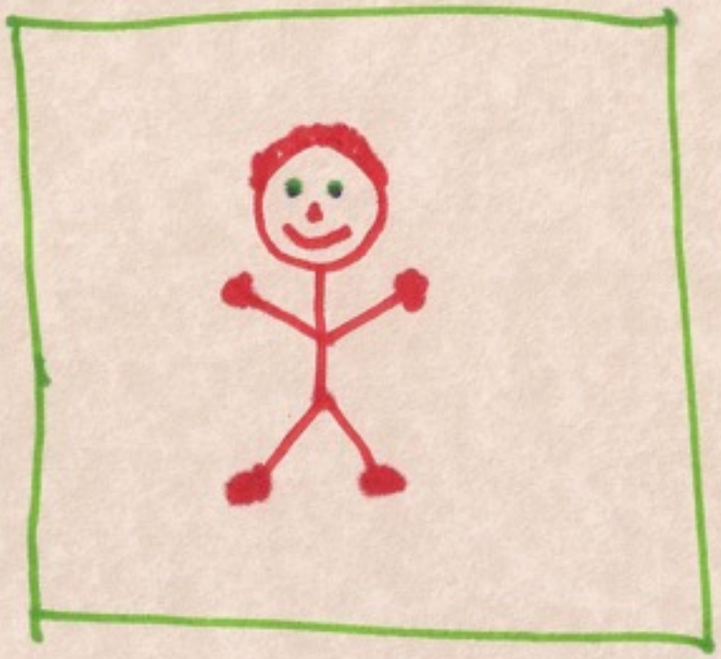
MICRO-SERVICES

UNCC CSC 2016

BY: JOHN MELTON

2a





JOHN MELTON

GITHUB: jtmelton

TWITTER: @_jtmelton

EMAIL: jtmelton@gmail.com


Y'ALL

AGENDA

→ WHAT IS MICRO-SERVICES?

→ WHAT IS MICRO-SERVICES SECURITY?

+ CHALLENGES
+ BENEFITS
+ HOW-TO

→ A (BRIEF) LOOK AT THE FUTURE

WHAT

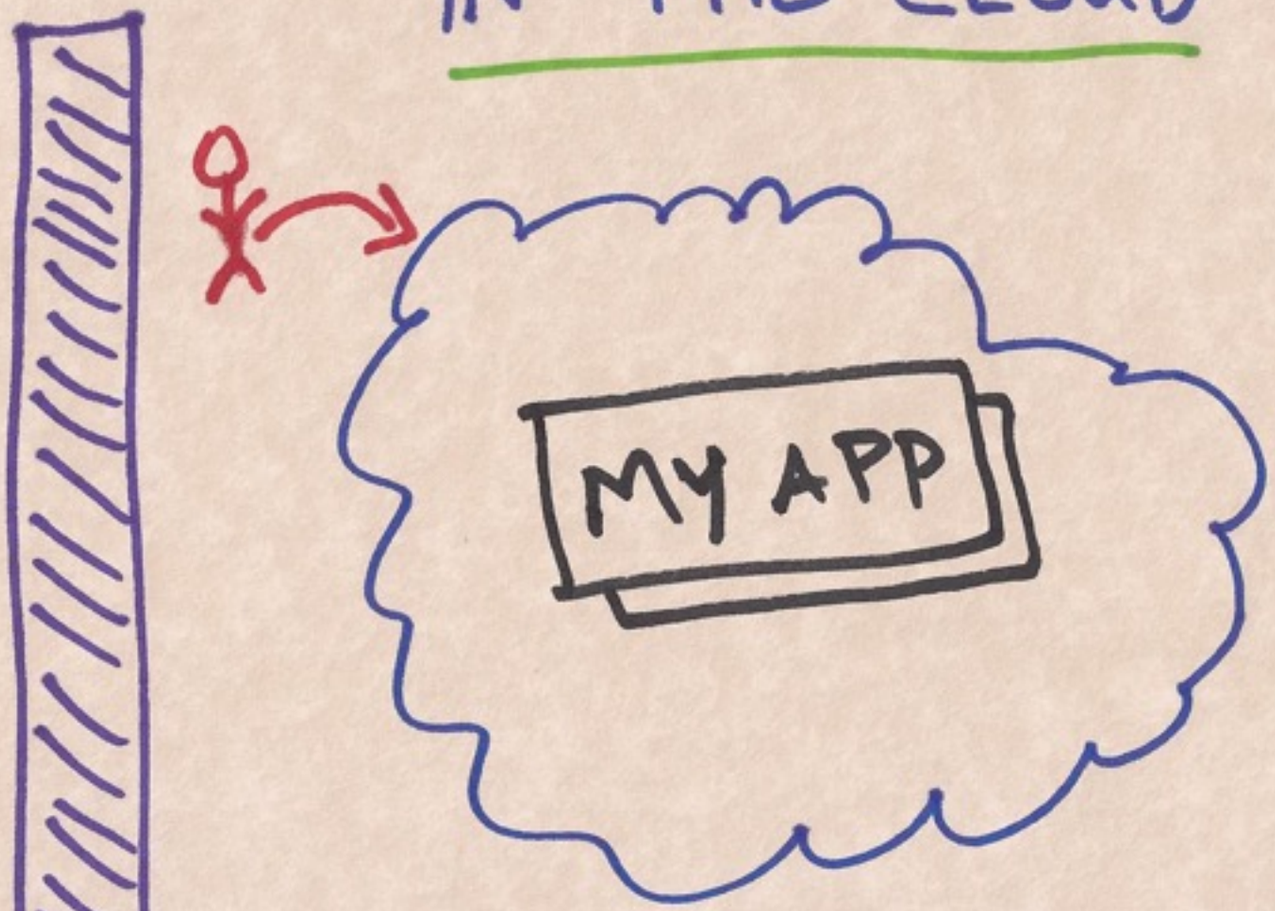
EXACTLY

ARE

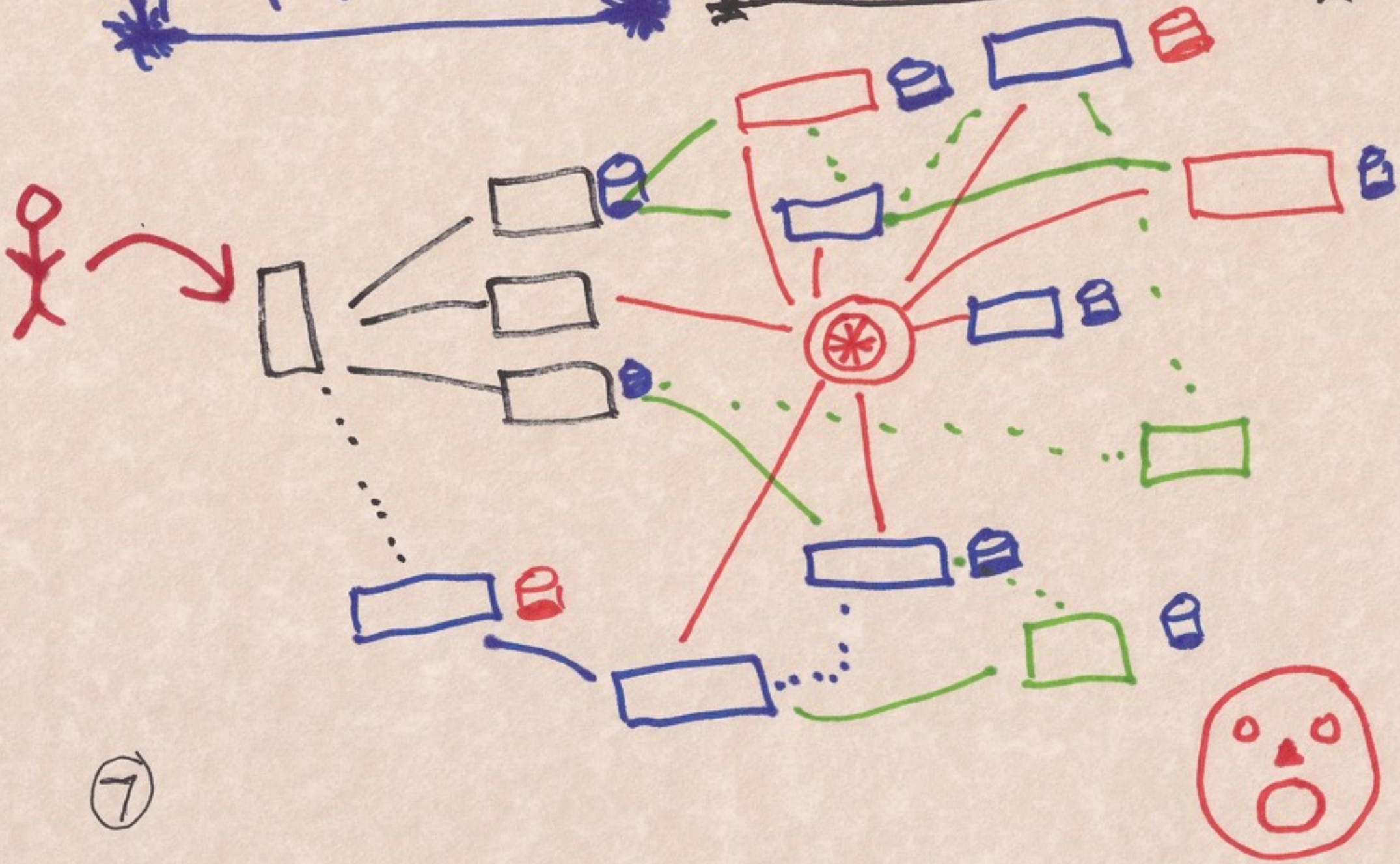
MICRO-SERVICES?

MONOLITH

MONOLITH IN THE CLOUD



MICRO~SERVICE



MICRO ~ SERVICES

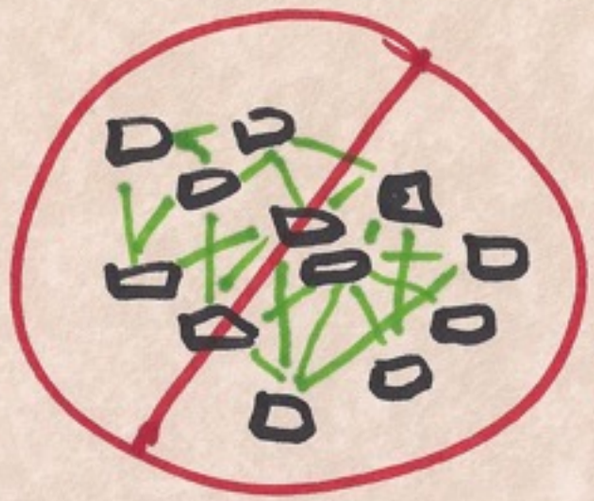
- 1 "APP", MANY SERVICES
- LIGHTWEIGHT COMMS
- AUTOMATED, INDEPENDENT DEPLOYMENT
- LANGUAGE · AGNOSTIC
- DATA-STORAGE AGNOSTIC

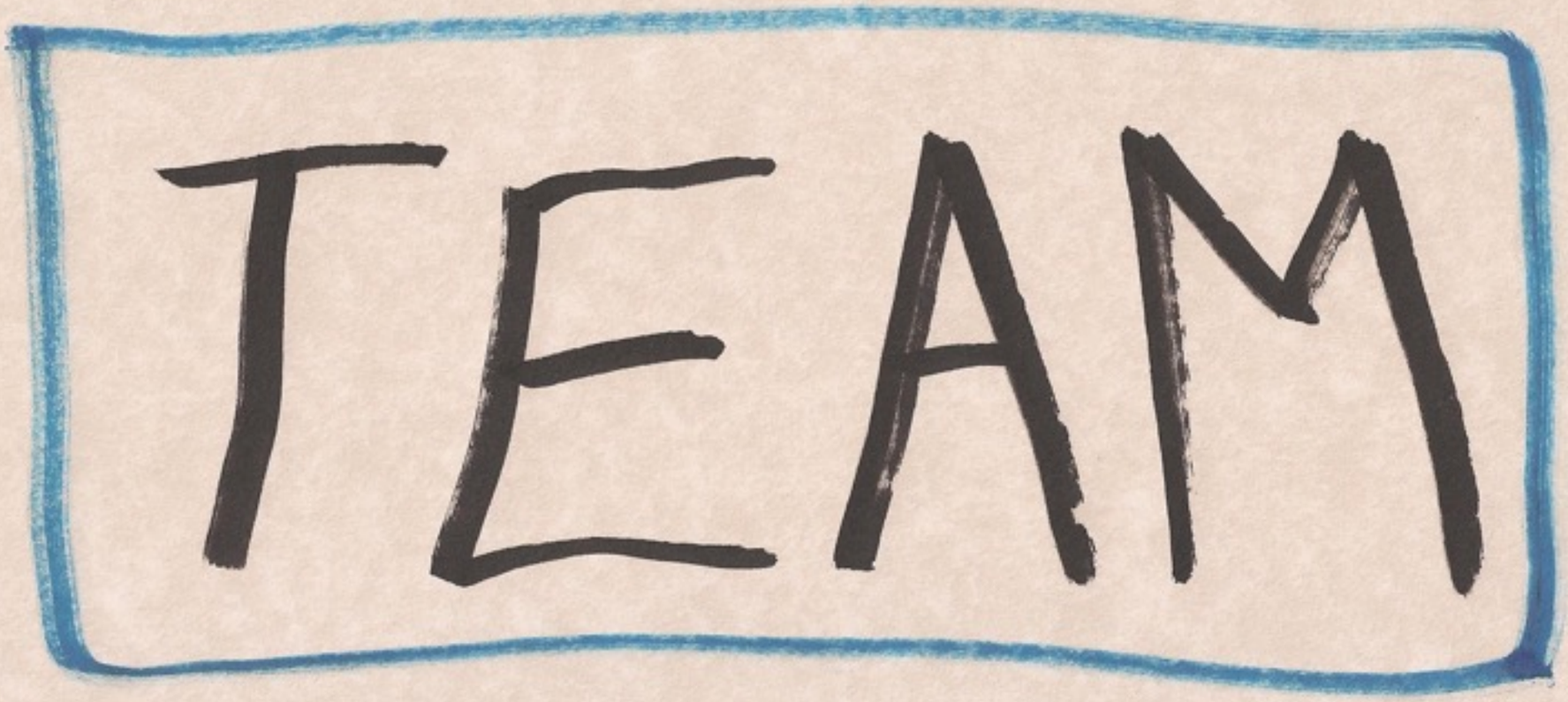
WHAT IS MICRO-SERVICES SECURITY?


