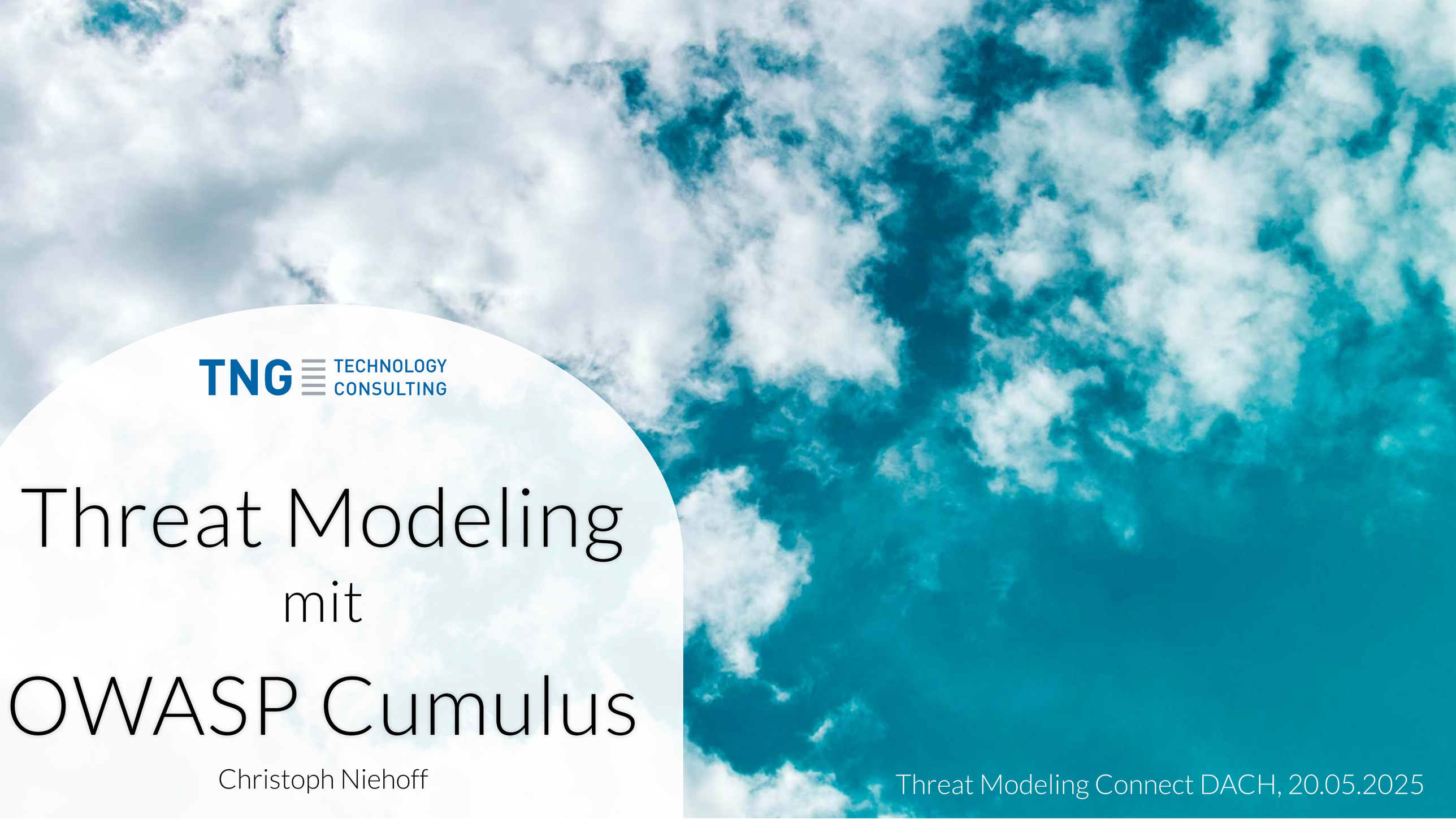


TNG TECHNOLOGY CONSULTING

Threat Modeling mit OWASP Cumulus

Christoph Niehoff

Threat Modeling Connect DACH, 20.05.2025

Agenda

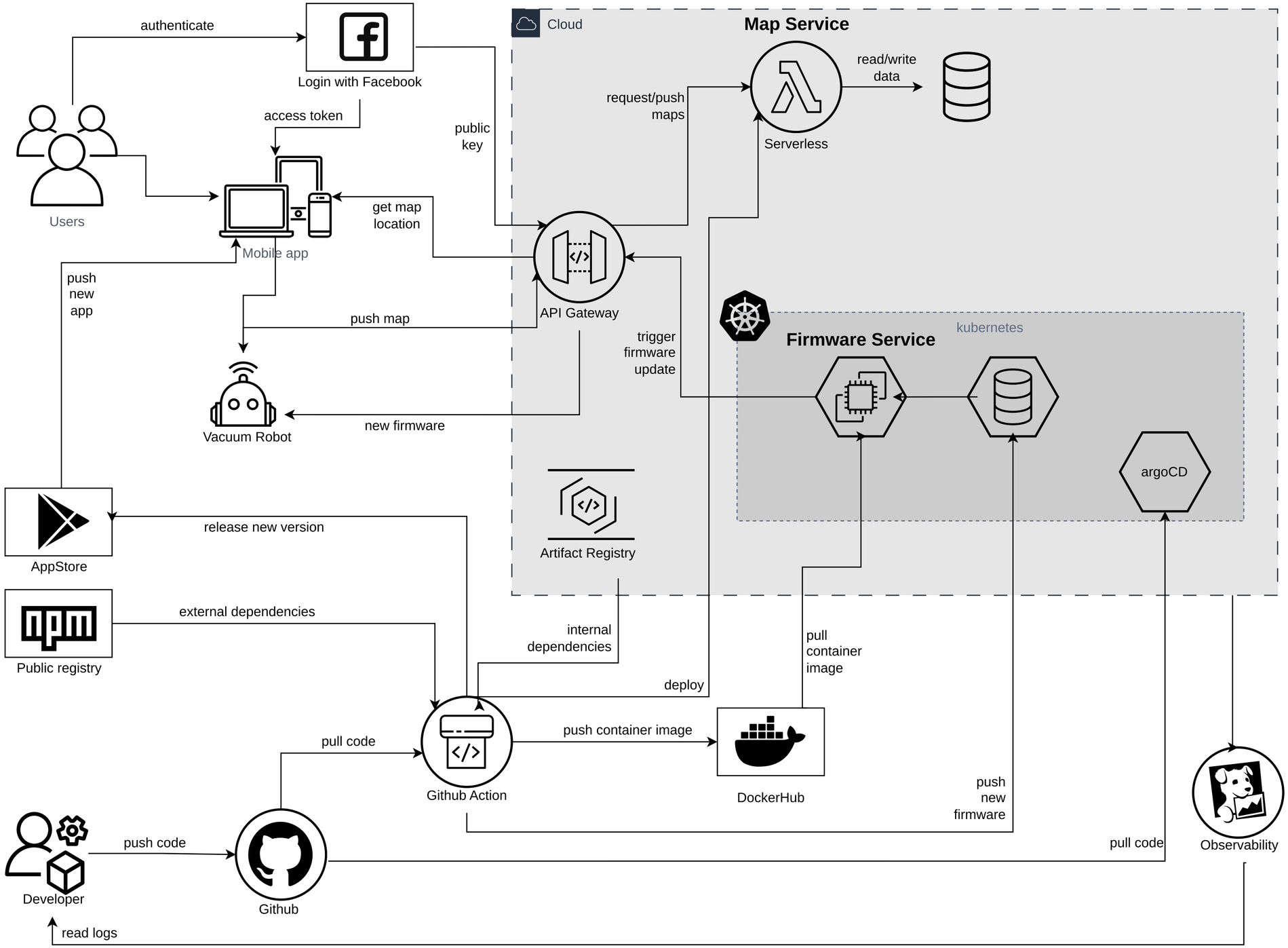
- Intro: Threat Modeling
- Scenario
- Ernsthafte Kartenspiele
- Conclusion

