# Transparency is at the ❤️ of Dependency-Track

And **TEA** fits right in!

# dependency track

is...

a platform to identify and reduce risk

in the software supply chain

by leveraging bill of materials

# dependency track

is...

not an SCA tool, not a scanner

inventory first

ecosystem-agnostic

## BOM Production

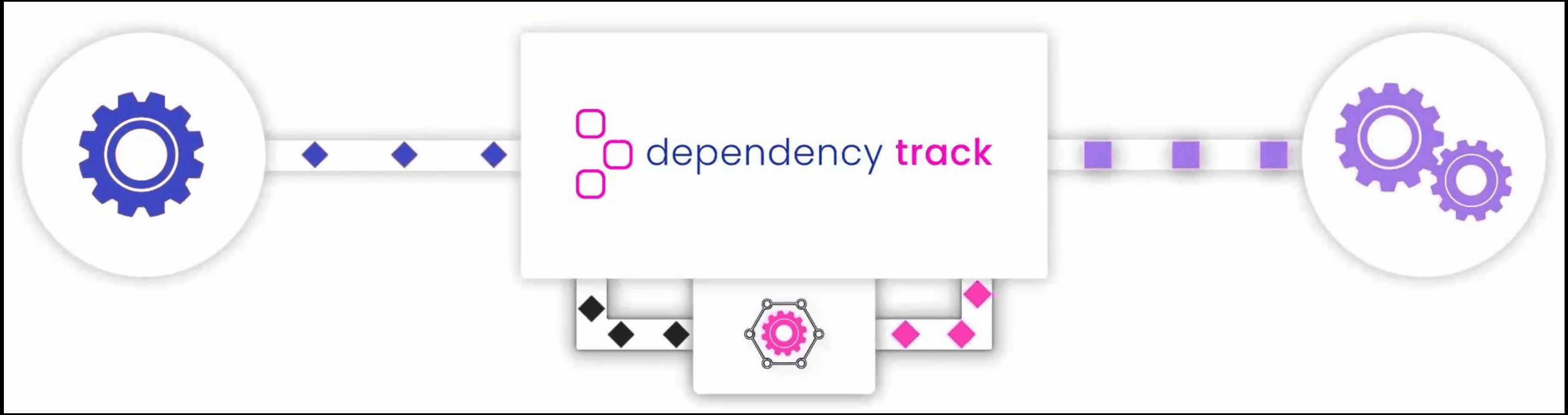
Generated during CI/CD or
acquired from suppliers.

## BOM Analysis

Component analysis for security,
operational, and license risk.

## Intelligence Streams

Real-time analysis and security
events delivering actionable
findings to external systems.



## BOM Ingestion

Via REST API, Web Interface,
Jenkins Plugin, GitHub Action.

## Continuous Monitoring

Continuous analysis of portfolio
for risk and policy compliance.

## Intelligent Response

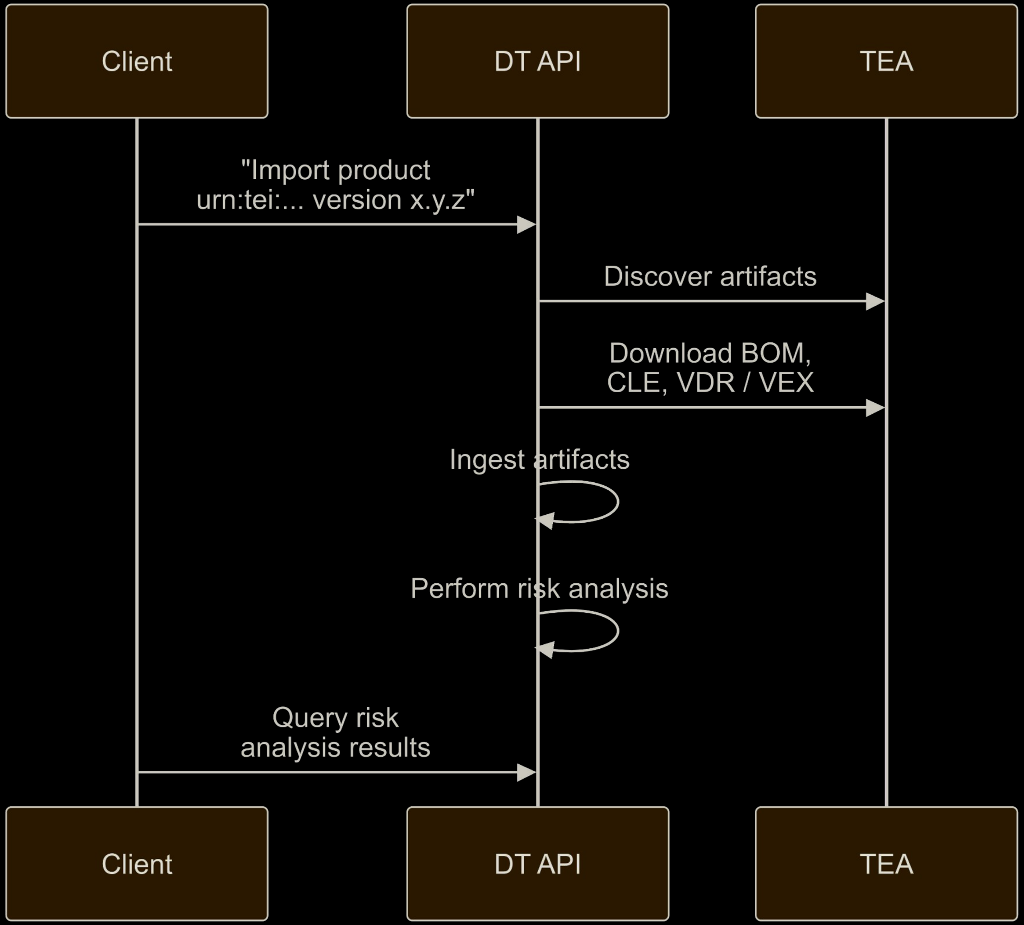
Events delivered via Webhooks
or ChatOps and findings published
to risk management and vulnerability
aggregation platforms.

