OWASP®

DEPENDENCY-TRACK COMMUNITY MEETING

MARCH 2024

THE DEPENDENCY-TRACK TEAM

www.owasp.org

OWASP

AGENDA

Project Updates 01

Cryptography Bill of Materials 02

Meeting Schedule 03

Q&A 04

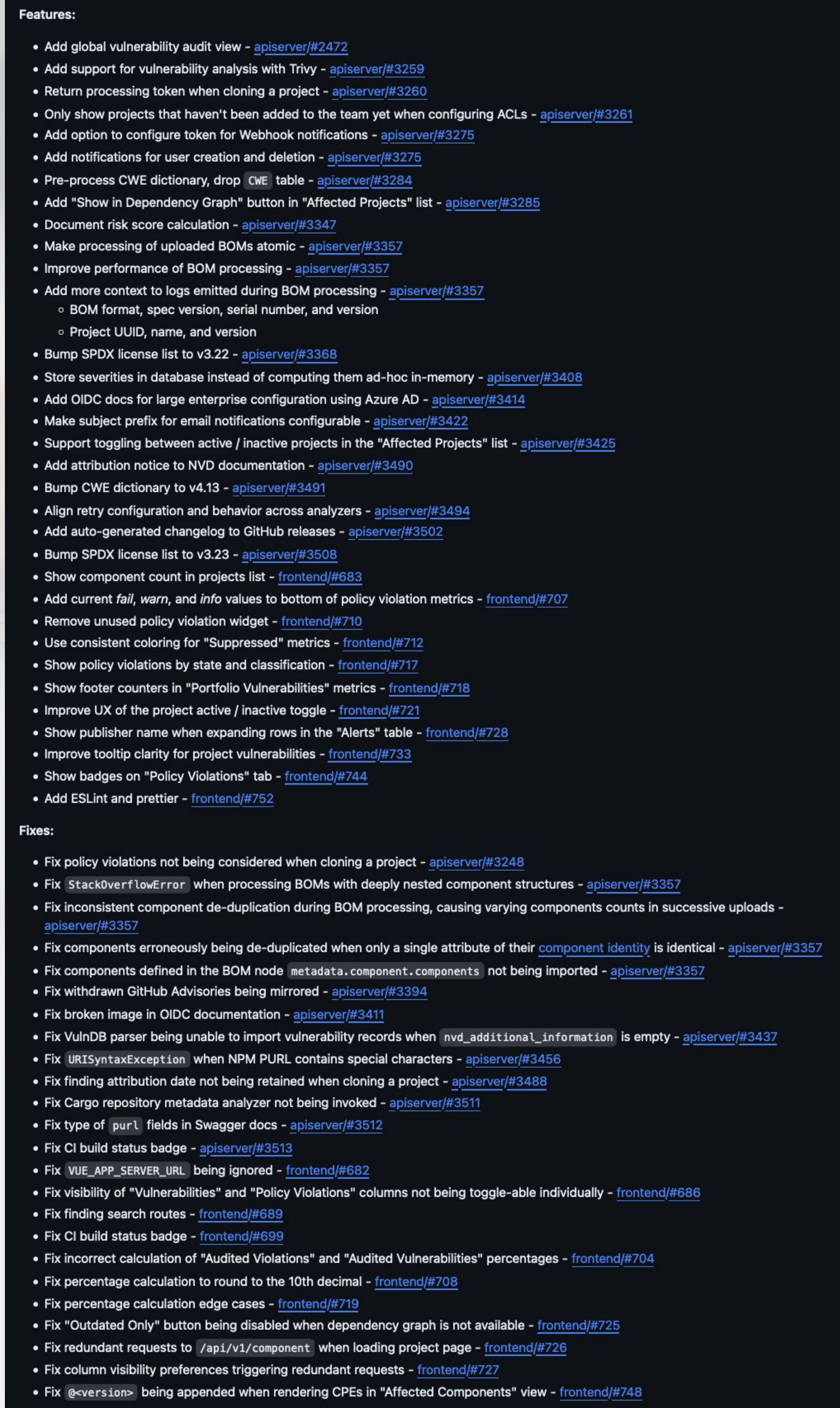
OWASP®

PROJECT UPDATES

PROJECT UPDATES

v4.11.0

- Behind release target, but making good progress
- Not immune to scope creep (._.)
- Numerous new contributors, thank you!



