

Cumulus

Threat Modeling the Ops of DevOps

Christoph Niehoff

OWASP Global AppSec Barcelona, 29/05/2025

About me

Christoph Niehoff

- ▶ Former theoretical physicist
- ▶ Full-stack developer
- ▶ DevOps engineer
- ▶ Wants to build secure products
- ▶ Project Lead of OWASP Cumulus



The card game OWASP Cumulus is licensed under CC-BY-4.0.

Outline

- ▶ Threat modeling card games
- ▶ Demo
- ▶ Conclusion



STANDING ON THE

Cumulus

Elevation
of
Privilege

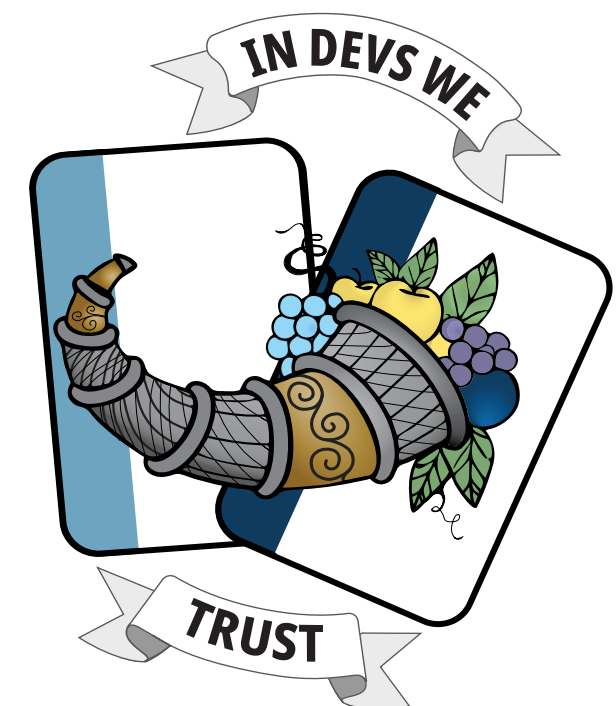
Cornucopia

Cloud
Experts

**SHOULDERS OF
GIANTS**

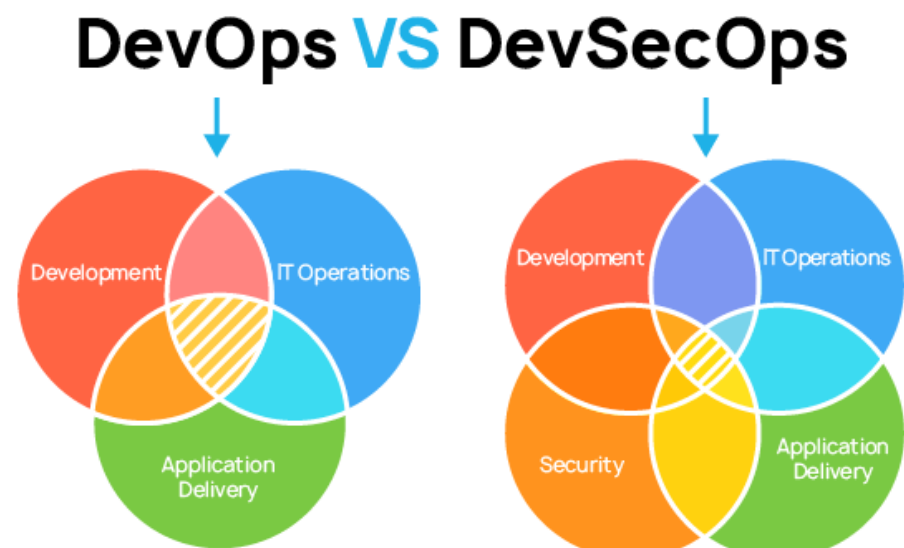


DevOps
is built on
self-responsibility.



DevSecOps?

Don't do this!

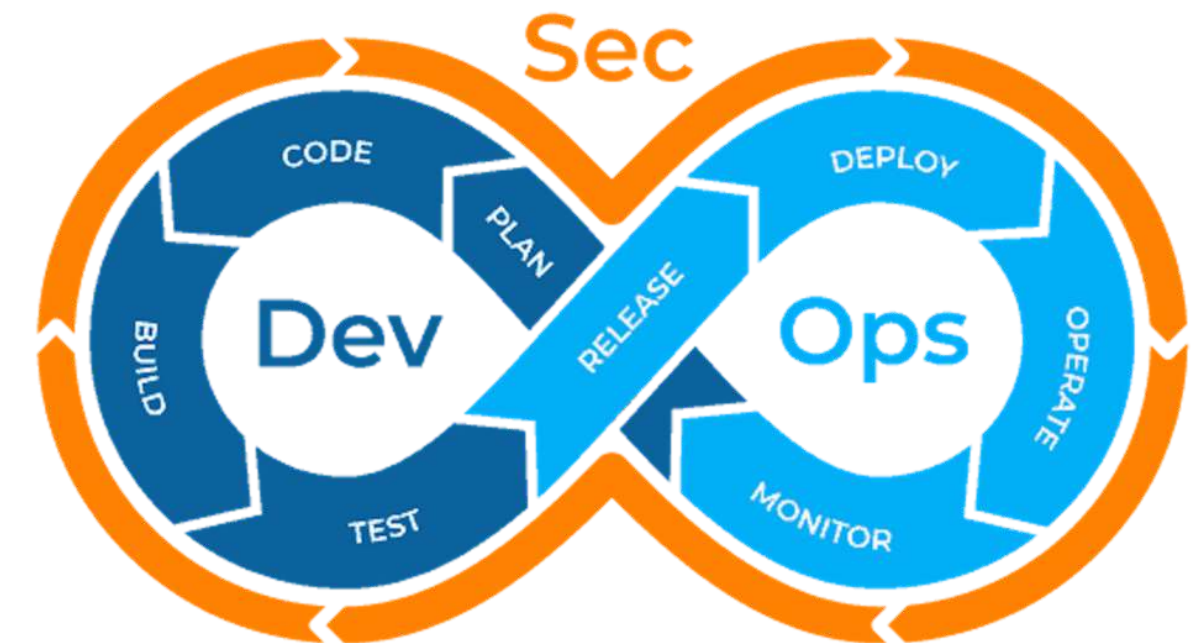


source: <https://pvs-studio.com/en/blog/posts/0710/>



source: <https://www.xalt.de/5-key-skills-for-devsecops/>

Do this!



source: <https://www.pagerduty.com/blog/devsecops-ops-guide/>

Shostack's Four Questions

Model System

What are you building?

Diagrams etc.

Find Threats

What can go wrong?

Knowledge, creativity, awareness, mindset?

🤔 Here we need help!

**Address
Threats**

What should we do about it?

Mitigations and risk

Validate

Did we do a decent job?

