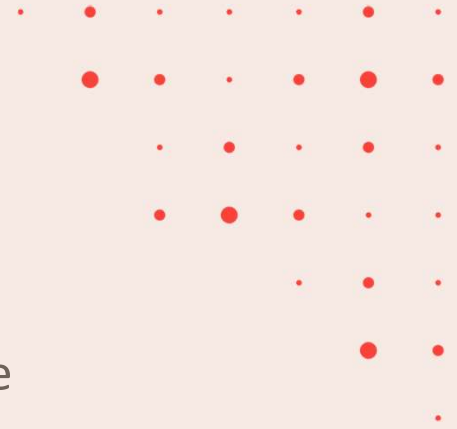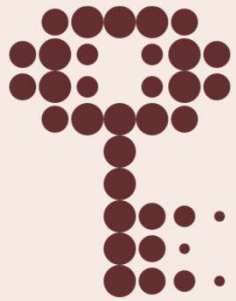TIETOEVRY CREATE

SBOM with Eiffel Protocol

Eiffel Summit 2025

Helena Slívová

tietoevry

Our focus

1. SBOM – benefits of having one

2. How it can be used?

3. Melting with Eiffel Protocol

4. Your needs

Software Bill Of Material

Detailed inventory of software product showing what other software is included.

Increase of software security
Managing software security vulnerabilities
Addressing licensing issues
Lowering supply chain risks
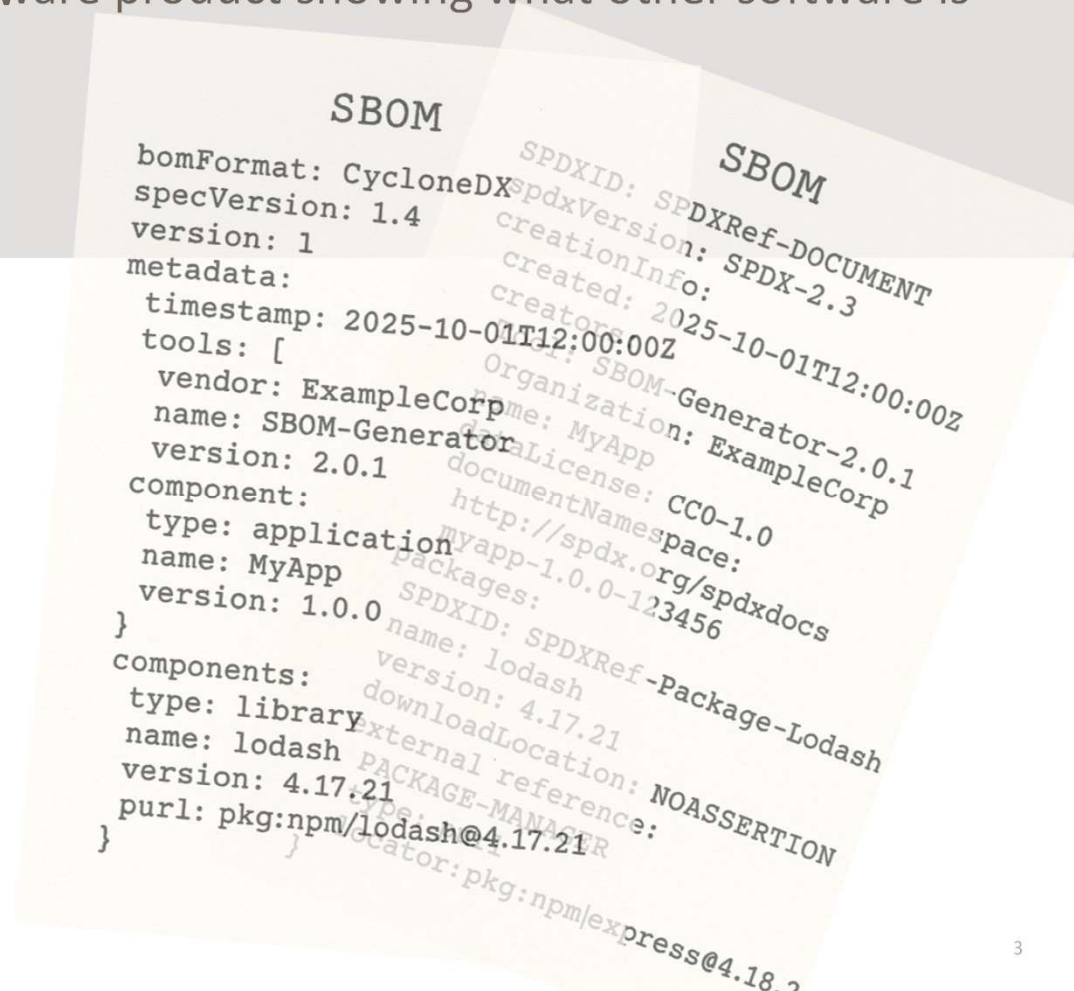
Software lifecycle

