TEADAL

Establishing trust across computing continuum boundaries

1st TEADAL Workshop

Dr. Sebastian Werner - TU Berlin, Germany

Milan, 14/03/2024

WWW.TEADAL.EU

Trust Across Computing Continuum

Computing Continuum:

- highly distributed
- running unknown software or configurations
- increased uncertainty

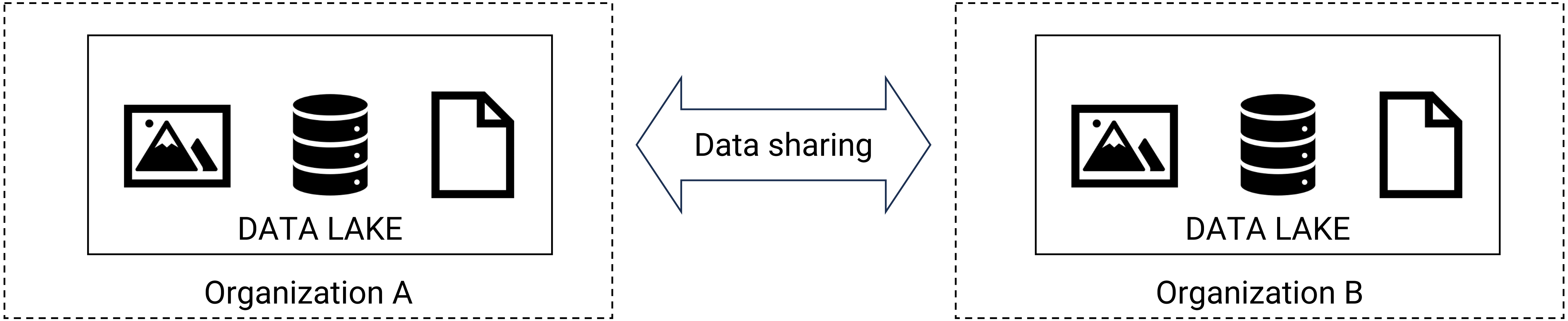
Trust in Software:

- a socio-technical concept
- focused on the people using software together
- reassurance that software is used according to shared understanding of it’s functionalities

