OWASP®

DEPENDENCY-TRACK COMMUNITY MEETING

JULY
2024

THE DEPENDENCY-TRACK TEAM

www.owasp.org

AGENDA

01 Project Updates

02 Global AppSec EU

03 Demos

04 CycloneDX 1.6 Ecma Standard

05 Q&A

OWASP®

PROJECT UPDATES

PROJECT UPDATES

v4.11.4, v4.11.5 Released 🎉

- v4.11.4: June 24th
  - ⚠️ Fixed XXE vulnerability, exploitable via upload of XML BOMs
  - Support for import of CycloneDX v1.6 BOMs
  - Translation improvements for Chinese 🇨🇳 and German 🇩🇪
- v4.11.5: July 8th
  - Fixed mirroring of NVD via REST API
- Few bugfixes backported from the in-progress v4.12.0

https://docs.dependencytrack.org/changelog/

OWASP®

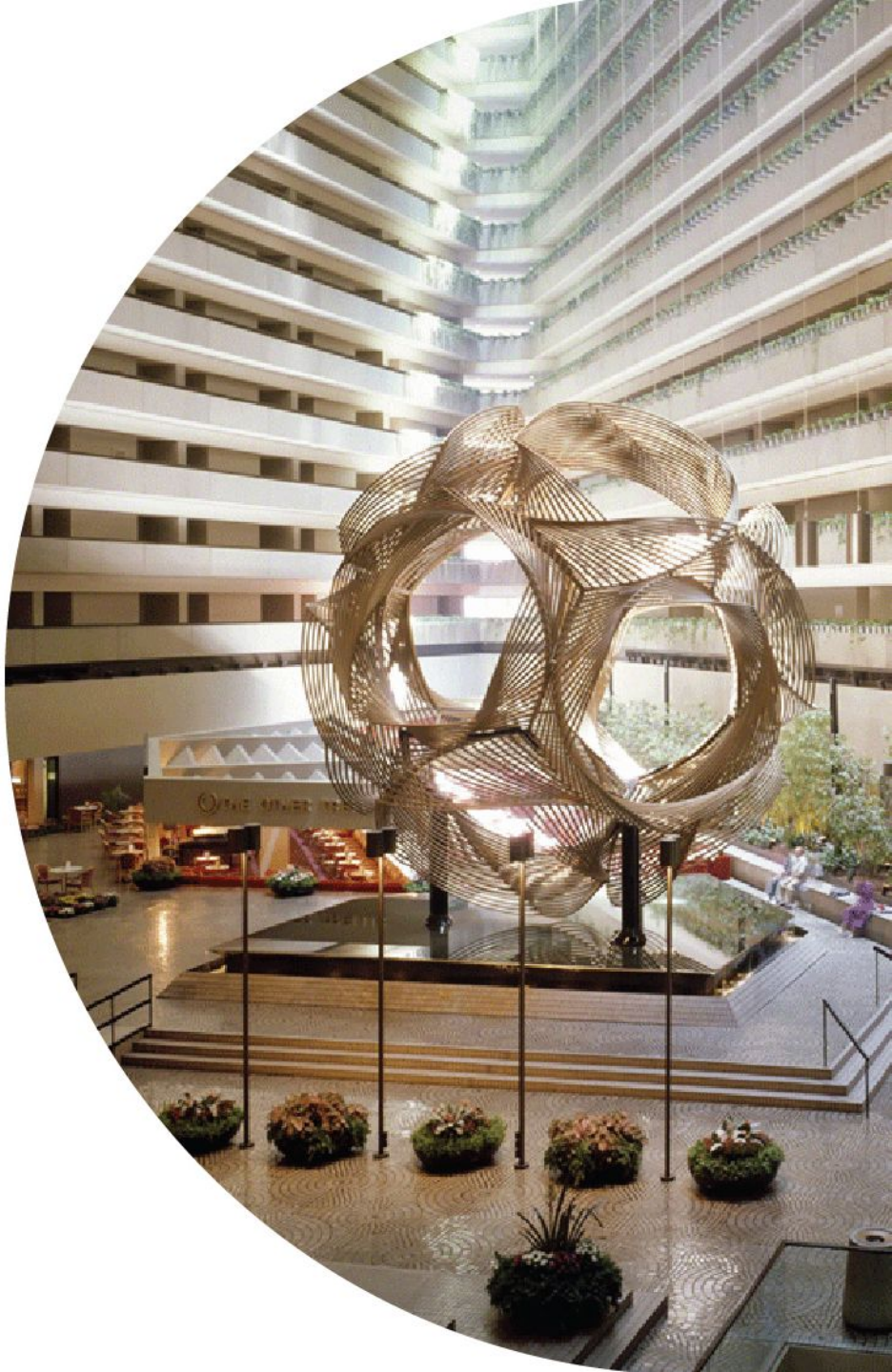
GLOBAL APPSEC EU

OWASP 2024 GLOBAL AppSec | SAN FRANCISCO SEPT 23-27 | HYATT REGENCY

CfP:

(ends July 16th)

https://owasp.submittable.com/submit/296405/2024-owasp-global-appsec-sf-cfp



PROJECT UPDATES

New in v4.12.0: Tag Management

- What tags do I have in my system?
- What projects/policies/notifications is a tag associated with?
- Tagging of projects upon BOM upload
- Un-tagging of projects/policies/notifications in a central place
- Deletion of tags in a central place
- Bulk tagging & un-tagging via REST API
- Bulk tag deletion via REST API
- Autocomplete for tag input fields in the UI

OWASP®

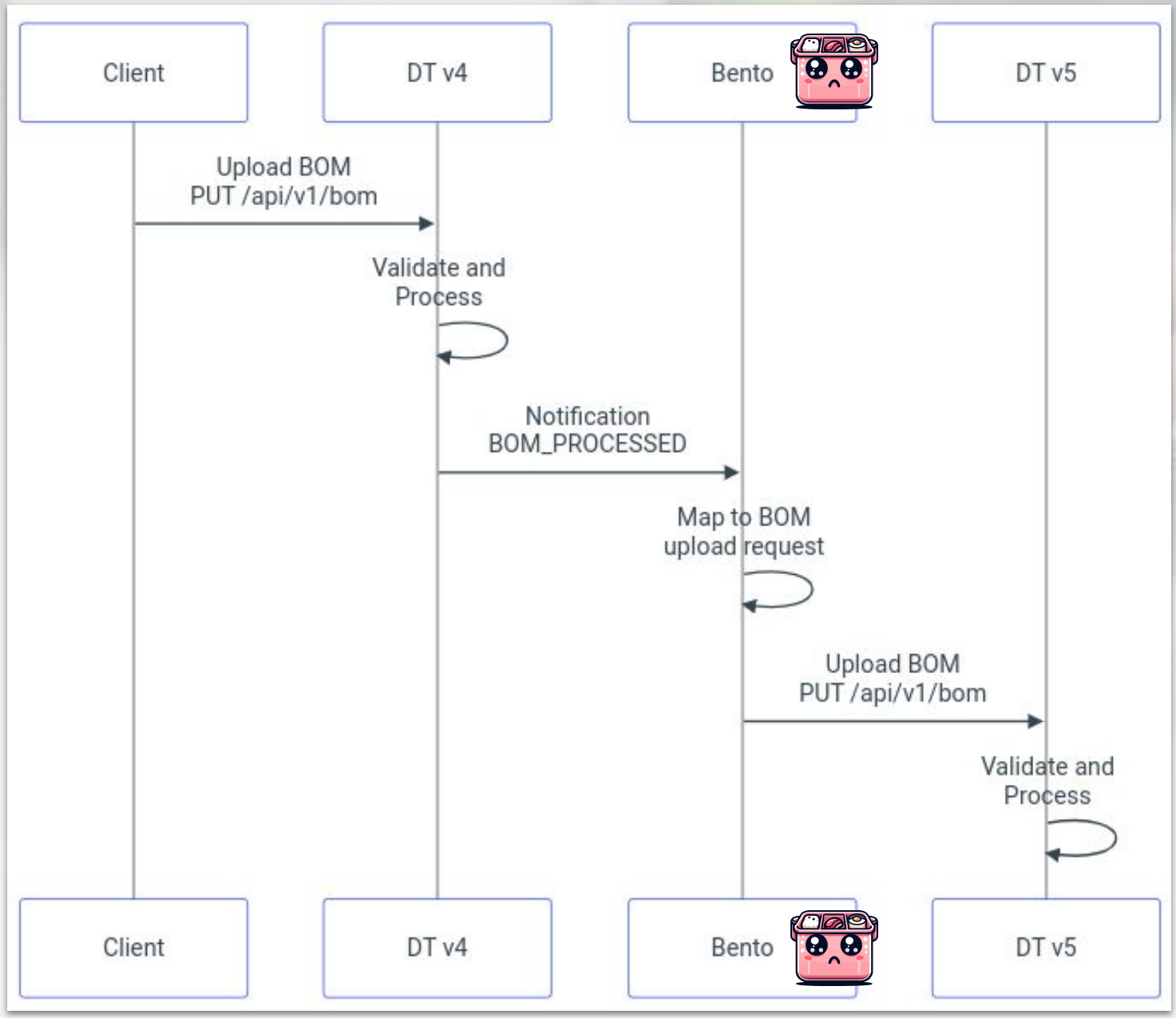
DEMO:
TAG MANAGEMENT

PROJECT UPDATES

Running multiple DT instances in parallel

- Use Cases:
  - Testing v5 (Hyades) while running v4 in production
  - Staging environment to test new releases
  - Test environment to test `snapshot` builds
- Problems:
  - How to get realistic test data (BOMs)?
  - How to get it in production-like velocity?
  - How to *not* impact the production system?

https://dependencytrack.github.io/hyades/latest/getting-started/migrating-from-v4/#running-v4-and-v5-in-parallel



DEMO: RUNNING MULTIPLE INSTANCES IN PARALLEL

OWASP®

CYCLONEDX 1.6 ECMA STANDARD

QUESTIONS & ANSWERS