SBOM can be generated at different moments of software development lifecycle

|	Development	Build	Test	Deployment	Runtime
Pros	Declared dependencies Easy to automate	All dependencies resolved Integrated in CI/CD pipelines	Reflects real environment Compare with Dev/build results	Production-like Release time compliance	Highly precise Zero trust Runtime compliance
Cons	Transitive dependencies not resolved Runtime env not considered	Unused dependencies Harder tracking of exact source	Not all environments are complete	Harder to track back to build time artifacts	Complexity Performance Security implications

Melting with Eiffel protocol

Event based CI/CD solution directly challenges the thinking if there could be way how to use those events together with SBOM creation at various states of software development and deployment.
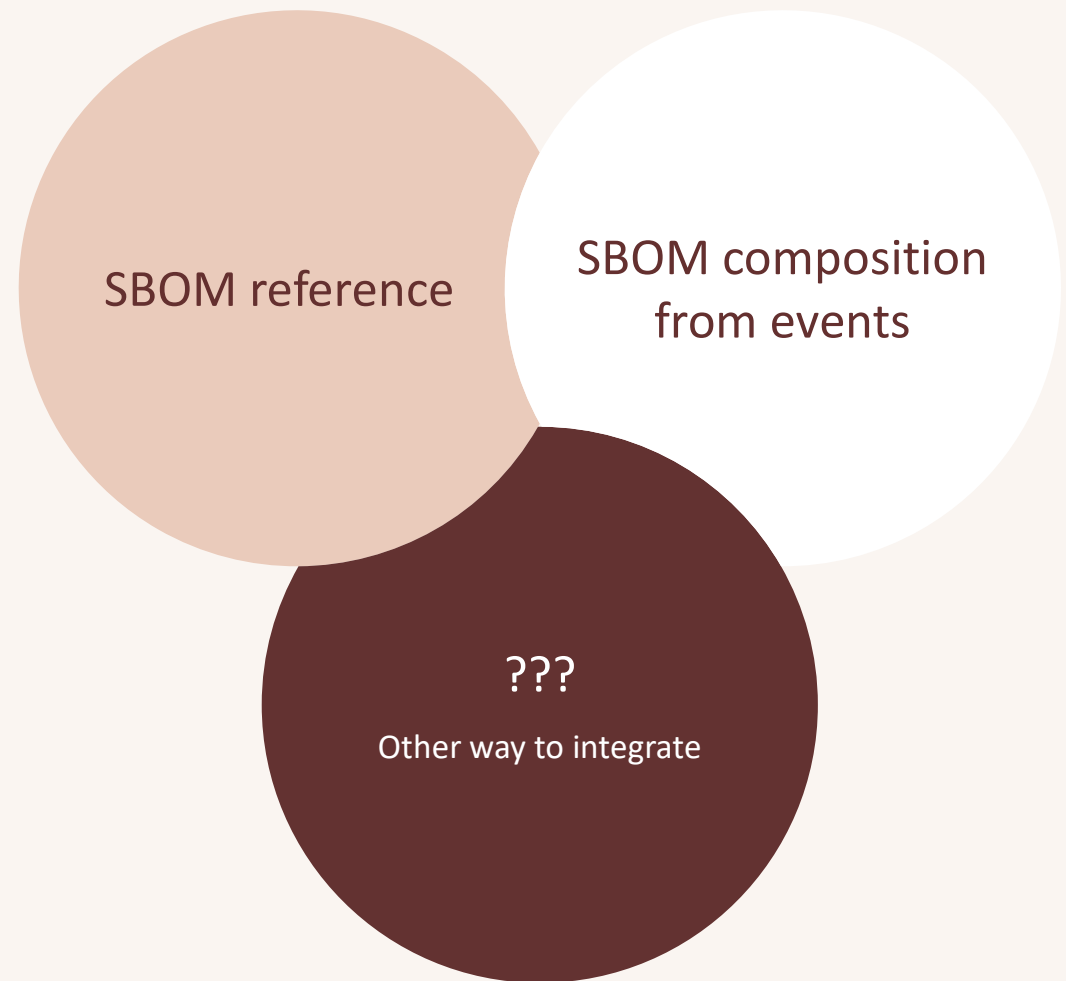
SBOM reference

