goto; conference

Click ‘engage’ to rate sessions and ask questions

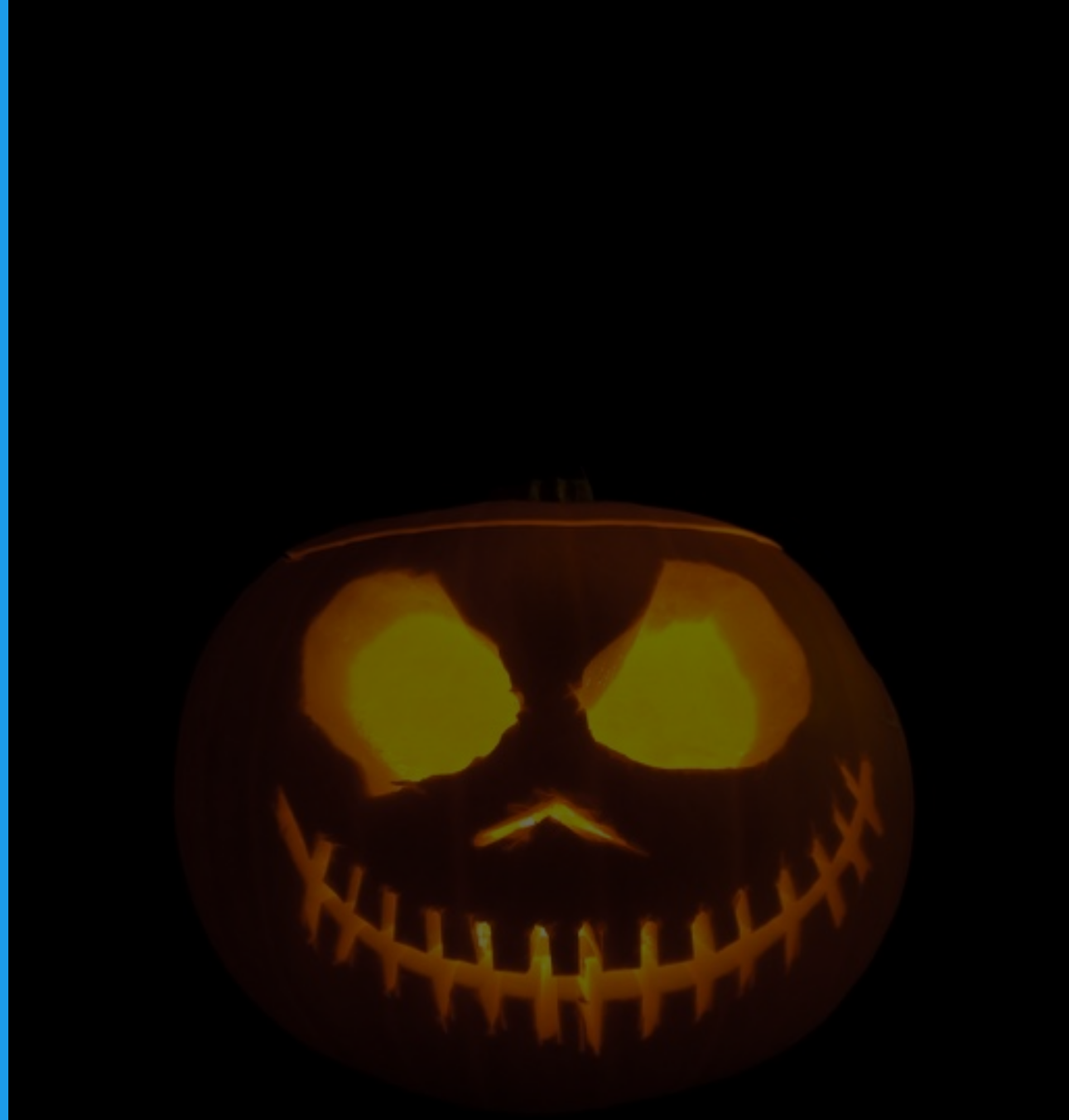
Follow us on Twitter @GOTOber

www.gotober.com

ContainerSolutions

Microservices – a security nightmare?

GOTO Berlin - Dec 2, 2015
Maximilian Schöfmann
Container Solutions Switzerland



Jetzt reisen:

ZU LAST MINUTE-PREISEN!

HolidayCheck

Wer nicht checkt, reist dumm.

Autonomy

Security

microservices…

small, hence **many** services

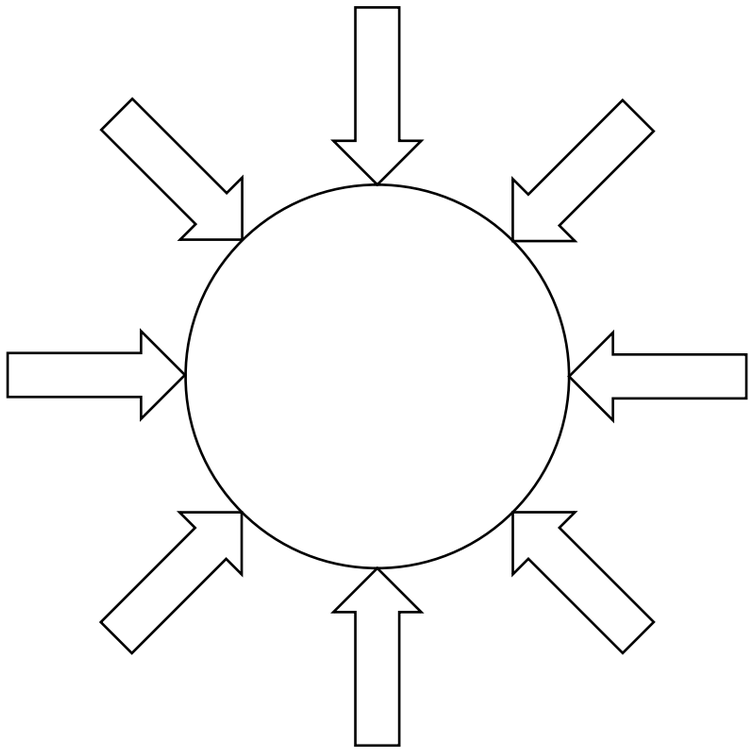
talking **over the network**

built **with different technologies**

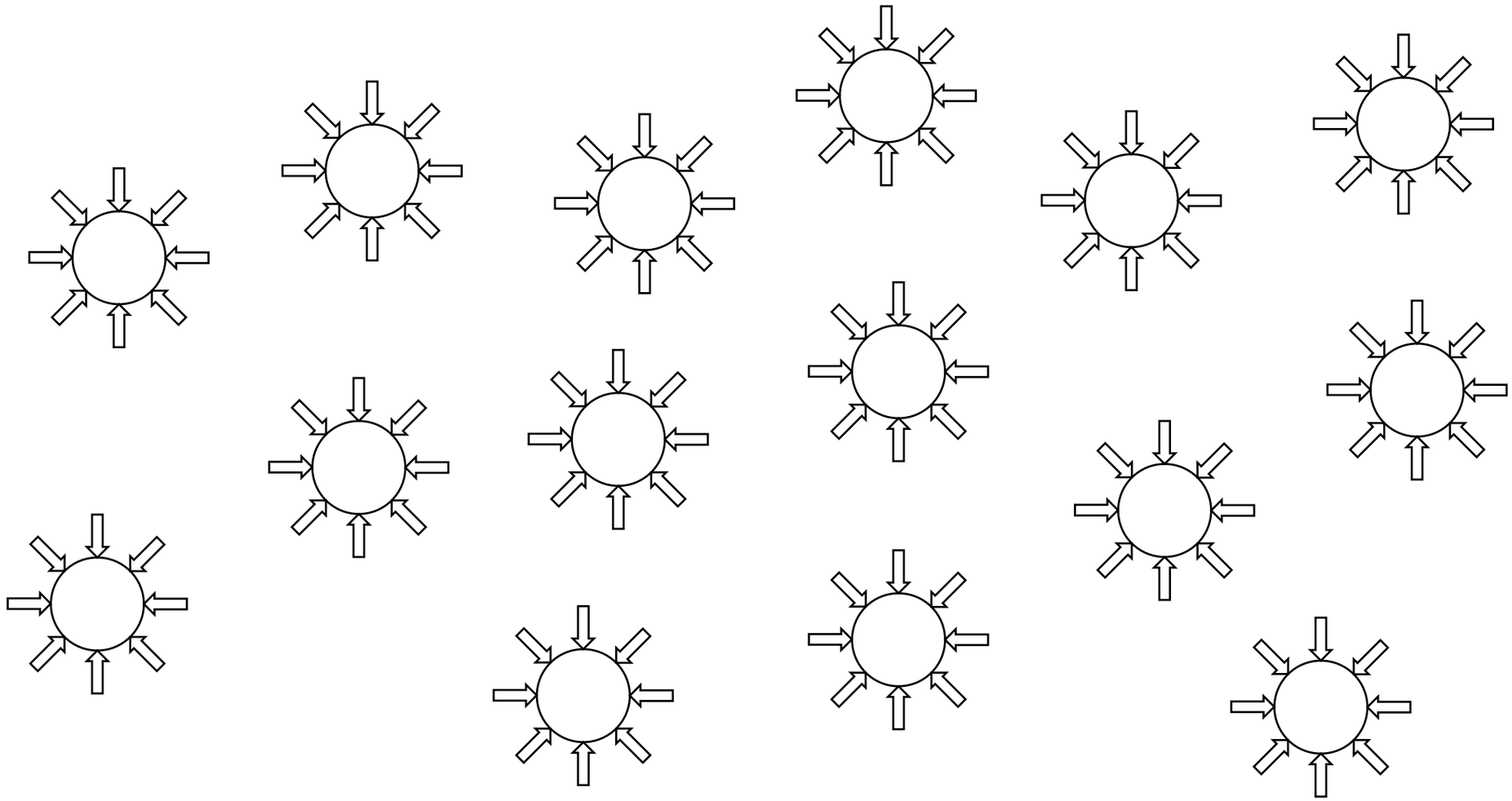
by **autonomous** teams with **end-to-end responsibility**