DevOps
Sec

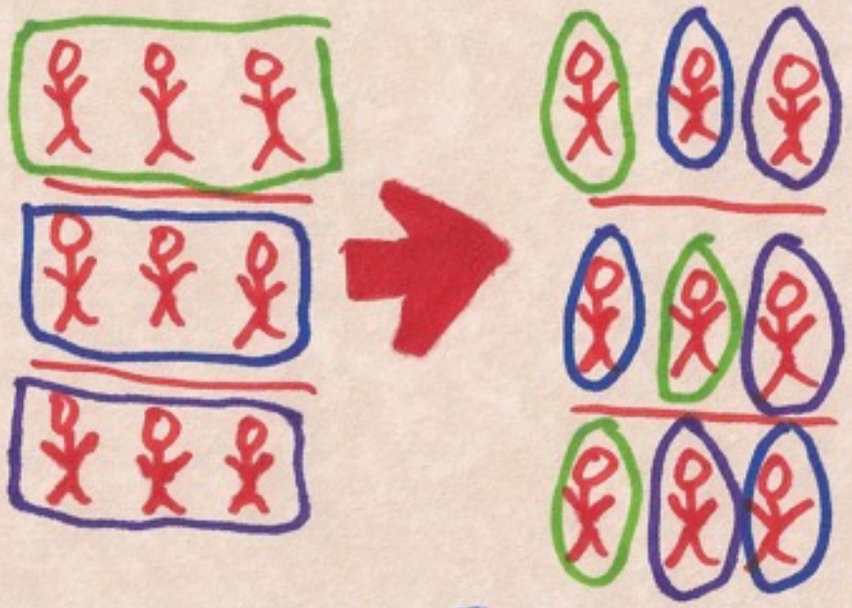
WHAT IS MICRO-SERVICES SECURITY?

- TEAM
- ARCH
- DEV
- OPS




TEAM

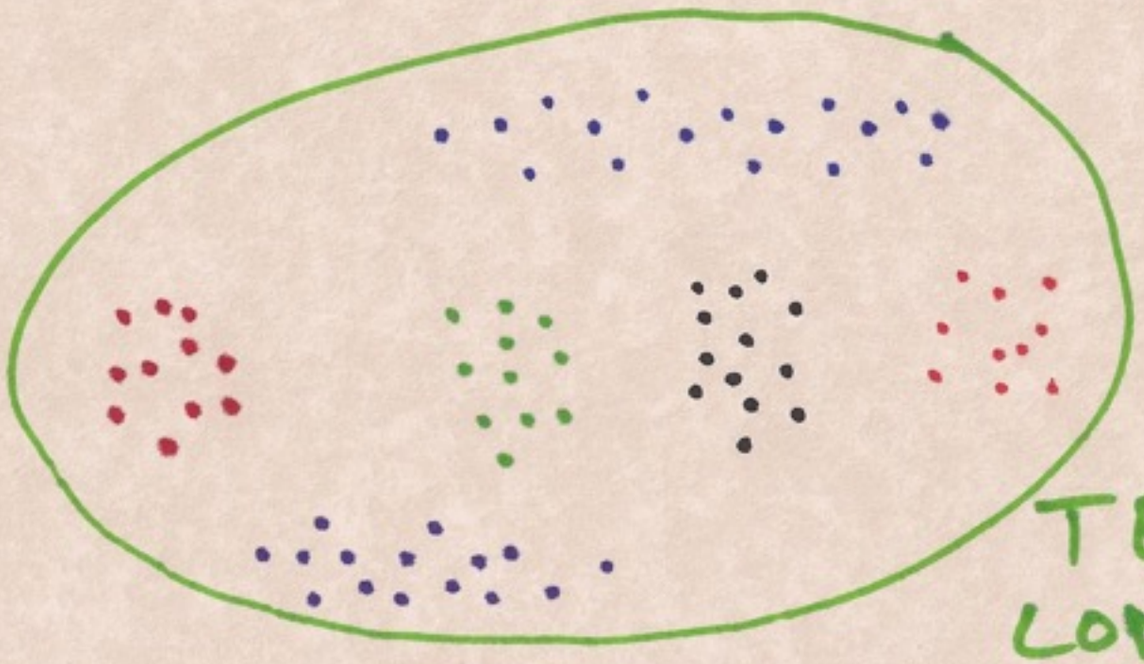
CHALLENGES



CULTURE

CHANGE

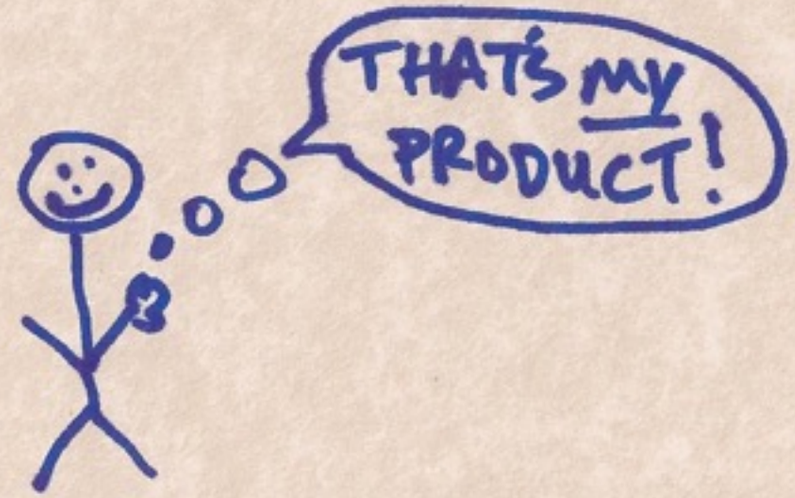
NOOOO!

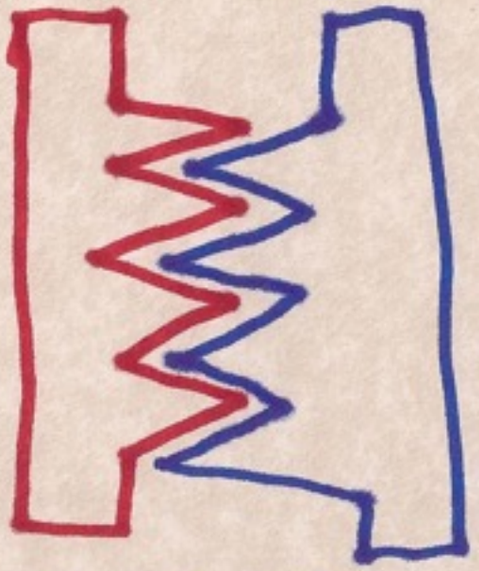


TEAM CONFIGURATION

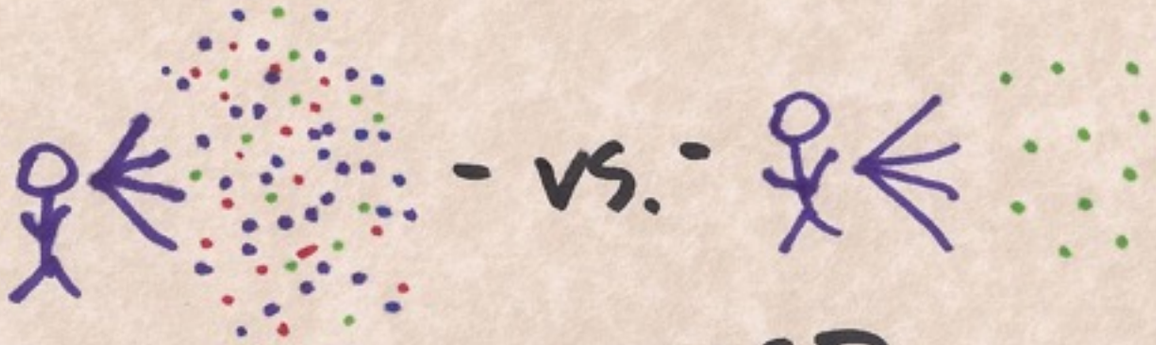
BENEFITS

TEAM AUTONOMY





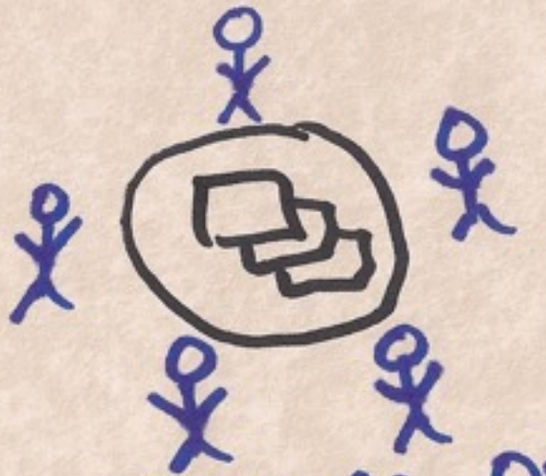
HIRING GAUNTLET



FOCUSED TRAINING

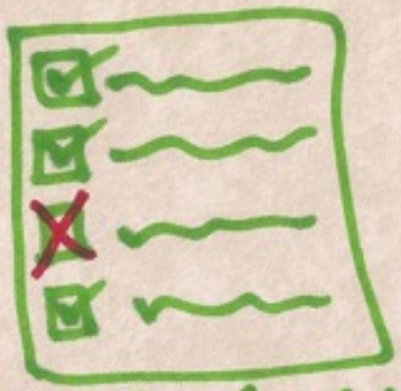
HOW TO EXPLOIT

DRIVE CULTURE CHANGE



TEAM OWNS PRODUCT

FOCUSED SEC TRAINING

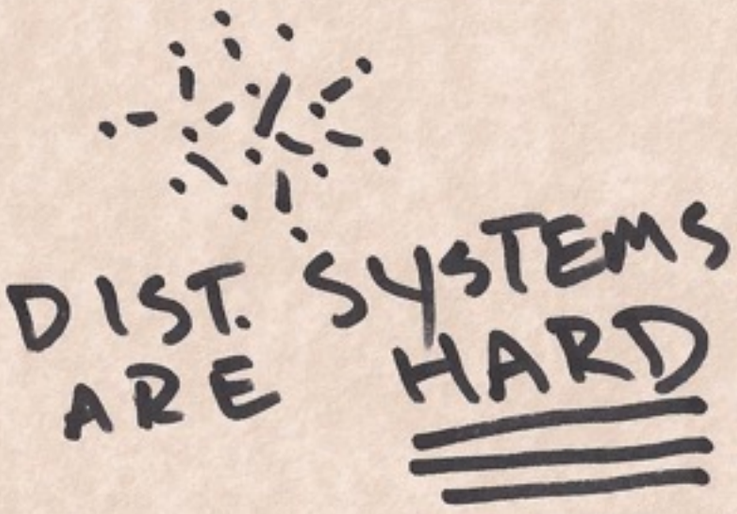


SIMPLE SUCCESS MEASUREMENTS

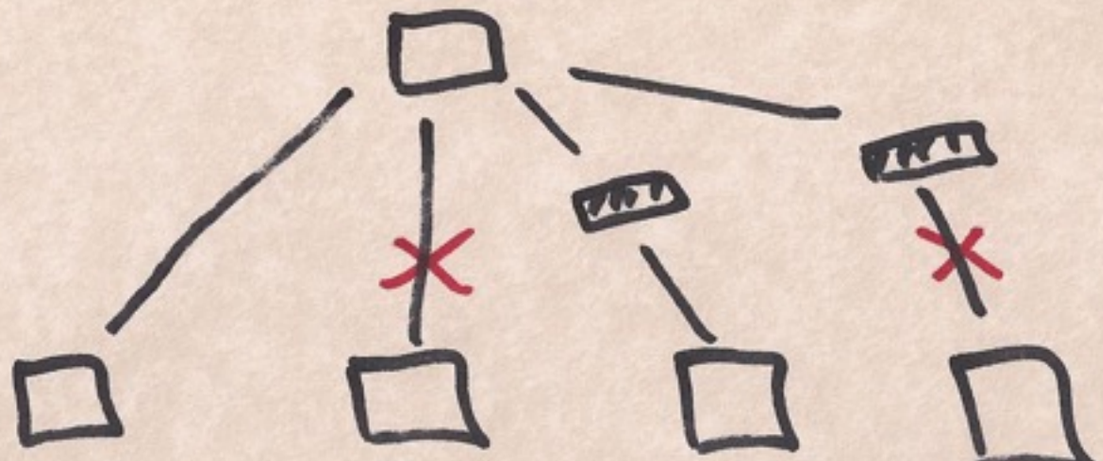
CELEBRATE SUCCESSES

(15)