SBOM composition from events

???
Other way to integrate

SBOM reference

Reference to existing SBOM
passed as link within event sent
over CI/CD pipeline

Protocol evolution

Modification of existing events

BuildEvent – adding reference to SBOM

DeploymentEvent – to include reference to SBOM of deployed
version ensuring traceability

Standardize SBOM metadata

Component information

Vulnerabilities

Generator metadata

SBOM reference

Reference to existing SBOM passed as link within event sent over CI/CD pipeline

Protocol evolution

SBOM as an artifact

```
{
 "eventType": "ArtifactLinkEvent",
 "timestamp": "2025-09-09T16:12:45Z",
 "artifact": {
     "name": "build-123456-sbom",
     "type": "SBOM",
     "location": "https://sbom-
     repository.com/sbom/123456"
 }
}
```

SBOM composition from events

Eiffel events passing through CI/CD pipeline and serving as source for SBOM composition

Protocol evolution

EiffelCompositionDefinedEvent – use to model component grouping for a product

EiffelArtifactCreatedEvent – modify to carry component SBOM related metadata

EiffelSBOMGeneratedEvent – new event to be triggered when specifically needed

SBOM composition from events

Eiffel events passing through CI/CD pipeline and serving as source for SBOM composition
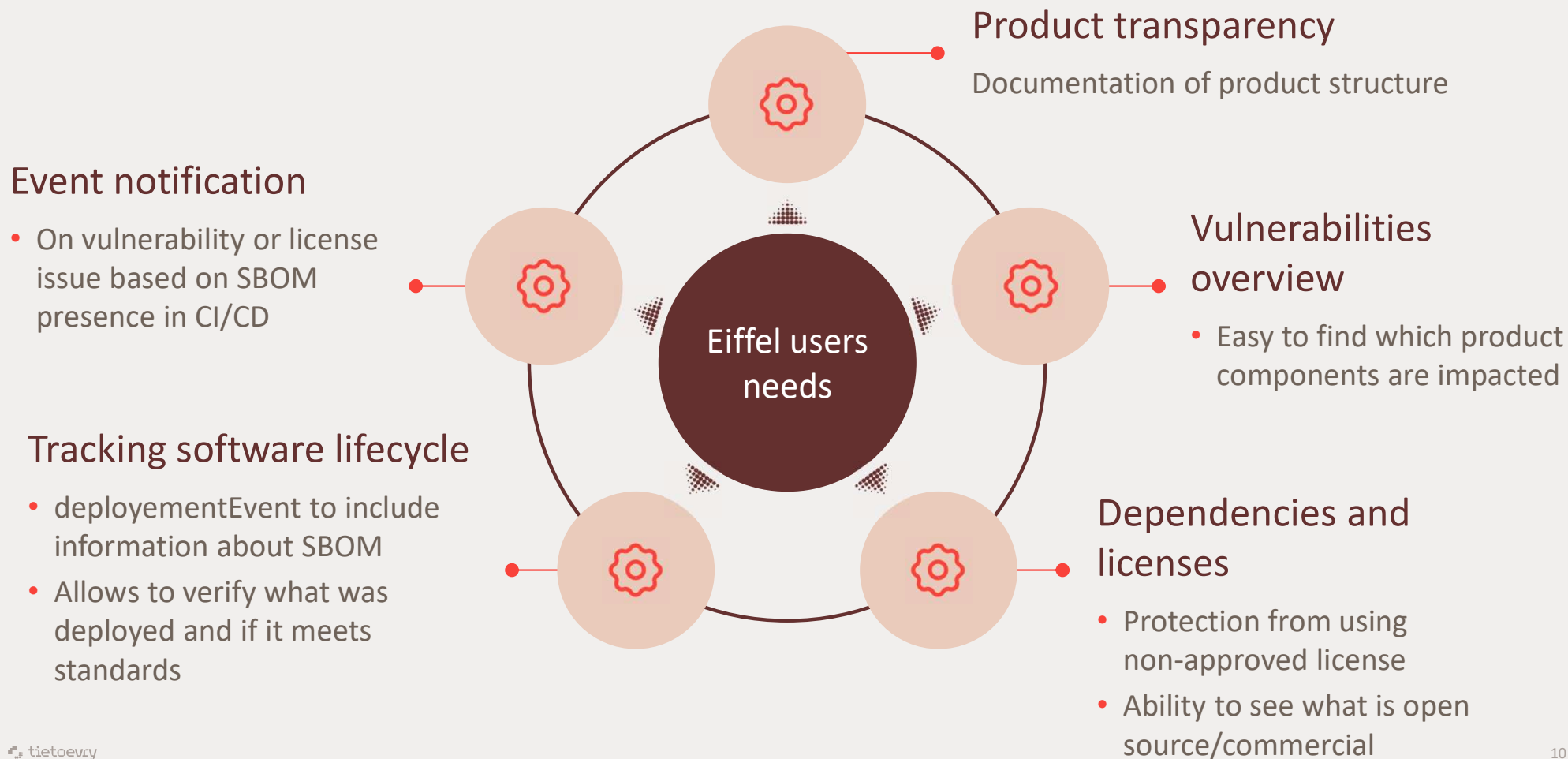
Protocol evolution