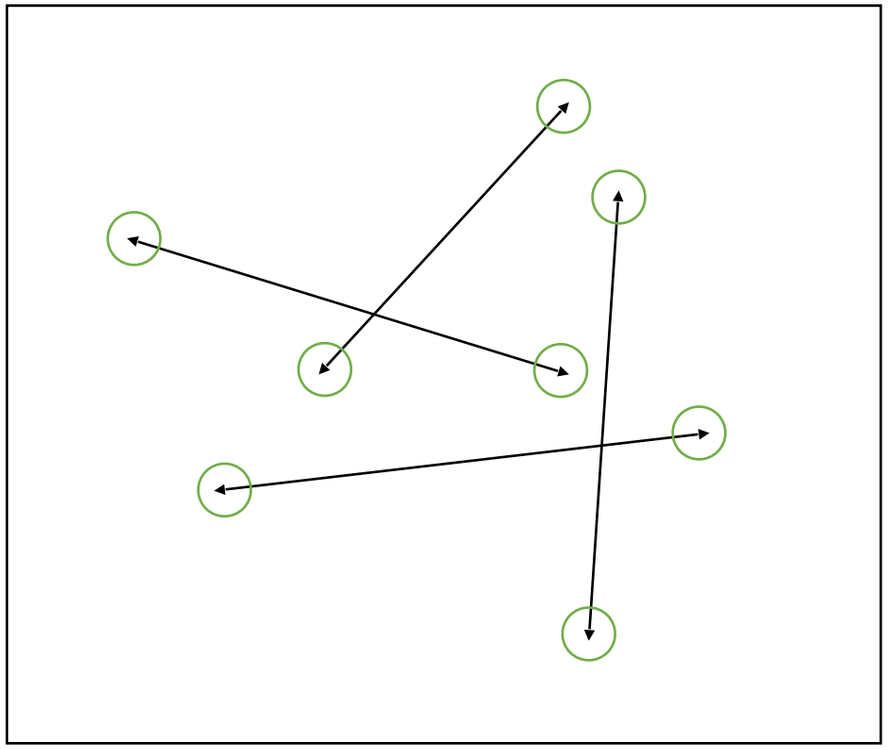
doing **DevOps** and **Continuous Delivery**

using **containers**

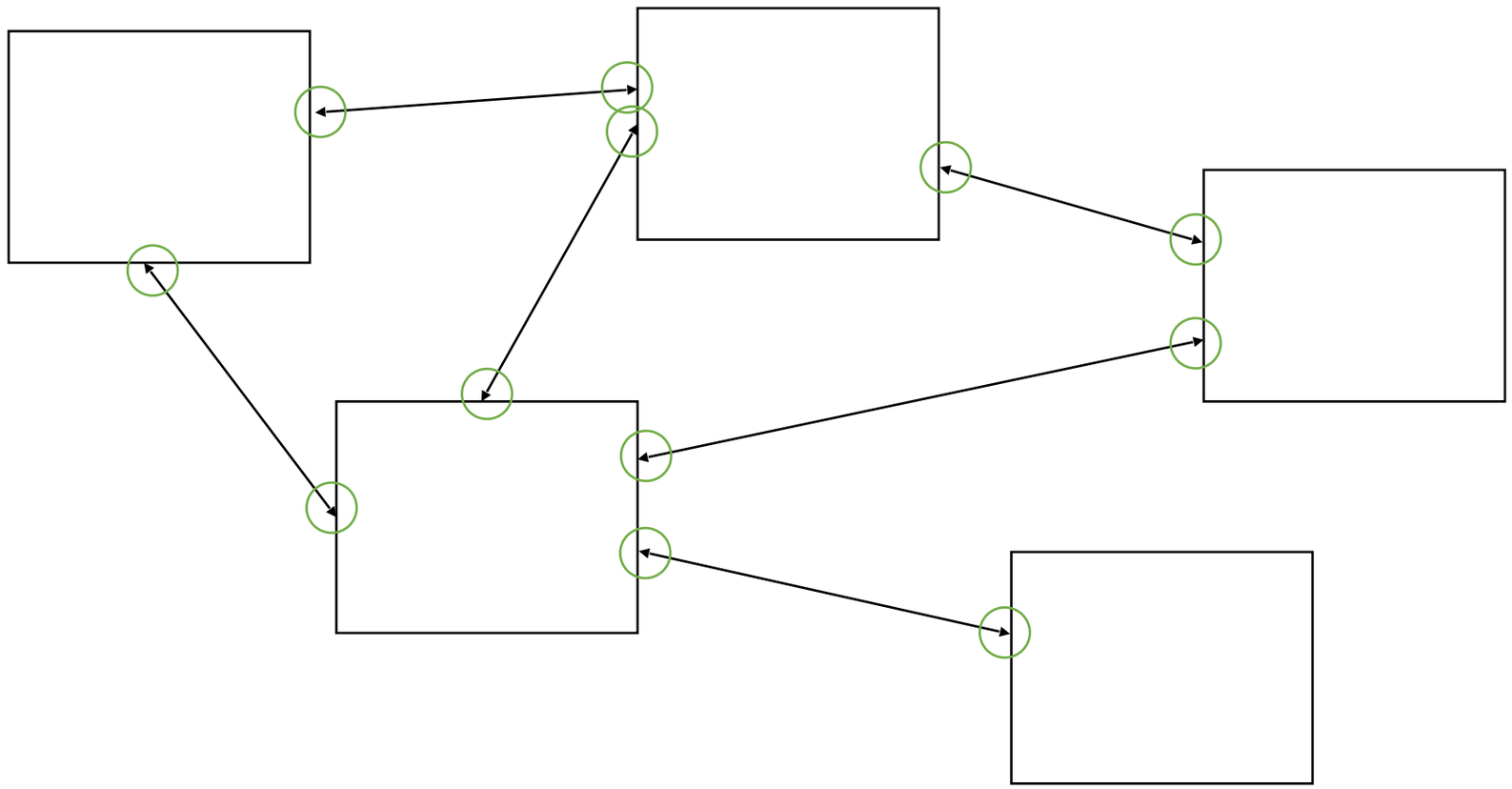


many small services





talking **over the network**



Java 7
(1.7.0_03)