CHALLENGES

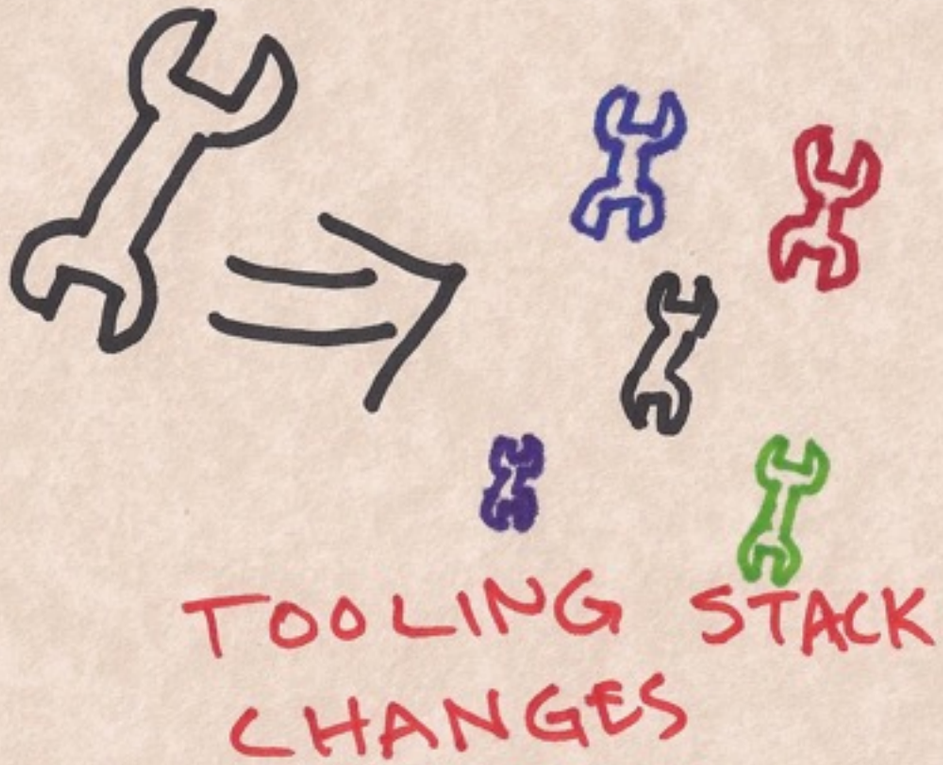

DIST. SYSTEMS ARE HARD


PEOPLE/TEAMS
ARCH
TOOLING
MICRO-SERVICES AFFECTS EVERYTHING

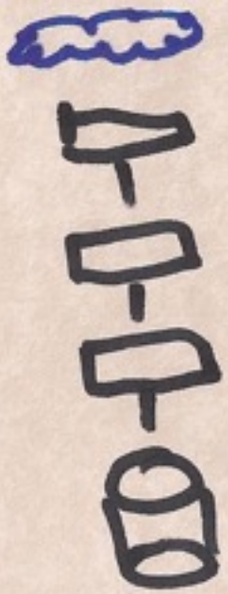

PARTIAL DATA
+
CACHING

CHALLENGES

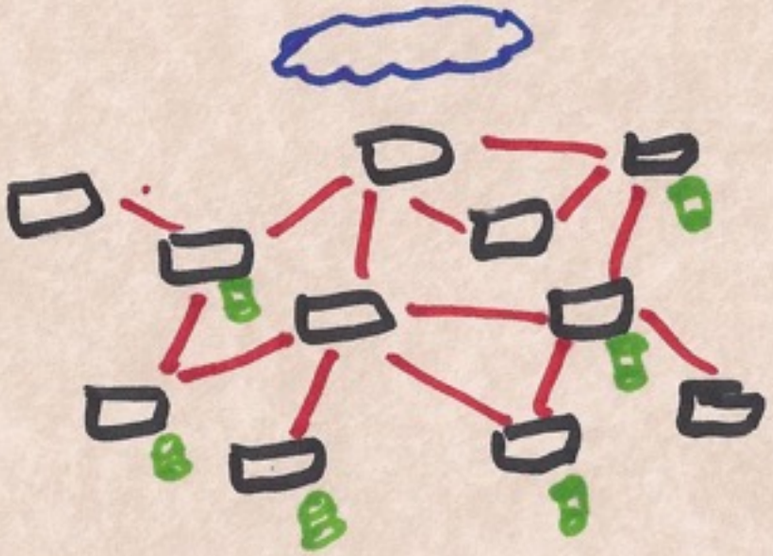
IAM

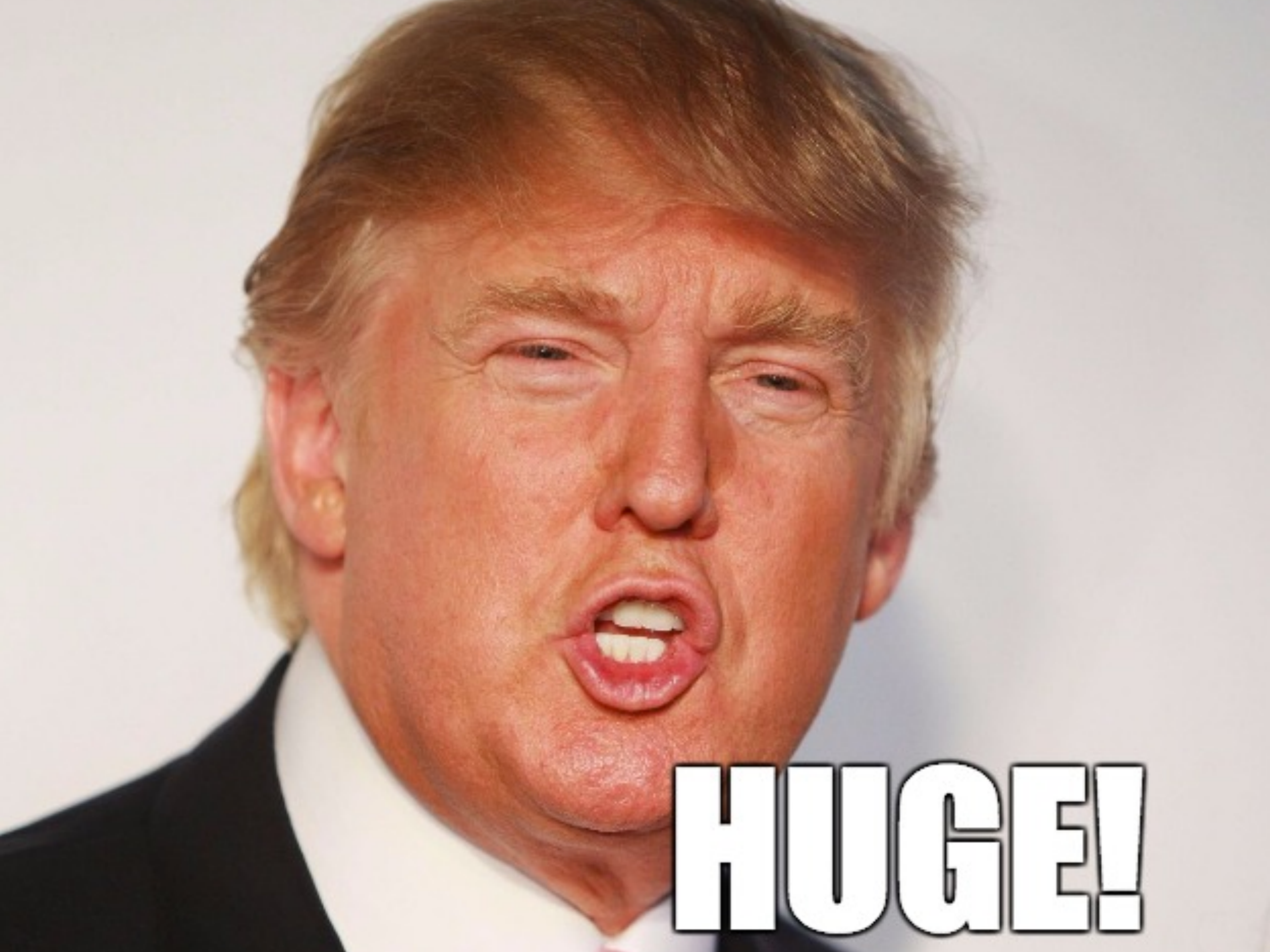


TOOLING STACK CHANGES

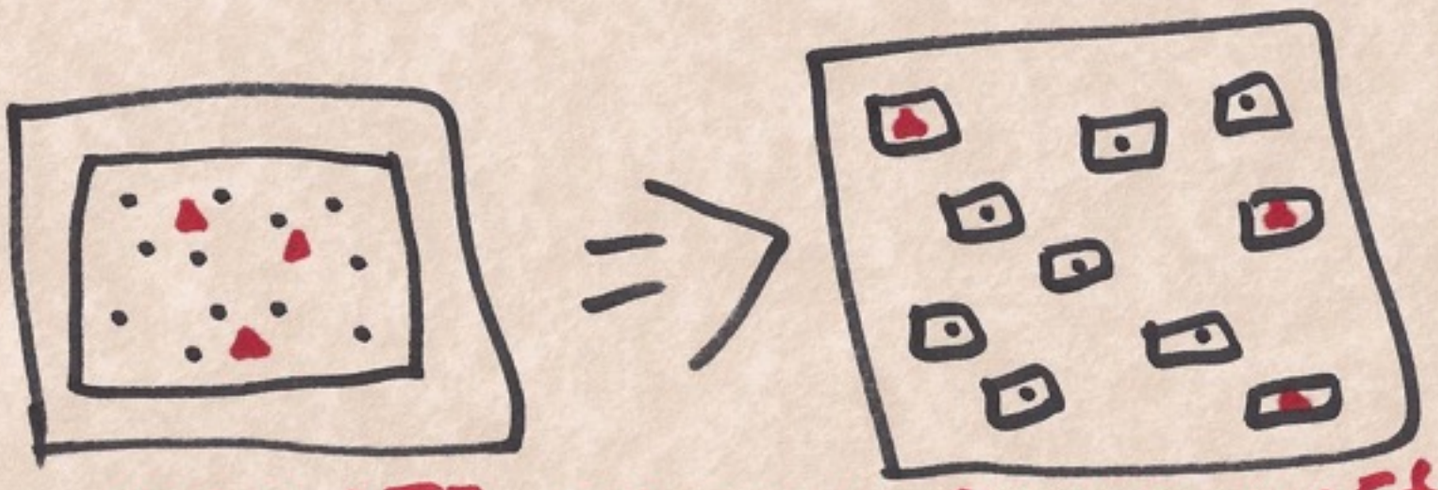


ARCH IS HUGE

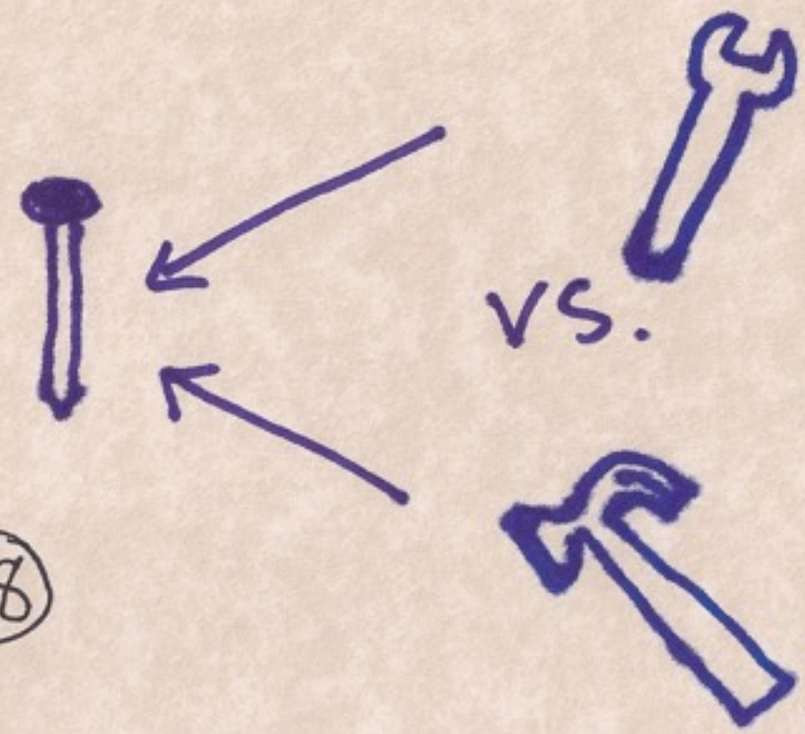



HUGE!

