Bedrohungsanalyse

für Devs

Meissa GmbH

- Sitz in Reutlingen | < 10 Mitarbeiter
- Fokus: DevOps, Cloud & Security
- Gemeinwohl & Datenschutz
  - OpenSource Ausbildung
  - Plastiksammeln



Was geht uns das an?

- **Richtlinie 2014/53/EU / Radio Equipment Directive (RED)**: ab 08.25
- **ISO/SAE 21434 - Road vehicles**
- **NIST 800-53**
- **Cyber Resilience Act (2024/2847/EU)**

Was geht uns das an?

Ich fände es tatsächlich gut, wenn keiner ...

- unsere Energieerzeugung abschaltet !
- mein Auto lahmlegt !
- den Zugfunk ausfallen lässt !
- Forgejo Sonntags um 4:00 Uhr morgens einen Sicherheits-Notfall antut !

Angriffe verstehen ?!

- Irgendwas schlimmes passiert ...



Das schwächste Glied ?!



Lebenslanges Lernen ?!

- Systeme verändern sich
- Bedrohungen verändern sich
- Ein Report, sie alle zu ...



threagile – das coole Vorbild

- System beschreiben mit Data Assets, Technical Assets, Trust Boundaries
- DevOps Style: yaml in git, Report Generierung mit CI
- Aber: Regeln als Domain Knowledge
  - Reglen in go → Kein Verständnis über Angriffe
  - Regeln sind opinionated – nicht allgemein

dda-tara

- Die Systembeschreibung aus threagile
- Angriffe mit Attack-Trees verstehen
- Well Known Attacks included
- Reports einfacher über die Kette Asciidoc → PDF
- Library, da jede Analyse immer Besonderheiten hat, die nicht in ein „Well Known“ passen.

Bsp forgejo-tara: Data Asset

```yaml
# yaml-language-server: $schema=https://run.threagile.io/schema.json
# SPDX-License-Identifier: CC-BY-SA-4.0
# SPDX-FileCopyrightText: 2026 The Forgejo Authors

data_assets:
  ap-like:
    description: >
      Represents a like. Links to a person and a repository.
    usage: business
    tags:
      - activity-pub
      - in-order-activities
    origin: distant-server-instance
    owner: actor (person or group)
    quantity: many
    confidentiality: public
    integrity: important
    availability: important
```

Bsp forgejo-tara: Technical Asset

```
technical_assets:
  local-forgejo-instance:
    description: The local forgejo instance, user is logged in at
    type: external-entity
    usage:
    used_as
    out_of_
    size: application
    technology: application-server
    tags:
    internet: true
    machine: container
    encryption: transparent
    owner: We
    confidentiality: public
    integrity: critical
    availability: critical
    multi_tenant: true
    redundant: false
    custom_developed_parts: false
    data_assets_processed: ...
    data_assets_stored: ...
    data_formats_accepted: ...
    communication_links: ...
```

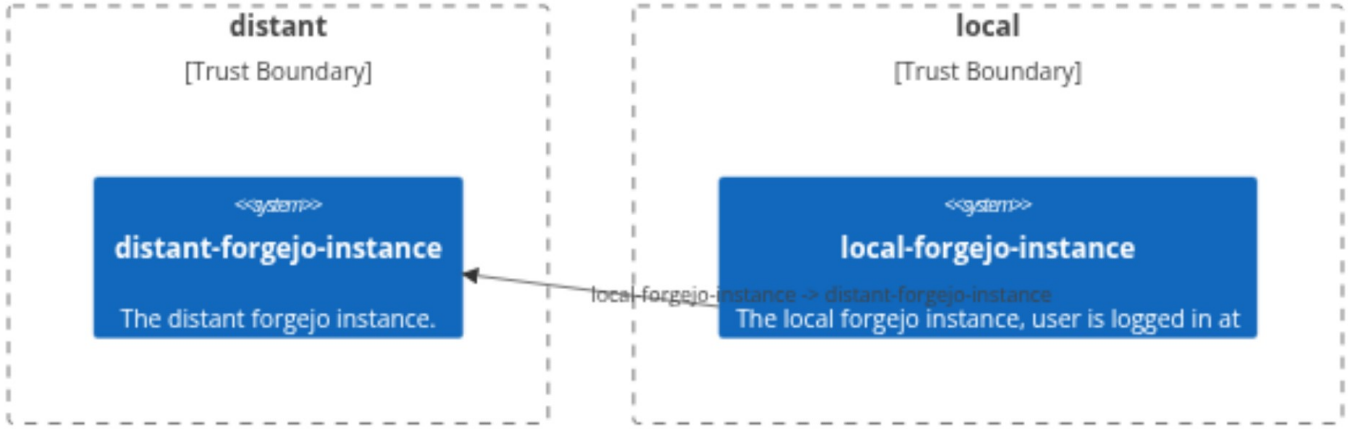
```
business
devops
```

Bsp forgejo-tara: Trust Boundary

```
trust_boundaries:
  local:
    description: Network of local server
    type: execution-environment
    tags:
    technical_assets_inside:
      - local-forgejo-instance
    trust_boundaries_nested:
```