built with **different technologies**

Java 8

nodejs
0.9

Java 7

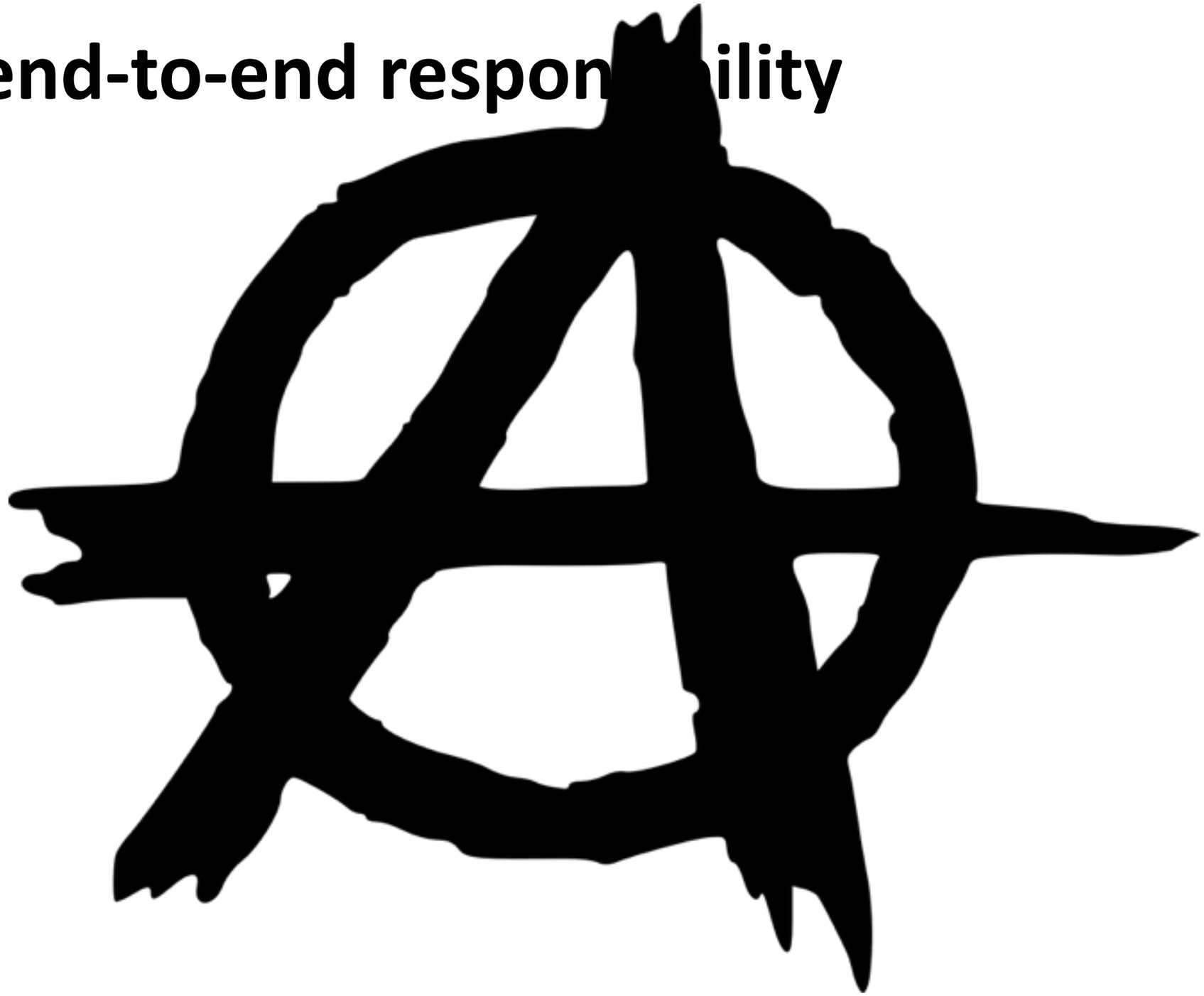
Ruby
2.1

Go 1.4


MICROSOFT

by **autonomous** teams

with **end-to-end respon ility**



(ISC)²®

doing **DevOps**


Specification
Implementation
Validation

and **Continuous Delivery**

using **containers**

using **containers**

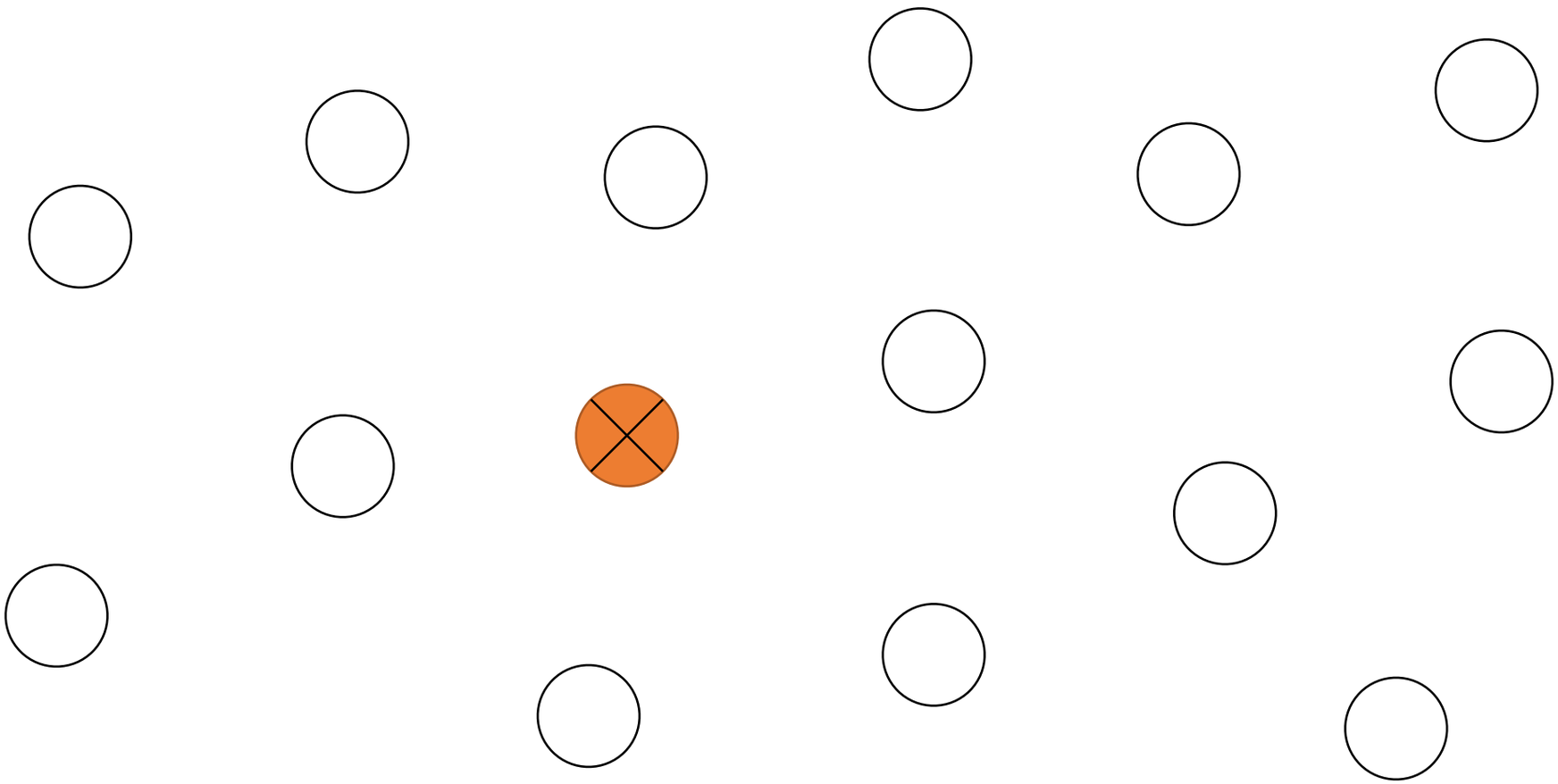
XEN Hypervisor - **10^5** LOC

Linux Kernel - **10^7** LOC

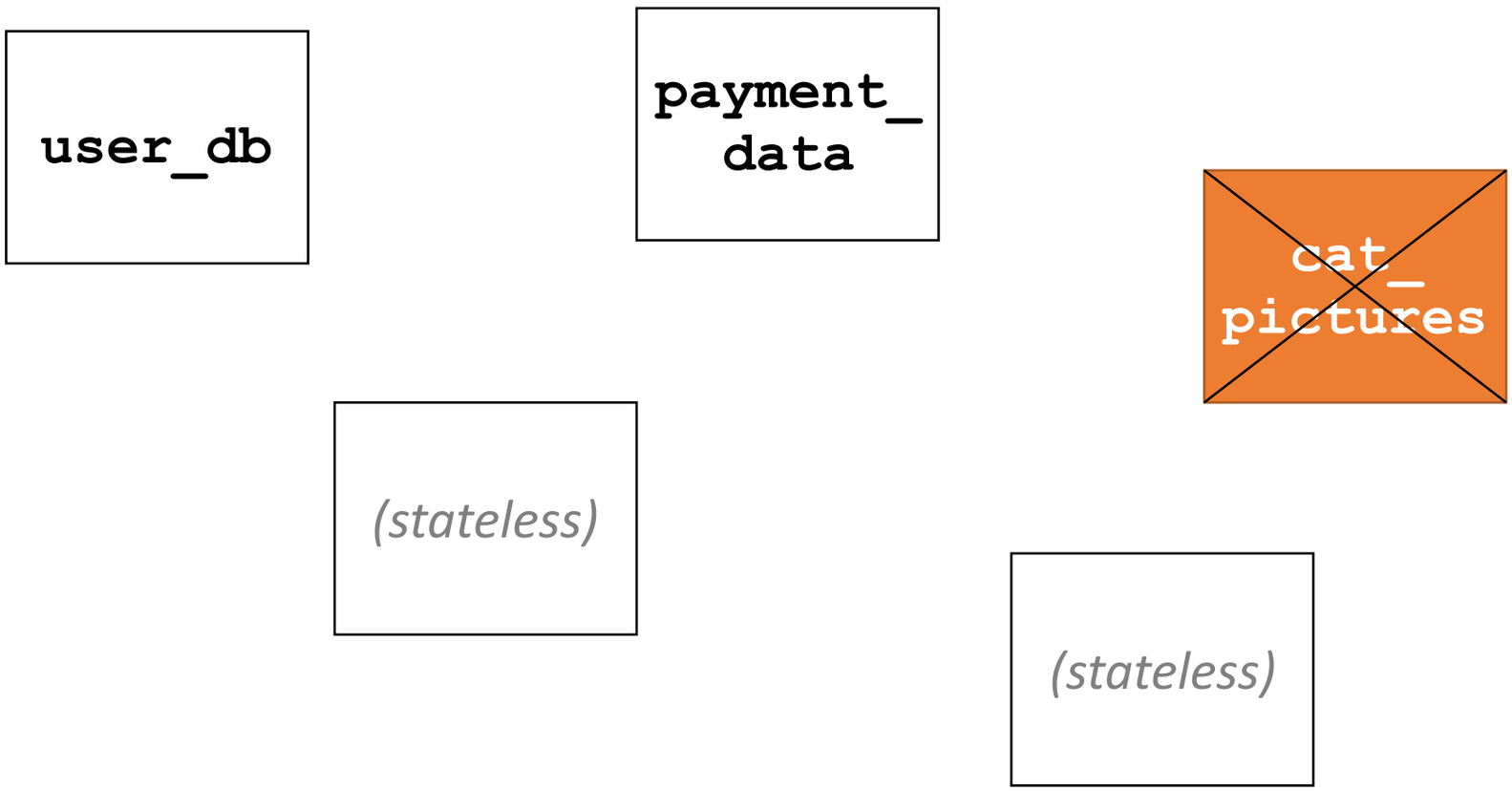
WELCOME TO YOUR NEW NIGHTMARE.