BENEFITS

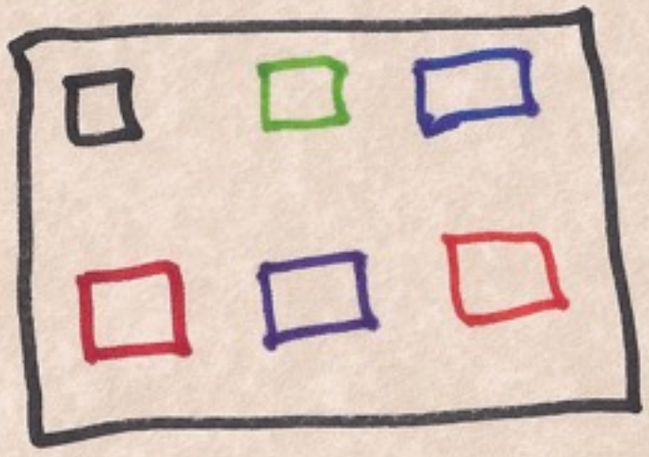


ISOLATE SECURITY SERVICES



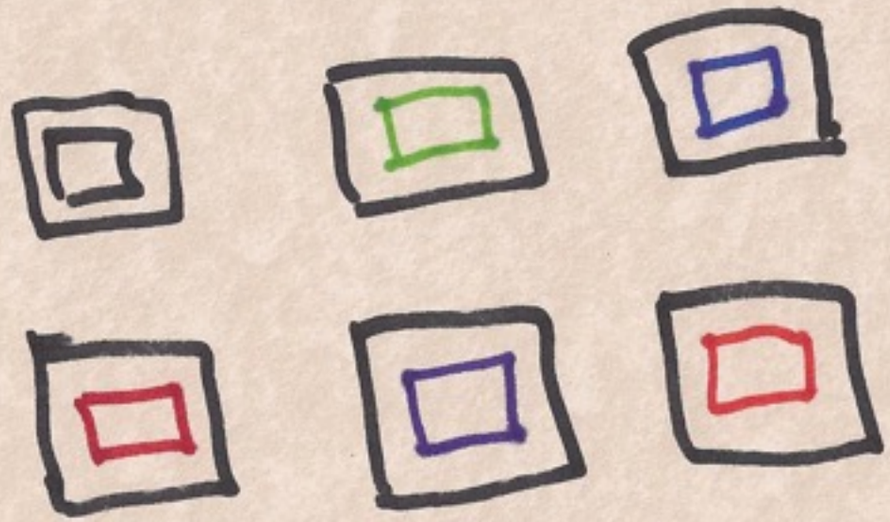
IAM
(BY NECESSITY)

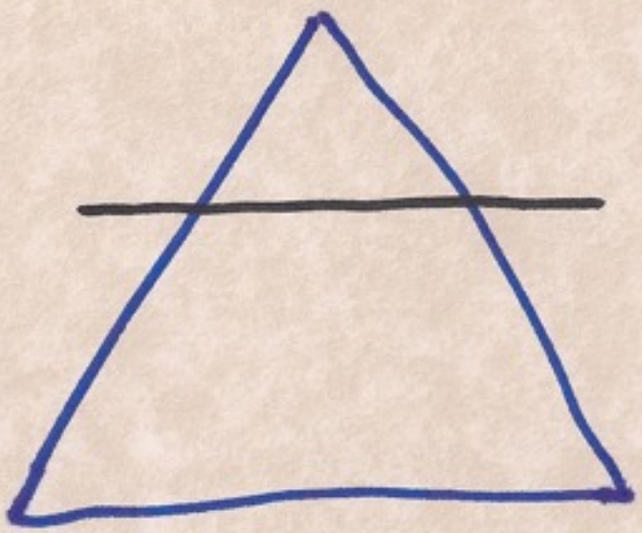
BENEFITS



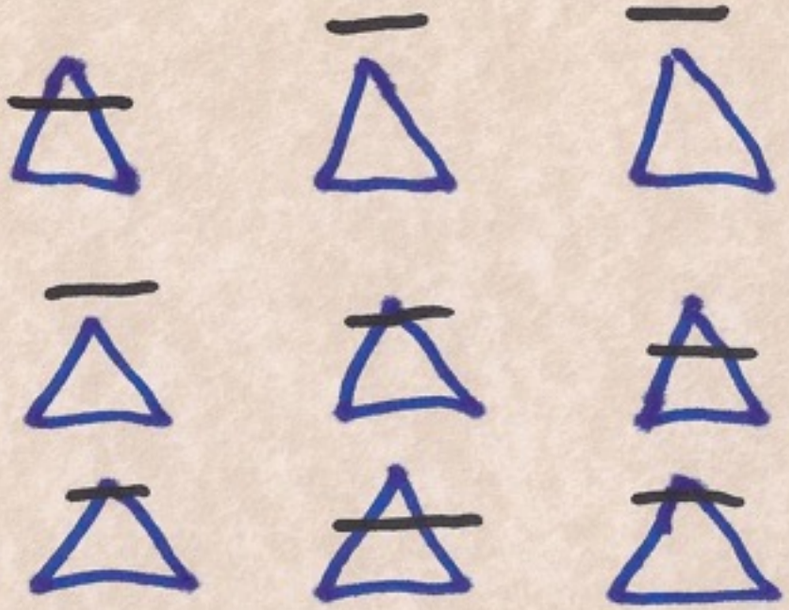
VS.

DATA HIDING



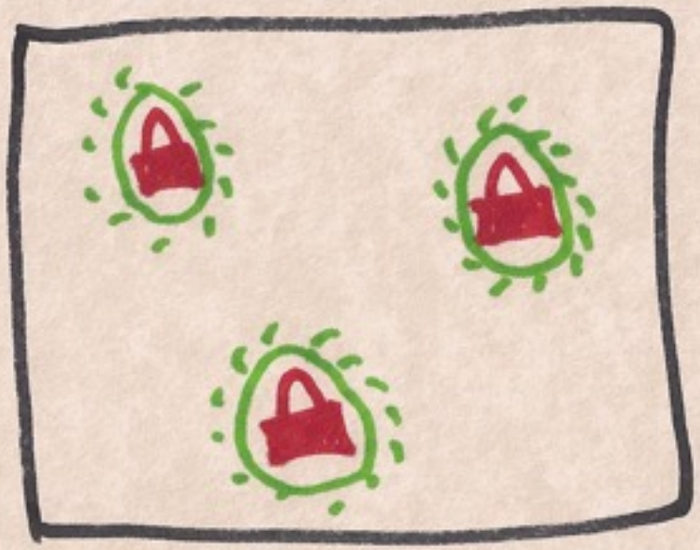


VS.



ATTACK SURFACE REDUCTION

HOW TO EXPLOIT



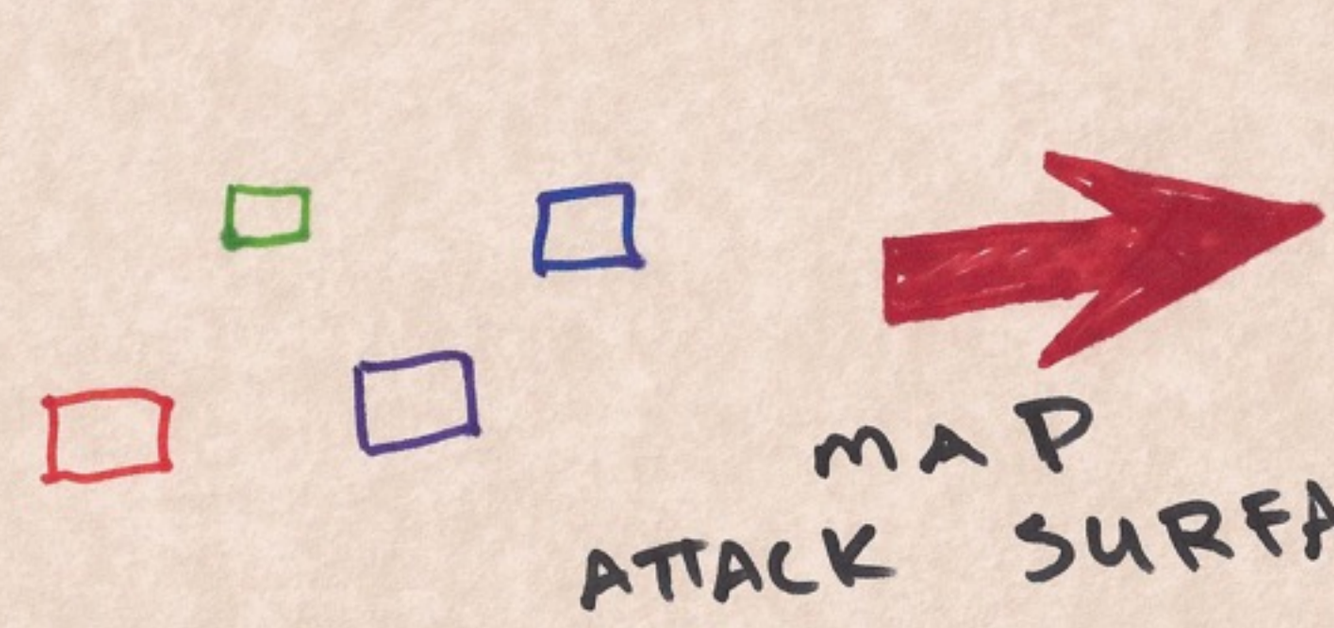
ISOLATE SECURITY SERVICES & THREAT MODEL

REQUIRE IAM

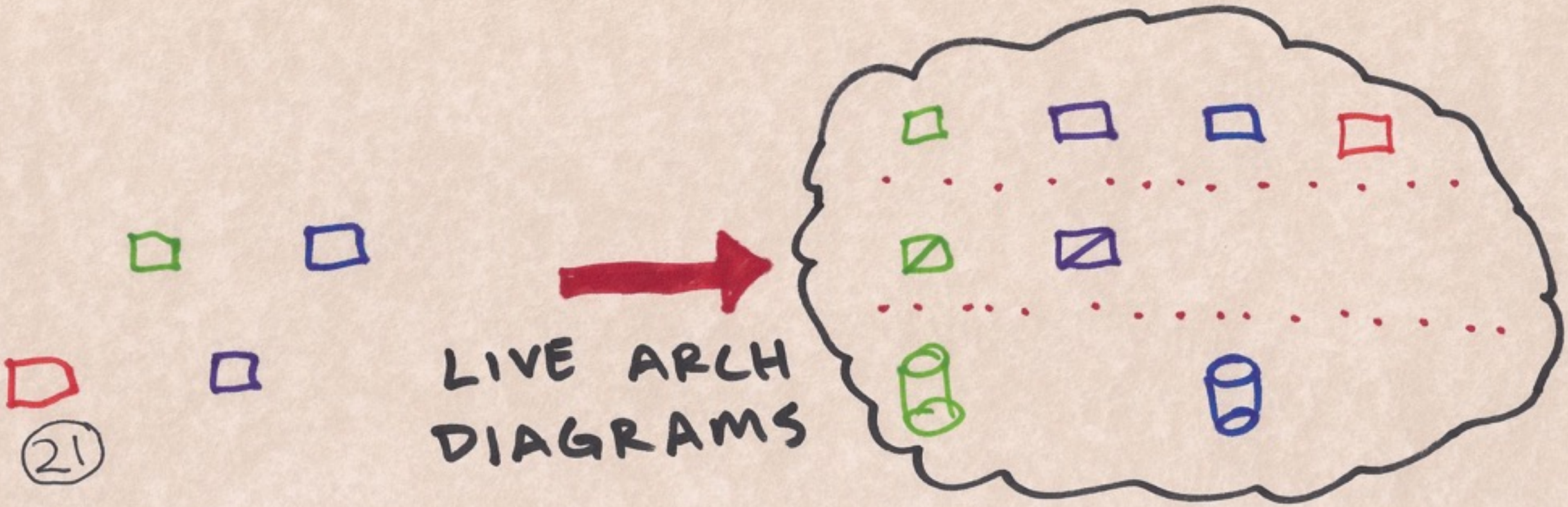
LIMIT ARCH'S / LANG'S

DISCUSS PRIVACY

HOW TO EXPLOIT

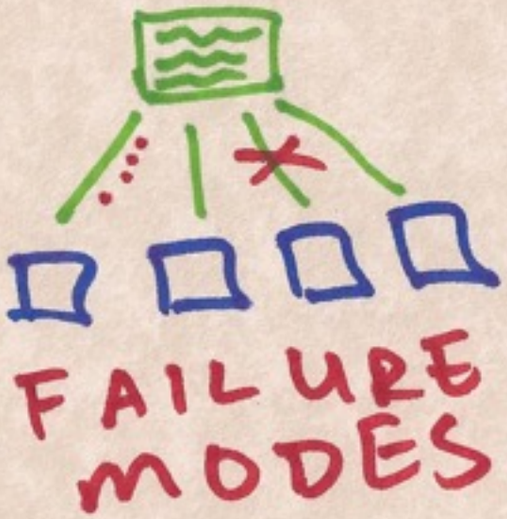


/a /b
/c /d
/e
/f /g
/h /i
/j
/k /l /m /n /o /p




DEV

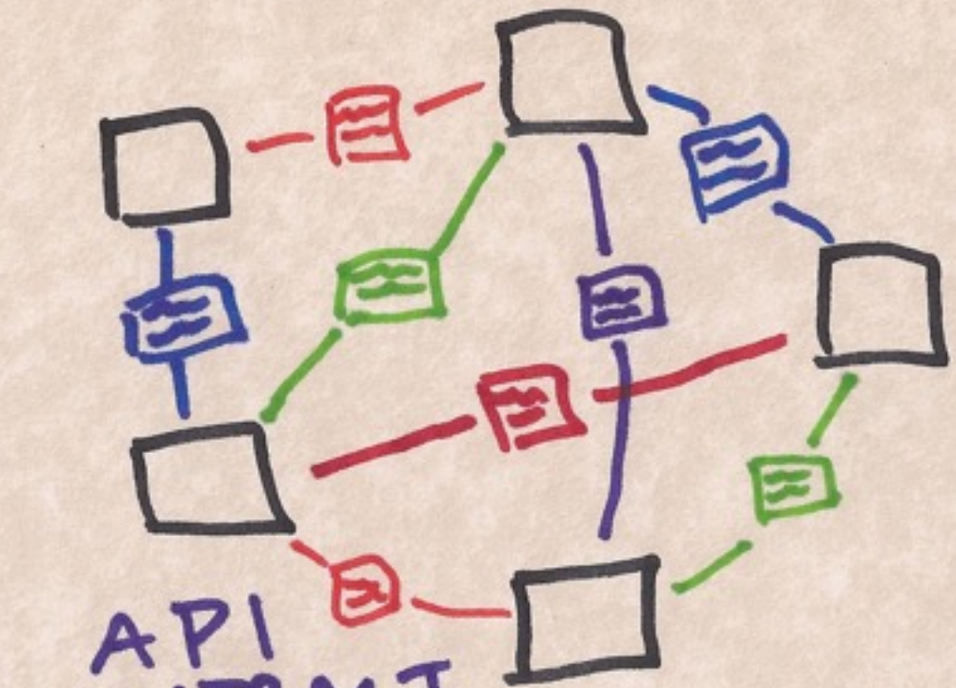
CHALLENGES



FAILURE MODES

LANG / FRAMEWORK SELECTION

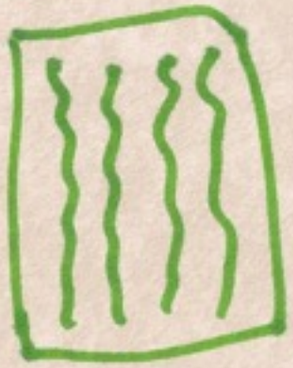
PROTOCOL SELECTION



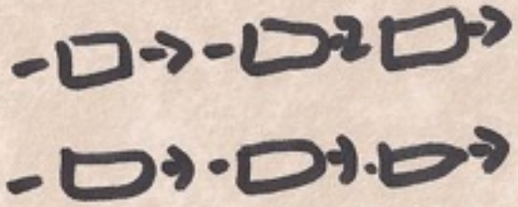
API CONTRACT SPRAWL

CHALLENGES

LANG CHANGES



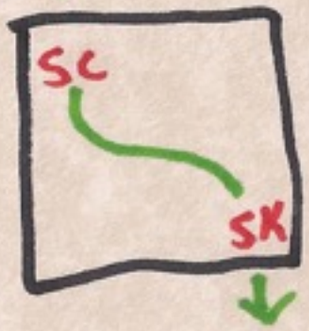
vs.

