facebook

Security as a Service

Wojciech Wojtyniak

Production Engineer

Who are you?

Why Security?

It’s not only about corp anymore

And it never was

- The days of clear separation are gone
- If attacker is after your data, prod is your main concern
- If you live in cloud, the Internet might be your prod network

New challenges

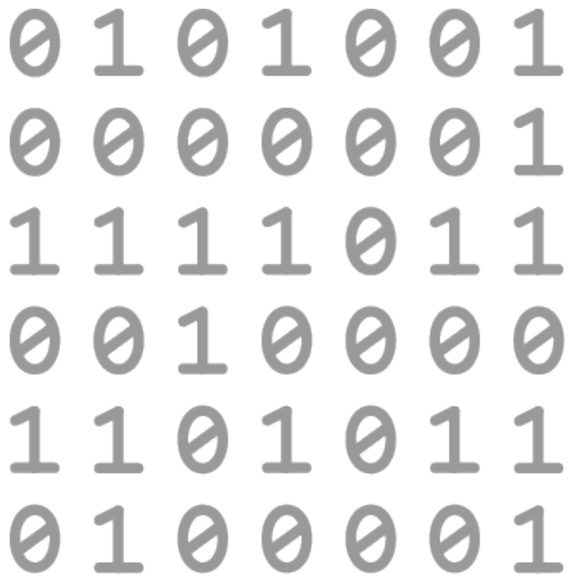
- CI and CD let you to deploy new vulns faster than ever
- Credential management for cloud services

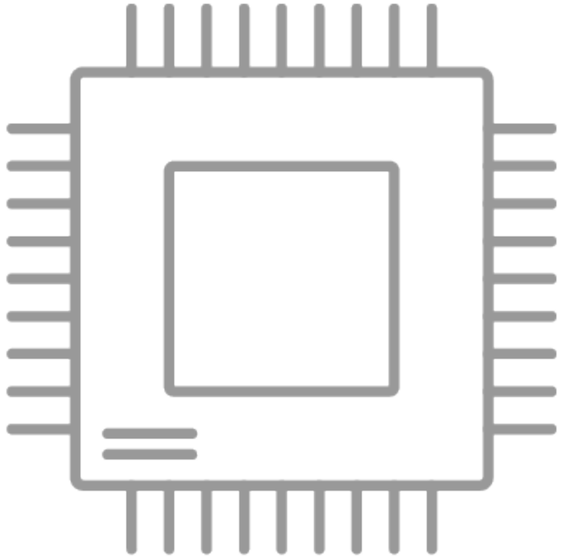
Is this really a job for SRE?

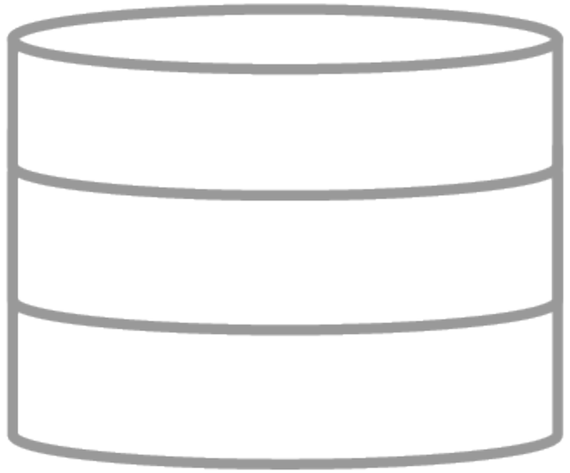
YE

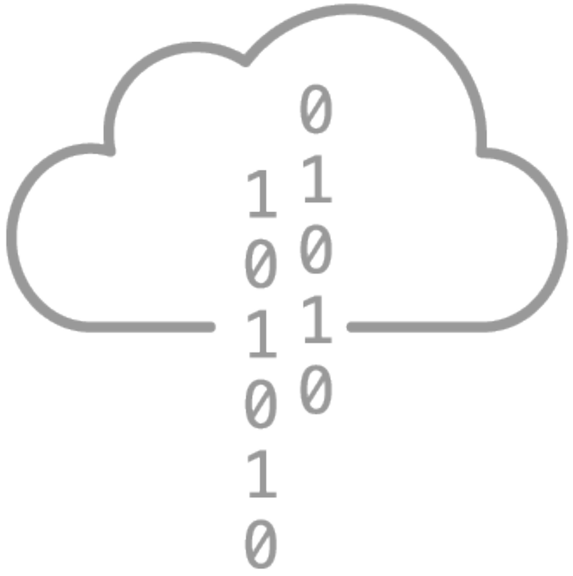
Is this really a job for SRE?