Shostacks Vier Fragen

`Model System`	*Woran arbeiten wir?*	▶ Diagramme ▶ Architektursichten ▶ Vertrauensgrenzen
`Find Threats`	*Was kann schiefgehen?*	▶ Denke abseits des vorgesehenen Pfads! ▶ "Denke wie ein Hacker!" ▶ 🤨*Ist das so einfach?*🤔
`Address Threats`	*Was werden wir dagegen tun?*	▶ Vermeiden ▶ Mitigieren ▶ Übertragen ▶ Akzeptieren
`Validate`	*Haben wir gute Arbeit geleistet?*	▶ Decken wir alles ab? ▶ Software ist ein bewegliches Ziel

Agenda

- Intro: Threat Modeling
- Scenario
- Ernsthafte Kartenspiele
- Conclusion


Cloud
Map Service
authenticate
Login with Facebook
access token
public key
request/push maps
read/write data
Serverless
Users
Mobile app
get map location
API Gateway
push new app
push map
trigger firmware update
kubernetes
Firmware Service
Vacuum Robot
new firmware
argoCD
Artifact Registry
release new version
AppStore
external dependencies
Public registry
internal dependencies
pull container image
deploy
pull code
push container image
Github Action
DockerHub
push new firmware
Observability
push code
Developer
Github
pull code
read logs

Agenda

- Intro: Threat Modeling
- Scenario
- Ernsthafte Kartenspiele
- Conclusion

Gamifizierung

- Elevation of Privilege (*2010 bei Microsoft)
- Idee: Bringe EntwicklerInnen ins Threat Modeling
- Jede Karte stellt eine konkrete Bedrohung dar
- Spielfarben == Bedrohungskategorien

S poofing

T ampering

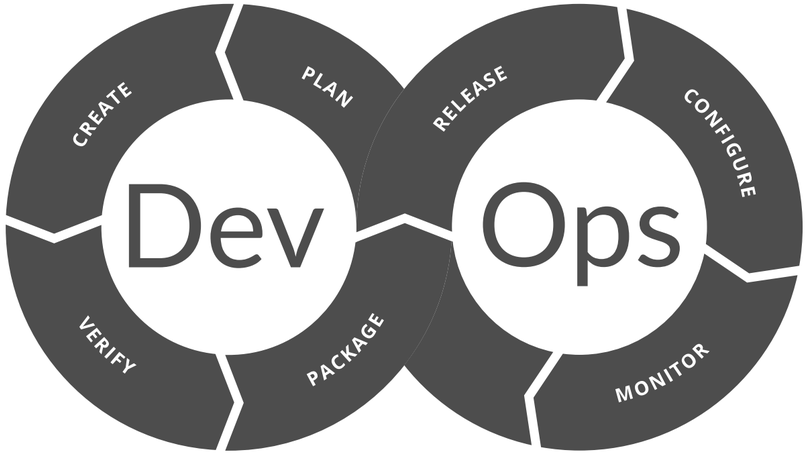
R epudiation

I nformation Disclosure

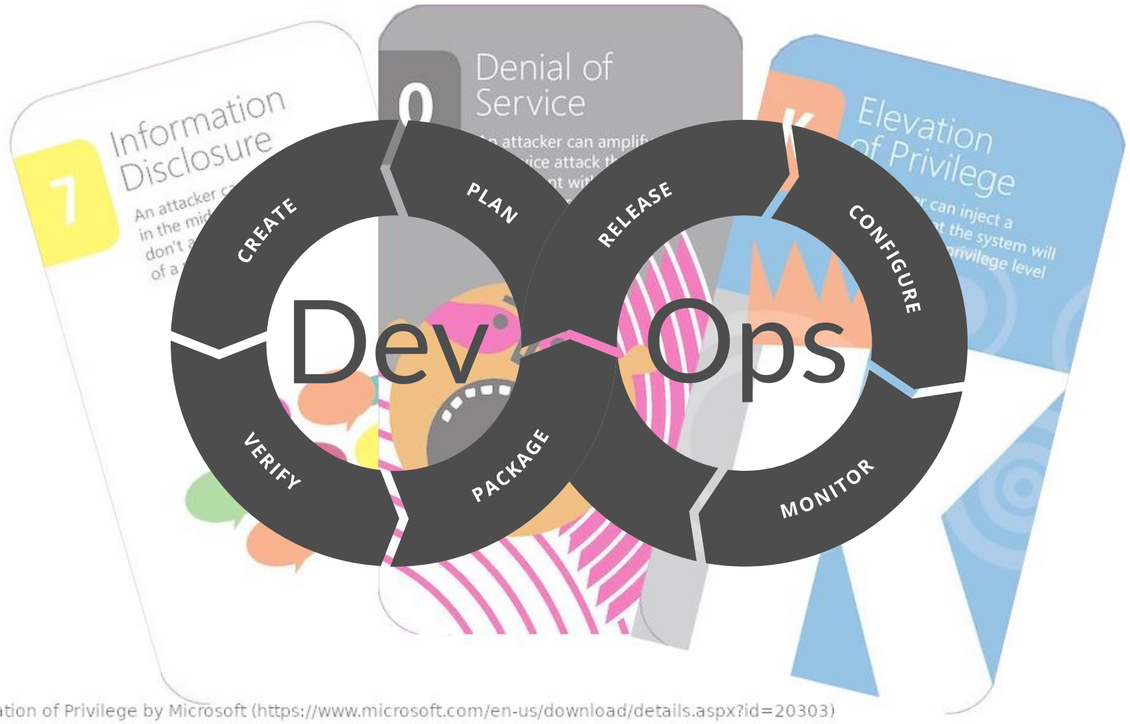
D enial of Service

E levation of Privilege

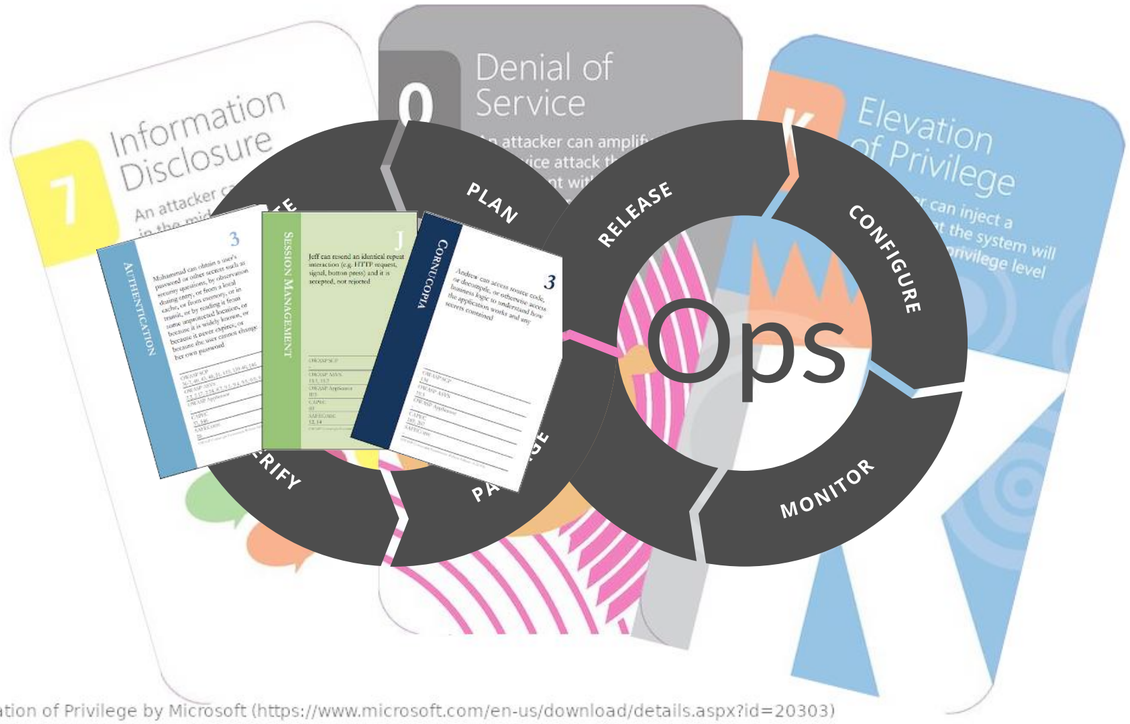
Was ist mit DevOps?