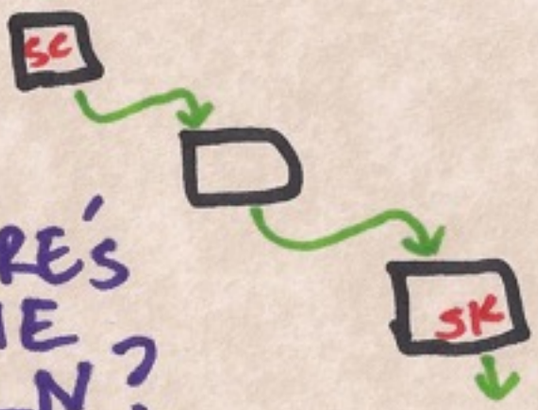


TESTING

CLOUD NATIVE?

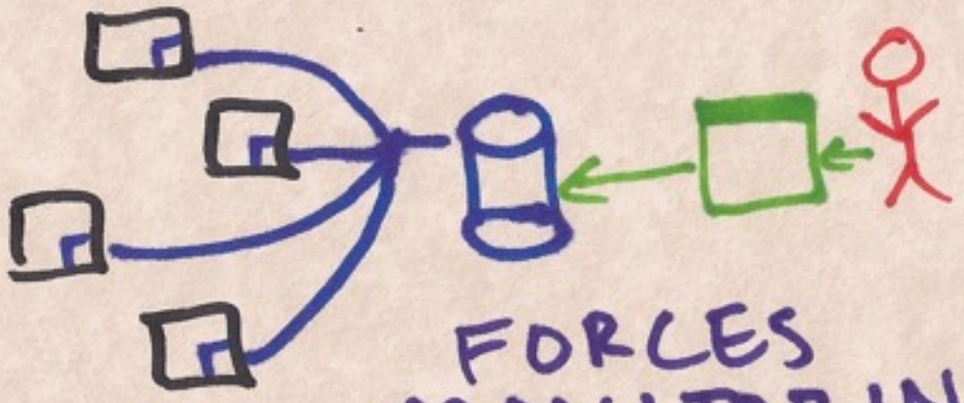
TRUST BOUNDARIES ++





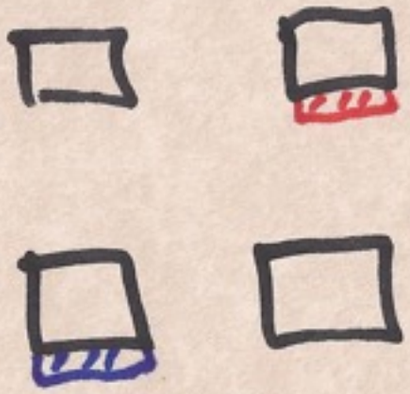
WHERE'S THE VULN?

BENEFITS

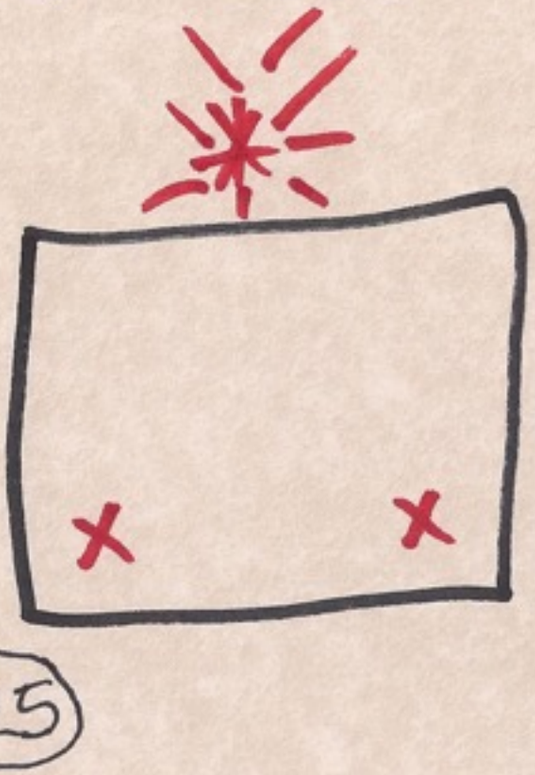


FORCES MONITORING

VS.

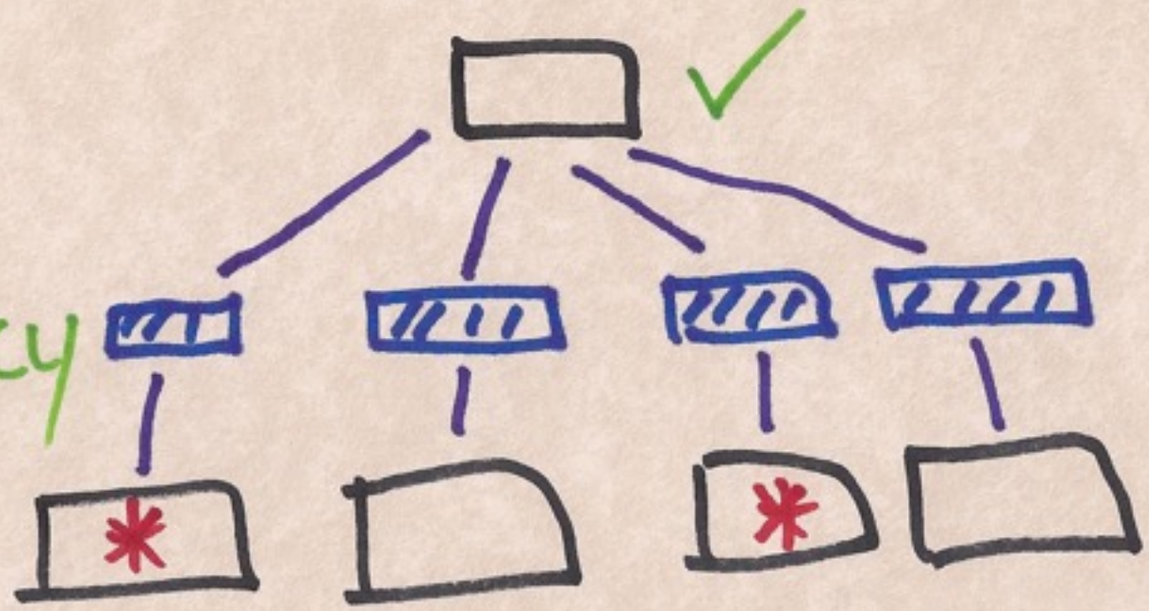


LIGHTER FRAMEWORKS

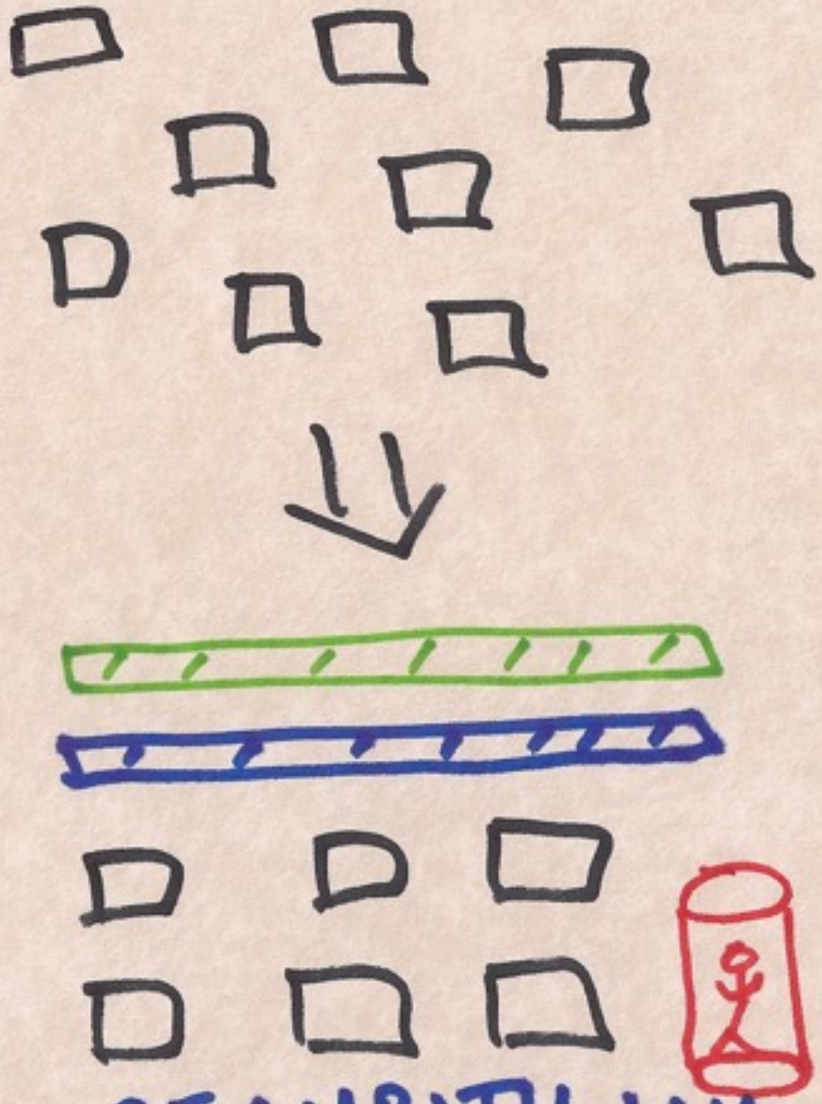


VS.

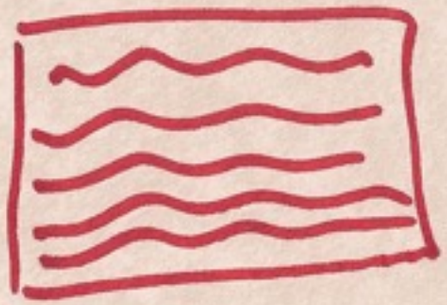
RESILIENCY



BENEFITS



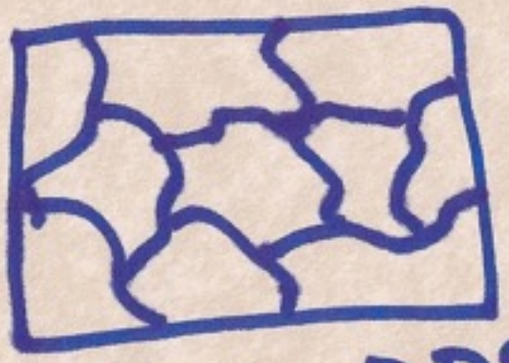
SECURITY UX



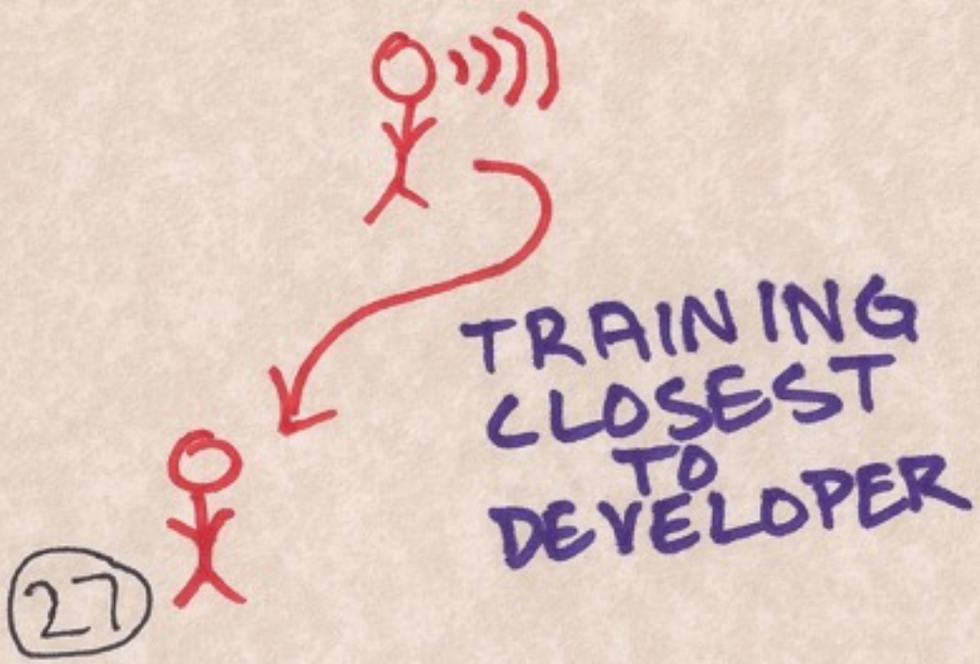
VS.

