OWASP®

DEPENDENCY-TRACK COMMUNITY MEETING

APRIL
2024

THE DEPENDENCY-TRACK TEAM

www.owasp.org

AGENDA

01 Project Updates

02 Contributing to Hyades

03 Insights from VulnCon

04 Q&A

© OWASP. This work is licensed under Creative Commons Attribution 4.0 International

OWASP®

PROJECT UPDATES

PROJECT UPDATES

v4.11.0 - New and Noteworthy

- Validation of uploaded BOMs against CycloneDX schema
  - Can be disabled in case it causes problems
  - CycloneDX v1.6 BOMs will *fail* schema validation in v4.11.0
- Optimized BOM ingestion
  - More efficient, faster, atomic, better logging
  - Opt-**in** for v4.11.0
- Max length of PURLs raised from 255 to **786** characters
  - Better compat. with *cyclonedx-node-npm* and *cdxgen* :)

© OWASP. This work is licensed under Creative Commons Attribution 4.0 International

PROJECT UPDATES

v4.11.0 - New and Noteworthy

- Global vulnerability audit view
  - Bird's-eye, *read-only* view of vulnerabilities across all projects
  - Equivalent feature for policy violations currently in review
  - Thanks Ralf and Richard @ M&M Software!
- Trivy integration
  - Leverages central Trivy instance running in server mode
  - Thanks Marlon @ Backbase!

© OWASP. This work is licensed under Creative Commons Attribution 4.0 International

PROJECT UPDATES

v4.11.0 - What's left?

- Support for Component properties
  - Required for accurate scanning OS packages with Trivy

    (Trivy uses properties for alternative component names)

© OWASP. This work is licensed under Creative Commons Attribution 4.0 International

PROJECT UPDATES

Official Helm Chart

- Currently working on: Dependency-Track v4.x
  - Let's collaborate to make it work for everyone!
- Next up: Hyades / Dependency-Track v5.x

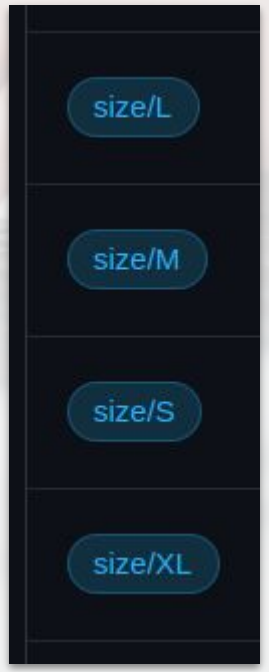
```
$ helm repo add dependency-track 'https://dependencytrack.github.io/helm-charts'
$ helm repo update
$ helm install dtrack dependency-track/dependency-track -n dtrack --create-namespace
```

© OWASP. This work is licensed under Creative Commons Attribution 4.0 International

PROJECT UPDATES

Organizational

- Copyright transferred from Steve Springett to OWASP Foundation
  - Thanks Steve for proposing and approving this change!
- Making an effort to use *good first issue* label more
- Now labelling issues with rough effort estimates



© OWASP. This work is licensed under Creative Commons Attribution 4.0 International

PROJECT UPDATES

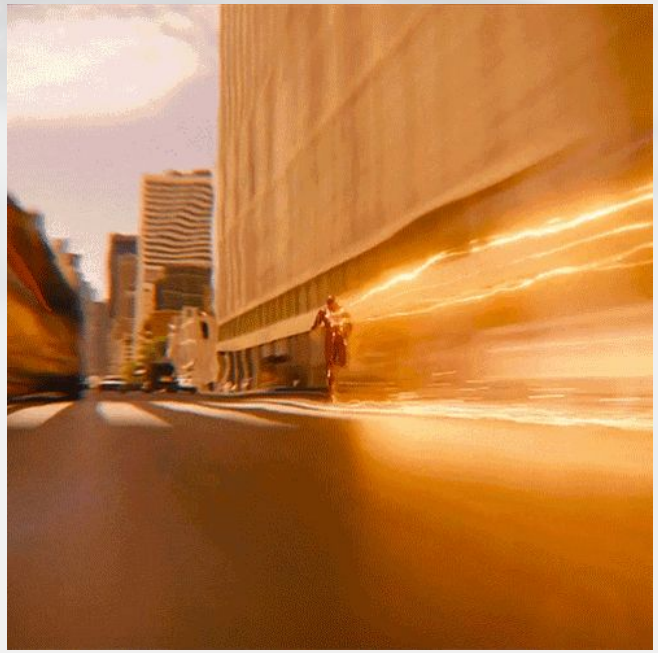
Hackathon?