Good processes

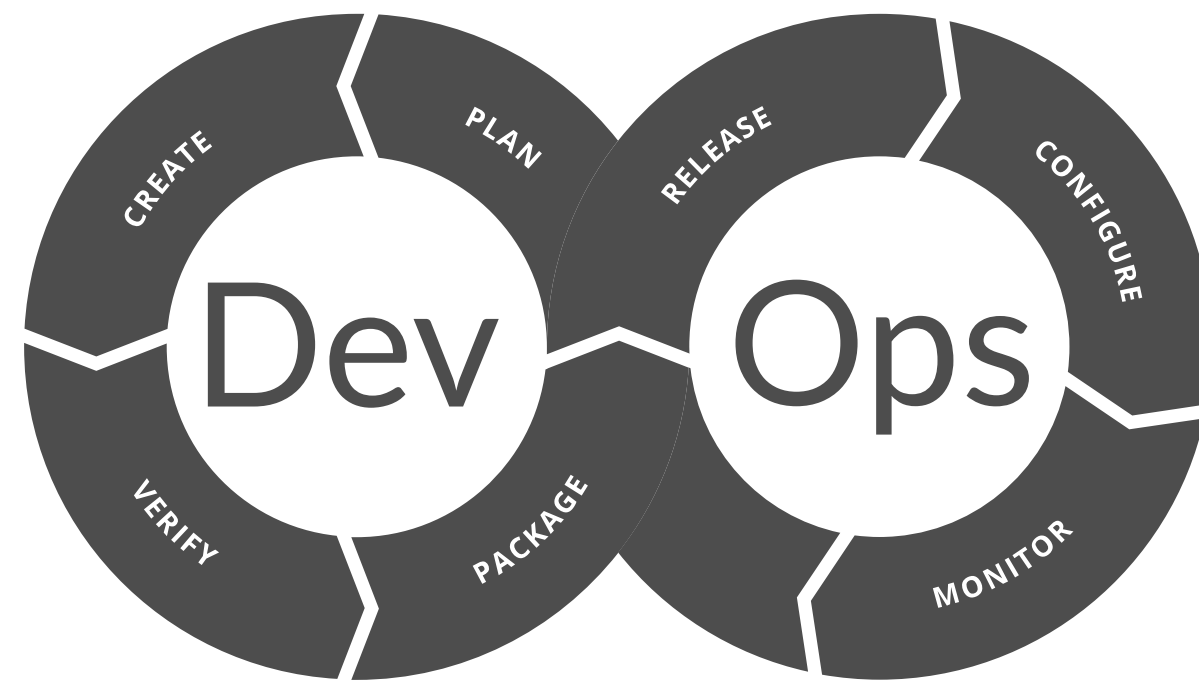
Gamification



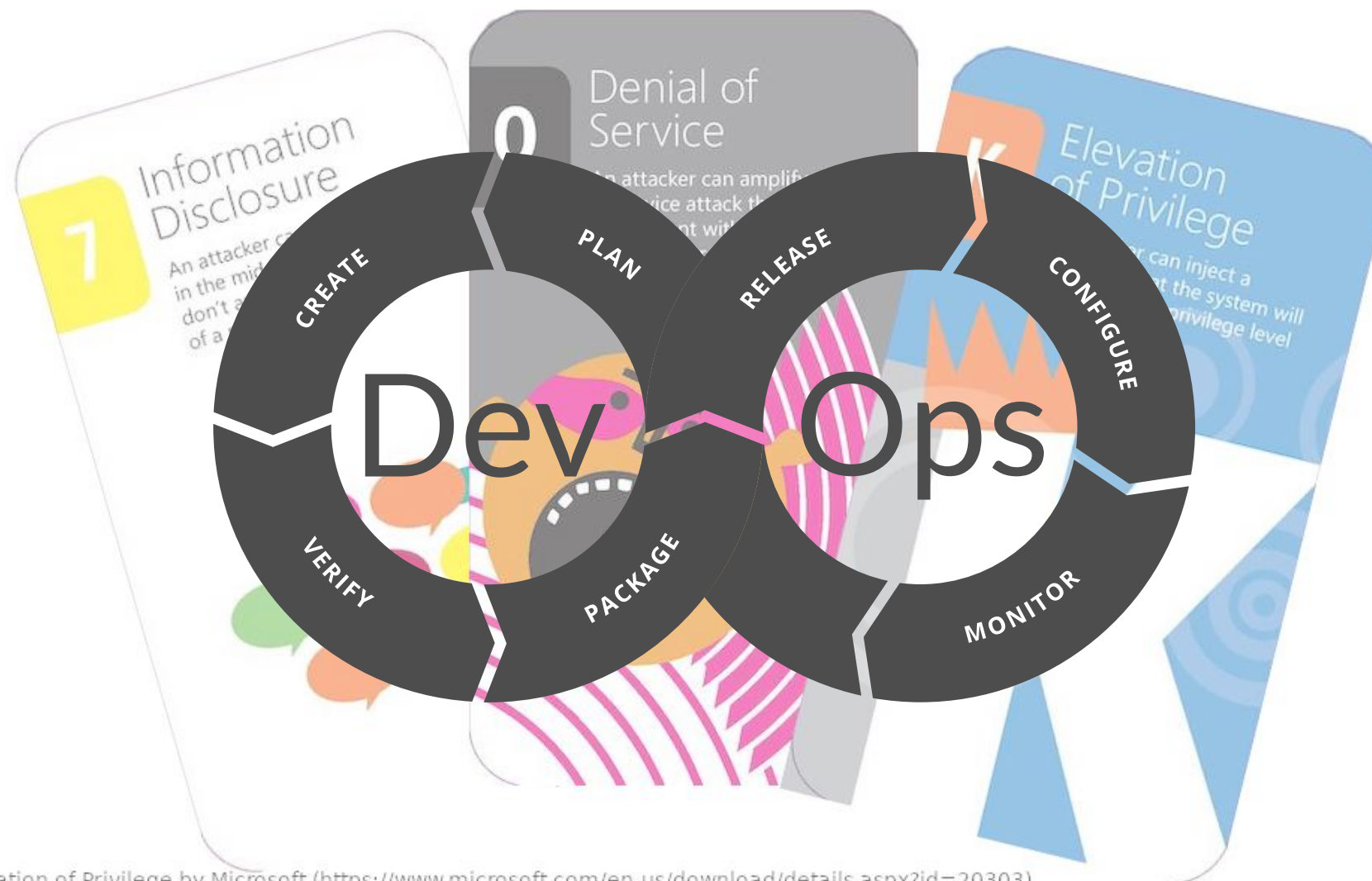
Elevation of Privilege by Microsoft (<https://www.microsoft.com/en-us/download/details.aspx?id=20303>)
licensed under CC-BY-3.0 <http://creativecommons.org/licenses/by/3.0/us/>

- ▶ Great idea by Adam Shostack (*2010 at Microsoft)
- ▶ Lightweight, low-barrier approach to get developers into threat modeling
- ▶ Each card represents a possible threat vector and is a basis for discussions
- ▶ Gaming fosters discussions, openness and fun while doing it

But what about the Ops in DevOps?



But what about the Ops in DevOps?