Was ist mit DevOps?



Was ist mit DevOps?



Was ist mit 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/

OWASP Cumulus

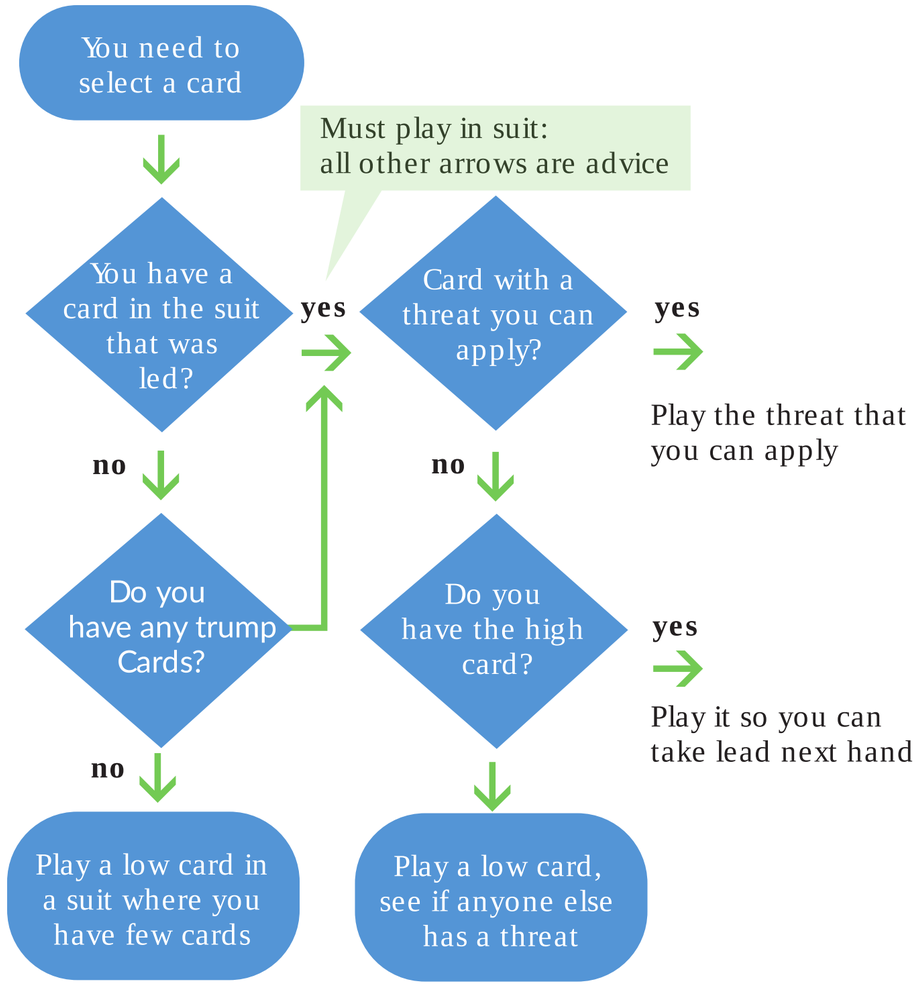
Access & Secrets	Berechtigungsmanagement und Geheimnisse
Delivery	Bau, Auslieferung und Lieferkette
Recovery	Sicherung und Wiederherstellung
Monitoring	Protokolle, Alarme und Nachvollziehbarkei
Resources	Ressourcen und deren Konfiguration

OWASP Cumulus

Design decisions:

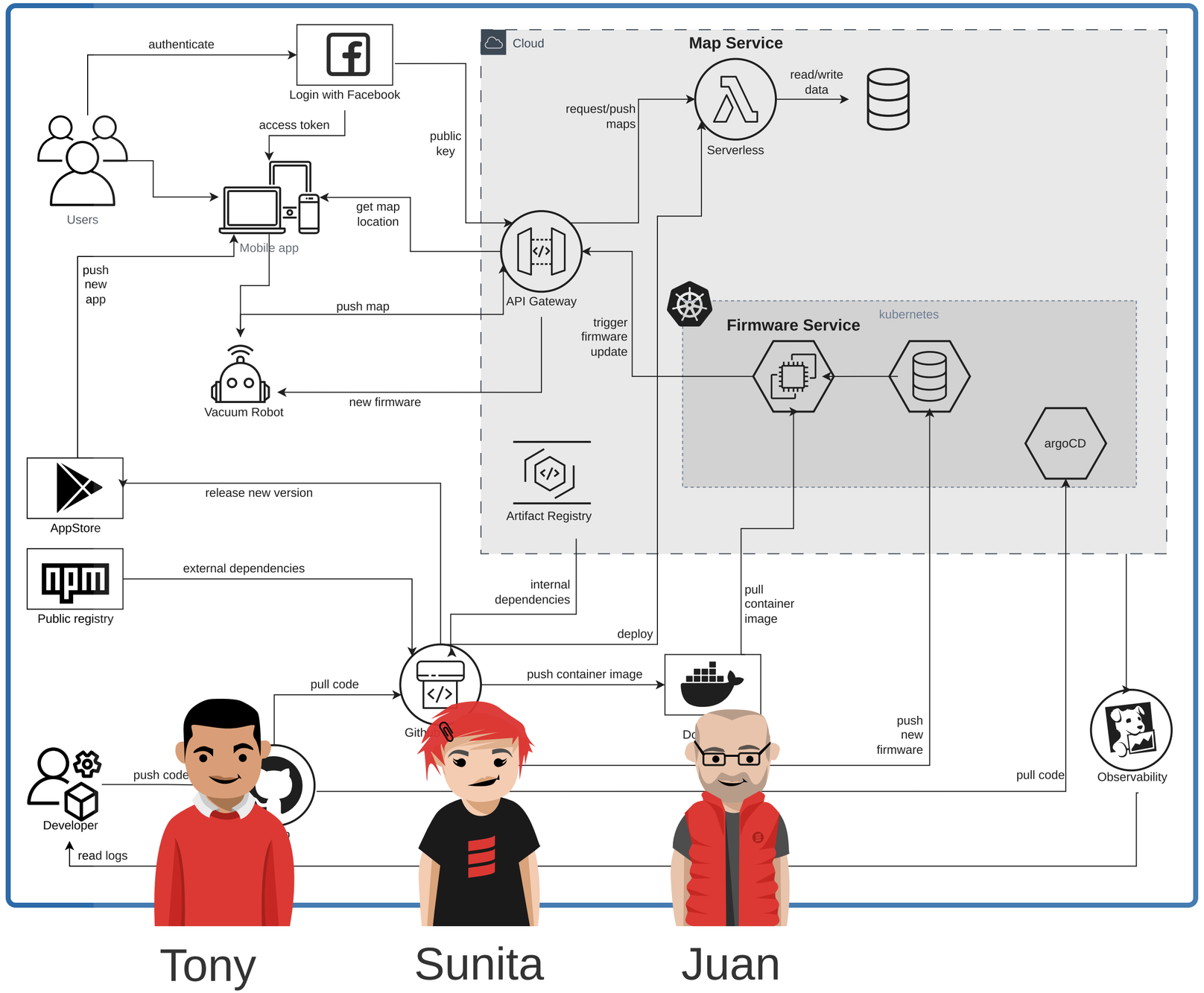
- Cloud-Anbieter-unabhängig
- Technologieunabhängig
- Allgemein genug, um Diskussionen anzuregen
- Konkret genug, um hilfreich zu sein
- *Wir*-Perspektive (betont die Eigenverantwortung in DevOps)