A NIGHTMARE ON ELM STREET

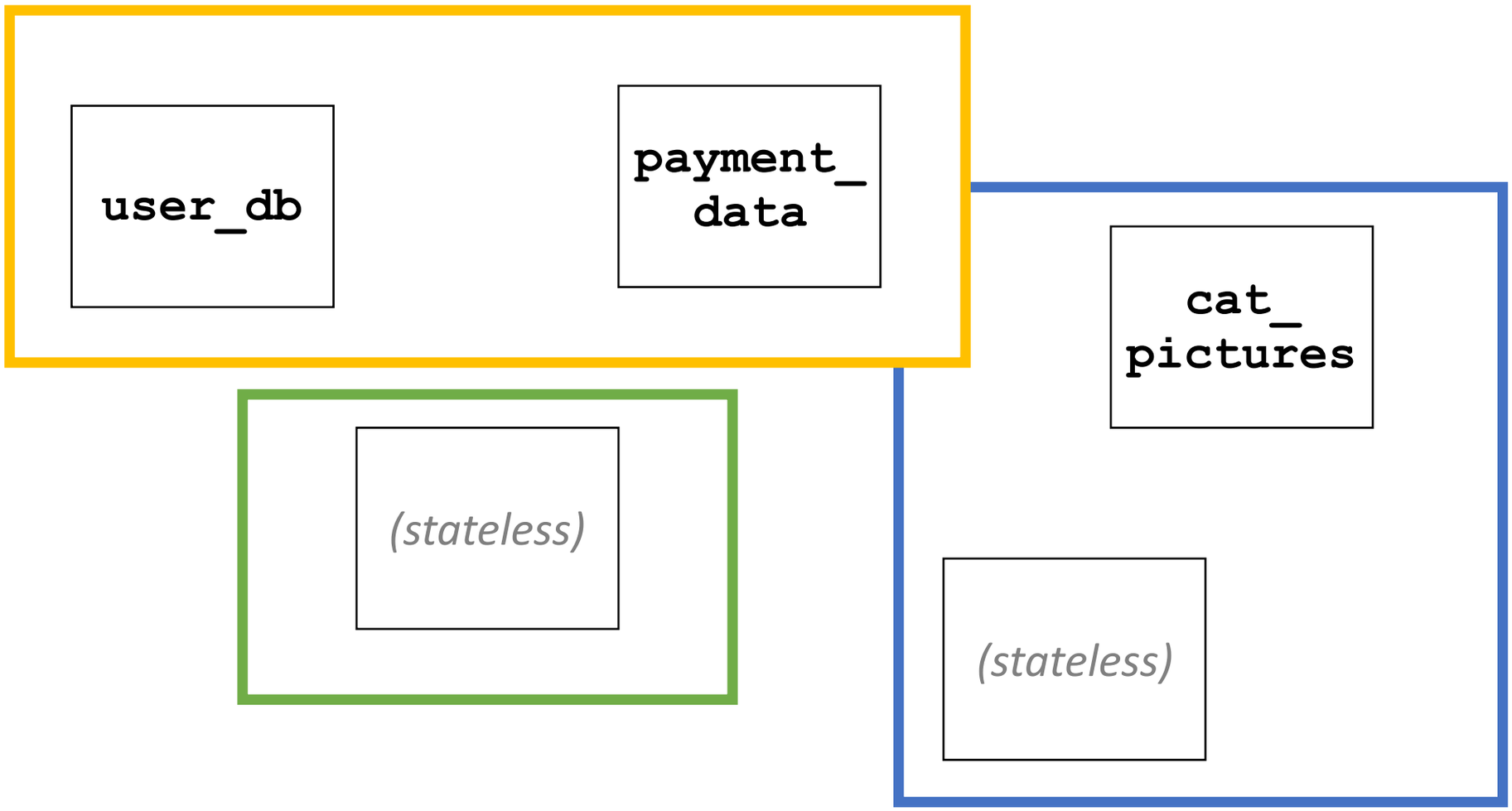
many small services



talking **over the network**



talking **over the network**



Authentication: Basic Auth

```
Authorization: Basic c21hcnRhc3MuLi4uCg==
```

Authentication: Client certificates

Authentication: API Keys

```
X-My-API-Key: YWxsIHVyIGJhc2UgYXJlIGJlbG9uZ3MgMiAgdXMK
```