Features:

- Add global vulnerability audit view - apiserver/#2472
- Add support for vulnerability analysis with Trivy - apiserver/#3259
- Return processing token when cloning a project - apiserver/#3260
- Only show projects that haven't been added to the team yet when configuring ACLs - apiserver/#3261
- Add option to configure token for Webhook notifications - apiserver/#3275
- Add notifications for user creation and deletion - apiserver/#3275
- Pre-process CWE dictionary, drop `CWE` table - apiserver/#3284
- Add "Show in Dependency Graph" button in "Affected Projects" list - apiserver/#3285
- Document risk score calculation - apiserver/#3347
- Make processing of uploaded BOMs atomic - apiserver/#3357
- Improve performance of BOM processing - apiserver/#3357
- Add more context to logs emitted during BOM processing - apiserver/#3357
  - BOM format, spec version, serial number, and version
  - Project UUID, name, and version
- Bump SPDX license list to v3.22 - apiserver/#3368
- Store severities in database instead of computing them ad-hoc in-memory - apiserver/#3408
- Add OIDC docs for large enterprise configuration using Azure AD - apiserver/#3414
- Make subject prefix for email notifications configurable - apiserver/#3422
- Support toggling between active / inactive projects in the "Affected Projects" list - apiserver/#3425
- Add attribution notice to NVD documentation - apiserver/#3490
- Bump CWE dictionary to v4.13 - apiserver/#3491
- Align retry configuration and behavior across analyzers - apiserver/#3494
- Add auto-generated changelog to GitHub releases - apiserver/#3502
- Bump SPDX license list to v3.23 - apiserver/#3508
- Show component count in projects list - frontend/#683
- Add current *fail*, *warn*, and *info* values to bottom of policy violation metrics - frontend/#707
- Remove unused policy violation widget - frontend/#710
- Use consistent coloring for "Suppressed" metrics - frontend/#712
- Show policy violations by state and classification - frontend/#717
- Show footer counters in "Portfolio Vulnerabilities" metrics - frontend/#718
- Improve UX of the project active / inactive toggle - frontend/#721
- Show publisher name when expanding rows in the "Alerts" table - frontend/#728
- Improve tooltip clarity for project vulnerabilities - frontend/#733
- Show badges on "Policy Violations" tab - frontend/#744
- Add ESLint and prettier - frontend/#752

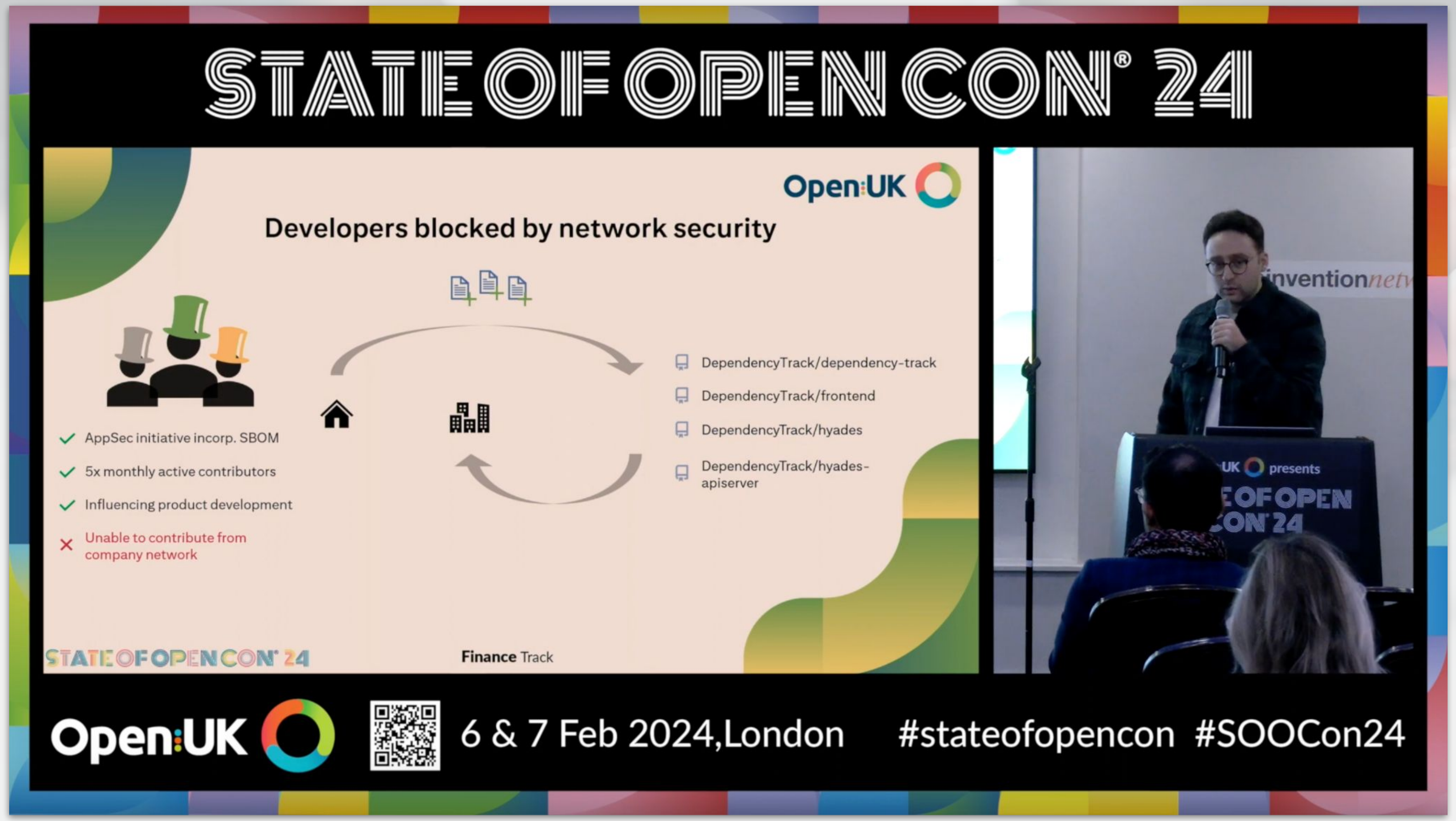
Fixes:

- Fix policy violations not being considered when cloning a project - apiserver/#3248
- Fix `StackOverflowError` when processing BOMs with deeply nested component structures - apiserver/#3357
- Fix inconsistent component de-duplication during BOM processing, causing varying components counts in successive uploads - apiserver/#3357
- Fix components erroneously being de-duplicated when only a single attribute of their component identity is identical - apiserver/#3357
- Fix components defined in the BOM node `metadata.component.components` not being imported - apiserver/#3357
- Fix withdrawn GitHub Advisories being mirrored - apiserver/#3394
- Fix broken image in OIDC documentation - apiserver/#3411
- Fix VulnDB parser being unable to import vulnerability records when `nvd_additional_information` is empty - apiserver/#3437
- Fix `URISyntaxException` when NPM PURL contains special characters - apiserver/#3456
- Fix finding attribution date not being retained when cloning a project - apiserver/#3488
- Fix Cargo repository metadata analyzer not being invoked - apiserver/#3511
- Fix type of `purl` fields in Swagger docs - apiserver/#3512
- Fix CI build status badge - apiserver/#3513
- Fix `VUE_APP_SERVER_URL` being ignored - frontend/#682
- Fix visibility of "Vulnerabilities" and "Policy Violations" columns not being toggle-able individually - frontend/#686
- Fix finding search routes - frontend/#689
- Fix CI build status badge - frontend/#699
- Fix incorrect calculation of "Audited Violations" and "Audited Vulnerabilities" percentages - frontend/#704
- Fix percentage calculation to round to the 10th decimal - frontend/#708
- Fix percentage calculation edge cases - frontend/#719
- Fix "Outdated Only" button being disabled when dependency graph is not available - frontend/#725
- Fix redundant requests to `/api/v1/component` when loading project page - frontend/#726
- Fix column visibility preferences triggering redundant requests - frontend/#727
- Fix `@<version>` being appended when rendering CPEs in "Affected Components" view - frontend/#748

PROJECT UPDATES

v5.x (Hyades)

- Focusing on PostgreSQL
  - Instead of trying(!!!) to support H2, MySQL, MSSQL, *and* PostgreSQL
  - Also looking at PostgreSQL compatible RDBMSes like CockroachDB and YugabyteDB
  - *Drastically* reduces effort for testing, maintenance, and feature development
  - Can’t expect contributors to be experts in 4+ RDBMS technologies
  - We want to ship software that comes optimized out-of-the-box
  - Tooling for v4.x → v5.x migration will be provided
  - We can still make adjustments, community feedback welcome!