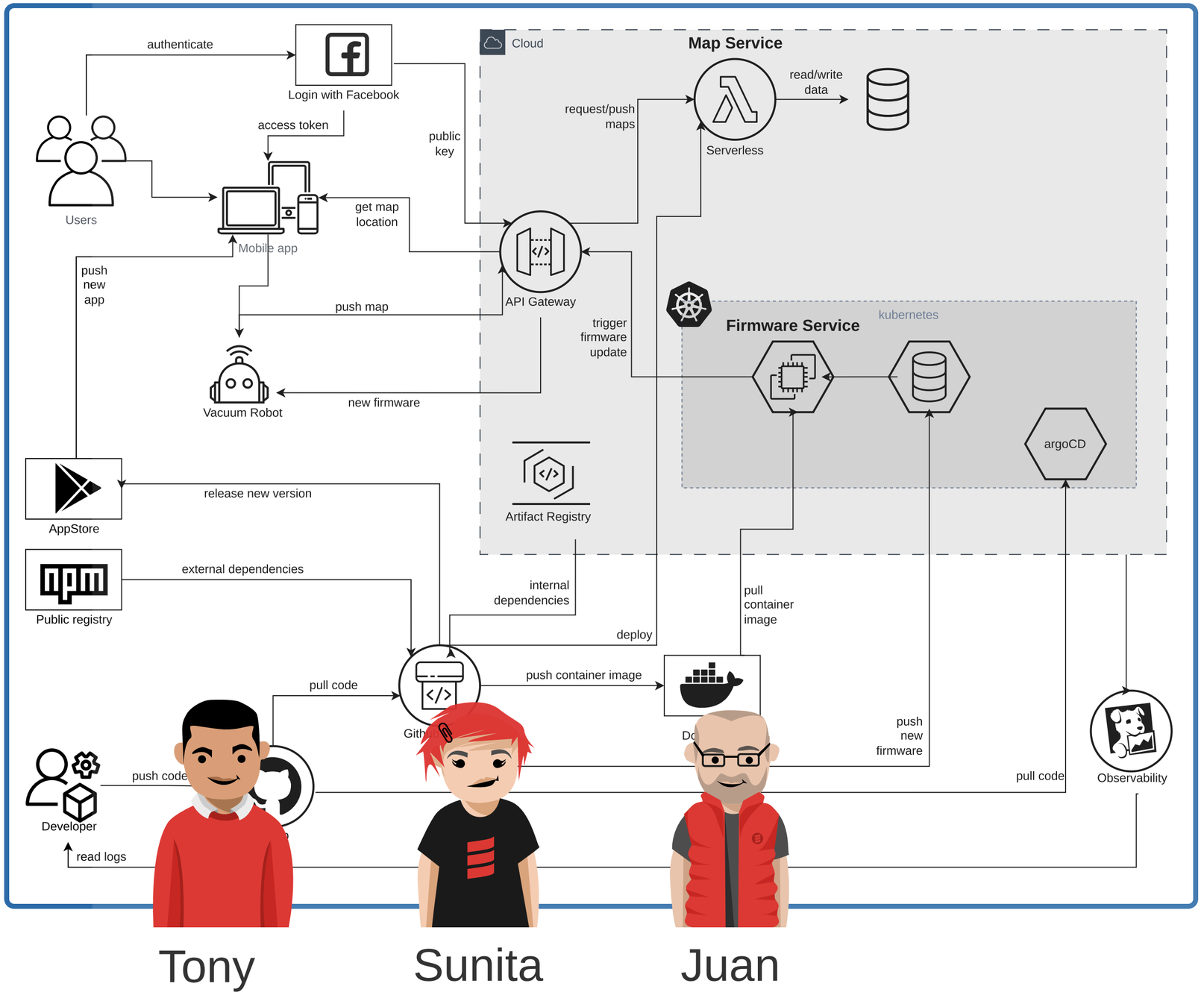
Rules



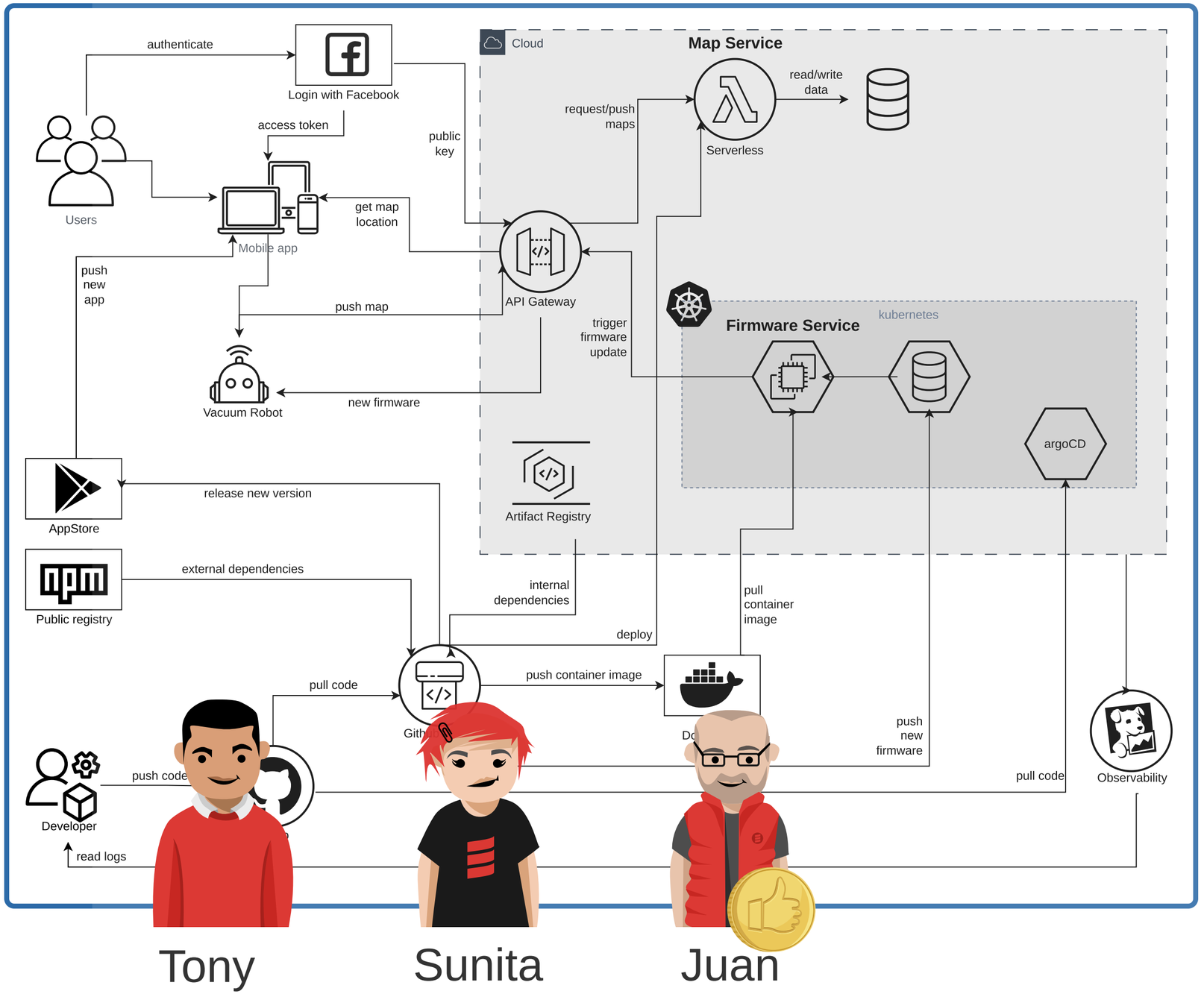
https://github.com/adamshostack/eop/blob/master/EoP_Card%20Game%20Images.pdf