Authentication: HMAC

```
Authorization: AWS FOOBR7EXAMPLE:frJIUN8h81ADYpKg=
```

Secrets management

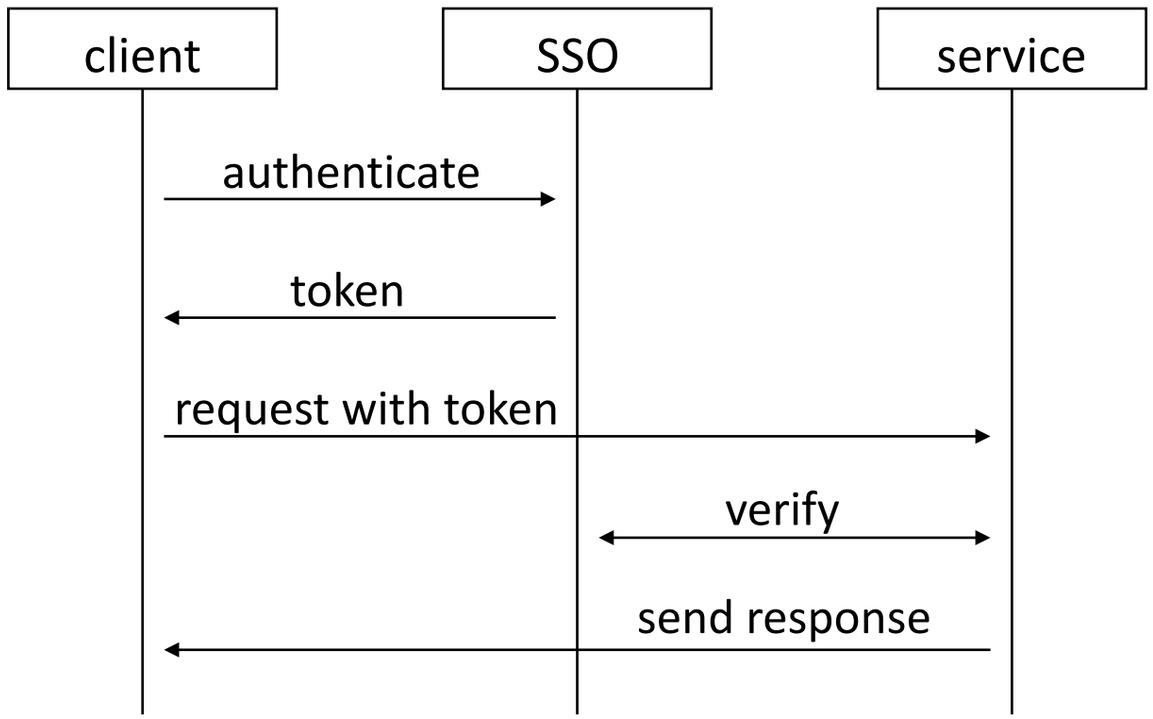
vaultproject.io

square.github.io/keywhiz

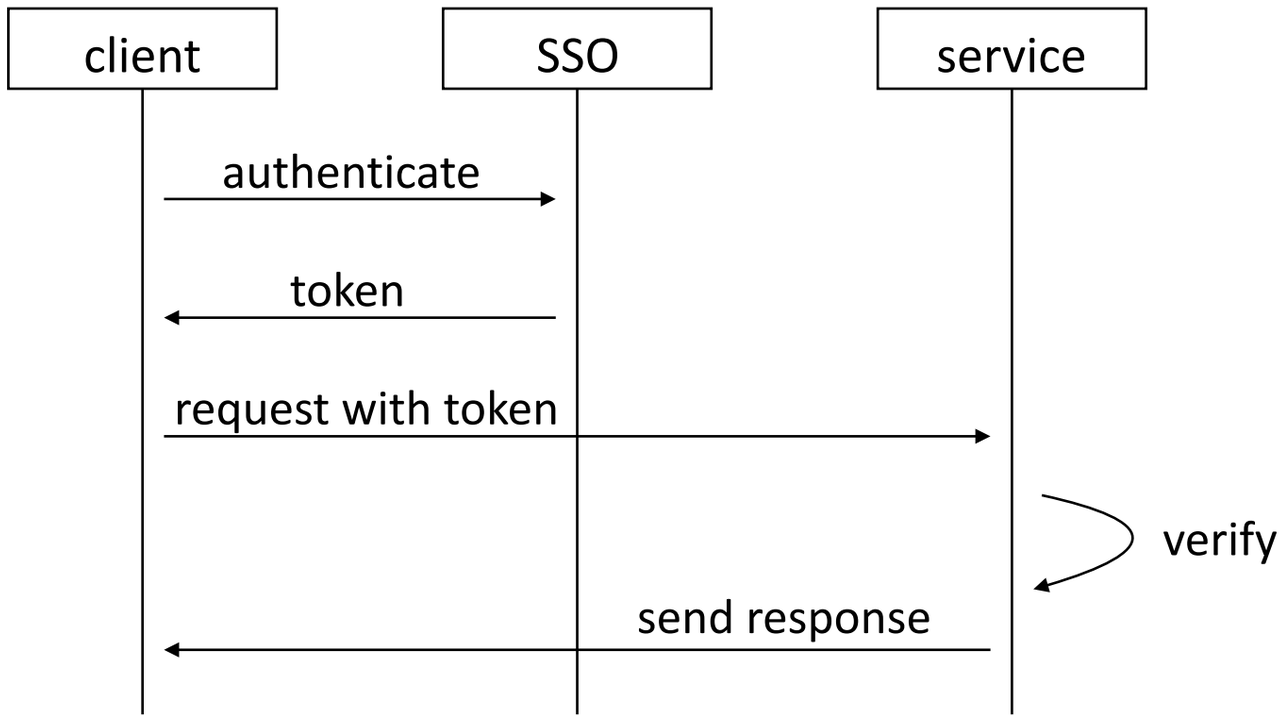
Single-Sign-On

SAML

Single-Sign-On



Single-Sign-On



Authorization

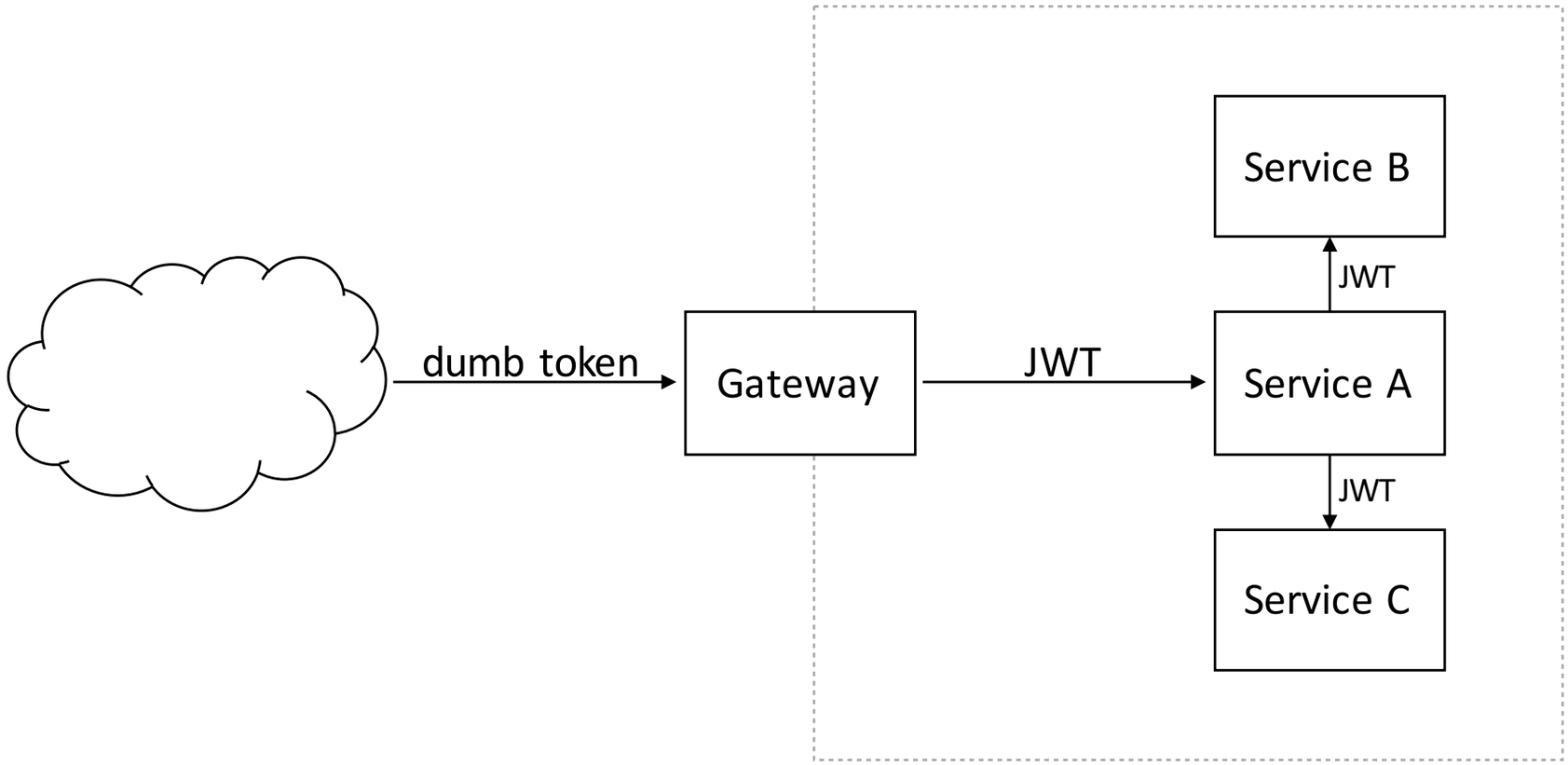
Authorization

```
{
  "iss":"myservice@developer.gserviceaccount.com",
  “scope”:”https://www.googleapis.com/auth/bigquery",
  "aud":"https://www.googleapis.com/oauth2/v3/token",
  "exp":1328554385,
  "iat":1328550785
}
```

ID Tokens

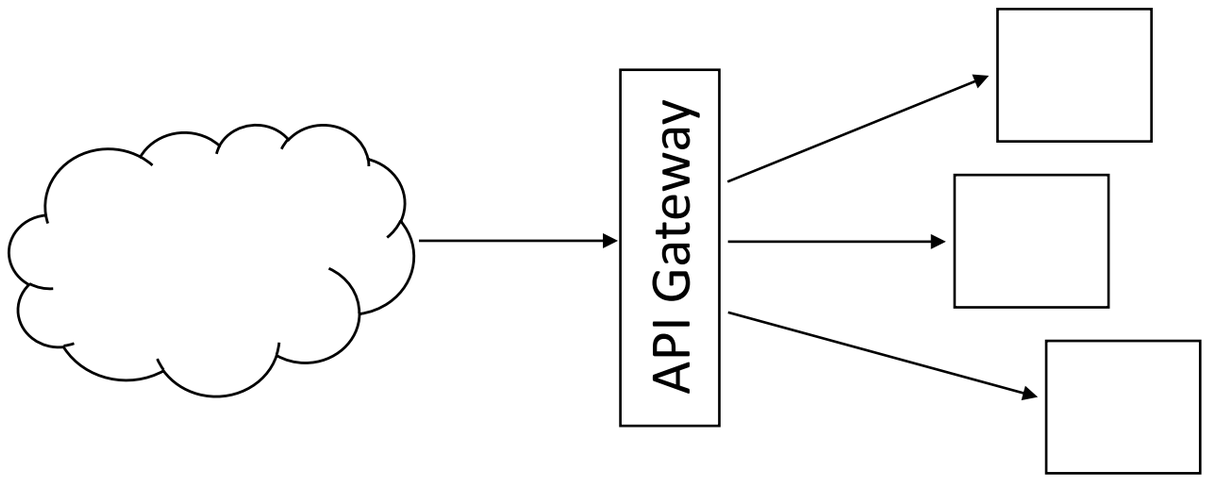
```
{
   "sub"                                  : "bob",
   "email"                                : "bob@example.com",
   "name"                                 : "Bob Example”,
   “exp"                                  : 1328672194,