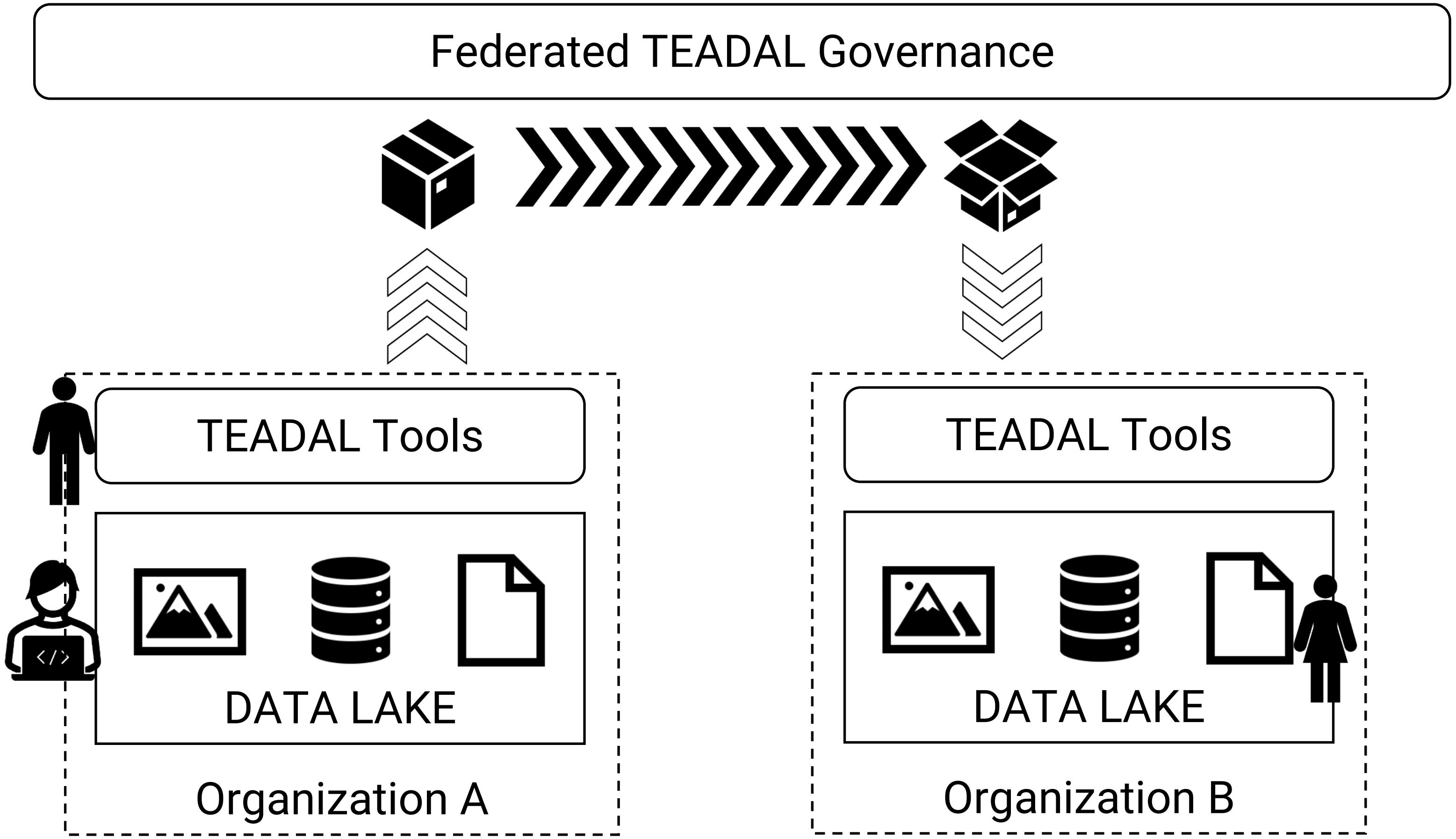
Trust Across Computing Continuum

- implies a need for assurances of functionality and their fulfilment
- transparency on the use of software (where, by whom)
- transparency in how software is functioning
- auditability, even within unreliable environments

Implication for data sharing in the cloud continuum?



Implication for data sharing in the cloud continuum?