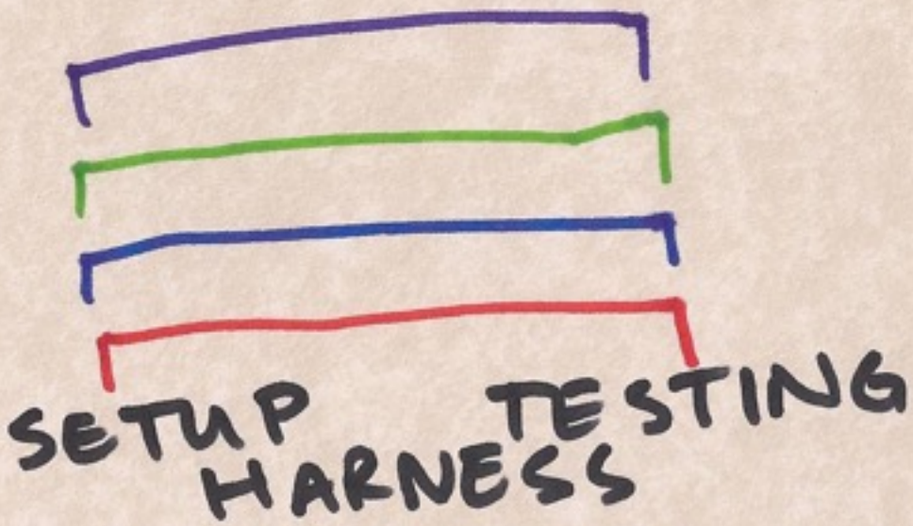
LIMITED LANGS
&
DSLs

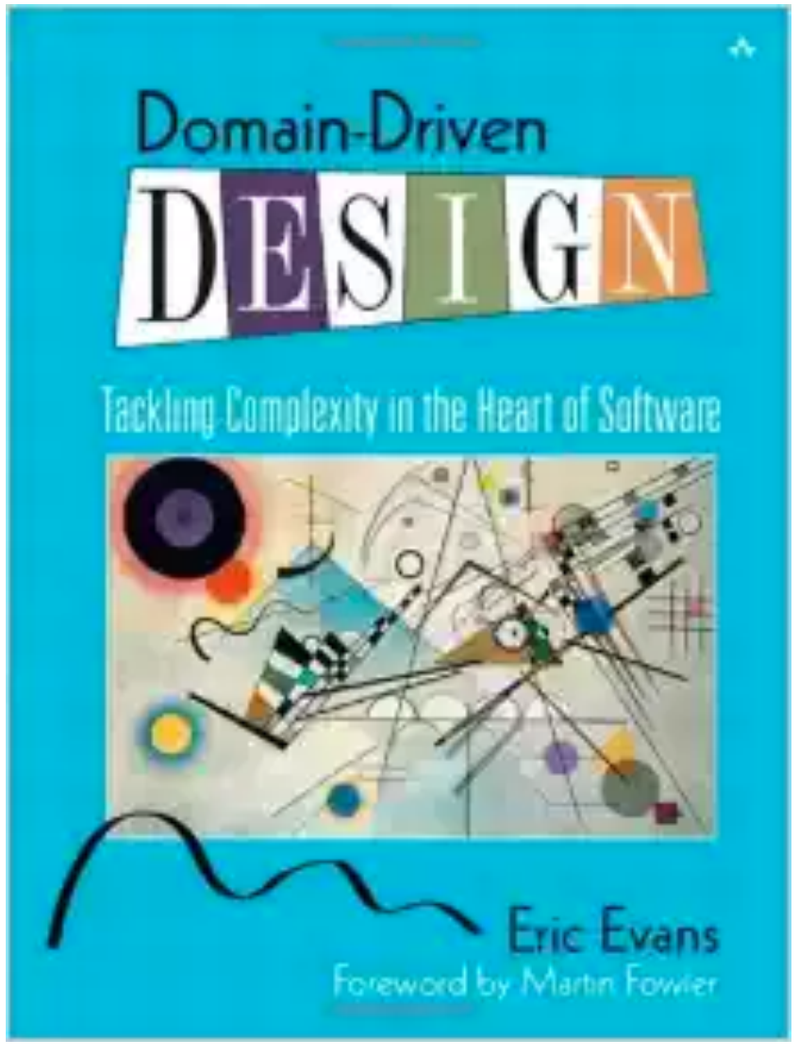
HOW TO EXPLOIT

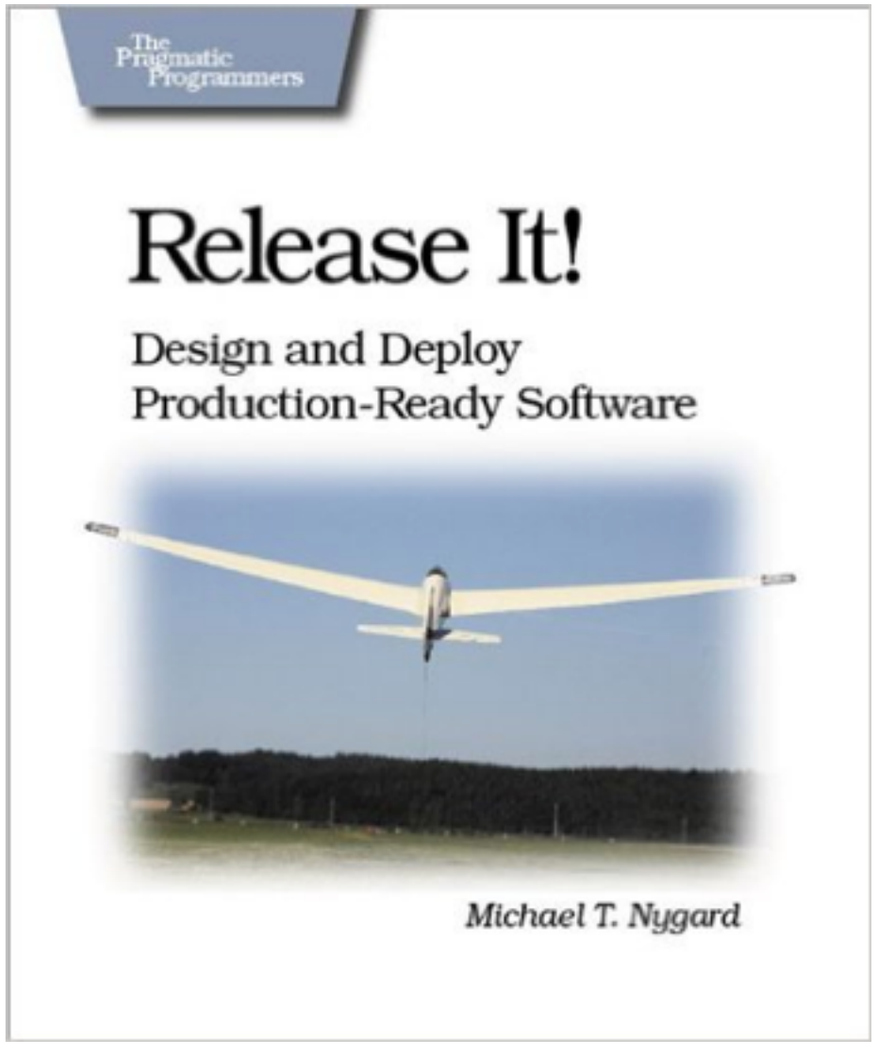


DDD + DDS

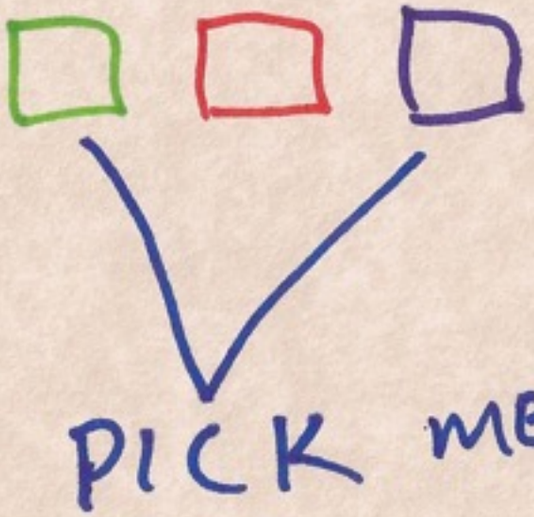





Domain-Driven
DESIGN
Tackling Complexity in the Heart of Software
Eric Evans
Foreword by Martin Fowler


The Pragmatic Programmers
Release It!
Design and Deploy
Production-Ready Software
Michael T. Nygard