Bsp forgejo-tara: Trust Boundary

```
trust_boundaries:
  local:
    description: Network of local server
    type: execution-environment
    tags:
    technical_assets_inside:
      - local-forgejo-instance
    trust_boundaries_nest
```



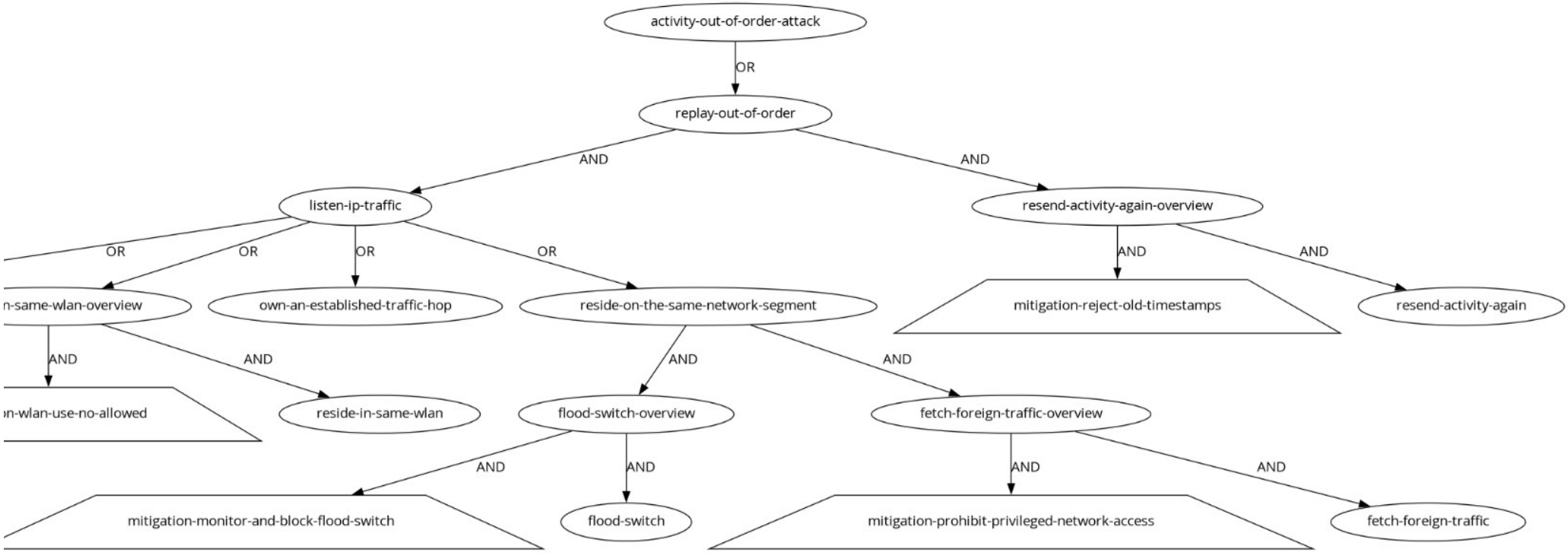
Bsp forgejo-tara: Attack Tree

```yaml
includes-as-text:
  - well-known-attack-tree-lib/out-of-order-information.yaml
  - well-known-attack-tree-lib/externally-controlled-reference.yaml
  - well-known-attack-tree-lib/injection.yaml
  - well-known-attack-tree-lib/authentication.yaml
  - well-known-attack-tree-lib/dos.yaml

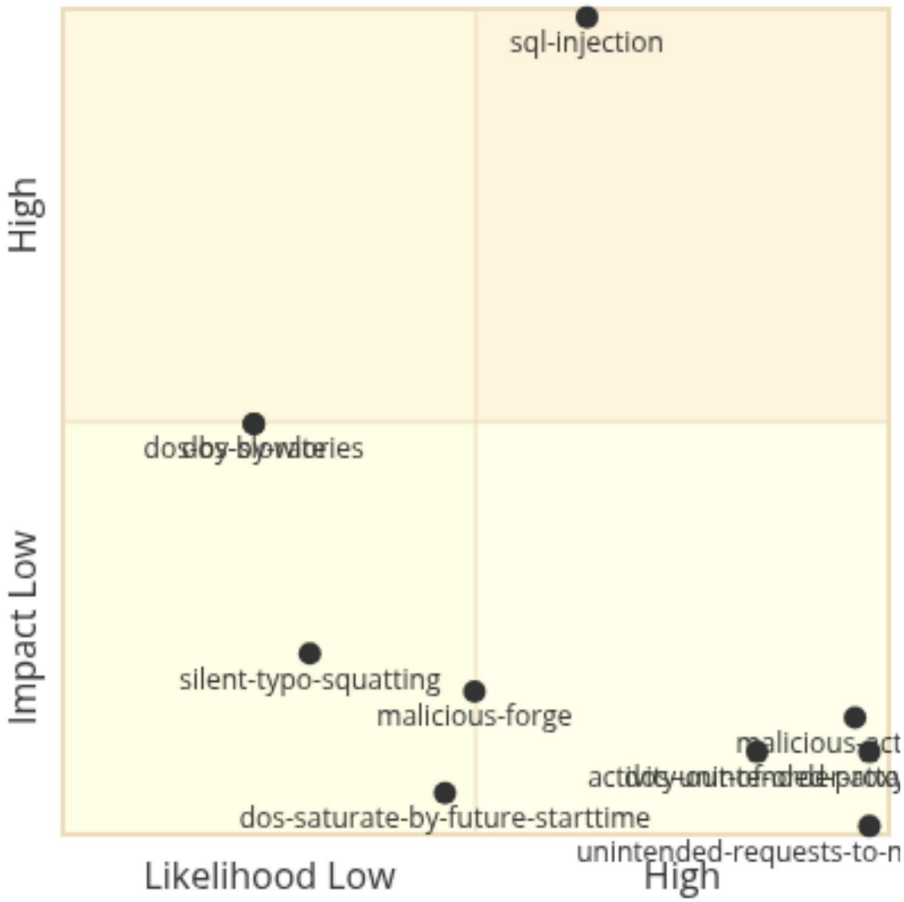
mitigations_active: …

attacks_used:
  activity-out-of-order-attack:
    <<: *out-of-order-attack
    description: >
      Experienced Hacker records activities sends again Unlike Activities hap
      but was succeeded by an Like. Our instance accept the Unlike and remove
      Our repository gets rated unintended bad.
    score:
      Damage: 10
      AffectedUsers: 10
  dos-unintended-proxy-or-intermediary: …
  sql-injection: …
```