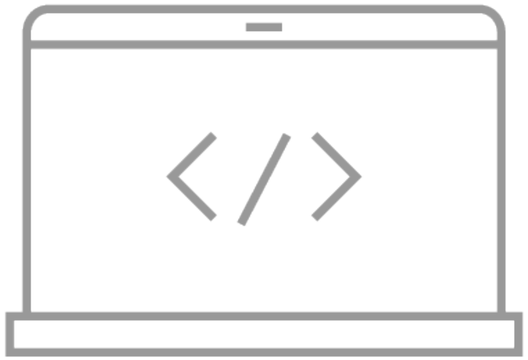
S


0 1 0 1 0 0 1
0 0 0 0 0 0 1
1 1 1 1 0 1 1
0 0 1 0 0 0 0
1 1 0 1 0 1 1
0 1 0 0 0 0 1

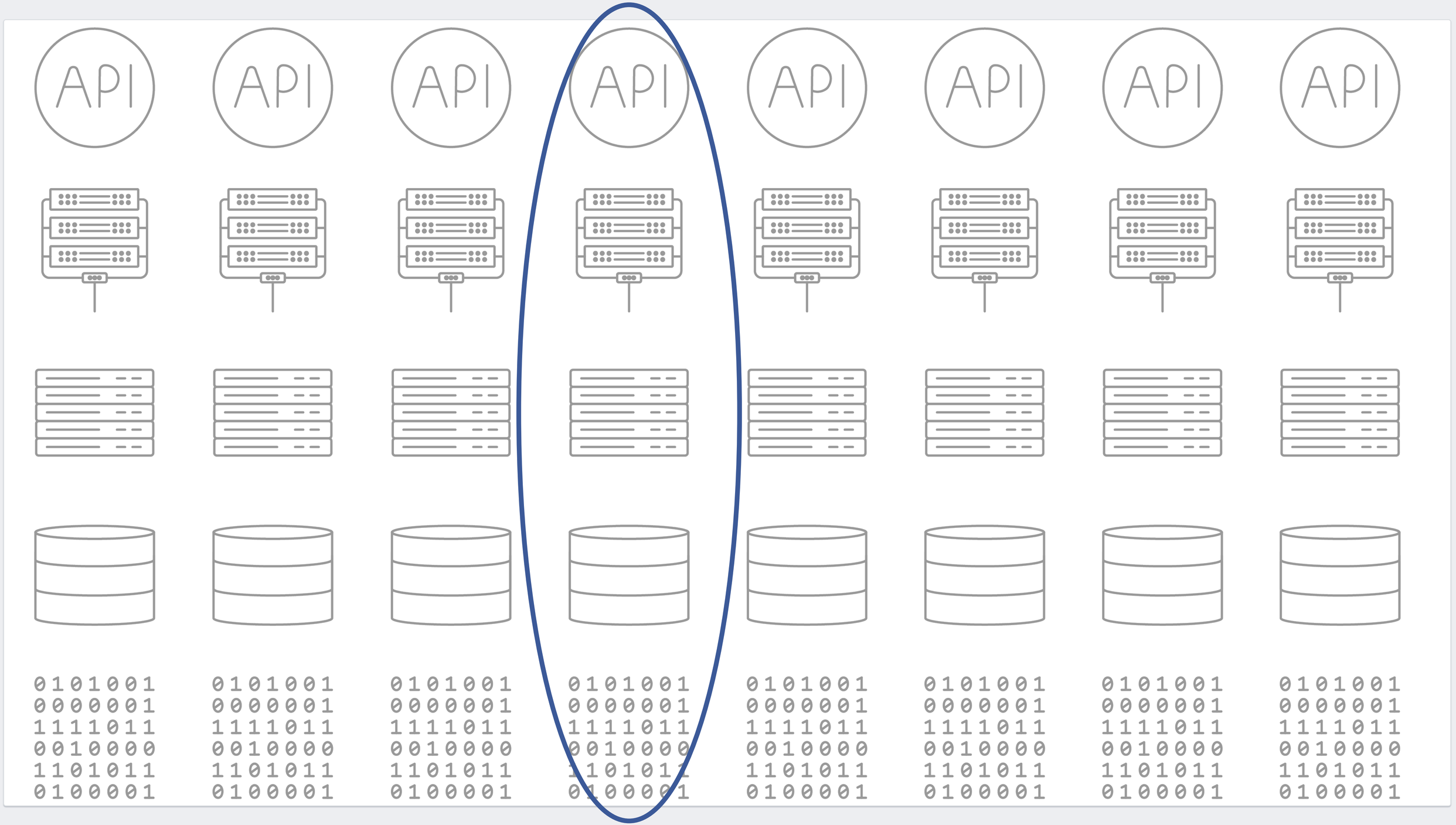


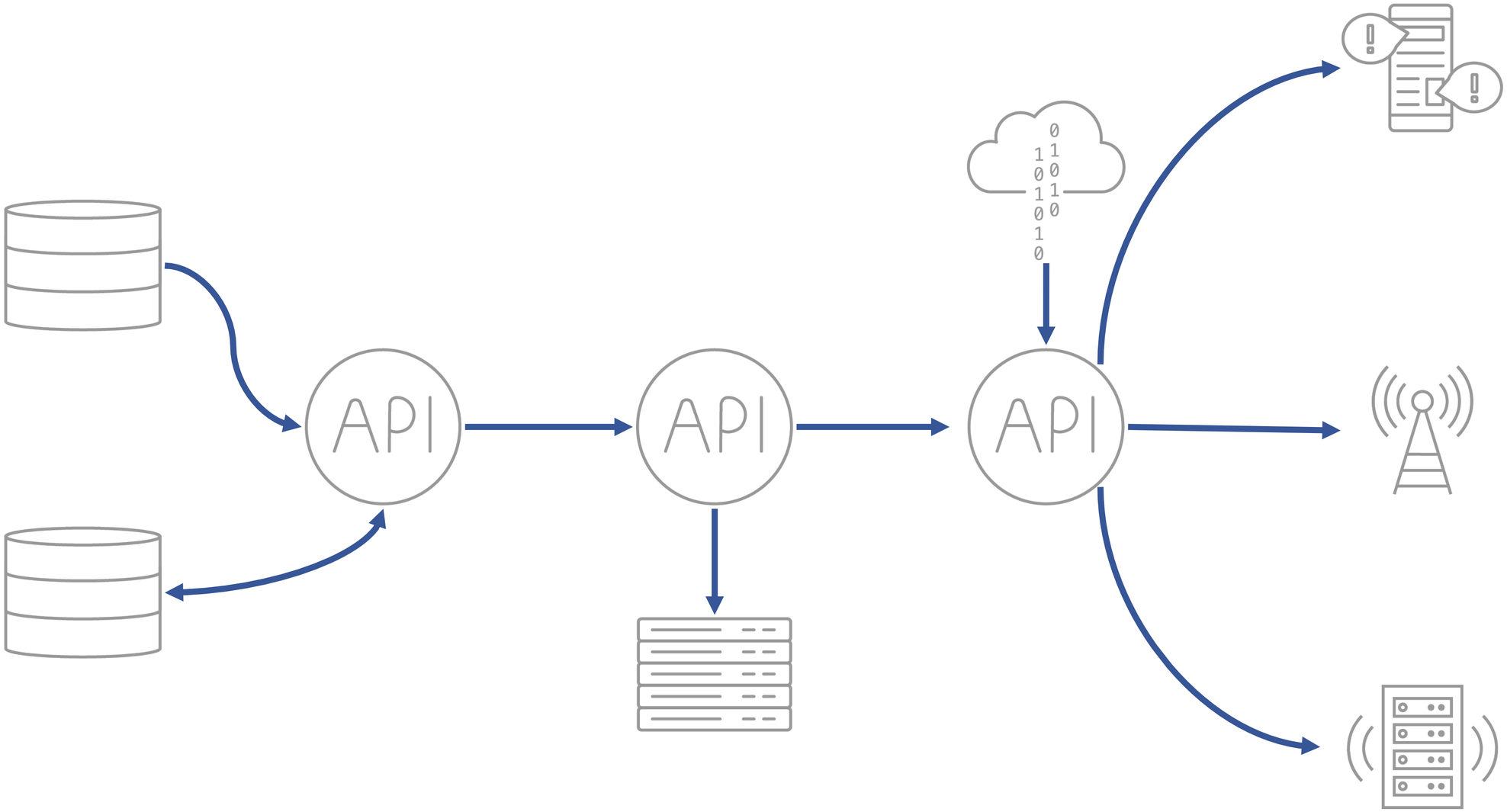



0
1 1
0 0
1 1
0 0
1
0




API


API
API
API
API
API
API
API
API
0101001
0000001
1111011
0010000
1101011
0100001


API
API
API
0
1
0
1
0
1
0
1
0
1
0
1
0
1
0
1
0
1
0

Security is a property of a system

Not its particular parts

Its main forte of PE teams to understand the whole stack

Security is no different

Support DBs, support networking, support the whole stack

- PE/SREs supporting database teams know thing or two about DBs
- Same goes for cache, webservers, proxy…
- … and security

There’s no Security in SRE

Is there Reliability without Security?

Security and reliability go hand in hand; if a service gets compromised and rendered useless (either due to loss of data or users' trust) there's no reliability to talk about

Your expertise is much needed

As if you didn’t know this already…

- Automatization
- Updates at scale
- Monitoring & Alerting
- Disaster recovery
- Systems accounting

How to engage?

Running security services

- All Open Source you can find in your infra
- SSH, Kerberos, LDAP
- Secrets’ broker
- Make sure they’re reliable

Building missing services

Arm in arm with your best friends - SWEs

- Authorization and Authentication services
- ACLs
- Secrets management
- Literally anything you need to provide full-stack

Internal consulting

- Leveraging security infra is like leveraging any other infra
- You have the best context already
- Drop in during the design phase of a new project