Elevation of Privilege by Microsoft (<https://www.microsoft.com/en-us/download/details.aspx?id=20303>)
licensed under CC-BY-3.0 <http://creativecommons.org/licenses/by/3.0/us/>

But what about the Ops in DevOps?



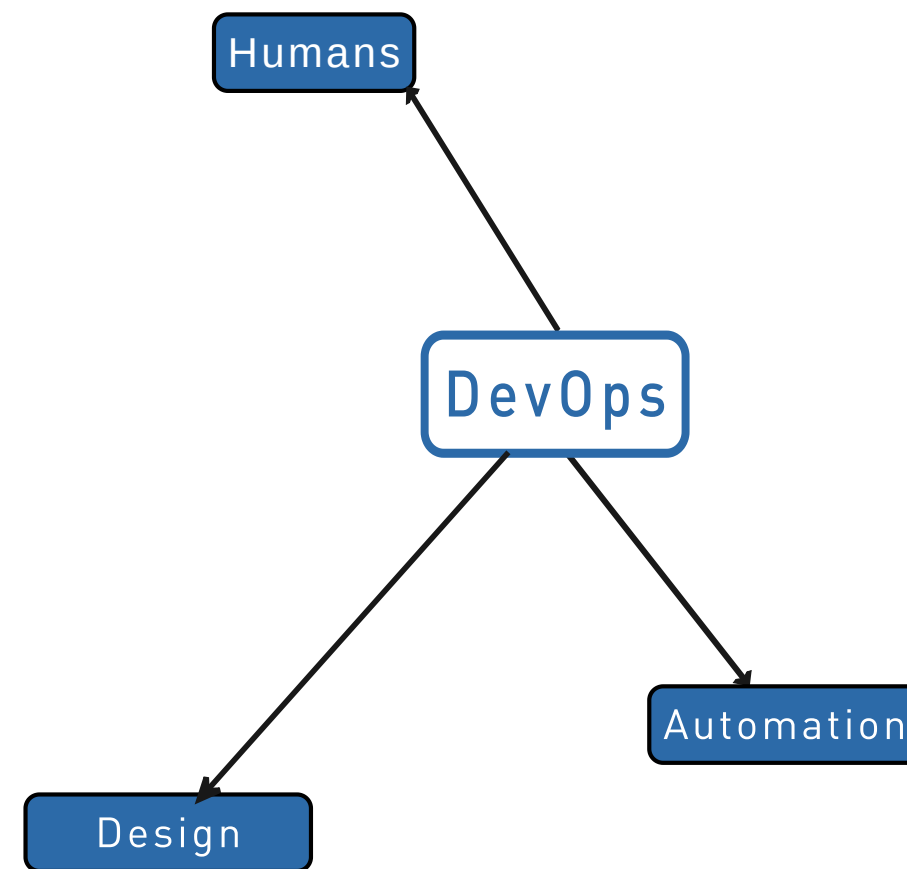
Elevation of Privilege by Microsoft (<https://www.microsoft.com/en-us/download/details.aspx?id=20303>)
licensed under CC-BY-3.0 <http://creativecommons.org/licenses/by/3.0/us/>

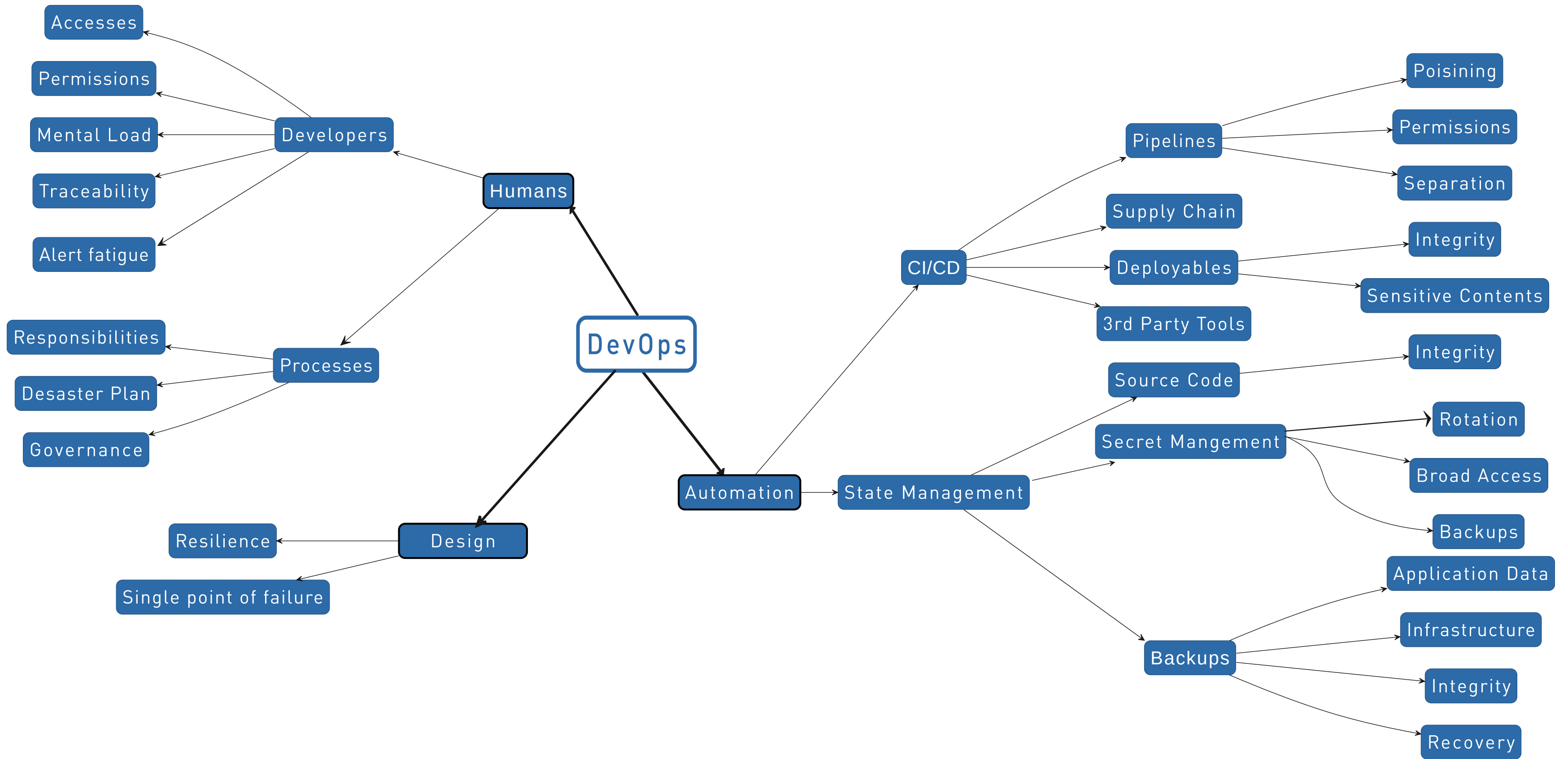
But what about the Ops in DevOps?