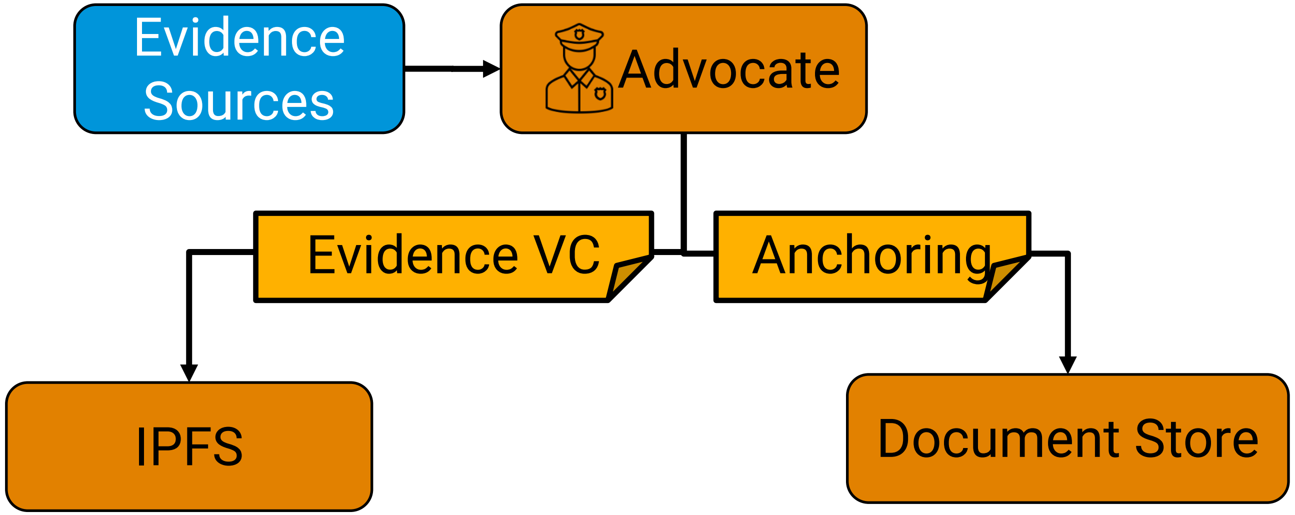
Finding Evidence

- What resources were used?
- What functions “took” the data?
- Who authorized the installation?
- Who allowed the data access?
- Who created the sharing pipeline?
- Who received the data?
- Where was the data moved to?
- Where was the data processed?

Edward Norton - Glass Onion: A Knives Out Mystery Netflix 2022

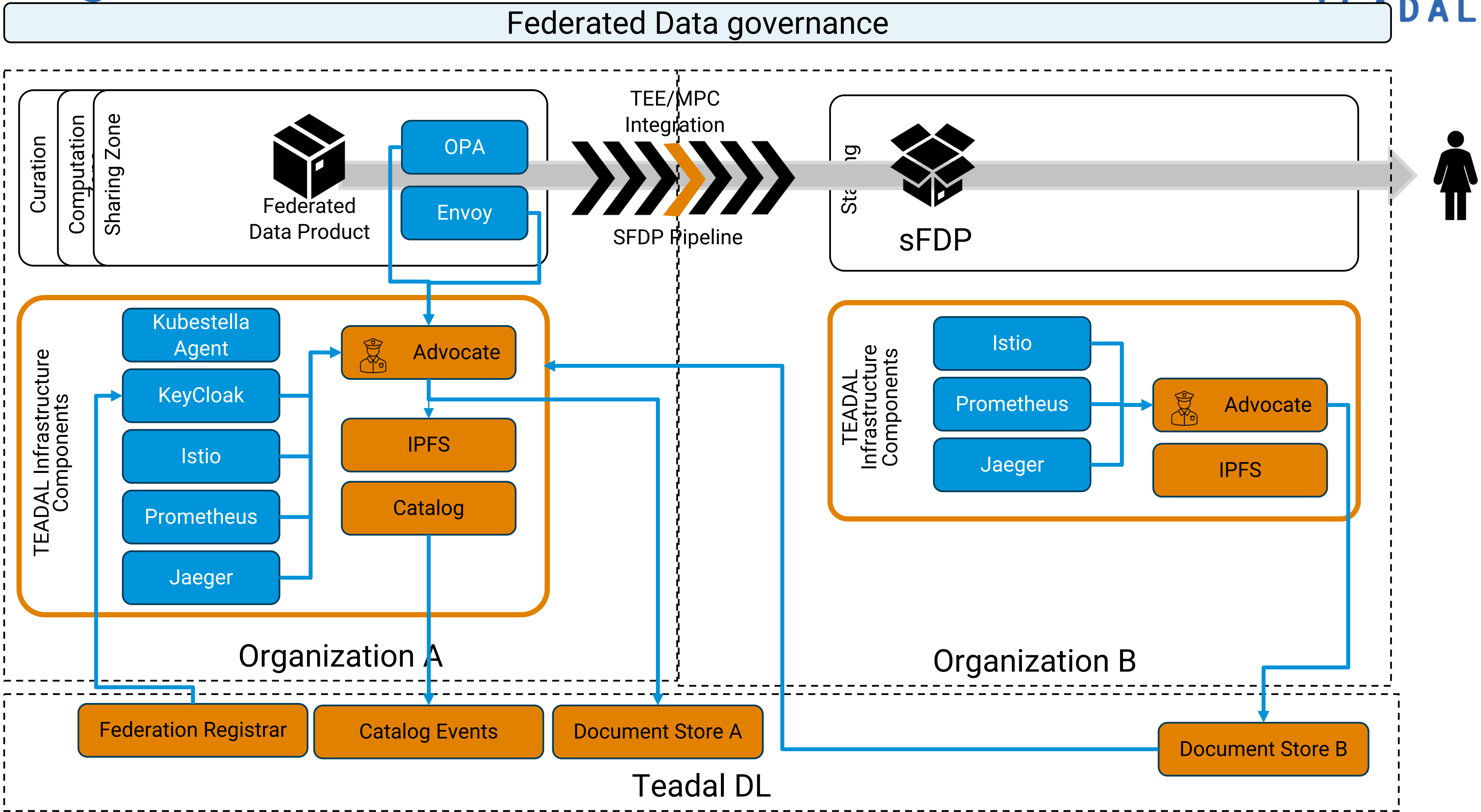
Who killed the host?