   "https://mycorp.tld/groups": ["admin", "publisher"]
}
```

Translating ID Tokens



The Confused Deputy

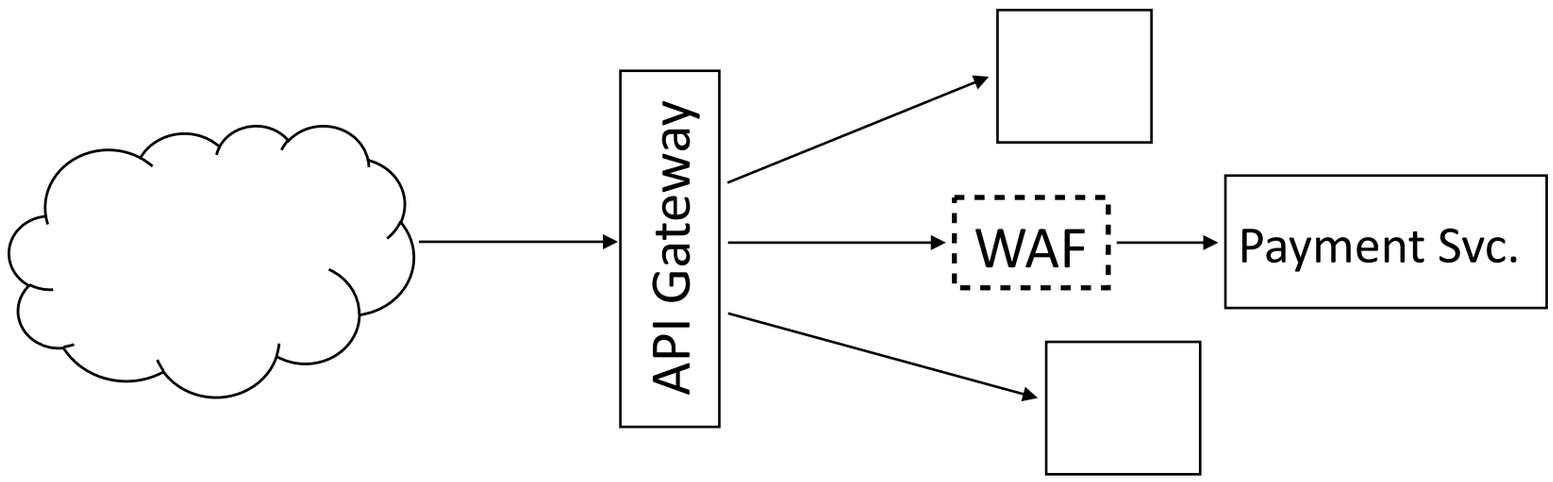
API Gateways



- Access control
- Rate limiting
- HTTPS termination

. . .

API Gateways



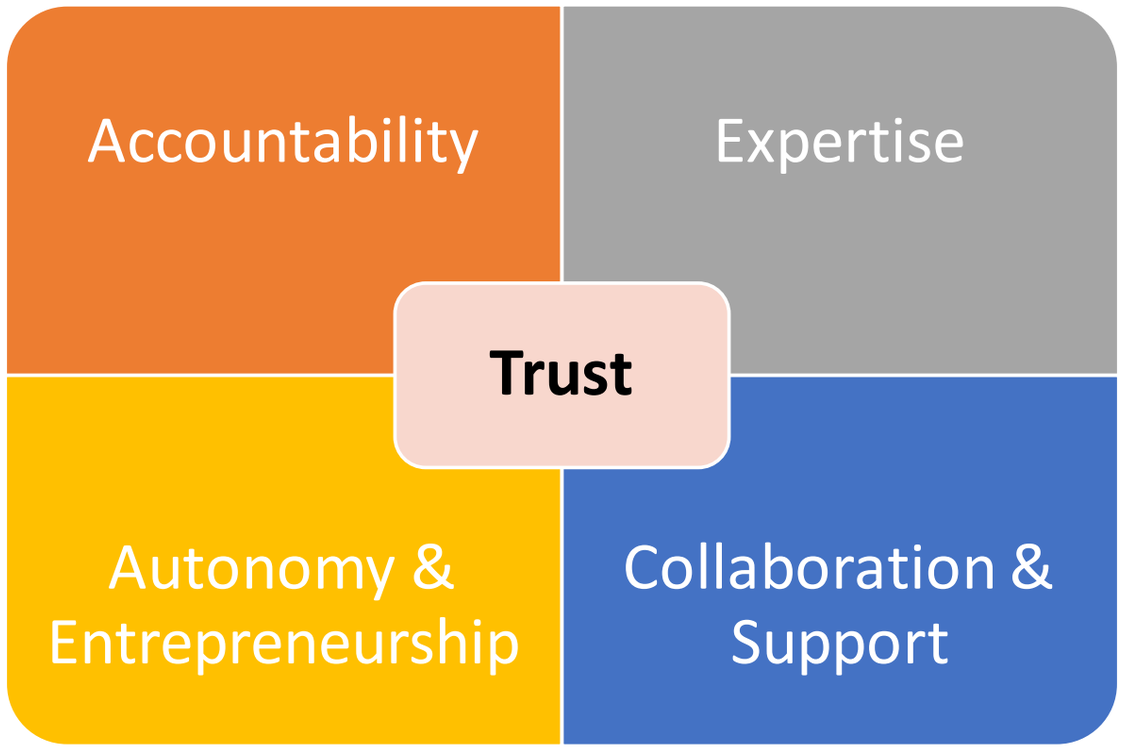
built with **different technologies**

by **autonomous** teams

with **end-to-end responsibility**

by **autonomous** teams with **end-to-end responsibility**

Trust



Idea from A.T. Kearny Analysis

by **autonomous** teams with **end-to-end responsibility**

Definition of Done

“It’s not done, before it’s fast!”

by **autonomous** teams with **end-to-end responsibility**

Definition of Done

“It’s not done, before it’s secure!”

by **autonomous** teams with **end-to-end responsibility**

Rugged Software Manifesto

ruggedsoftware.org

doing **DevOps**

SecDevOps?