Benefits

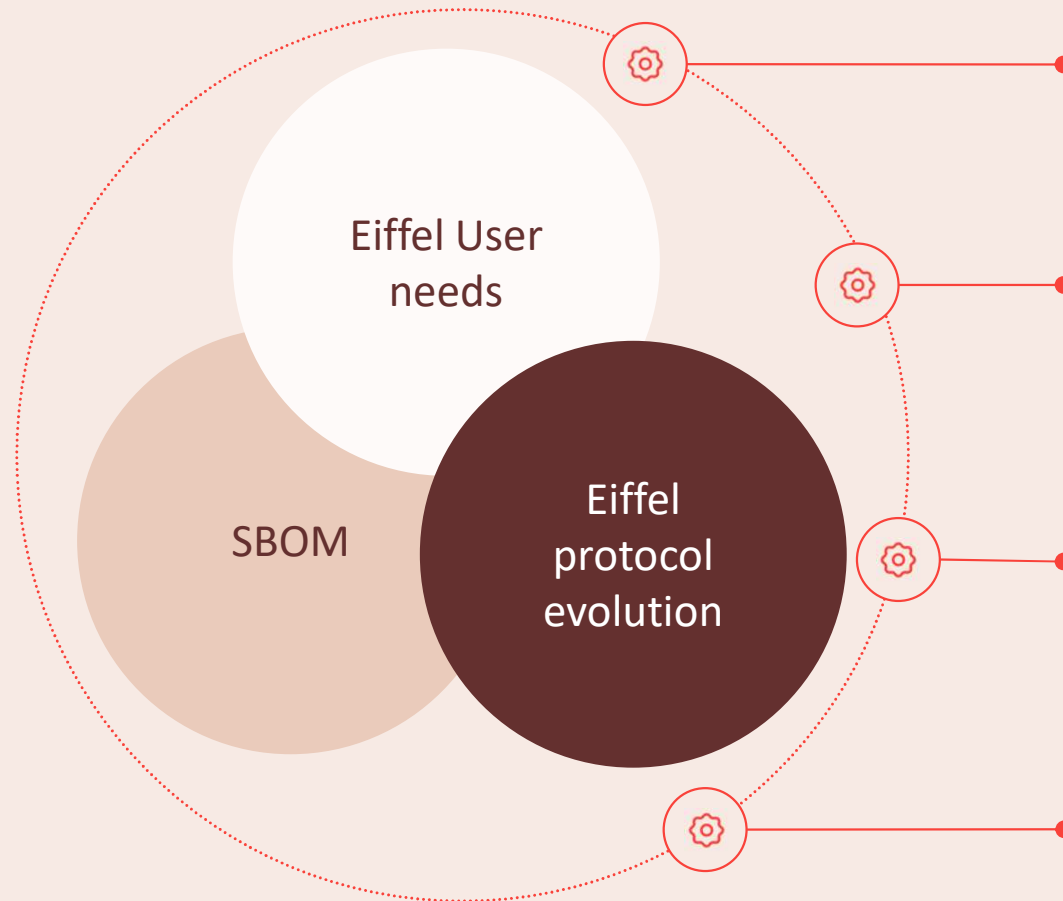No extra SBOM scan step

Versioned and traceable

Composable

Scalable

What are Eiffel users needs?

Event notification

- On vulnerability or license issue based on SBOM presence in CI/CD

Tracking software lifecycle

- deployementEvent to include information about SBOM
- Allows to verify what was deployed and if it meets standards

Product transparency

Documentation of product structure

Vulnerabilities overview

- Easy to find which product components are impacted

Dependencies and licenses

- Protection from using non-approved license
- Ability to see what is open source/commercial

Eiffel users needs

Union

Eiffel User needs

SBOM

Eiffel protocol evolution

Brainstorm

Thank you

tietoevry