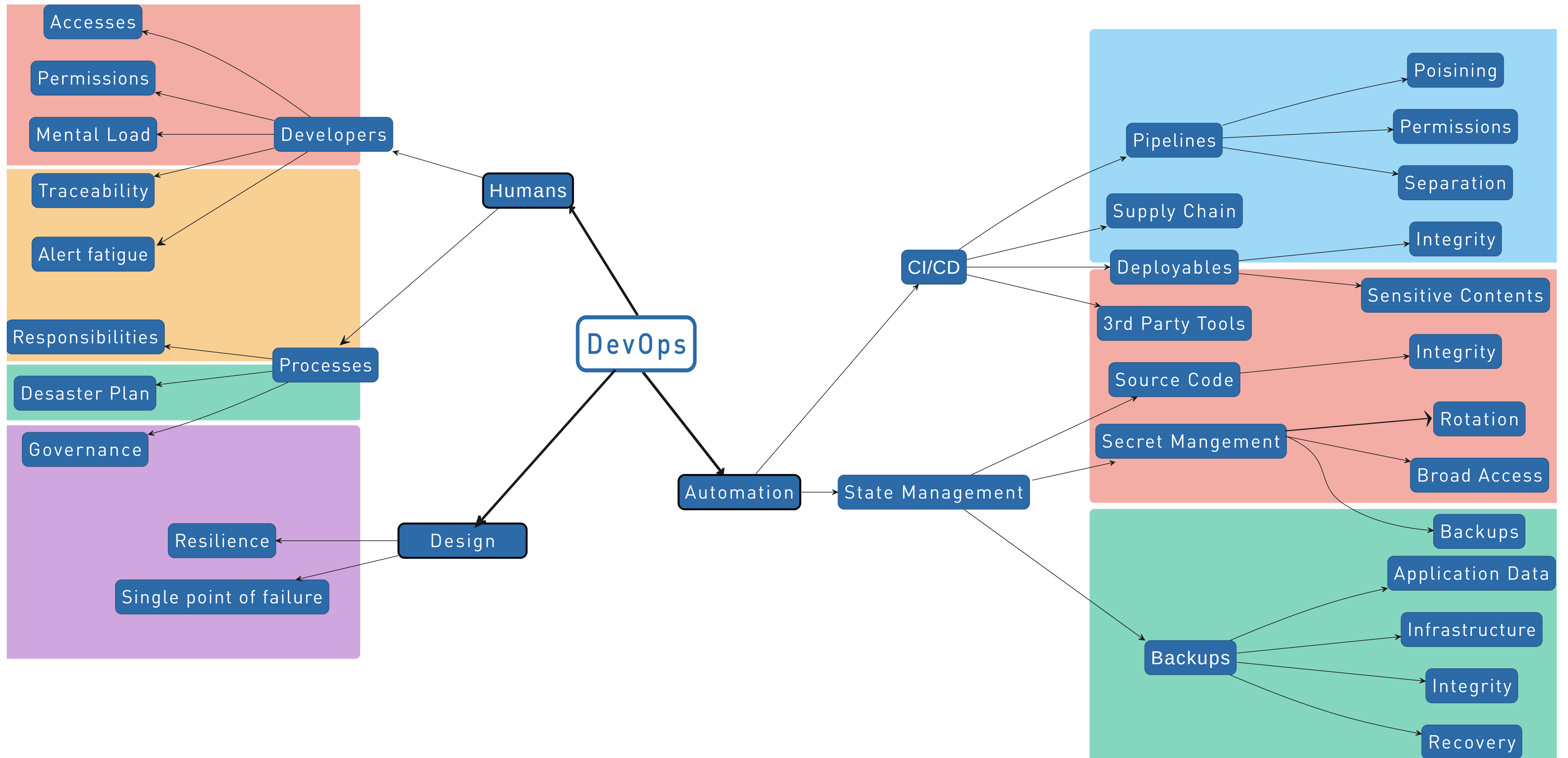


The card game OWASP Cumulus is licensed under CC-BY-4.0.

Elevation of Privilege by Microsoft (<https://www.microsoft.com/en-us/download/details.aspx?id=20303>)
licensed under CC-BY-3.0 <http://creativecommons.org/licenses/by/3.0/us/>







OWASP Cumulus



The card game OWASP Cumulus is licensed under CC-BY-4.0.

Access & Secrets

Threats related to IAM and secrets management

Delivery

Build and ship software, and its supply chain

Recovery

Backup and restore

Monitoring

Logs, alerts and traceability

Resources

Threats on resources and their configuration

OWASP Cumulus



The card game OWASP Cumulus is licensed under CC-BY-4.0.

Design decisions:

- ▶ Vendor-independent
- ▶ Technology-independent
- ▶ General enough to foster discussions
- ▶ Concrete enough to be helpful
- ▶ We-perspective (to emphasize the responsibility in DevOps)