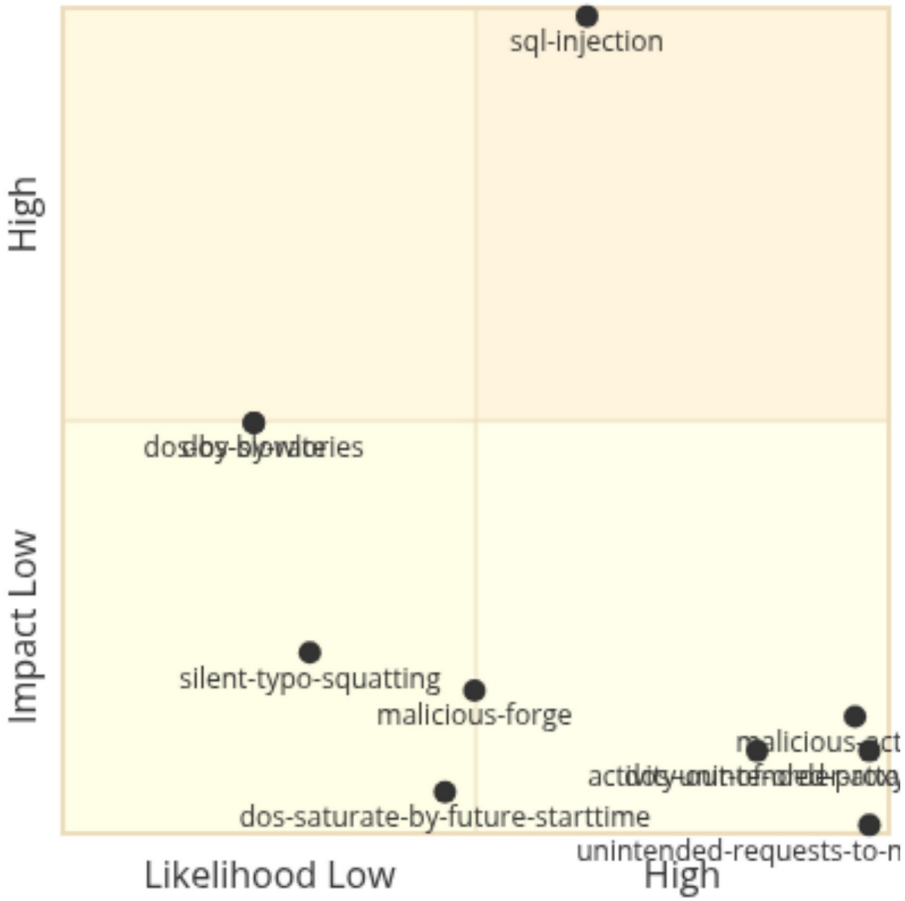
Bsp forgejo-tara: Attack Tree



Bsp forgejo-tara: Mitigations active



Bsp forgejo-tara: Mitigations active





Bsp forgejo-tara: individual rules

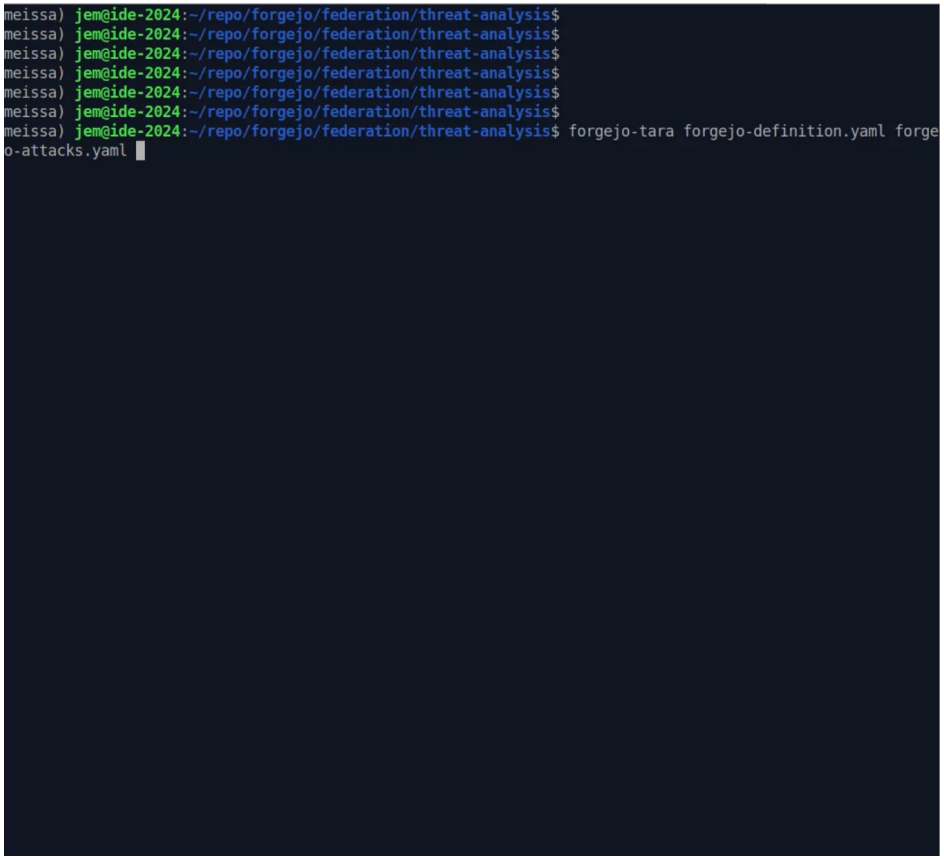
```yaml
attacks_used:
  activity-out-of-order-attack:
    <<: *out-of-order-attack
    description: >
      Experienced Hacker records ac
      but was succeeded by an Like.
      Our repository gets rated uni
    score:
      Damage: 10
      AffectedUsers: 10
```

Bsp forgejo-tara: individual rules

```
attacks_used:
  activity-out-of-order-attack:
    <<: *out-of-order-attack
    des
      E
      b
      O
    sco
      D
      A
```

```
(defn-spec order-related-assets ::m/threat
  [source ::ta/technical-asset …
  (let [in-order-assets (ta/data-asset-filtered
                         assets-affected
                         (fn [x] (some #(= "in-order-activities" %) (:tags x)))
                         threagile)]
    (when (pos? (count in-order-assets))
      {:id (str "out-of-order-threat: " (:id source) " -> " (:id target))
       :data-assets in-order-assets
       :link link
       :attack (get-in attacks [:attacks_used :activity-out-of-order-attack])})))
```

Demo


meissa) jem@ide-2024:~/repo/forgejo/federation/threat-analysis$
meissa) jem@ide-2024:~/repo/forgejo/federation/threat-analysis$
meissa) jem@ide-2024:~/repo/forgejo/federation/threat-analysis$
meissa) jem@ide-2024:~/repo/forgejo/federation/threat-analysis$
meissa) jem@ide-2024:~/repo/forgejo/federation/threat-analysis$
meissa) jem@ide-2024:~/repo/forgejo/federation/threat-analysis$
meissa) jem@ide-2024:~/repo/forgejo/federation/threat-analysis$ forgejo-tara forgejo-definition.yaml forge
o-attacks.yaml

Fazit

- Git & CI
- IDE Unterstützung
- Attack-Tree sind sprechend
- Well known Attacks
- Mach schon fast Spass

URLs und Quellen



dda-tara



meissa/plastik



forgejo-tara



forgejo-contrib/federation