TEADAL Advocate



- Ingest evidence soruces
- Verify the origin and generate verifable and immutable evidecve credentials
- Link evidence together
- Combine evidence across all advocate instances

Using Advocate in Practice



Make it accessible

- Using cryptographic programmable poofs to check the evidence against agreements

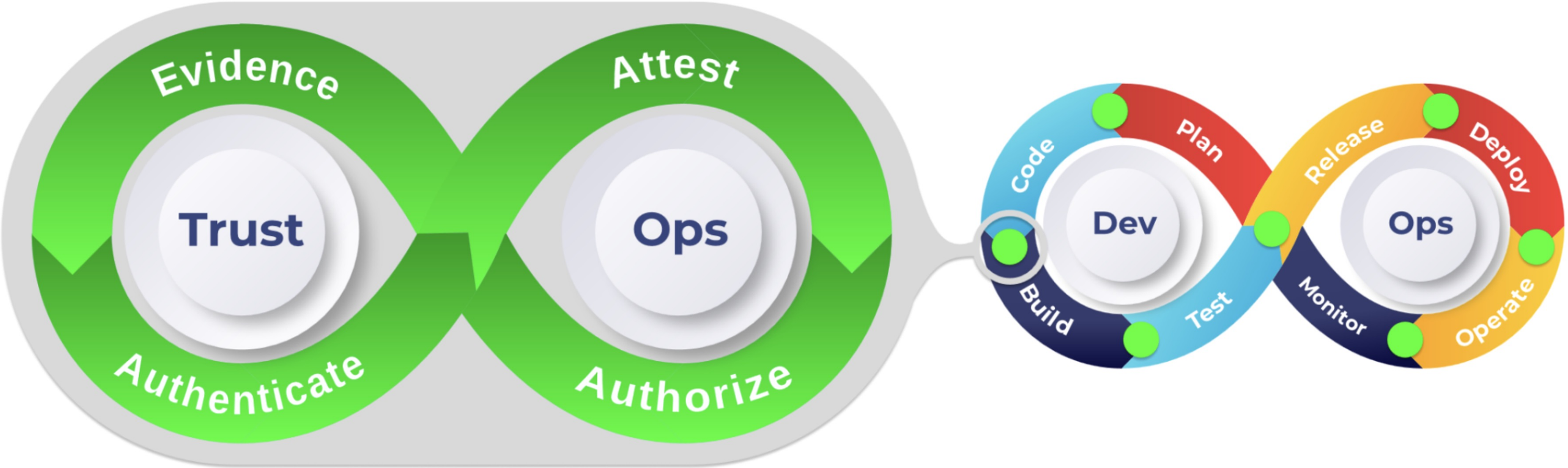
- Build up evidence chains across all TEADAL Nodes