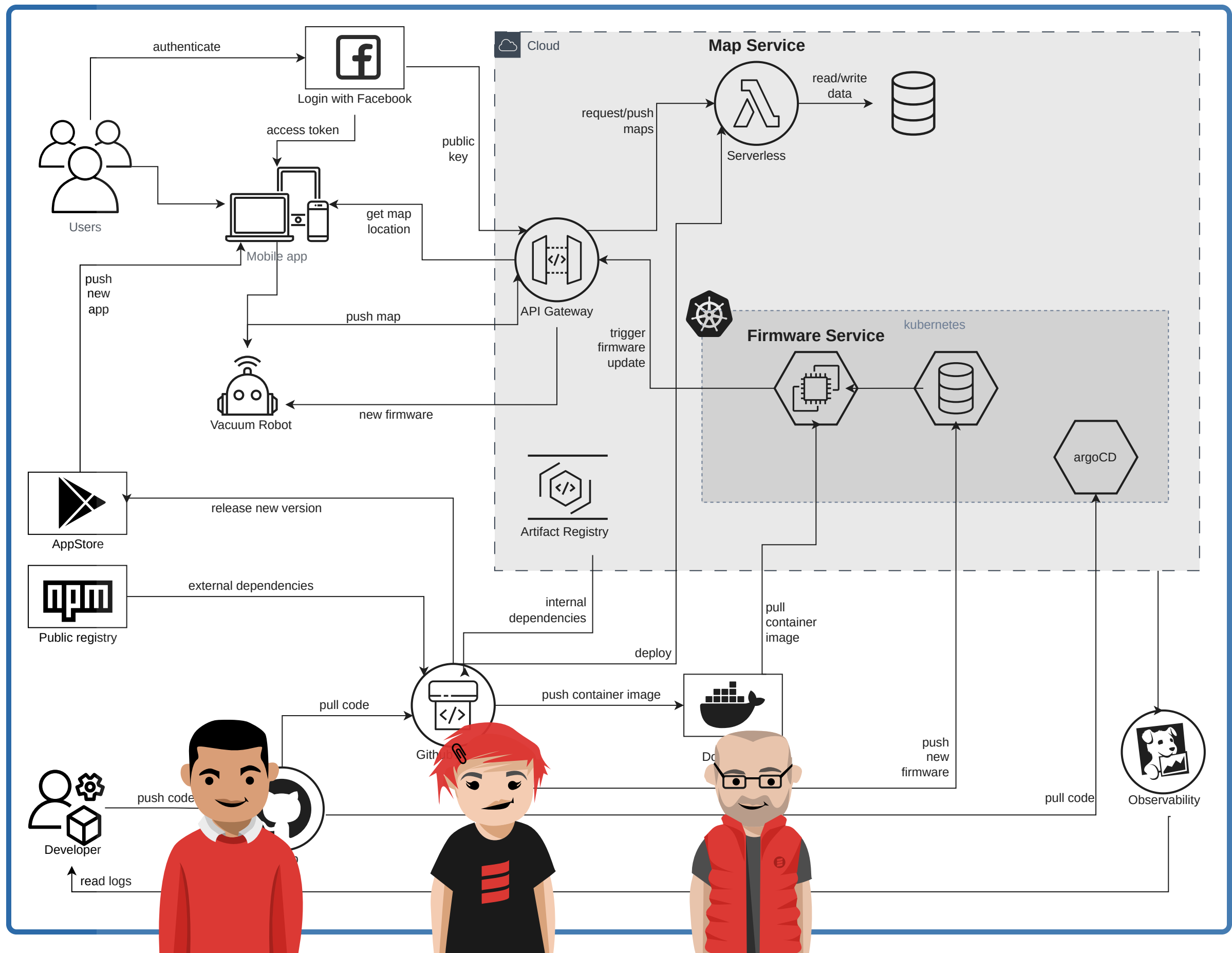
Rules



Outline

- ▶ Threat modeling card games
- ▶ Demo
- ▶ Conclusion

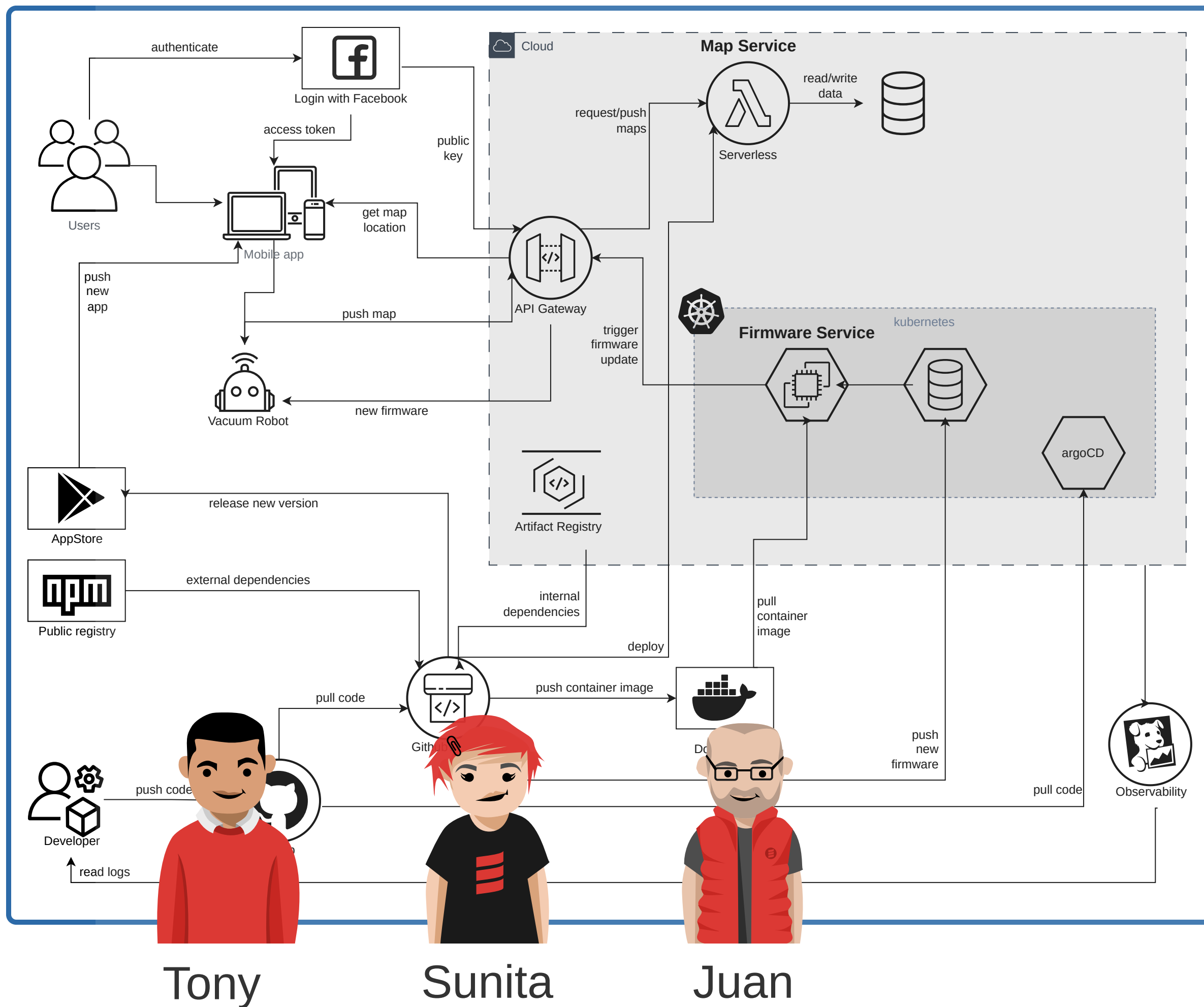


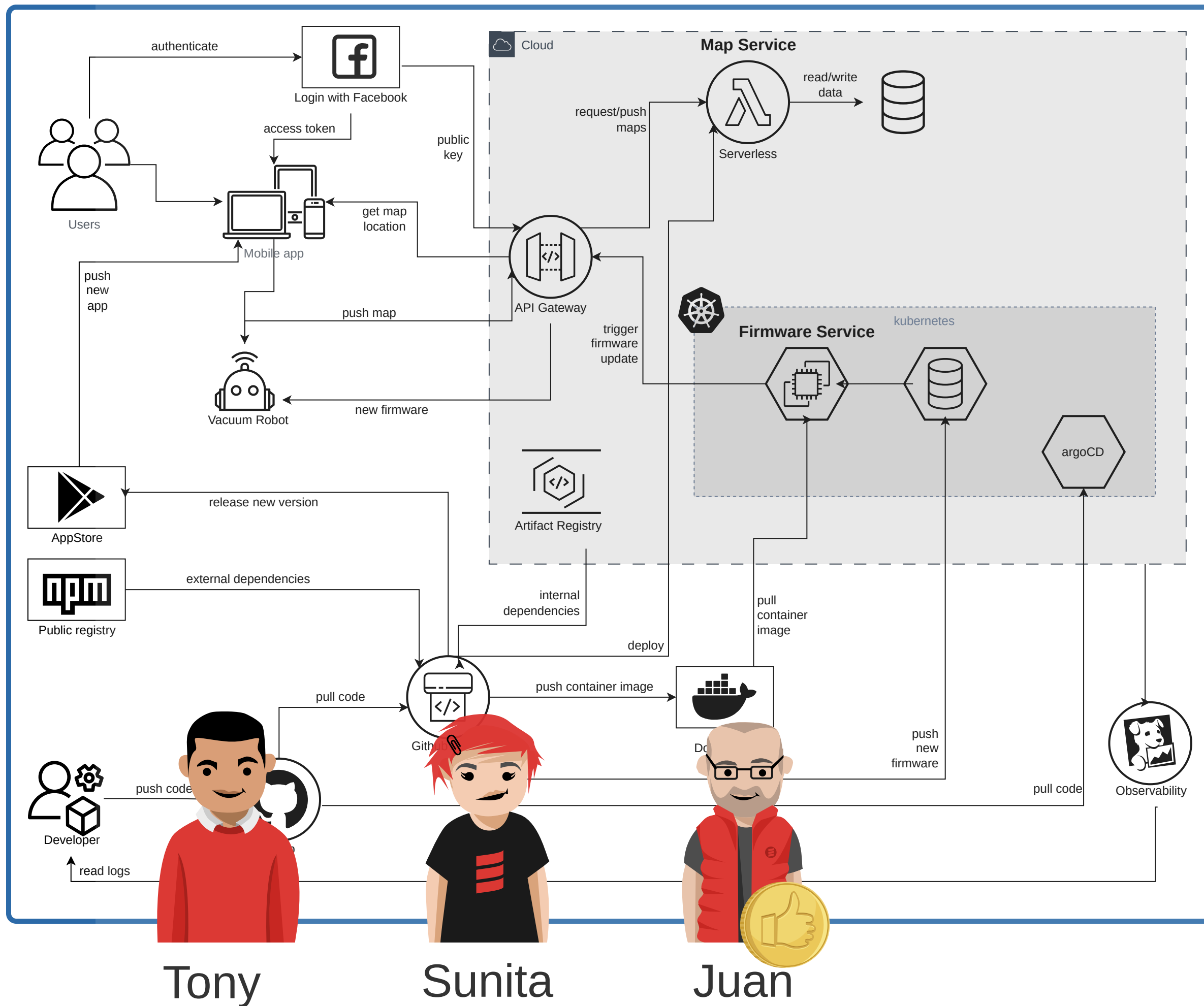


Tony

Sunita

Juan