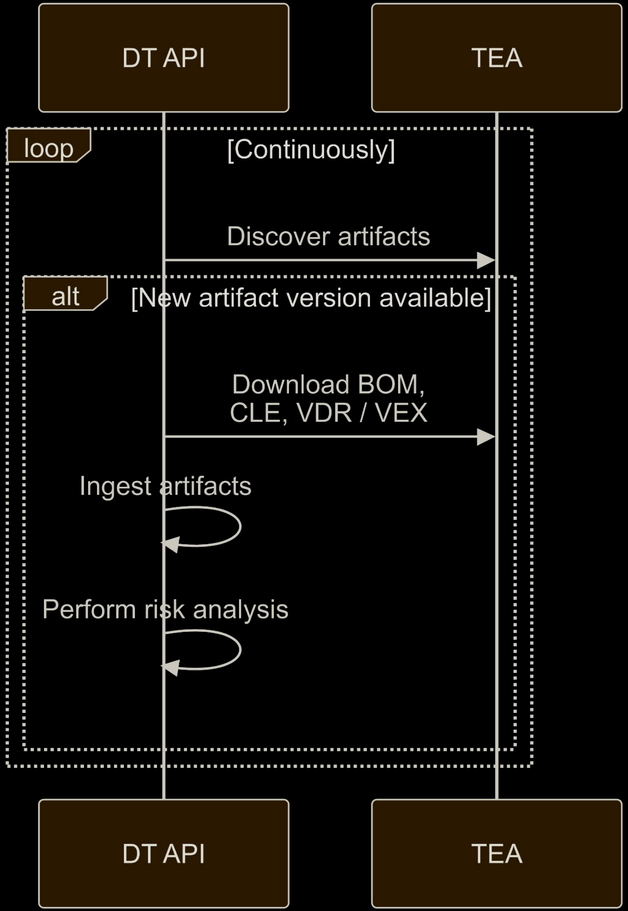
Easy for internal products.

Hard for external products.

# Users don’t care about BOMs.

Dependency-Track
will **consume** from TEA.


Client
DT API
TEA
"Import product urn:tei:... version x.y.z"
Discover artifacts
Download BOM, CLE, VDR / VEX
Ingest artifacts
Perform risk analysis
Query risk analysis results
Client
DT API
TEA


DT API
TEA
loop
[Continuously]
Discover artifacts
alt
[New artifact version available]
Download BOM,
CLE, VDR / VEX
Ingest artifacts
Perform risk analysis
DT API
TEA