Developers blocked by network security

- ✓ AppSec initiative incorp. SBOM
- ✓ 5x monthly active contributors
- ✓ Influencing product development
- ✗ Unable to contribute from company network

- DependencyTrack/dependency-track
- DependencyTrack/frontend
- DependencyTrack/hyades
- DependencyTrack/hyades-apiserver

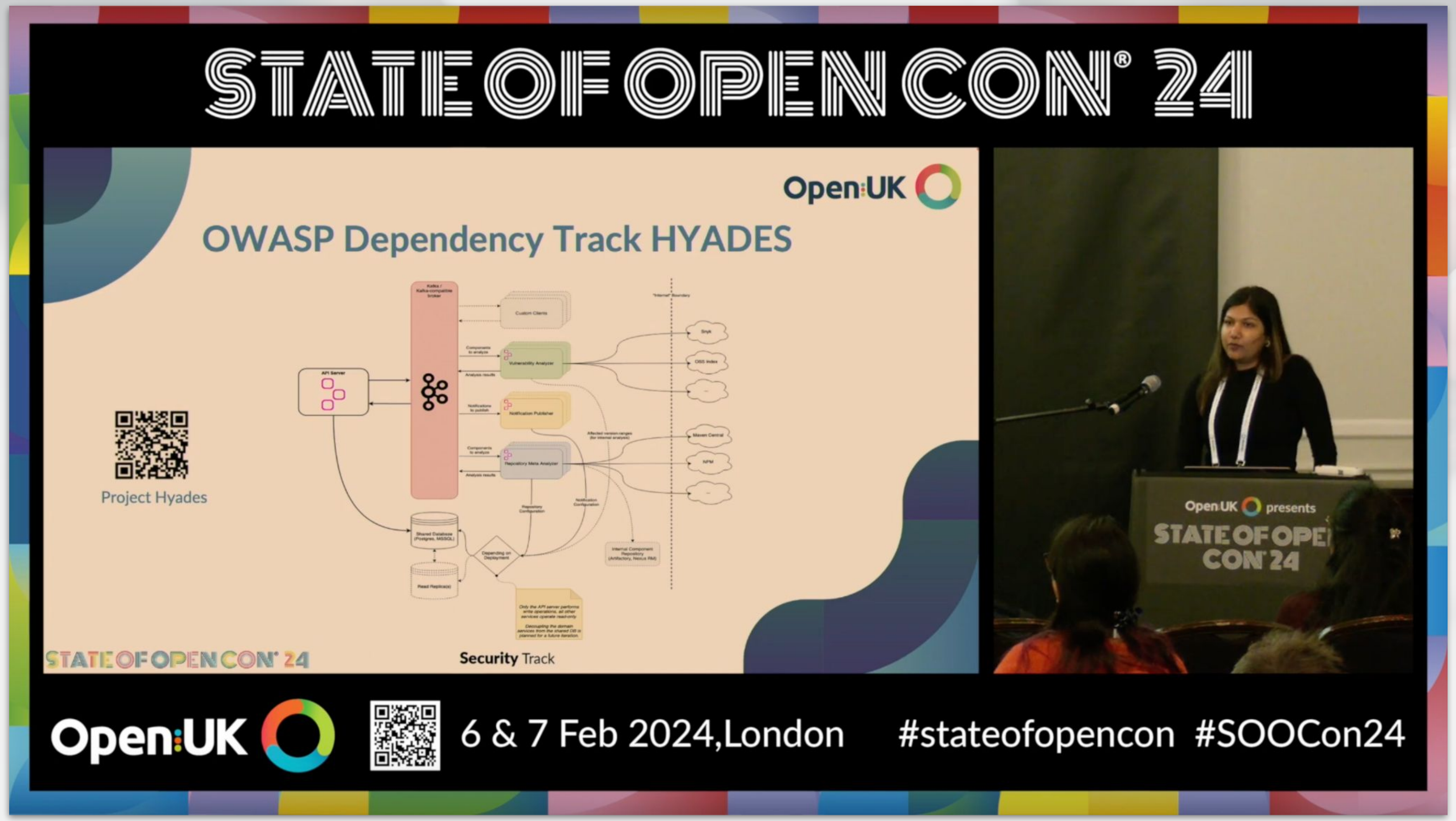
STATE OF OPEN CON® 24

Finance Track

Open:UK 6 & 7 Feb 2024,London #stateofopencon #SOOCon24

DevEx: Making Open Source Contribution Easier for Developers | Jamie Slome & Katrina Novakovic | OpenUK State of Open Con 24