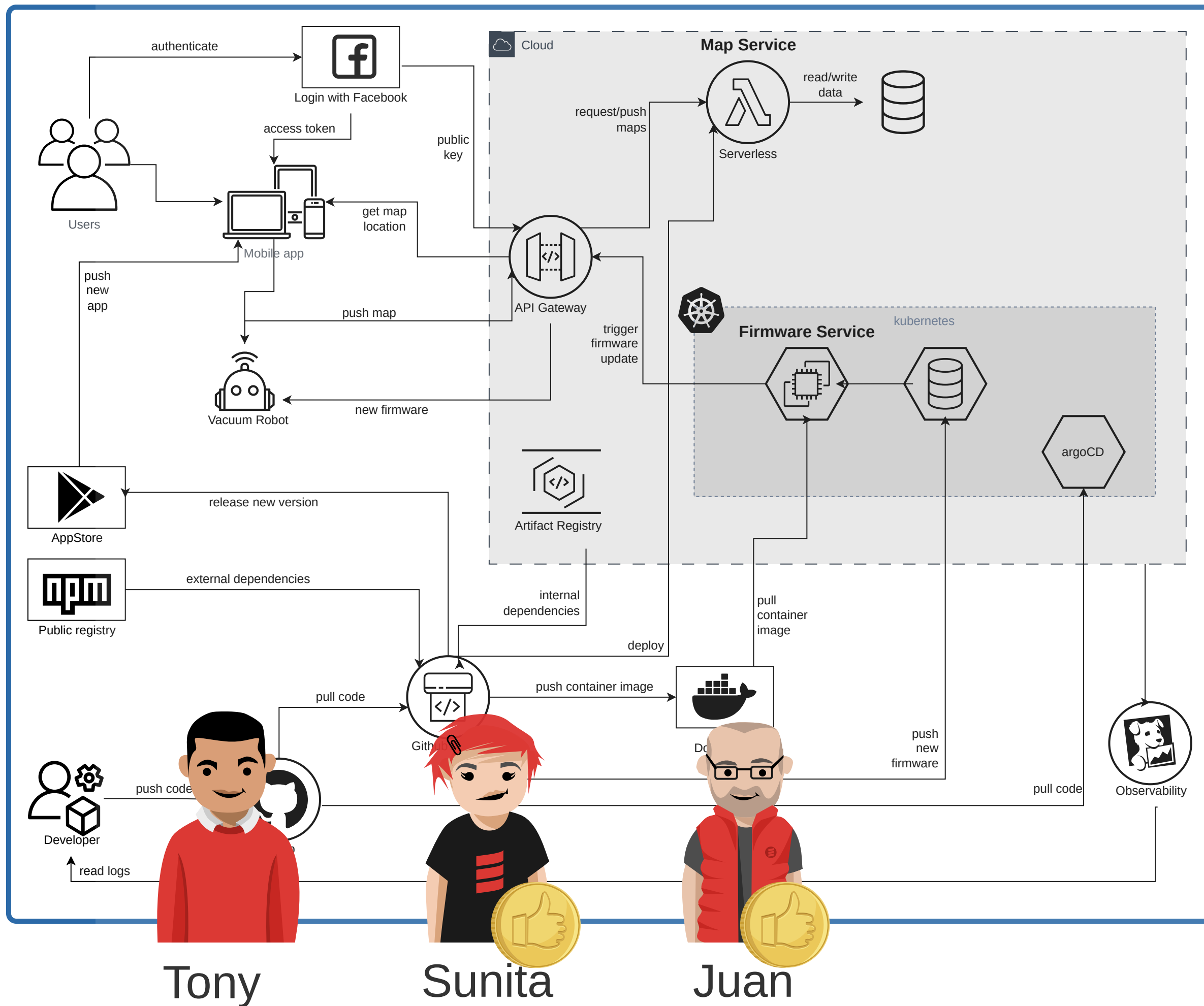
can reach internet from CI pipeline

8 eight/delivery

Outdated dependencies

We use outdated dependencies of our runtime platform (OS, container image, serverless runtime).