Demo

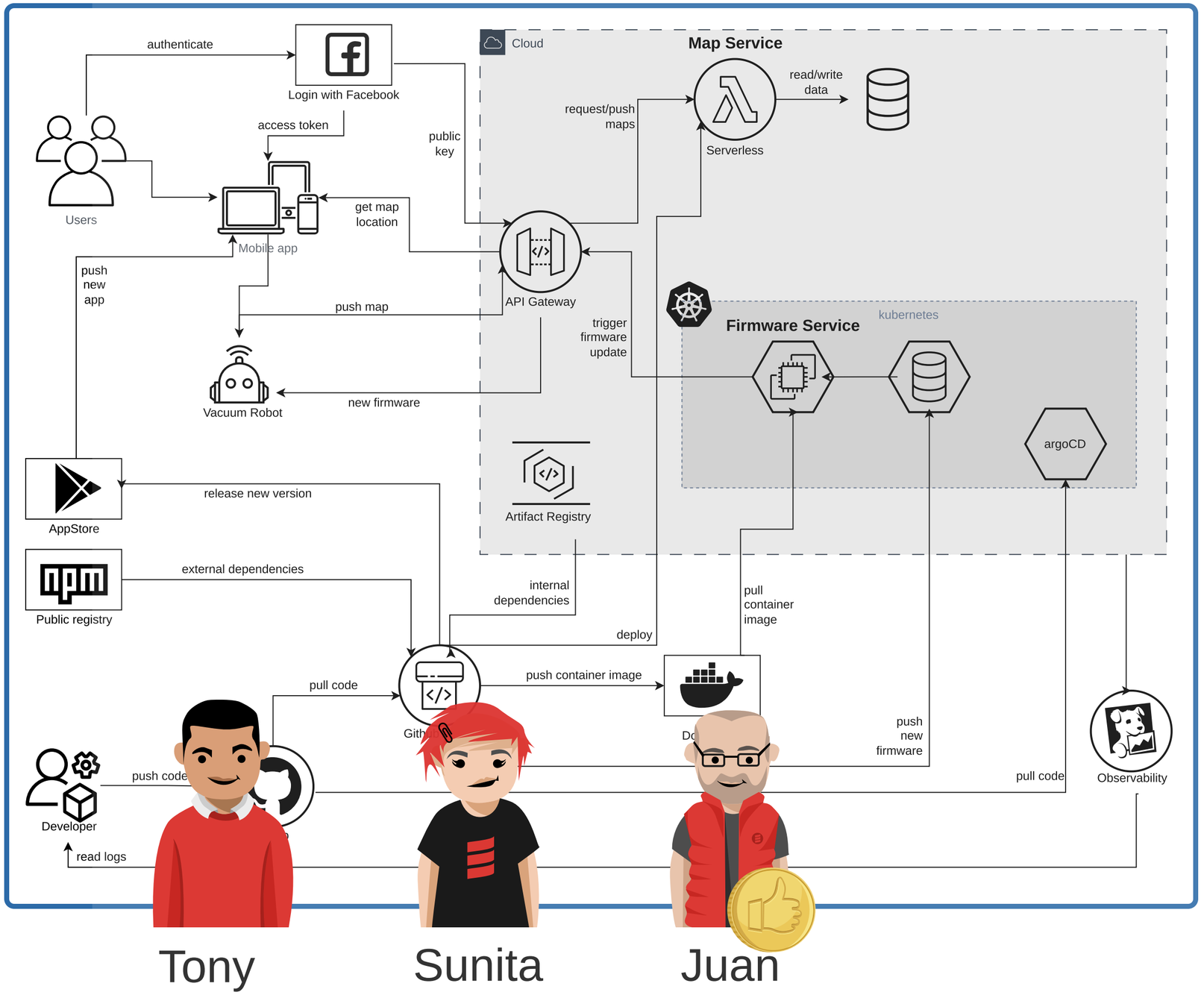

authenticate
Login with Facebook
Cloud
Map Service
read/write
data
request/push
maps
Serverless
access token
public
key
Users
Mobile app
get map
location
API Gateway
push
new
app
push map
trigger
firmware
update
kubernetes
Firmware Service
Vacuum Robot
new firmware
argoCD
Artifact Registry
release new version
AppStore
external dependencies
Public registry
internal
dependencies
pull
container
image
deploy
pull code
push container image
Gith
Do
push
new
firmware
push code
pull code
Observability
Developer
read logs
Tony
Sunita
Juan


authenticate
Login with Facebook
Cloud
Map Service
read/write data
request/push maps
Serverless
access token
public key
Users
Mobile app
get map location
API Gateway
push new app
push map
trigger firmware update
kubernetes
Firmware Service
Vacuum Robot
new firmware
argoCD
Artifact Registry
release new version
AppStore
external dependencies
Public registry
internal dependencies
pull container image
deploy
pull code
push container image
push new firmware
push code
pull code
Observability
Developer
read logs
Tony
Sunita
Juan

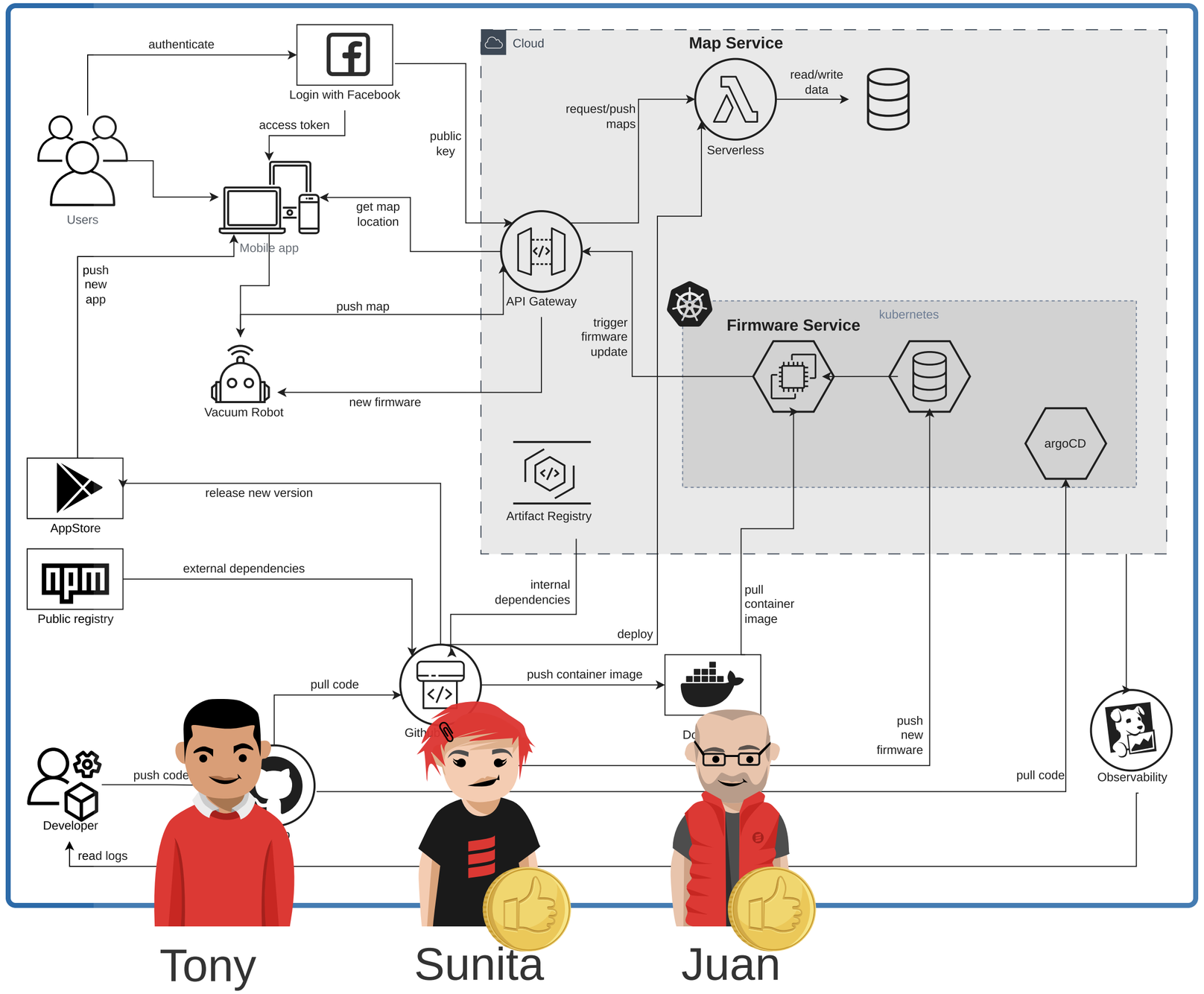

10
ten/delivery
We don't limit ingress or egress when running CI pipelines.
Missing network control
TNG
TECHNOLOGY CONSULTING