SecOps?

DevSec?

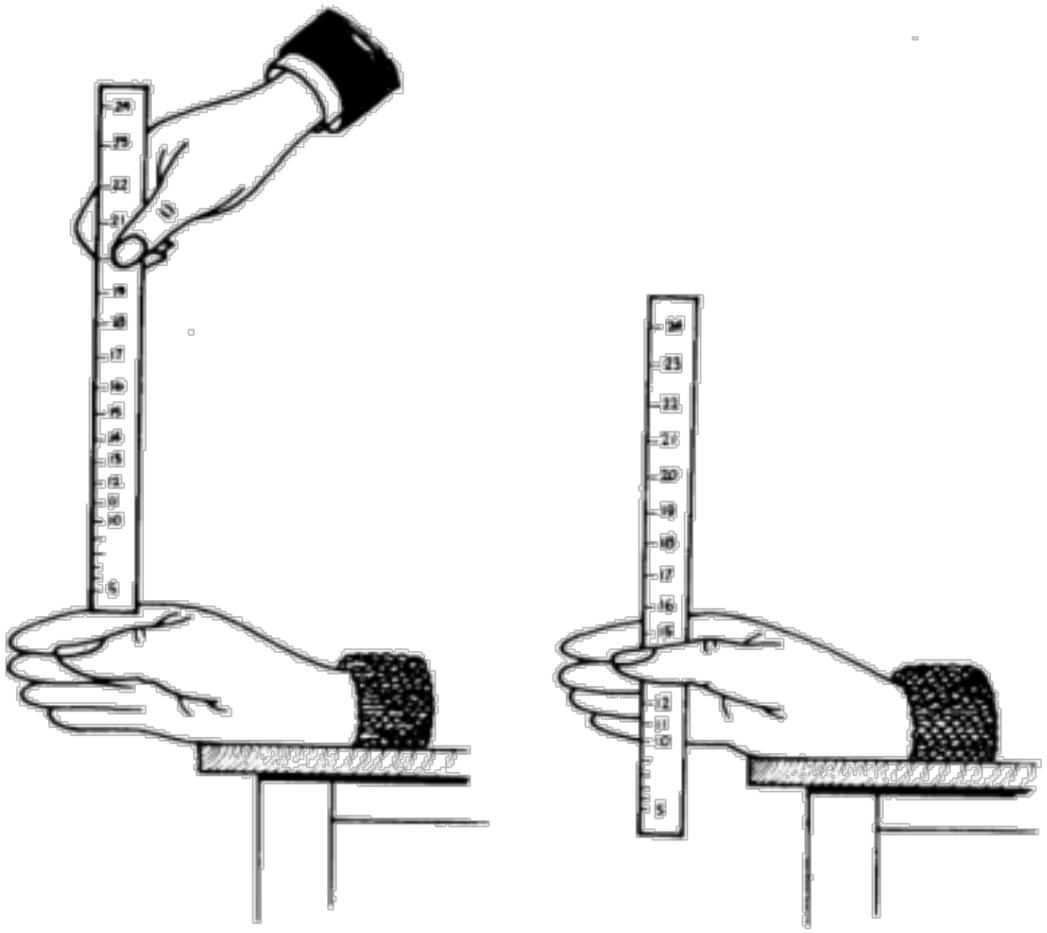
doing **DevOps**

SecDevOps

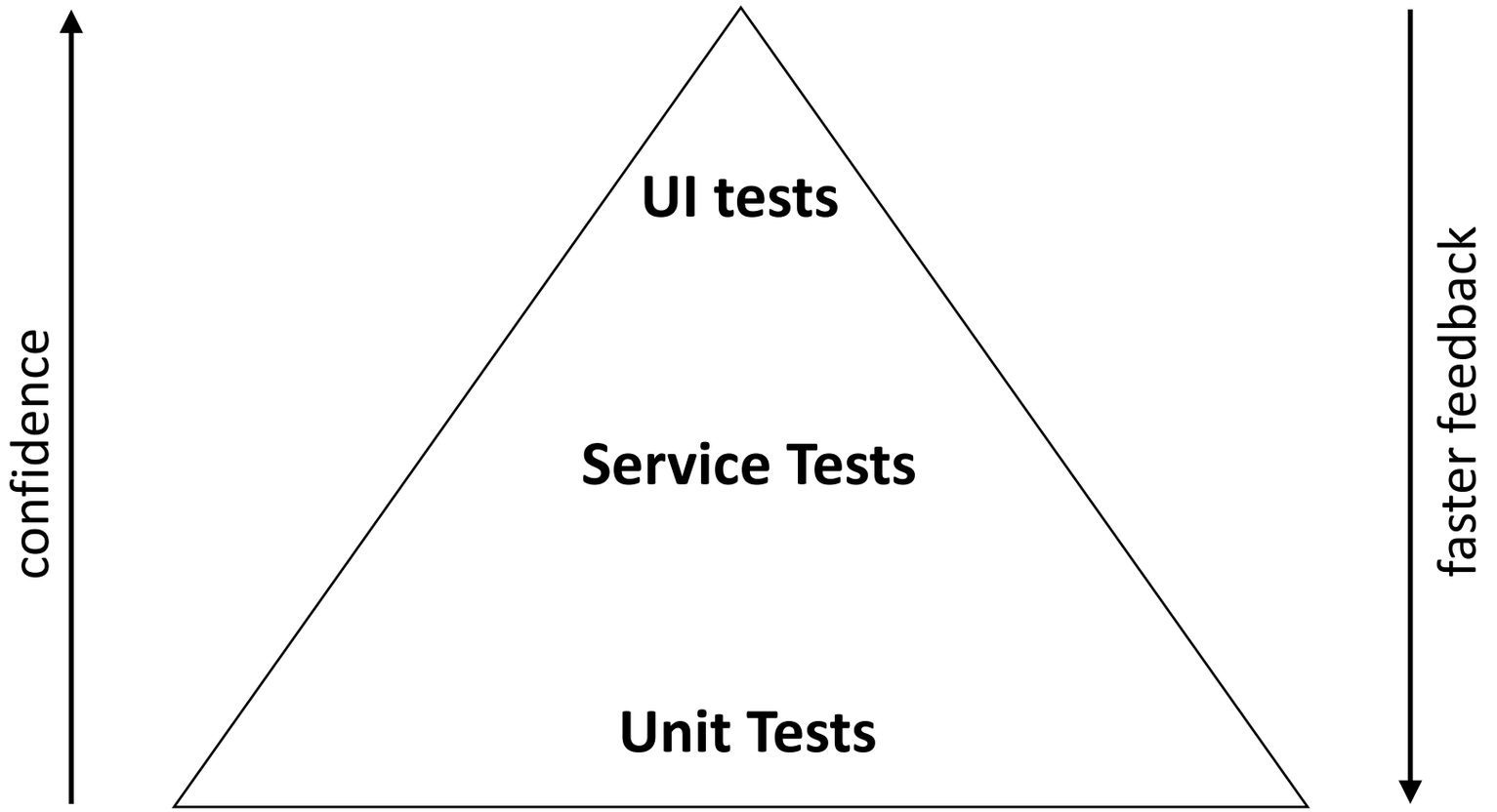
=

Mindset + Tooling

and **Continuous Delivery**

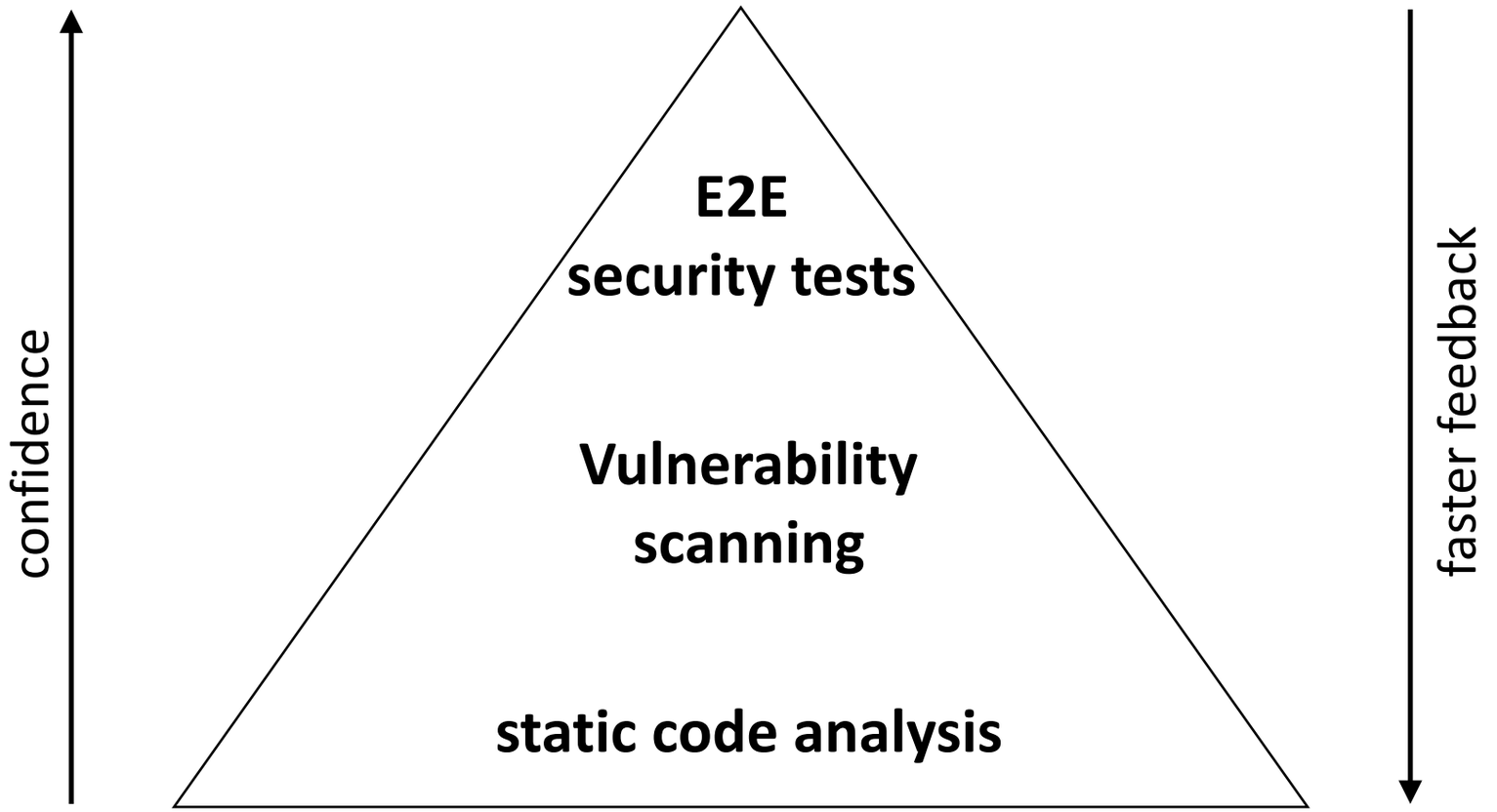


Test pyramid



from "Succeeding with Agile" (Mike Cohn)

Security-Test pyramid

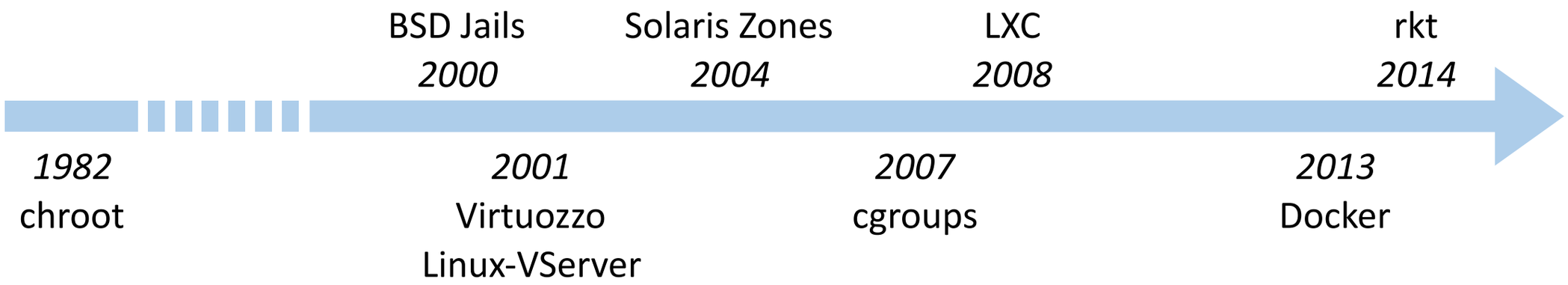


BDD style

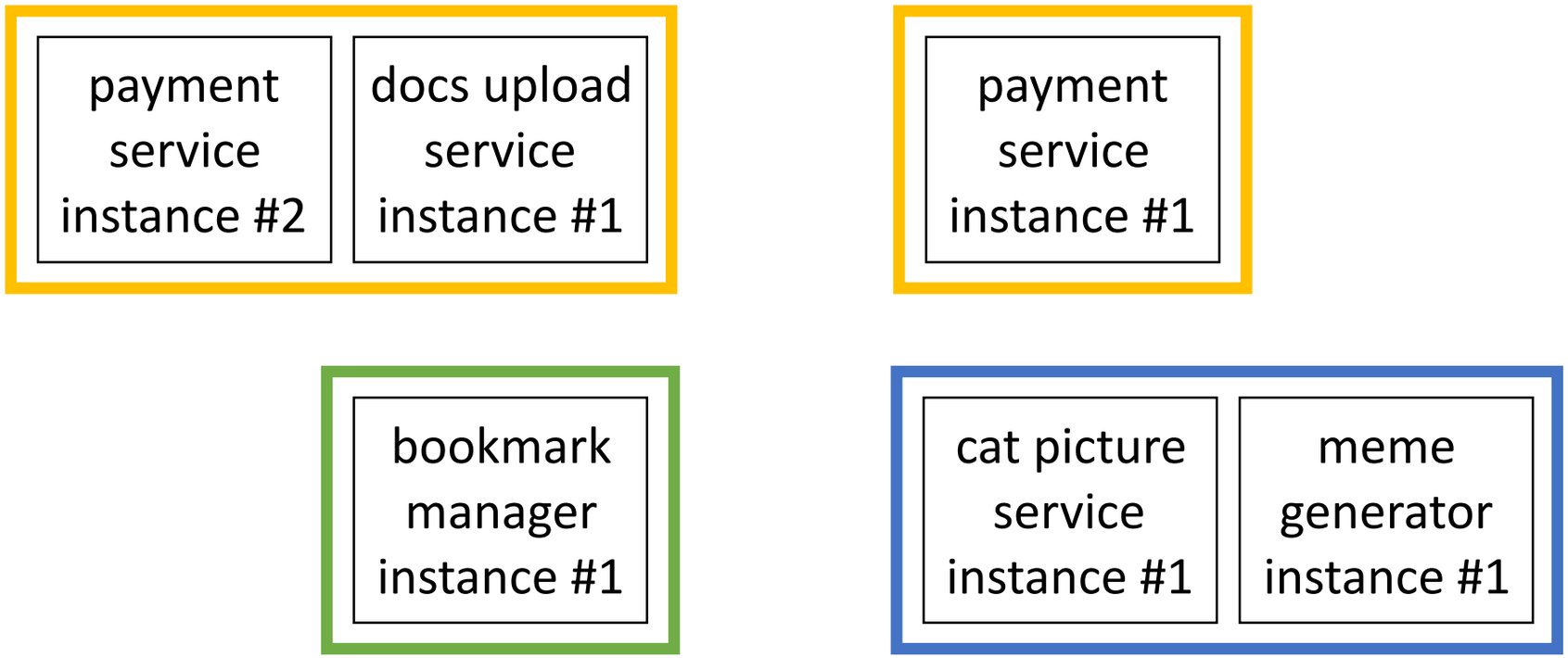
```
Scenario: Passwords should be case sensitive
Meta: @id auth_case
When the default user logs in with credentials from: users.table
Then the user is logged in
When the case of the password is changed
And the user logs in from a fresh login page
Then the user is not logged in
```