TNG TECHNOLOGY CONSULTING



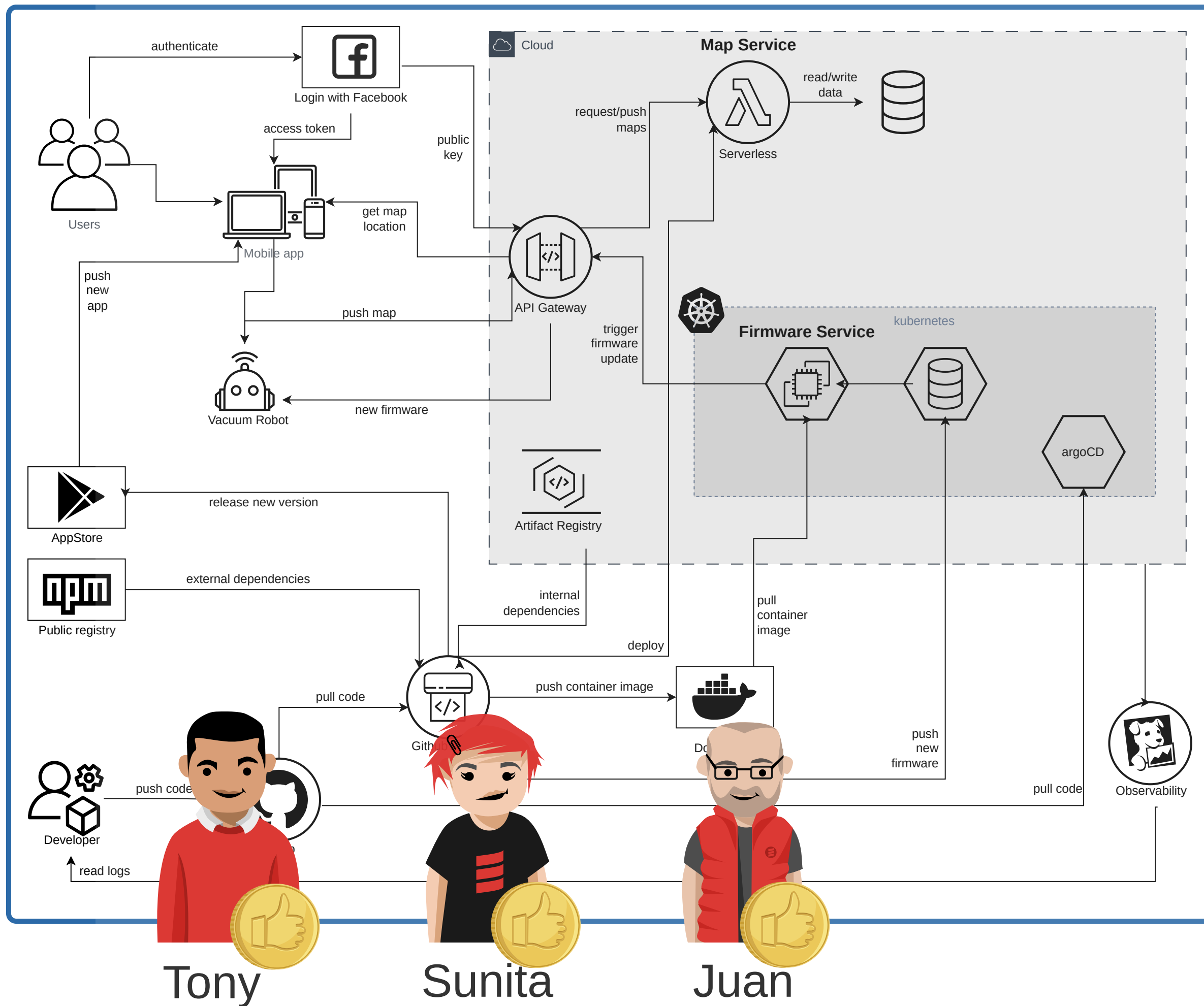
Old FB client
in mobile app

8 eight/delivery

Outdated dependencies

We use outdated dependencies of our runtime platform (OS, container image, serverless runtime).

TNG TECHNOLOGY CONSULTING



NodeJS
version
in lambda

8
eight/delivery

Outdated dependencies

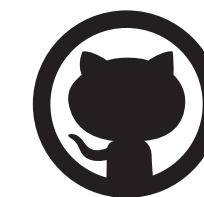
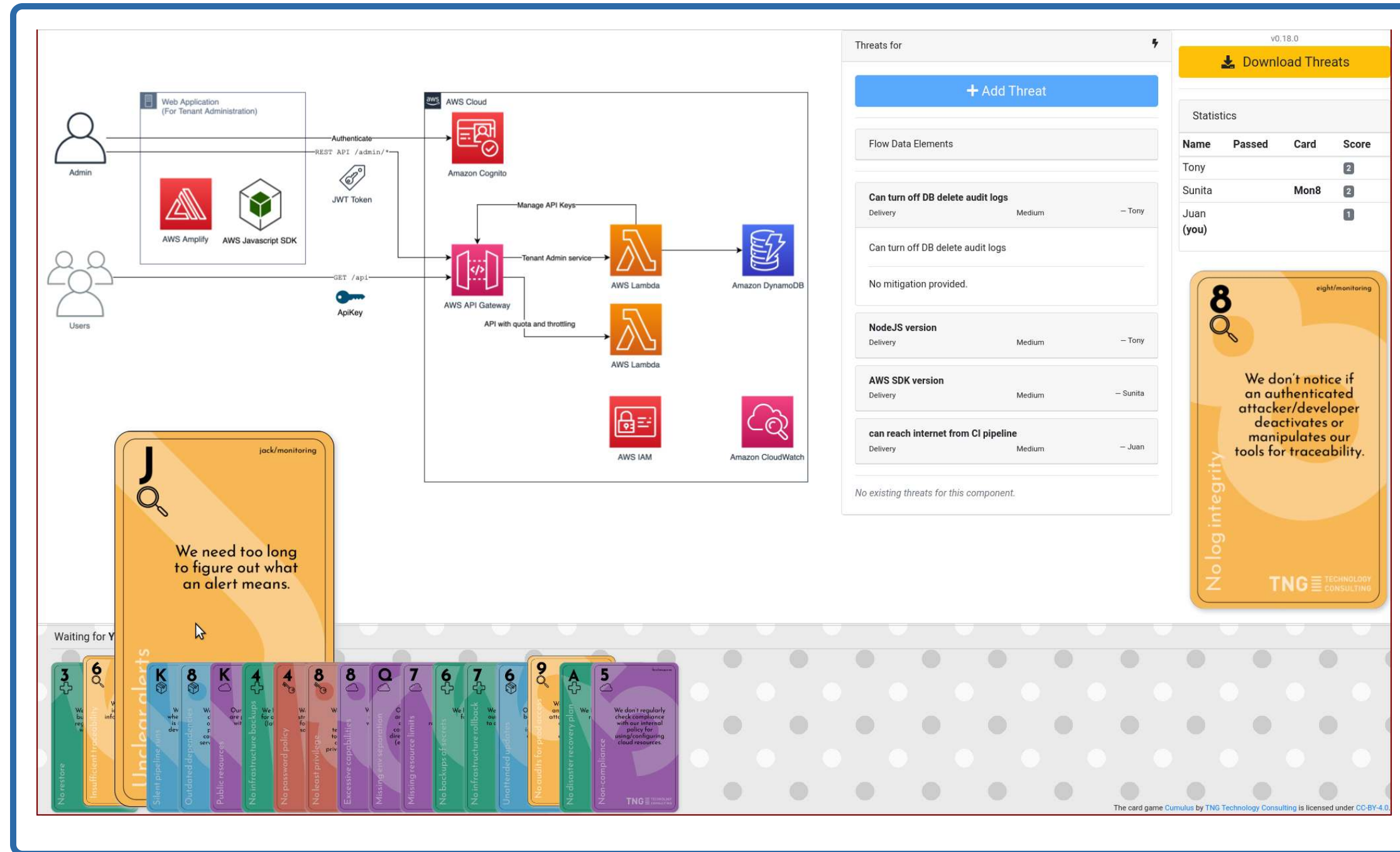
We use outdated dependencies of our runtime platform (OS, container image, serverless runtime).