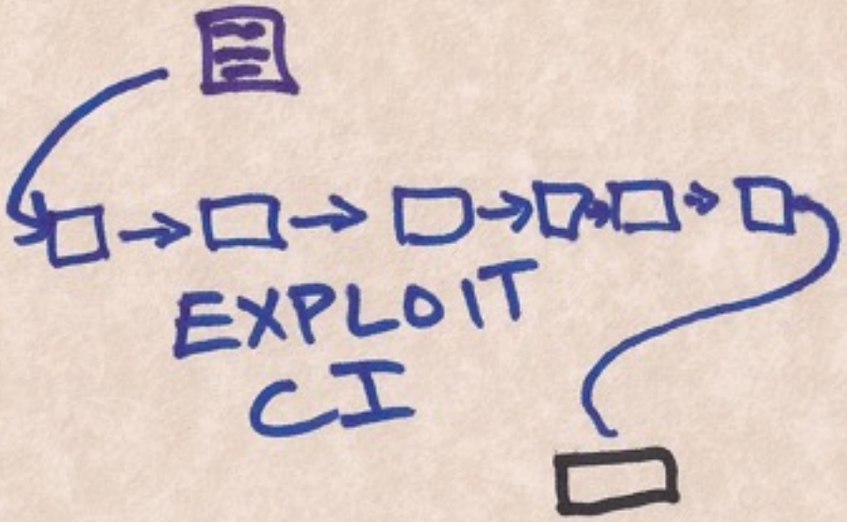
HOW TO EXPLOIT



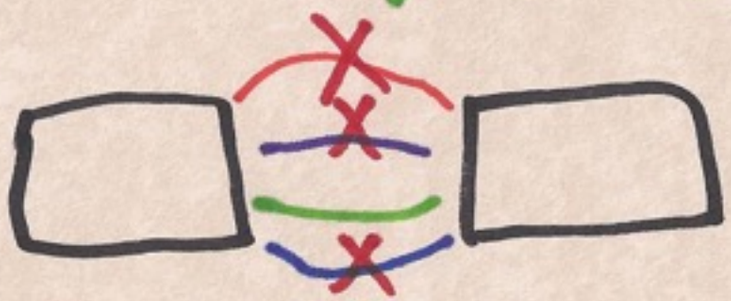
ME

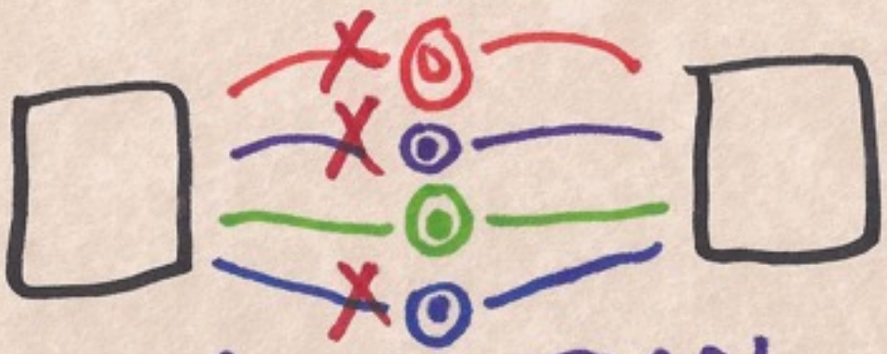
DEPS

KNOW YOUR DEPENDENCIES

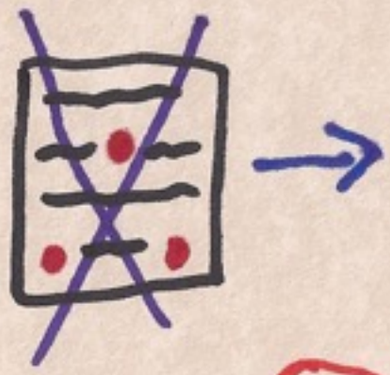


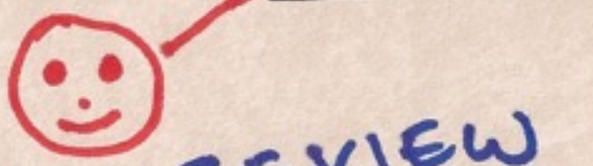
HOW TO EXPLOIT





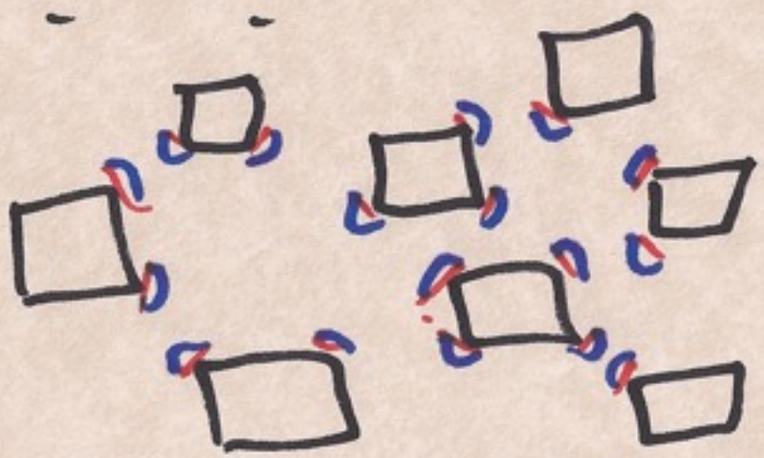
PICK 1 PROTOCOL PER INTERACTION





CODE SENSITIVE

REVIEW COMPONENTS



TRUST BOUNDARIES

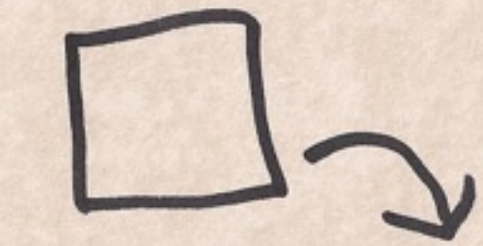
INPUT VALIDATION

VALIDATE EVERYWHERE

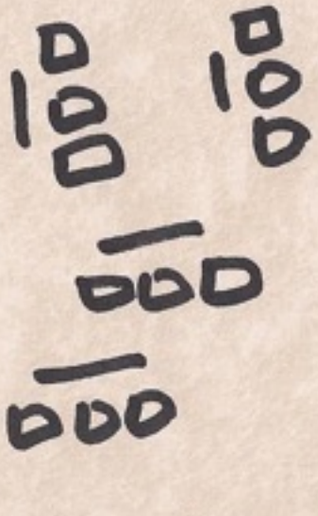
COMMON CONTROLS FRAMEWORK

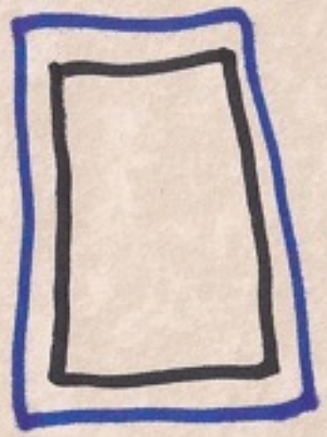

OPS

CHALLENGES

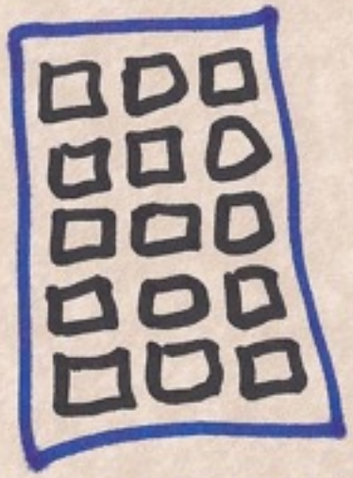


RESOURCE SPRAWL



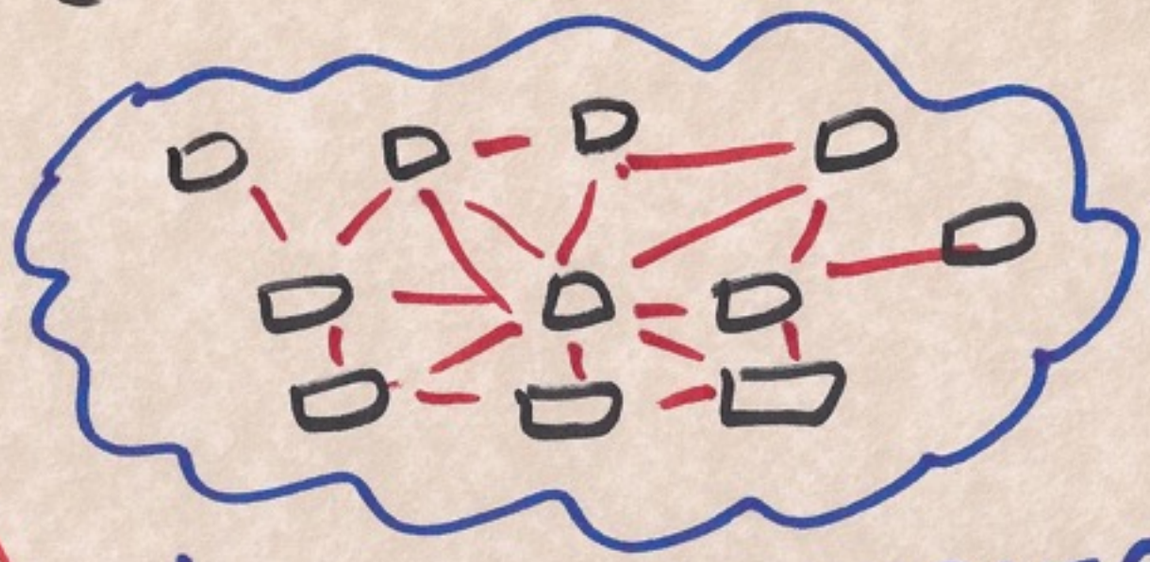


VS.



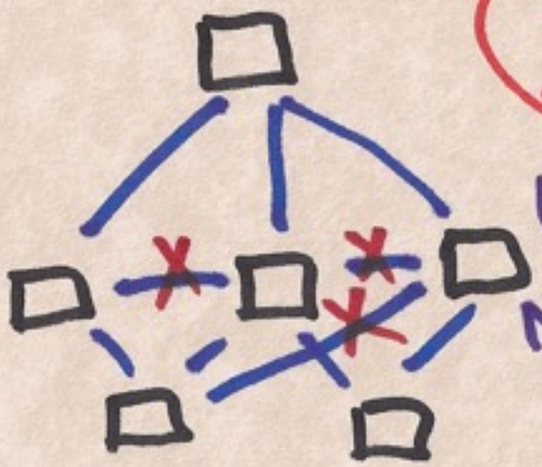
RESOURCE LIMITS

VS.



I'm TUNING SERVERS???

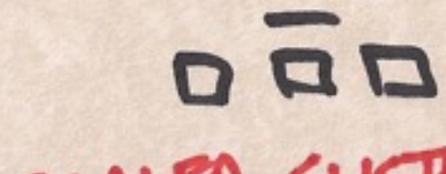
CHALLENGES

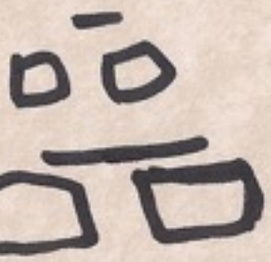


I'M MAKING NETWORK CHANGES NOW???

CREDS EVERYWHERE

DIFFERENTLY SCALED SYSTEMS

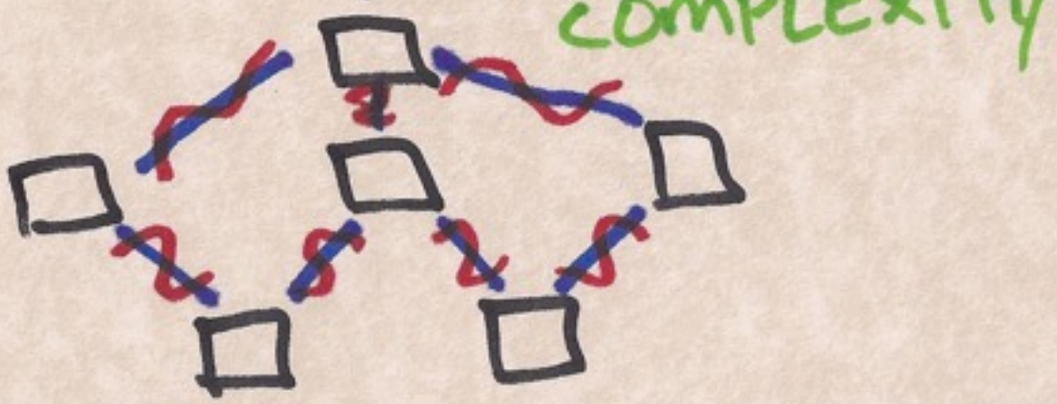




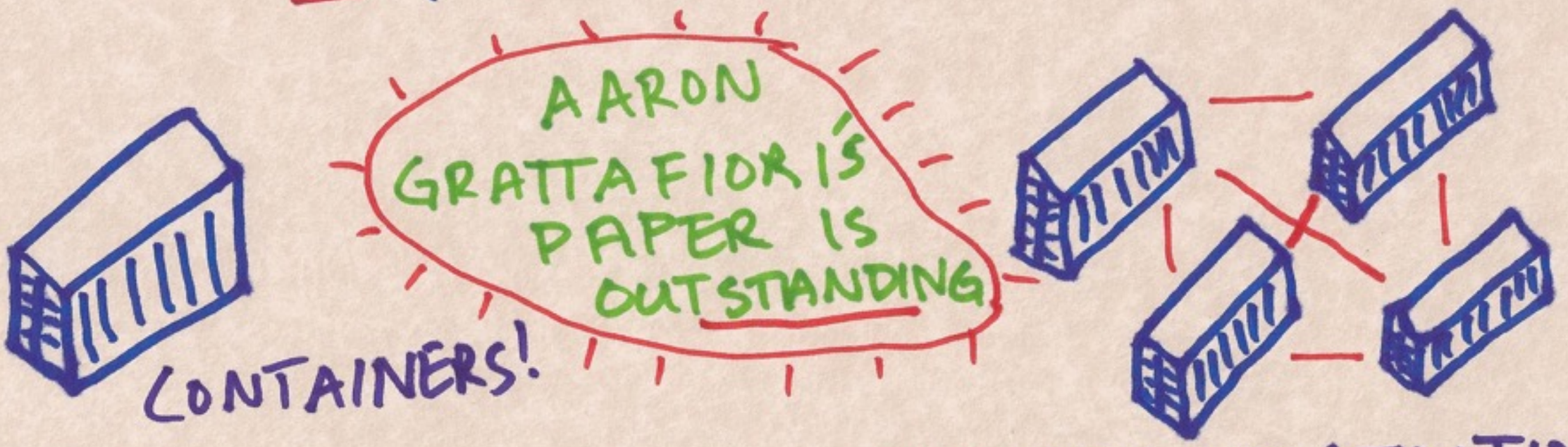
32

VS.

TLS COMPLEXITY



CHALLENGES

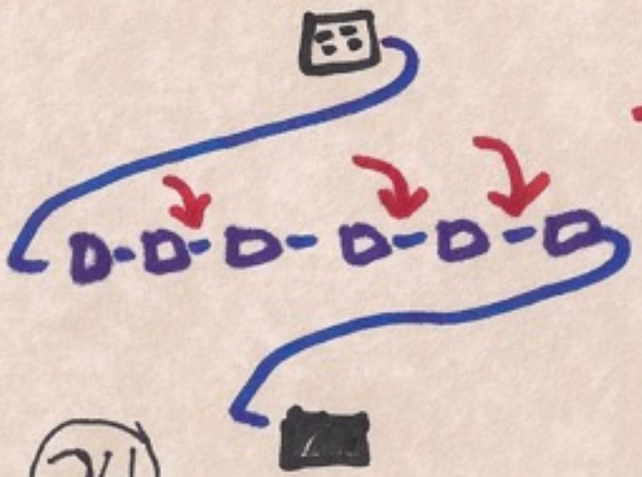


I OWN
ALL
THE THINGS

BENEFITS

FORCES MONITORING

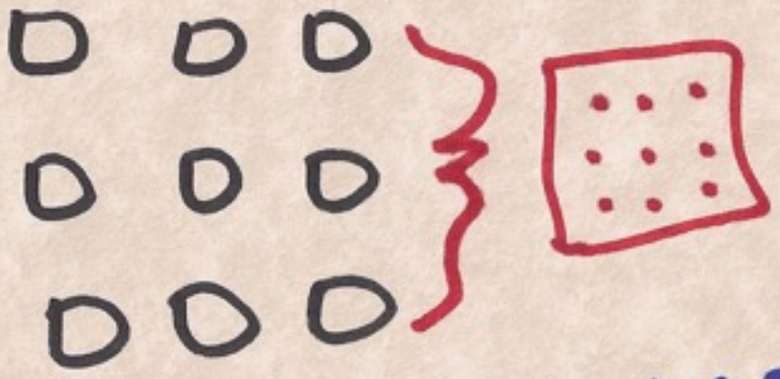
CONSTRAINTS DONT ALLOW CRUFT



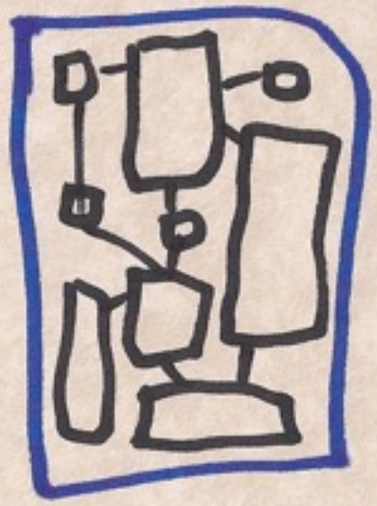
SECURITY TOUCHPOINTS IN CI

CONFIG MGMT TOOLING

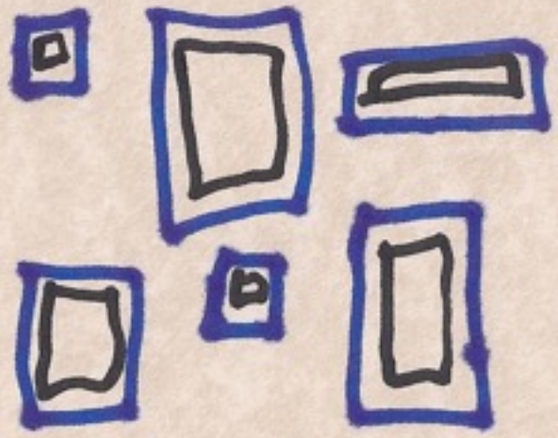
BENEFITS



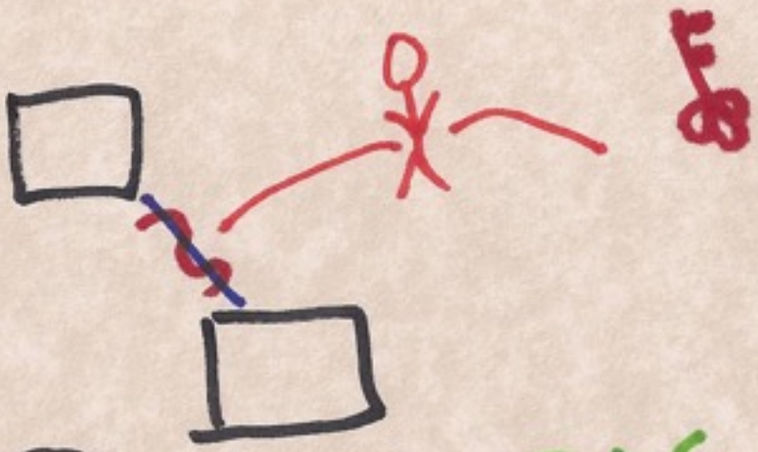
CRED STORAGE VAULT



VS.