Managing dependencies

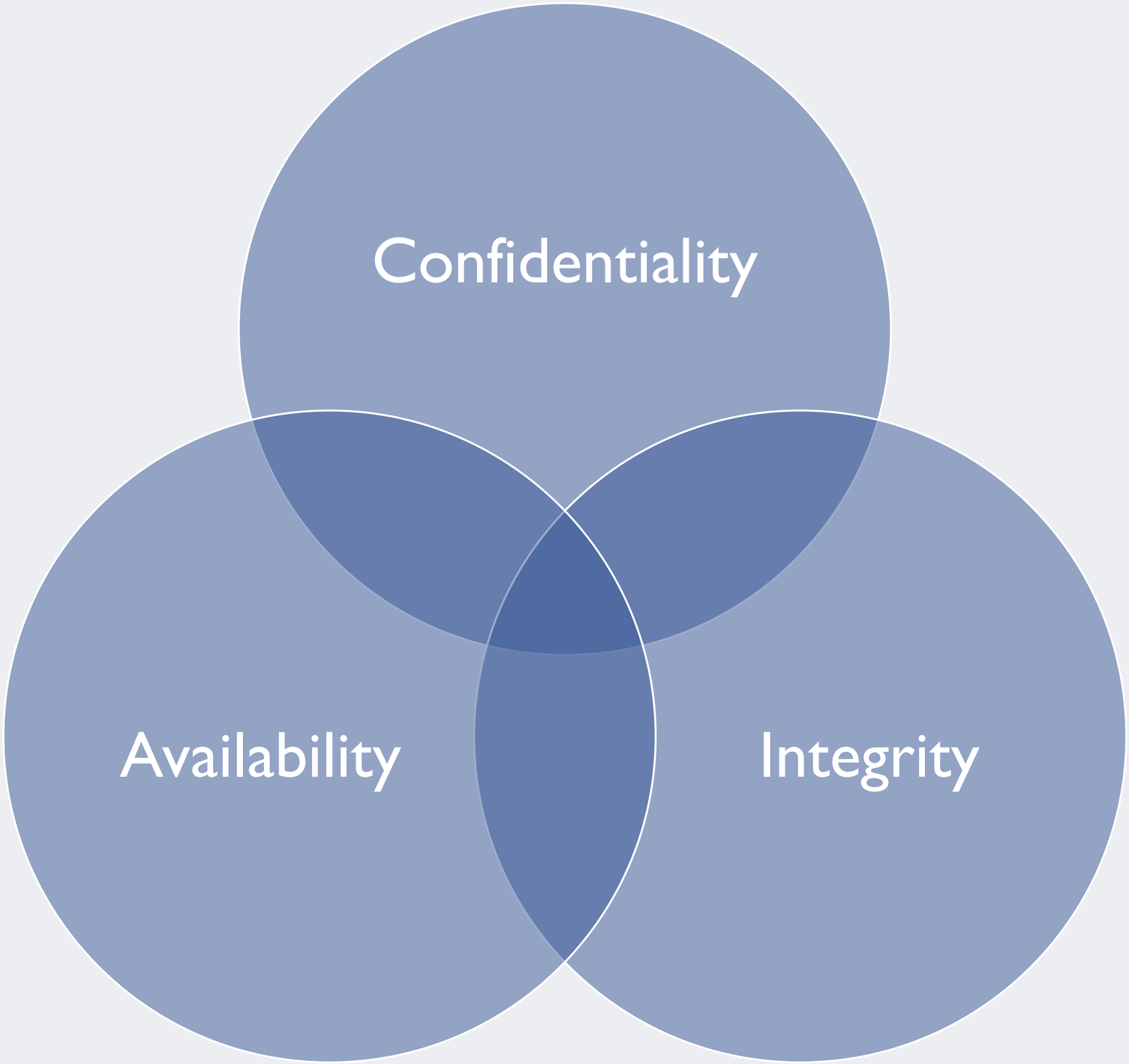
- Preventing circular dependencies
- Understanding changes happening in the whole stack

There’s no secret sauce

- Even with the best understanding of environment, flawless tooling, and libraries, we cannot fix bad design
- However we can encourage people to engage early enough and loop us in the design phase

How to think about security?


CENTRAL INTELLIGENCE AGENCY
UNITED STATES OF AMERICA


Confidentiality
Availability
Integrity

Understand your threats

Know your fears

What do I want to prevent from happening?

Understand your threats

Do you really need to have a strategy for Yellowstone’s eruption?

What do I want to prevent from happening?

If that happens, would I have a bigger problems?

Defense in depth

Arcadia had 400 sky trenches, how many do you have?

- No silver bullet/armor
- Make the life of your enemies hell
- They have to get lucky multiple times

How to convince others?

Make it simple

And stable

- Nothing trumps simplicity
- … but stability

Make it cheap

- People are unwilling to trade their precious CPU cycles
- And bytes of memory
- And IO
- It has to seem free until proven otherwise

Help ’em

- Volunteer to migrate large services
- If they can use it, everybody can
- Strive to say YES!

Where to look first?

Resource inventory

- What is running? Where is it? How is it being provisioned, accessed and separated from other entities?
- What version of hardware and software is being used? Are there any known vulnerabilities?
- Do you know how to roll your secrets? Update all machines/services in a timely manner? Deal with emergencies?

Authentication and authorization

- How employees get their credentials, can they move them out of trusted machines?
- How do you know that given machine or service is really what it advertised to be?

Access management

- Who can access given endpoint, secret or machine?
- How is the access granted and is it taken away after it's not needed anymore?

Secrets management

- Where do you store secrets? Are they encrypted at rest?
- Do you have backups?
- How are you preventing unauthorized access?
- How are they distributed? Are you sure only authorized recipients are getting them?

facebook