TNG TECHNOLOGY CONSULTING

Online Version

Supports:

- Elevation of Privilege
- OWASP Cornucopia
- OWASP Cumulus
- Elevation of MLSec



github.com/TNG/elevation-of-privilege




Where to get it?

Either print it yourselves



or get it at Agile Stationary / CyberSecGames

I'm not getting any money out of it!



All

Search for produ



HomeShopPlayMakeAbout us

Home > Threat Modeling > OWASP Cumulus – Threat Modeling the CL

6

Missing rate limits

We have not configured any rate limits for our services.

10

Insufficient monitoring

We cannot react to problems in time because our monitoring has blind spots.

8

No application rollback

We cannot restore our application to a previous state.

2

Too many permissions

We grant permissions to 3rd parties (e.g. CI/CD systems).

4

Insufficient response

We can't get contacted by our cloud provider in case of emergency.

10

Uncontrolled ingress/egress

We don't limit ingress or egress when running CI pipelines.

OWASP Cumulus – Threat Modeling the Cloud

☆ Description

OWASP Cumulus is a gamified approach to integrating security into cloud and DevOps teams. As a variant of the popular card game Elevation of Privilege by Adam Shostack, Cumulus enables teams to threat model DevOps systems.

Developed and supported by TNG Technology Consulting, Cumulus helps DevOps teams enhance their security through collaboration and discussion and seamlessly integrates into agile development processes.

Threat model the Ops of DevOps

Outline

- ▶ Threat modeling card games
- ▶ Demo
- ▶ Conclusion



Takeaways

- ▶ In DevOps, Security is a team's responsibility
- ▶ Should be a natural element and nothing special
- ▶ Threat modeling with serious card games is a lightweight approach to enable the Team
- ▶ The triplet (EoP, Cornucopia, Cumulus) covers all aspects of modern DevOps projects
- ▶ Cumulus can help you!
 - ▶ DevOps Teams
 - ▶ Site reliability engineers
 - ▶ Cloud admins
 - ▶ Security practitioners

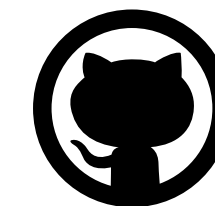
Please participate!

Input for Cumulus:

- ▶ Cloud Security Best Practices
- ▶ OWASP Top10 CI/CD
- ▶ CIS Benchmarks
- ▶ *But mostly:* experience at \$COMPANY

🙏 Please raise issues and create pull requests! 🙏

💪 Let's make this a community project! 💪



github.com/OWASP/cumulus



See you tomorrow in the
Demo Lab! 14:15h in
Room 133-134

Thank you!

Any questions?



Christoph Niehoff

christoph.niehoff@owasp.org



github.com/OWASP/cumulus





2  two/delivery

No SBOM

We don't know the versions of our dependencies or whether they are up to date.

TNG TECHNOLOGY CONSULTING

4  four/delivery

Dependency confusion

We don't know the source repository of our dependencies.

TNG TECHNOLOGY CONSULTING

10  ten/delivery

Missing network control

We don't limit ingress or egress when running CI pipelines.

TNG TECHNOLOGY CONSULTING

Q  queen/delivery

No source code integrity

We are not certain which code/artifacts we are deploying.

TNG TECHNOLOGY CONSULTING

K  king/delivery

Silent pipeline runs

We won't notice when a deployment is started from a developer account.

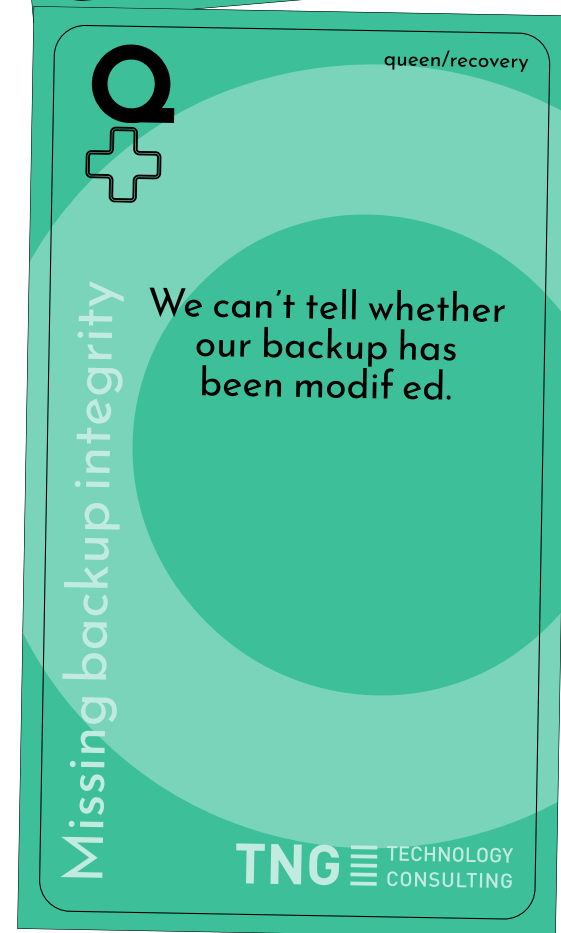
TNG TECHNOLOGY CONSULTING

A  ace/delivery

Silent pipeline changes

We won't notice when someone alters the deploy pipeline.

TNG TECHNOLOGY CONSULTING





four/resources

4

Unreachable contact details

We can't get contacted by our cloud provider in case of emergency.

TNG TECHNOLOGY CONSULTING

nine/resources

9

Single point of failure

Our whole system can be affected by a single rogue service.

TNG TECHNOLOGY CONSULTING

jack/resources

J

Missing egress control

We don't control egress traffic.

TNG TECHNOLOGY CONSULTING

queen/resources

Q

Missing env separation

Our production and staging environments are connected, either directly or indirectly (e.g. via CI/CD).

TNG TECHNOLOGY CONSULTING

king/resources

K

Public resources

Our cloud resources are publicly exposed without any need.

TNG TECHNOLOGY CONSULTING

ace/resources

A

No cloud policy

We have no clear policy for using/configuring cloud resources.

TNG TECHNOLOGY CONSULTING