CI Pipeline kann ins Internet telefonieren

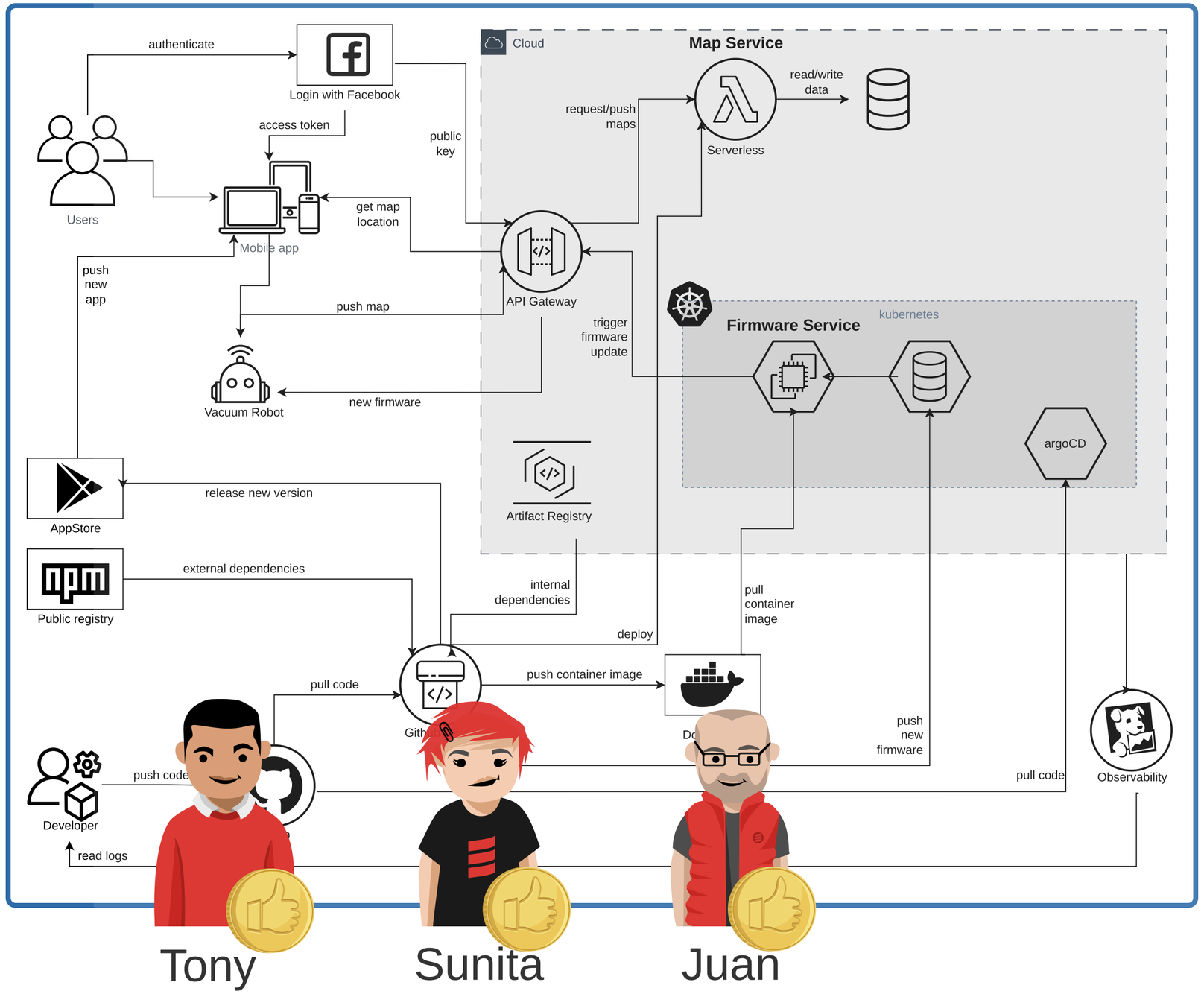


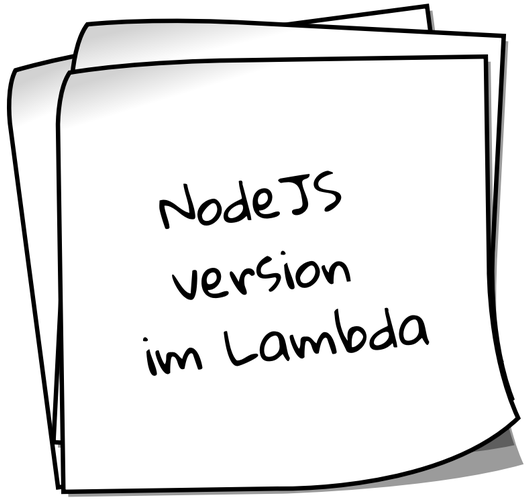
CI Pipeline kann ins Internet telefonieren


authenticate
Login with Facebook
access token
public key
Users
Mobile app
get map location
push new app
push map
Cloud
Map Service
request/push maps
read/write data
Serverless
API Gateway
trigger firmware update
kubernetes
Firmware Service
argoCD
Vacuum Robot
new firmware
Artifact Registry
release new version
AppStore
external dependencies
Public registry
internal dependencies
deploy
pull container image
pull code
push container image
push new firmware
pull code
Observability
push code
Developer
read logs
Tony
Sunita
Juan