https://www.youtube.com/watch?v=egm308m1n0o



STATE OF OPEN CON® 24

Open:UK

OWASP Dependency Track HYADES

Project Hyades

STATE OF OPEN CON® 24

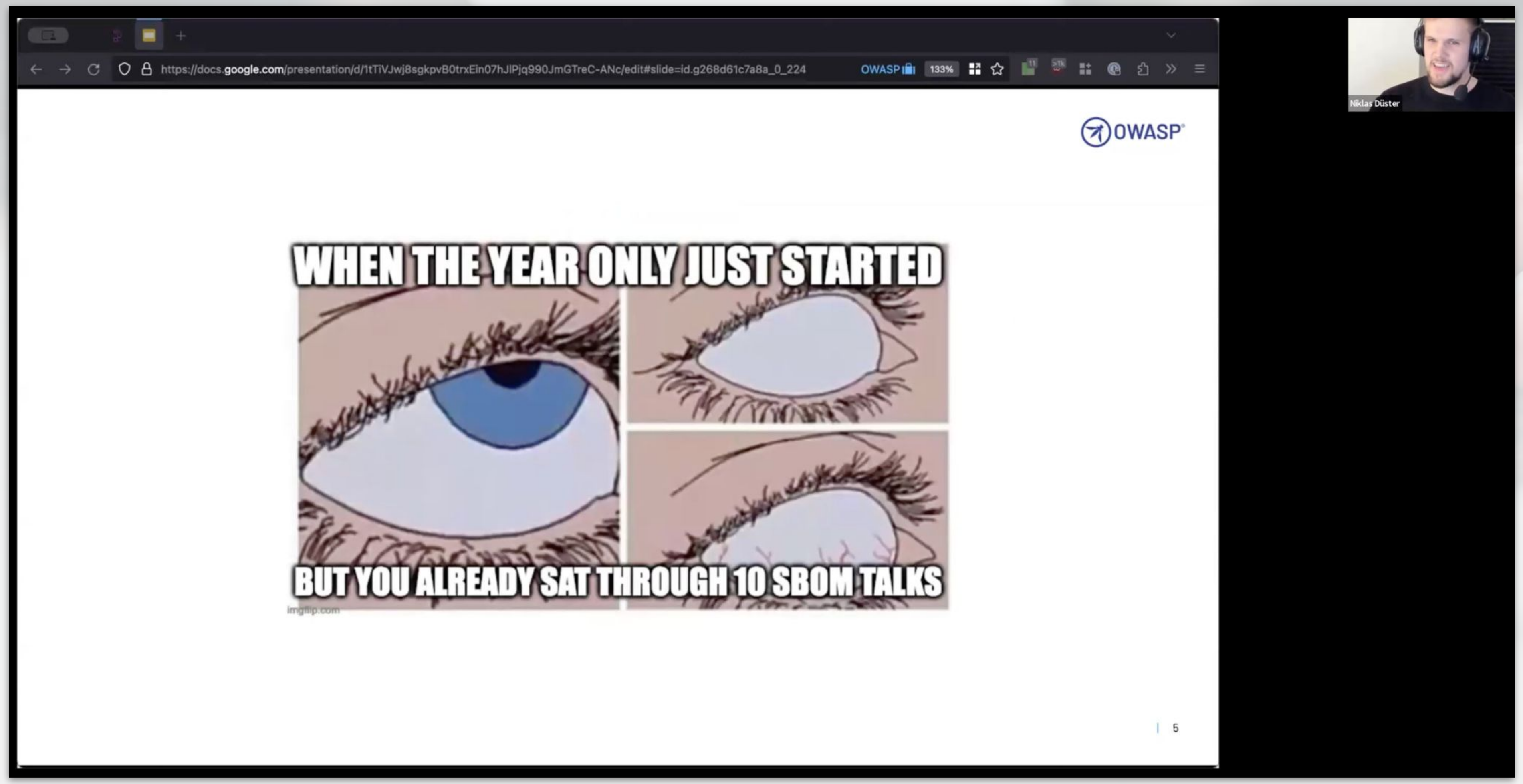
Security Track

Open:UK

6 & 7 Feb 2024,London #stateofopencon #SOOCon24

Hyades - Dependency Track for Enterprise Supply Chain Security with SBOM | Meha Bhargava & Sahiba Mittal | OpenUK State of Open Con 24

https://www.youtube.com/watch?v=hD06WaqW_2w


https://docs.google.com/presentation/d/1tTiVJwj8sgkpvB0trxEin07hJIPjq990JmGTreC-ANc/edit#slide=id.g268d61c7a8a_0_224
OWASP
WHEN THE YEAR ONLY JUST STARTED
BUT YOU ALREADY SAT THROUGH 10 SBOM TALKS
imgflip.com
5
Niklas Düster

https://www.youtube.com/watch?v=Os2wVzp2oNA

OWASP Dependency-Track | Niklas Düster | OWASP Netherlands Chapter

OWASP®

CRYPTOGRAPHY BILL OF MATERIALS

OWASP®

MEETING SCHEDULE

OWASP®

QUESTIONS & ANSWERS