- Accessible, e.g., through easy indicators

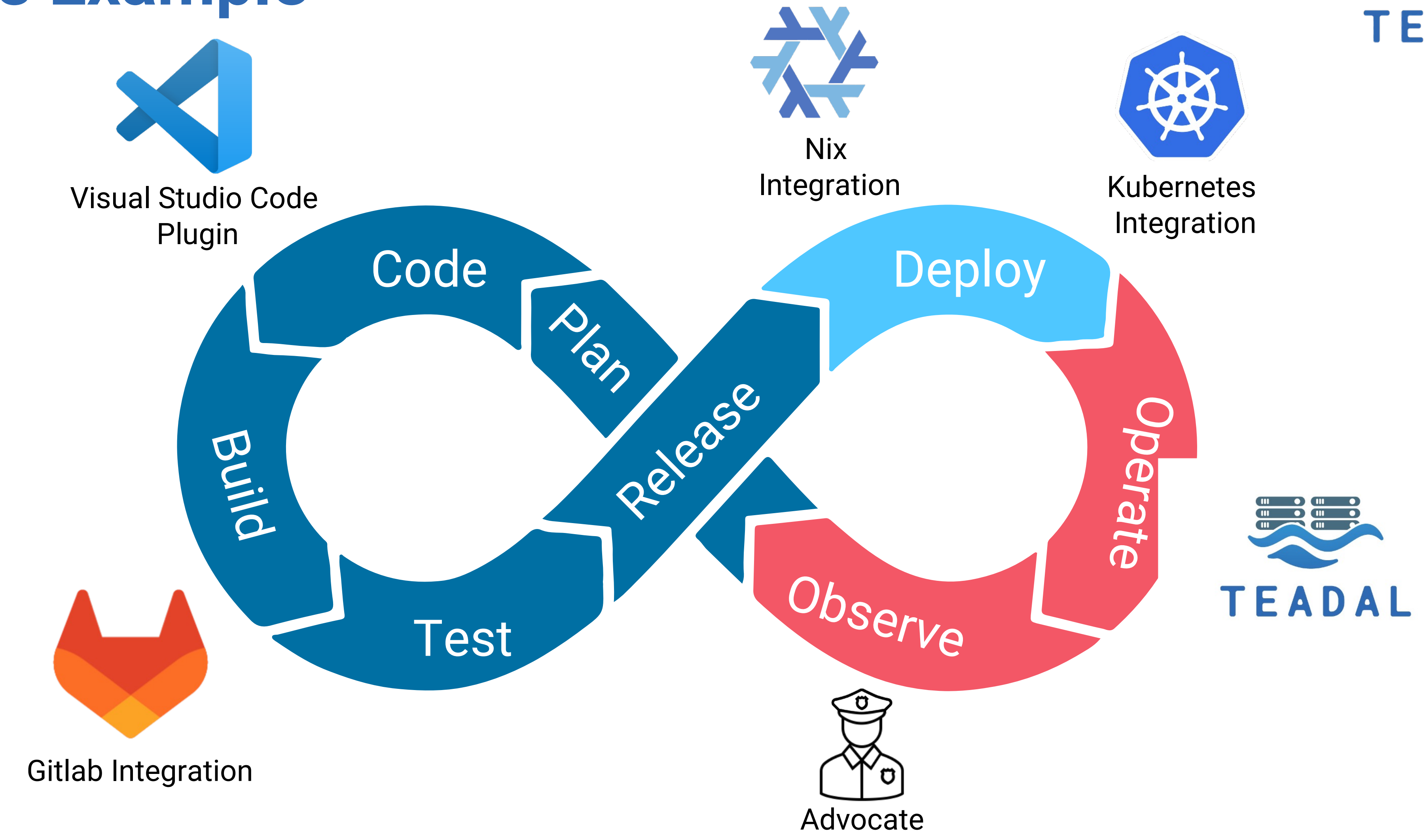
Danial Craig - Knives Out Netflix 2020

Can we extend the evidence collection, verification and proving to all aspects of the development and operation?