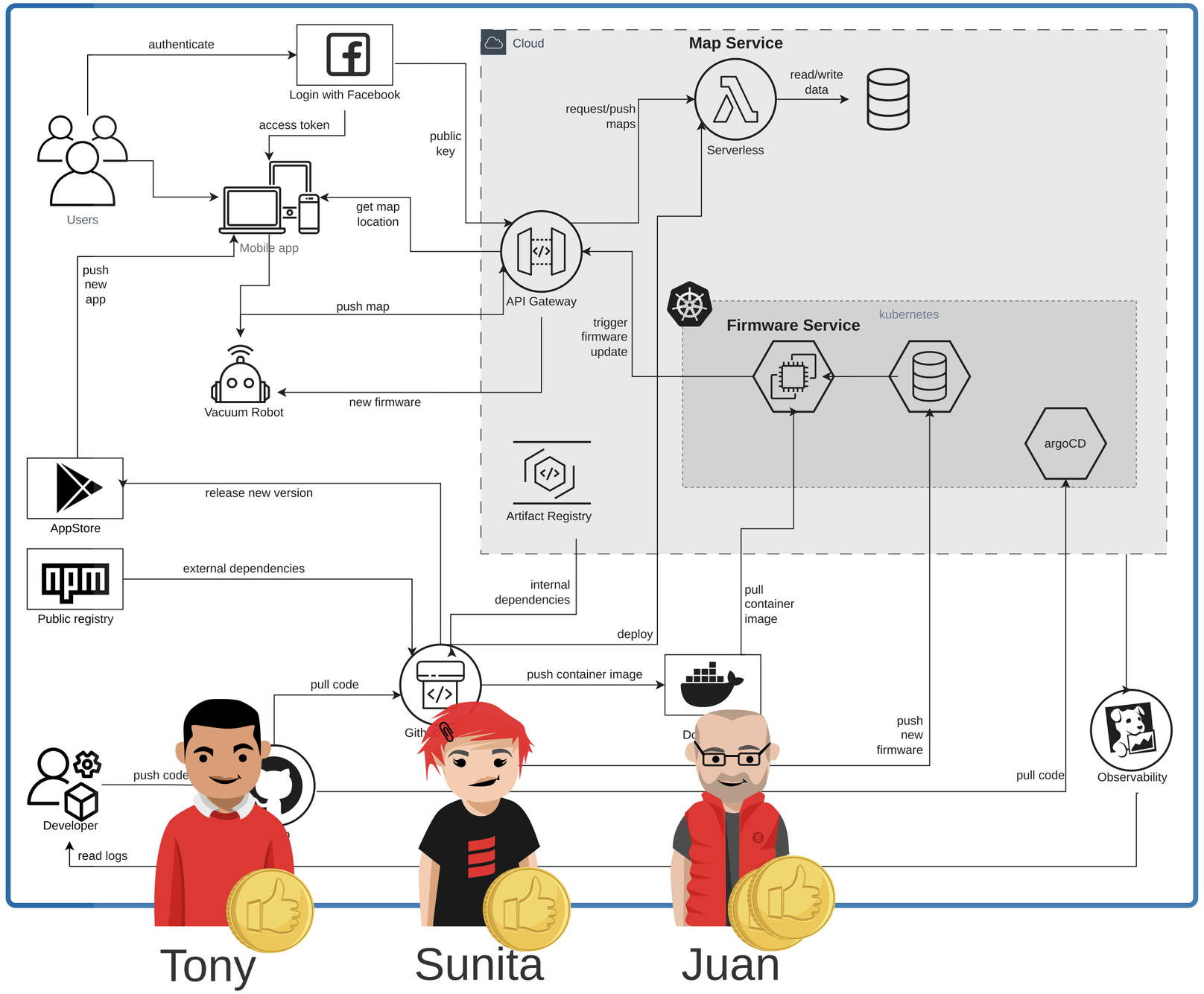

Ganz alter FB Client in der Handy-App

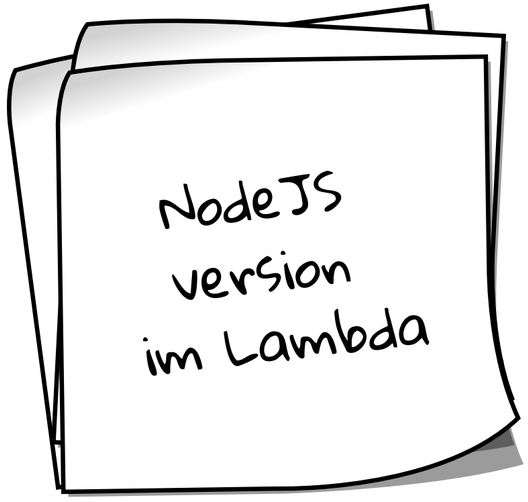

8
eight/delivery
Outdated dependencies
We use outdated dependencies of our runtime platform (OS, container image, serverless runtime).
TNG TECHNOLOGY CONSULTING


authenticate
Login with Facebook
Cloud
Map Service
read/write
data
request/push
maps
Serverless
access token
public
key
Users
get map
location
Mobile app
API Gateway
push
new
app
push map
trigger
firmware
update
kubernetes
Firmware Service
argoCD
Vacuum Robot
new firmware
Artifact Registry
release new version
AppStore
external dependencies
Public registry
internal
dependencies
pull
container
image
deploy
pull code
push container image
push
new
firmware
push code
pull code
Observability
Developer
read logs
Tony
Sunita
Juan

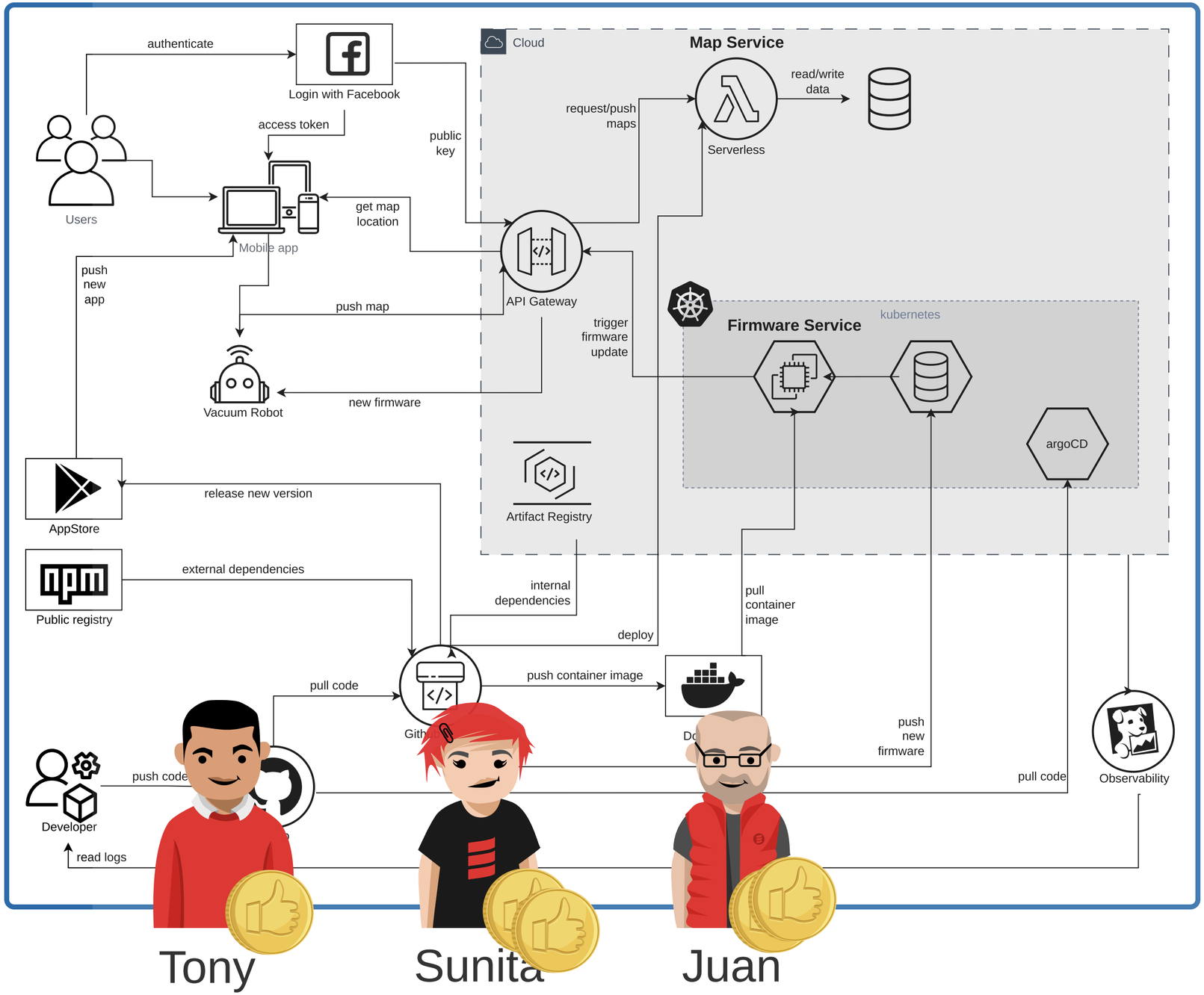

NodeJS
version
im Lambda


8
eight/delivery
Outdated dependencies
We use outdated dependencies of our runtime platform (OS, container image, serverless runtime).
TNG
TECHNOLOGY CONSULTING


authenticate
Login with Facebook
access token
public key
Users
Mobile app
get map location
push new app
push map
API Gateway
Cloud
Map Service
request/push maps
Serverless
read/write data
trigger firmware update
kubernetes
Firmware Service
argoCD
Vacuum Robot
new firmware
Artifact Registry
AppStore
release new version
Public registry
external dependencies
internal dependencies
deploy
pull container image
pull code
push container image
push new firmware
pull code
push code
Developer
read logs
Observability
Tony
Sunita
Juan


NodeJS
version
im Lambda


8
9
nine/access & secrets
Our Identity and Access Management lets authenticated users/developers grant themselves additional permissions.
Privilege escalation
TNG
TECHNOLOGY CONSULTING