© OWASP. This work is licensed under Creative Commons Attribution 4.0 International

CONTRIBUTING TO HYADES

Why

- The future version of Dependency-Track (v5)
- Supports Scalable Architecture
- Supports High Availability
- Supports “Vulnerability Policies” using CEL
- Supports Integrity Analysis
- Coming soon !!!!



© OWASP. This work is licensed under Creative Commons Attribution 4.0 International

CONTRIBUTING TO HYADES

How

- Documentation
- Testing
- Bug fix
- New features

Join our slack channel : **#proj-dependency-track-hyades**
https://github.com/DependencyTrack/hyades
https://github.com/DependencyTrack/hyades/issues/860
https://github.com/DependencyTrack/hyades#great-can-i-try-it-

© OWASP. This work is licensed under Creative Commons Attribution 4.0 International

CONTRIBUTING TO DT

2024 Global AppSec Lisbon CfP

Ends on Thu, Apr 4, 2024 5:00 AM (in 11 hours)

https://owasp.submittable.com/submit/288433/2024-global-appsec-lisbon-cfp

© OWASP. This work is licensed under Creative Commons Attribution 4.0 International

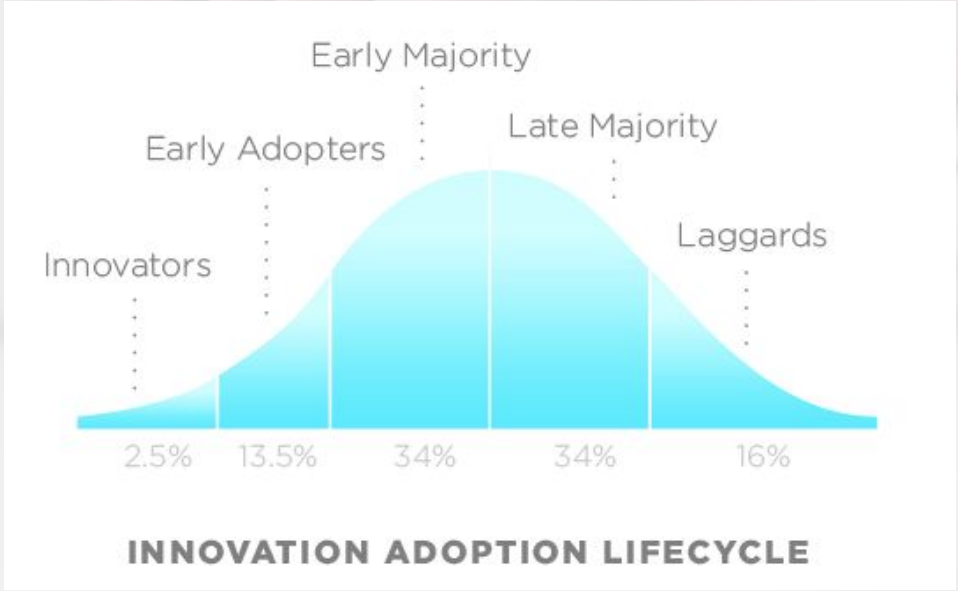
OWASP®

INSIGHTS FROM VULNCON

Insights from VulnCon

VEX, VEX, VEX … and more VEX!

- Adoption: VEX vs SBOM
- Clarity: VDR, VEX, OpenVEX, CycloneDX, SPDX, CSAF
- Community Insights
- Resources:
  - CVE/FIRST VulnCon 2024 & Annual CNA Summit
  - Technology life cycle - Wikipedia



© OWASP. This work is licensed under Creative Commons Attribution 4.0 International

QUESTIONS & ANSWERS