Trust Ops Approach



Trust Ops Example



Visual Studio Code Plugin

Nix Integration

Kubernetes Integration

Gitlab Integration

Advocate

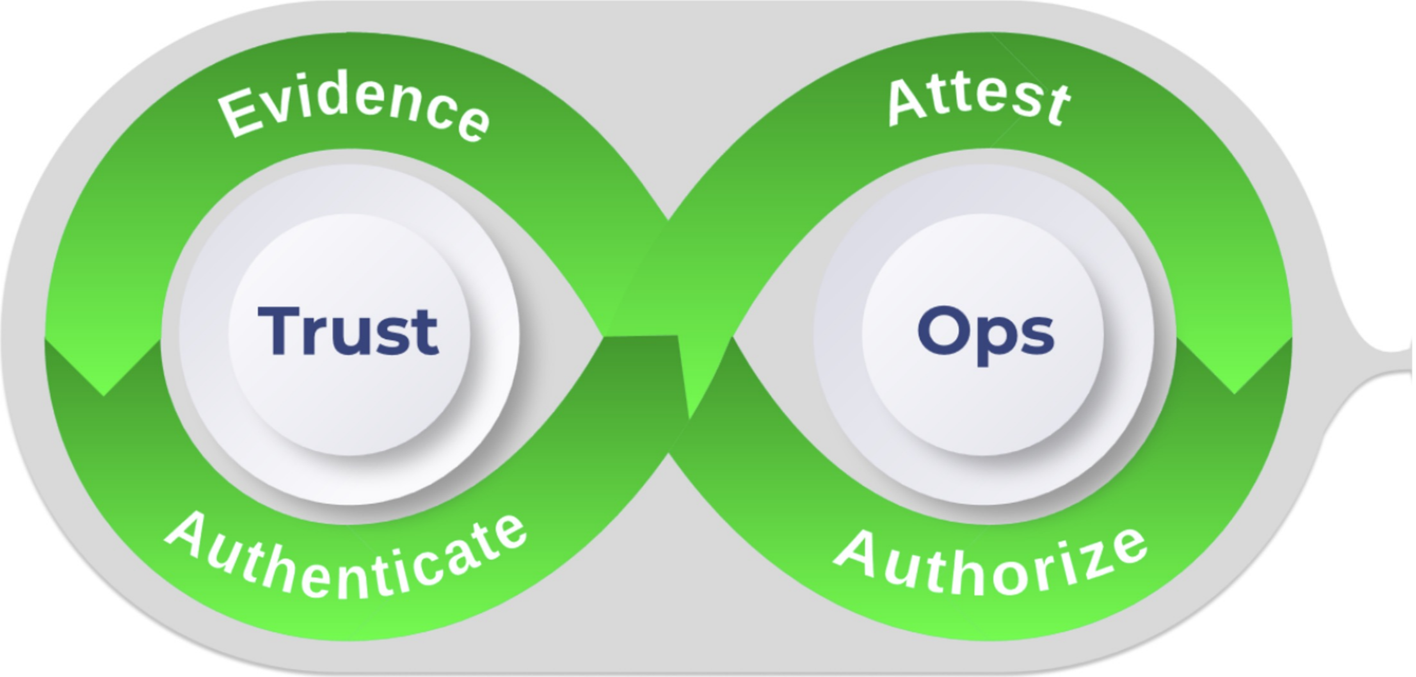
- Collect commits and author identities
- Enable commit policy enforcement, e.g., review all dependencies
- Ensure that the origin of code-changes are tracked

- Track the lifecycle of commits (PRs)
- Track testing (what thesis, where, …)

- verifiable installation of infrastructure using nix
- Kubernetes audits to track deployed and exposed components

- using runtime observations to attest interactions with deployed services
- register runtimes to organizations
- publish interaction observations as verifiable credentials
- record access decisions
- record data movement decisions from scheduling componentes

TrustOps applied in TEADAL



Provide end-user verifiable links to usage of the FDP, linking together evidence of FDP creation and deployment, data sharing process execution and access observations.

Take aways

… TODO for next time ;)