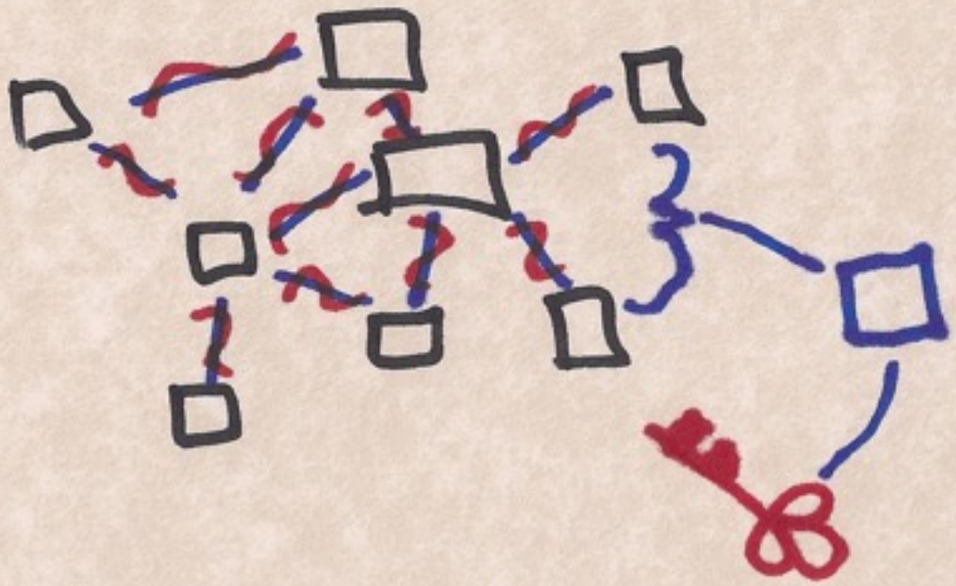


SERVICE SCALING



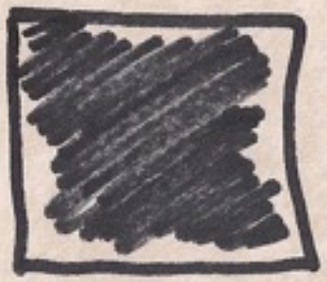
VS.

TLS CA



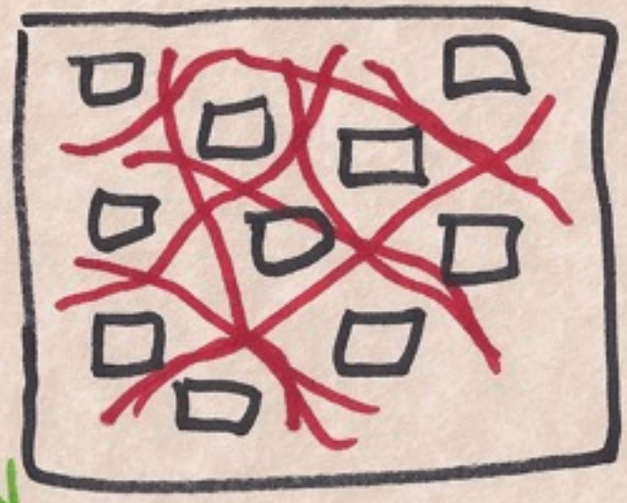
BENEFITS

CONTAINERS & ORCHESTRATION

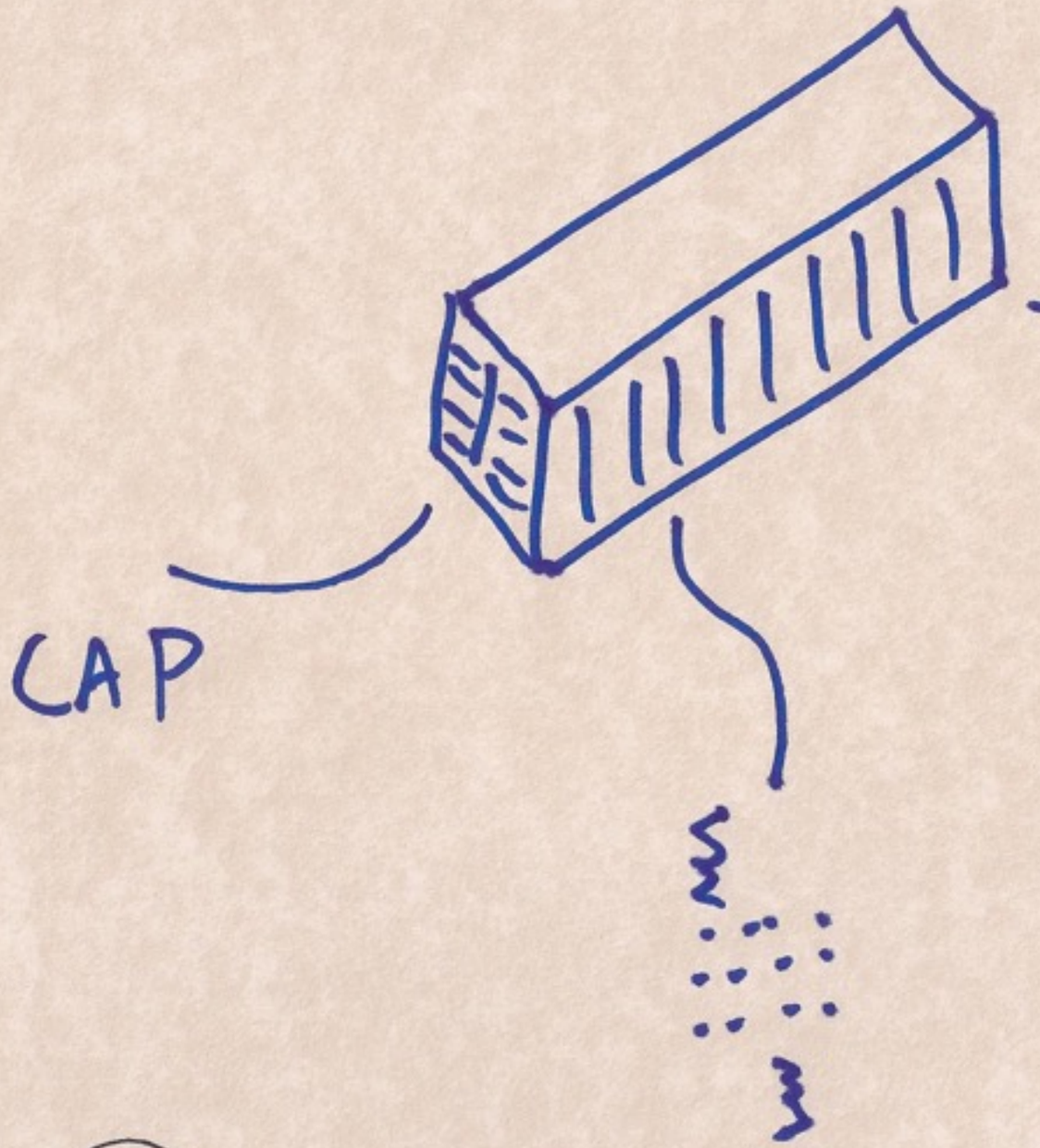


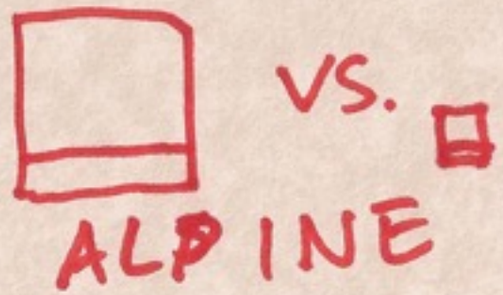
VS.

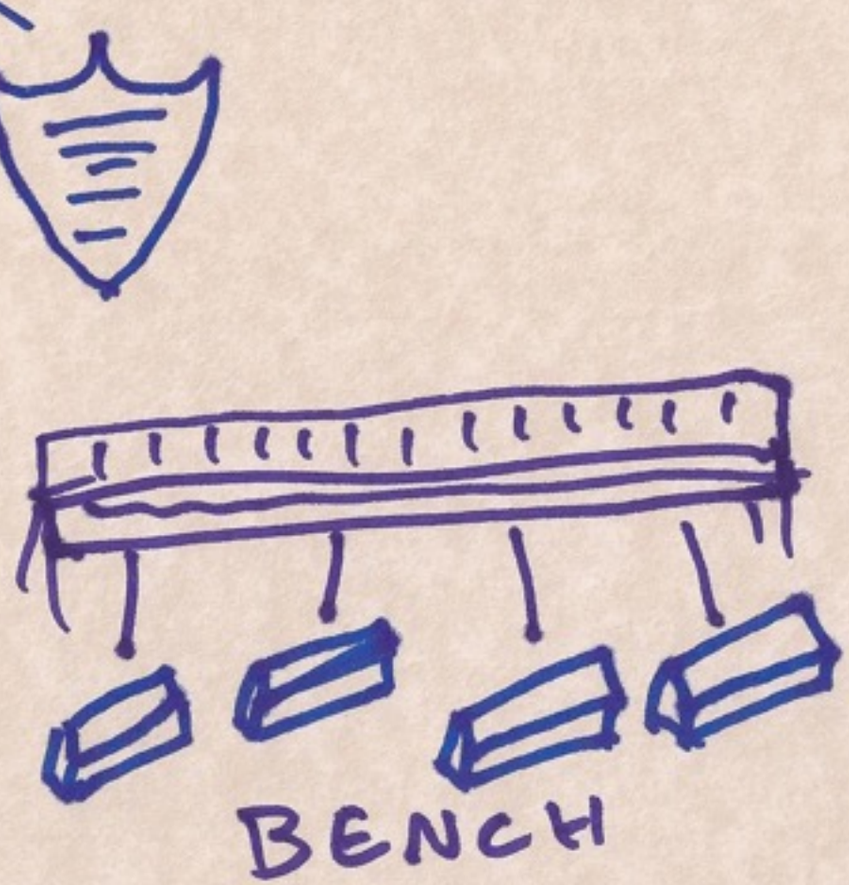
VISIBILITY
&
SELF-PROTECTION



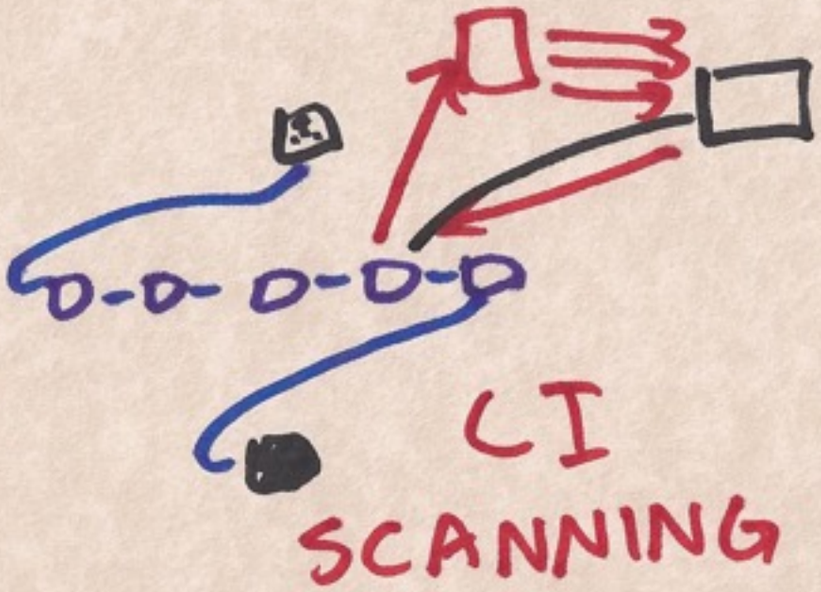
HOW TO EXPLOIT



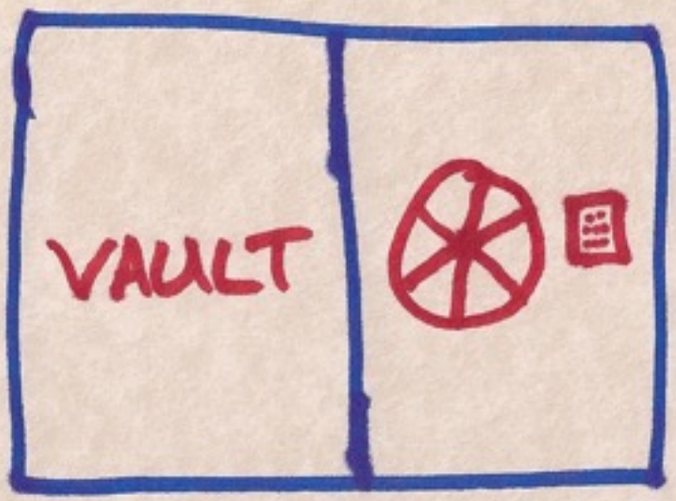




HOW TO EXPLOIT



- PUPPET
- CHEF
- ANSIBLE
- SALT
- ....



LETS ENCRYPT

TLS

VAULT

CFSSL

HOW TO EXPLOIT

FOCUS ON MONITORING

SELF DEFENDING APPS

RUNTIME INTELLIGENCE

BLOW STUFF UP!

BATMAN, I CAN SEE THE FREAKIN FUTURE!

CAN YOU SEE THIS COMING?

TO THE FUTURE

- NETFLIX
- BEYOND CORP
- SPIFFE.IO

CREDITS

- AARON GRATTAFIORI's UNDERSTANDING & HARDENING CONTAINERS

- JVNS.CA SLIDE FORMAT

- PAPERS / SYSTEMS WE LOVE

THANKS

?

twitter: @_jtmelton
github: jtmelton
email: jtmelton@gmail.com