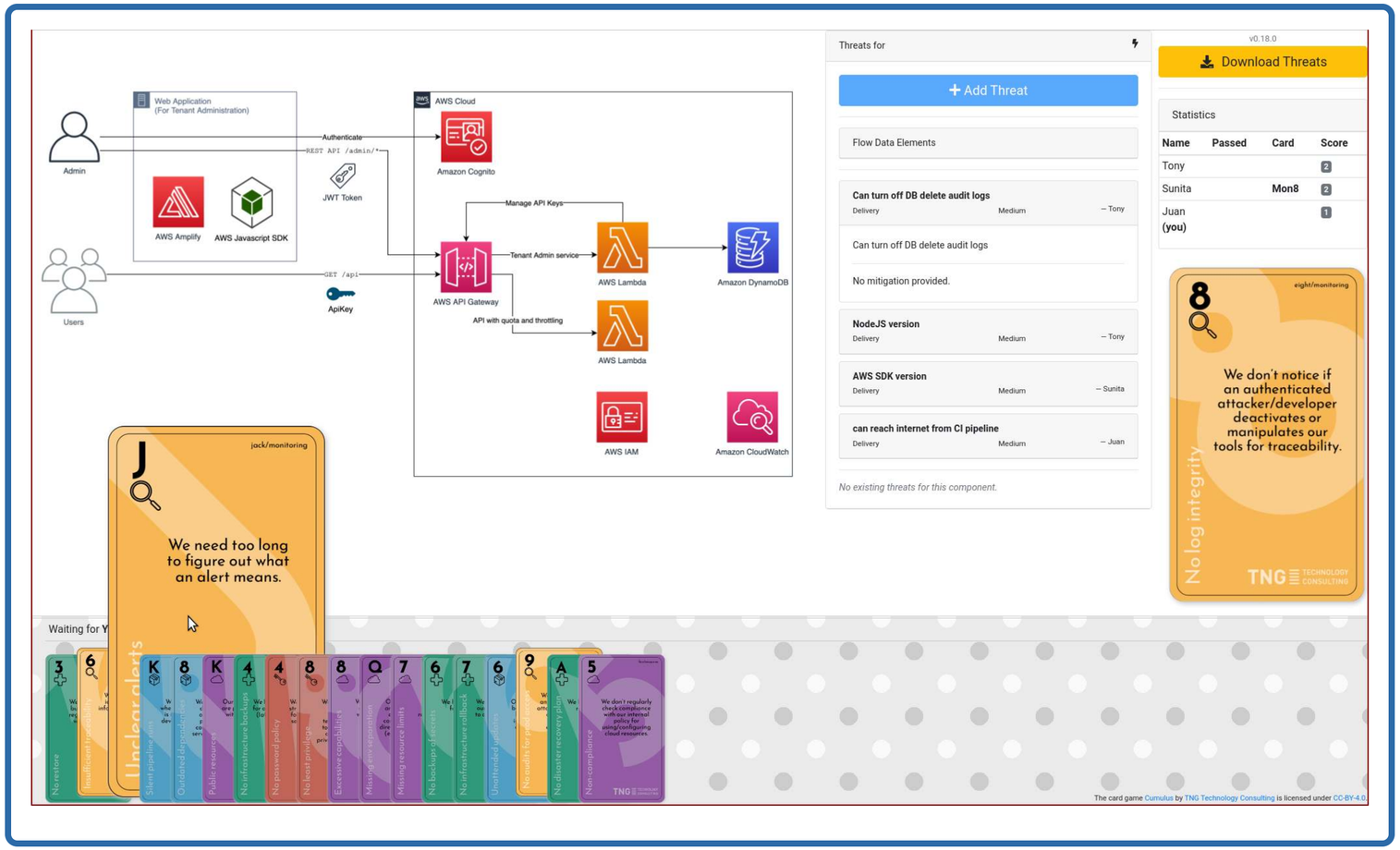

authenticate
Login with Facebook
access token
public key
Users
Mobile app
get map location
push new app
push map
Cloud
Map Service
request/push maps
read/write data
Serverless
API Gateway
trigger firmware update
kubernetes
Firmware Service
argoCD
Vacuum Robot
new firmware
Artifact Registry
release new version
AppStore
external dependencies
Public registry
internal dependencies
deploy
pull container image
pull code
push container image
push new firmware
pull code
Observability
push code
Developer
read logs
Tony
Sunita
Juan


Devs können
DB logs
überschreiben


8
9
nine/access & secrets
Our Identity and Access Management lets authenticated users/developers grant themselves additional permissions.
Privilege escalation
TNG
TECHNOLOGY CONSULTING

Online Version

Kein Darkmode! 😢



github.com/TNG/elevation-of-privilege

Agenda

- Intro: Threat Modeling
- Scenario
- Ernsthafte Kartenspiele
- Conclusion

Wir brauchen Hilfe!

Input für Cumulus:

- Cloud Security Best Practices
- OWASP Top10 CI/CD
- CIS Benchmarks
- *Aber größtenteils:* Erfahrung bei TNG

🙏 Bitte erstellt issues and pull requests! 🙏

💪 Es soll ein Community Projekt werden! 💪

github.com/OWASP/cumulus

Thank you!

Any questions?

Christoph Niehoff

christoph.niehoff@tngtech.com

github.com/OWASP/cumulus


3
three/access & secrets
Our secrets are long-lived and can be reused when they get leaked.
Long-living secrets
TNG TECHNOLOGY CONSULTING


5
f ve/access & secrets
We (as developers) have access to technical credentials.
Access to credentials
TNG TECHNOLOGY CONSULTING


8
eight/access & secrets
We don't restrict permissions (developers, technical users) to the minimum, allowing for a privilege escalation.
No least privilege
TECHNOLOGY


10
ten/access & secrets
We don't enforce MFA for developer access.
No MFA
TNG TECHNOLOGY CONSULTING


J
jack/access & secrets
Our deployment artifacts contain secrets that can be extracted.
Secrets in artifacts
TNG TECHNOLOGY CONSULTING


K
king/access & secrets
We don't use an established solution for credential management.
Poor secrets management
TNG TECHNOLOGY CONSULTING


2
two/delivery
We don't know the versions of our dependencies or whether they are up to date.
No SBOM
TNG TECHNOLOGY CONSULTING


4
four/delivery
We don't know the source repository of our dependencies.
Dependency confusion
TNG TECHNOLOGY CONSULTING


10
ten/delivery
We don't limit ingress or egress when running CI pipelines.
Missing network control
TNG TECHNOLOGY CONSULTING


Q
queen/delivery
We are not certain which code/artifacts we are deploying.
No source code integrity
TNG TECHNOLOGY CONSULTING


K
king/delivery
We won't notice when a deployment is started from a developer account.
Silent pipeline runs
TNG TECHNOLOGY CONSULTING


A
ace/delivery
We won't notice when someone alters the deploy pipeline.
Silent pipeline changes
TNG TECHNOLOGY CONSULTING


6
six/recovery
No backups of secrets
We have no backups for our secrets.
TNG TECHNOLOGY CONSULTING


7
seven/recovery
No infrastructure rollback
We cannot restore our infrastructure to a previous state.
TNG TECHNOLOGY CONSULTING


10
ten/recovery
Unsafe data deletions
We don't create backups before deleting important data.


J
jack/recovery
No backup redundancy
All our backups can be destroyed at once, due to lack of redundancy.
TNG TECHNOLOGY CONSULTING


Q
queen/recovery
Missing backup integrity
We can't tell whether our backup has been modif ed.
TNG TECHNOLOGY CONSULTING


K
king/recovery
Broad delete permissions
We can have the same person deleting resources and their backups.
TNG TECHNOLOGY CONSULTING


5
f ve/monitoring
Information disclosure
We don't restrict access to the sensitive parts of our logs.
TNG TECHNOLOGY CONSULTING


6
six/monitoring
Insuf cient traceability
We can't easily identify useful information in logs.
TNG TECHNOLOGY


7
seven/monitoring
Missing cost alerting
We won't get an alert if an end user generates huge cloud bills for us.
TNG TECHNOLOGY CONSULTING


8
eight/monitoring
No log integrity
We don't notice if an authenticated attacker/developer deactivates or manipulates our tools for traceability.
TNG TECHNOLOGY CONSULTING


9
nine/monitoring
No audits for prod access
We don't know if an authenticated attacker/developer accessed the production environment.
TNG TECHNOLOGY CONSULTING


Q
queen/monitoring
No incident response plan
We do not know how to react when our monitoring sends alerts.
TNG TECHNOLOGY CONSULTING


4
four/resources
Unreachable contact details
We can't get contacted by our cloud provider in case of emergency.
TNG TECHNOLOGY CONSULTING


9
nine/resources
Single point of failure
Our whole system can be af ected by a single rogue service.
TNG TECHNOLOGY CONSULTING


J
jack/resources
Missing egress control
We don't control egress traf c.
TNG TECHNOLOGY CONSULTING


Q
queen/resources
Missing env separation
Our production and staging environments are connected, either directly or indirectly (e.g. via CI/CD).
TNG TECHNOLOGY CONSULTING


K
king/resources
Public resources
Our cloud resources are publicly exposed without any need.
TNG TECHNOLOGY CONSULTING


A
ace/resources
No cloud policy
We have no clear policy for using/conf guring cloud resources.
TNG TECHNOLOGY CONSULTING