continuumsecurity.net/bdd-intro

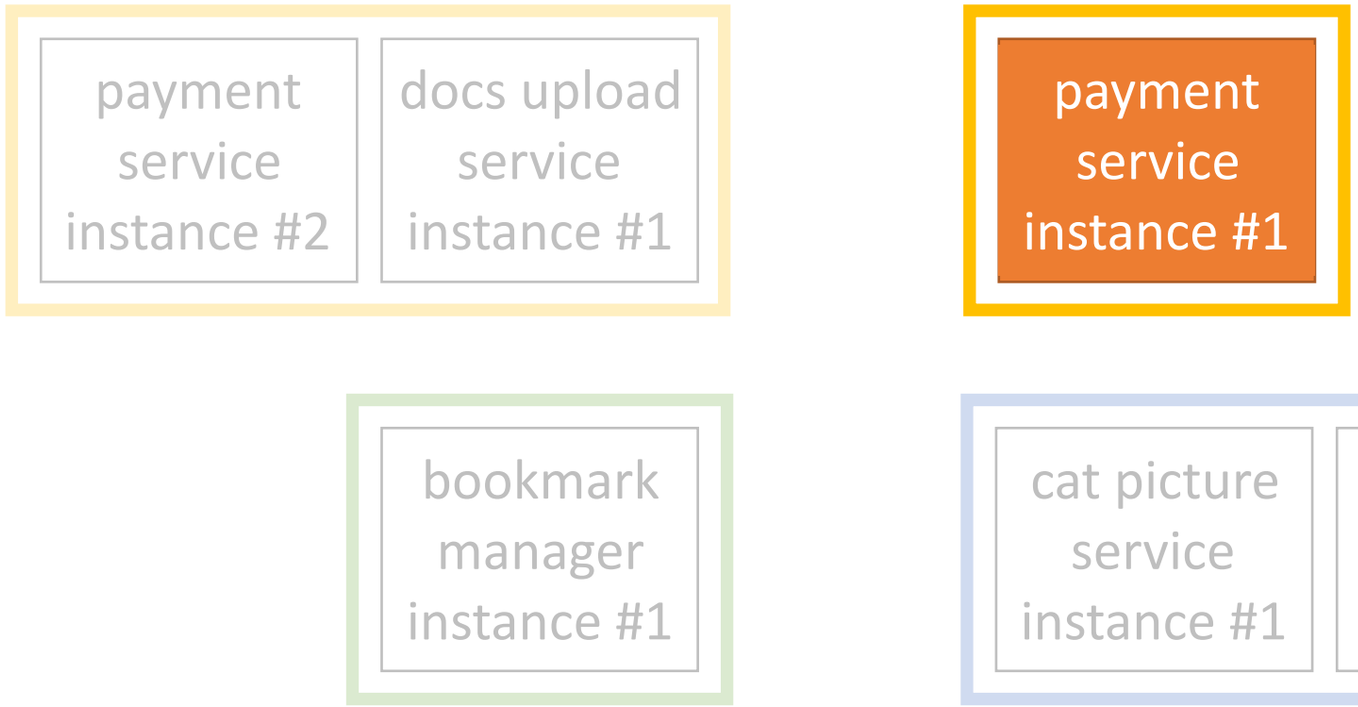
using **containers**



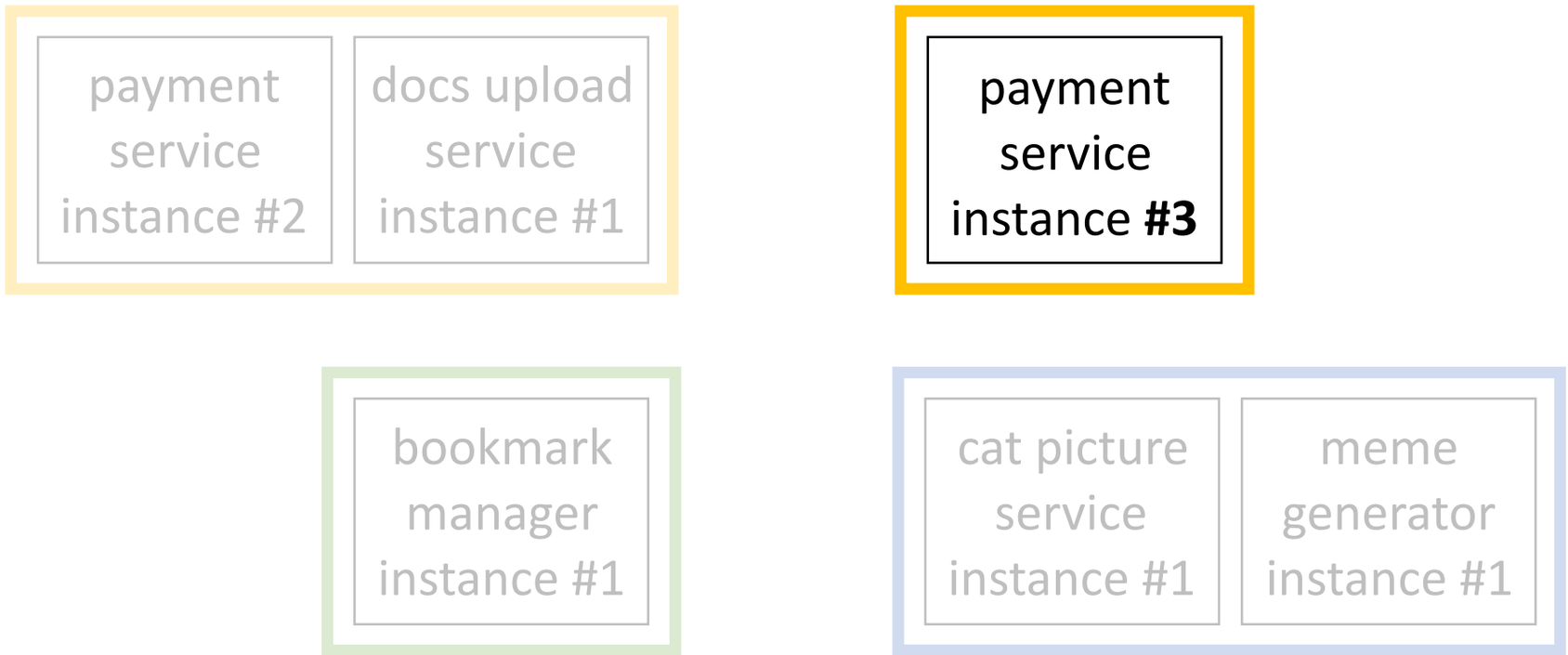
Defense in depth



Freeze & replace



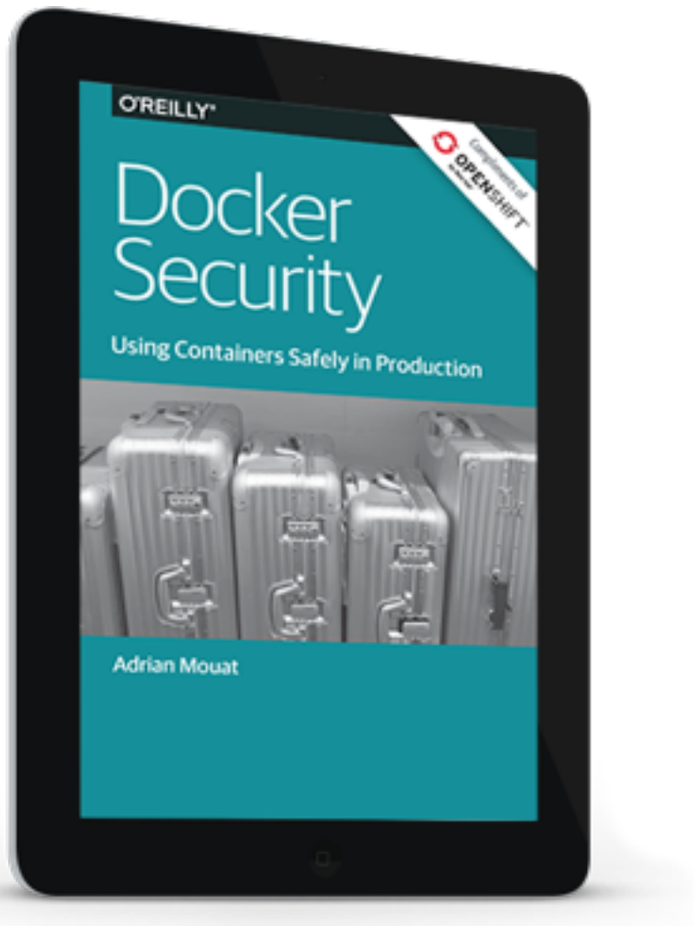
Freeze & replace



Docker security

- read-only containers
- minimal base images
- drop capabilities
- verify signed images
- traditional hardening
  (AppArmor, SELinux…)

. . .



tinyurl.com/docker-security

Scan images for vulnerabilities

Nautilus (Docker Inc.)

Clair (CoreOS)

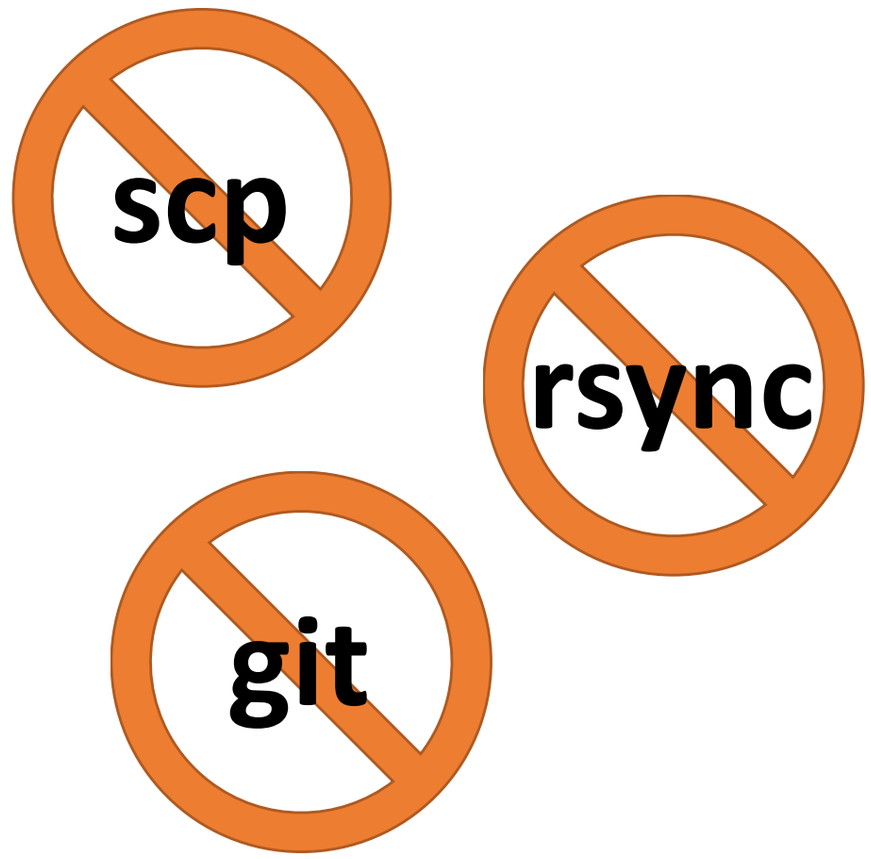
Twistlock

Scalock

Secure deployments

Docker daemon - “just HTTP”

- TLS
- Authentication
- Authorisation
- Logging & Auditing



Summary

small, distributed services can
limit the impact of breaches

isolate services with different
security requirements

use **standard mechanisms for auth**,
but make sure they are scalable

consider an **API gateway**,
but **don't overuse** this pattern

Summary

monocultures can do harm

embrace **rugged software** principles

accountability ensures **security is built in**,
not bolted on

invest in **automation and tooling**
around security tools and security testing

Summary

use containers as **additional line of defense**

use containers as **immutable infrastructure**

if you need to, use containers to do **forensics**

secure your container **hosts** thoroughly

scan images centrally for vulnerabilities

abolish obsolete **deployment** methods

Nightmare?

Image References

(all CC-BY or public domain)

Pumpkin:
https://www.flickr.com/photos/wwarby/5144858705

Bill Gates:
https://c2.staticflickr.com/8/7331/16335705267_b6e9d9b223.jpg

Anarchy Symbol:
https://pixabay.com/p-32917/

Sandwich:
https://upload.wikimedia.org/wikipedia/commons/6/6a/Peanut-Butter-Jelly-Sandwich.png

Wasp:
https://pixabay.com/p-538470

Whack-a-mole:
https://c1.staticflickr.com/9/8484/8195620894_4b68d7df76_b.jpg

Rusty container:
https://www.flickr.com/photos/annspan/3912153466

Server:
https://upload.wikimedia.org/wikipedia/commons/0/0c/Chassis-Plans-3U.jpg

Rugged vehicle:
https://c1.staticflickr.com/5/4036/4669861882_742023ed7a_b.jpg

Certificate:
https://pixabay.com/p-576790

Confused Deputy:
https://en.wikipedia.org/wiki/Confused_deputy_problem

Aphid:
https://en.wikipedia.org/wiki/Aphid#/media/File:Acyrthosiphon_pisum_(pea_aphid)-PLoS.jpg

container-solutions.com

goto; conference

Please

Remember to rate session

Thank you!

Follow us on Twitter @GOTOber

www.gotober.com