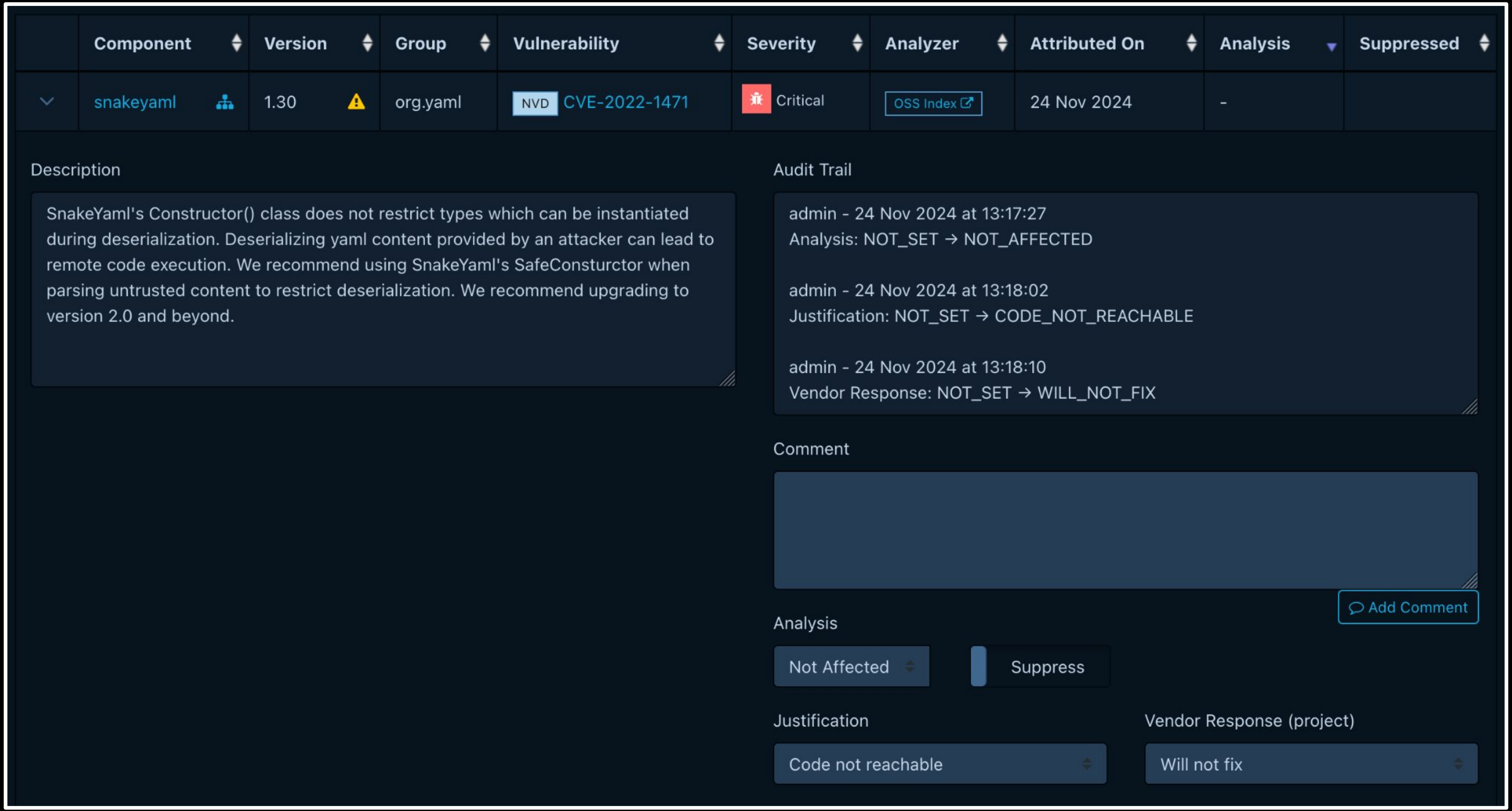
“Tell me what product you use,
and I will track its risk.”

Transparency artifacts are an implementation detail.

# Transparency artifact retention decoupled from processing.

# Finally a reliable source for product lifecycle information?

Dependency-Track
will **publish** to TEA.



| | Component | Version | Group | Vulnerability | Severity | Analyzer | Attributed On | Analysis | Suppressed |
|---|---|---|---|---|---|---|---|---|---|
| | snakeyaml | 1.30 ⚠ | org.yaml | NVD CVE-2022-1471 | Critical | OSS Index | 24 Nov 2024 | - | |

Description

SnakeYaml's Constructor() class does not restrict types which can be instantiated during deserialization. Deserializing yaml content provided by an attacker can lead to remote code execution. We recommend using SnakeYaml's SafeConsturctor when parsing untrusted content to restrict deserialization. We recommend upgrading to version 2.0 and beyond.

Audit Trail

admin - 24 Nov 2024 at 13:17:27
Analysis: NOT_SET → NOT_AFFECTED

admin - 24 Nov 2024 at 13:18:02
Justification: NOT_SET → CODE_NOT_REACHABLE

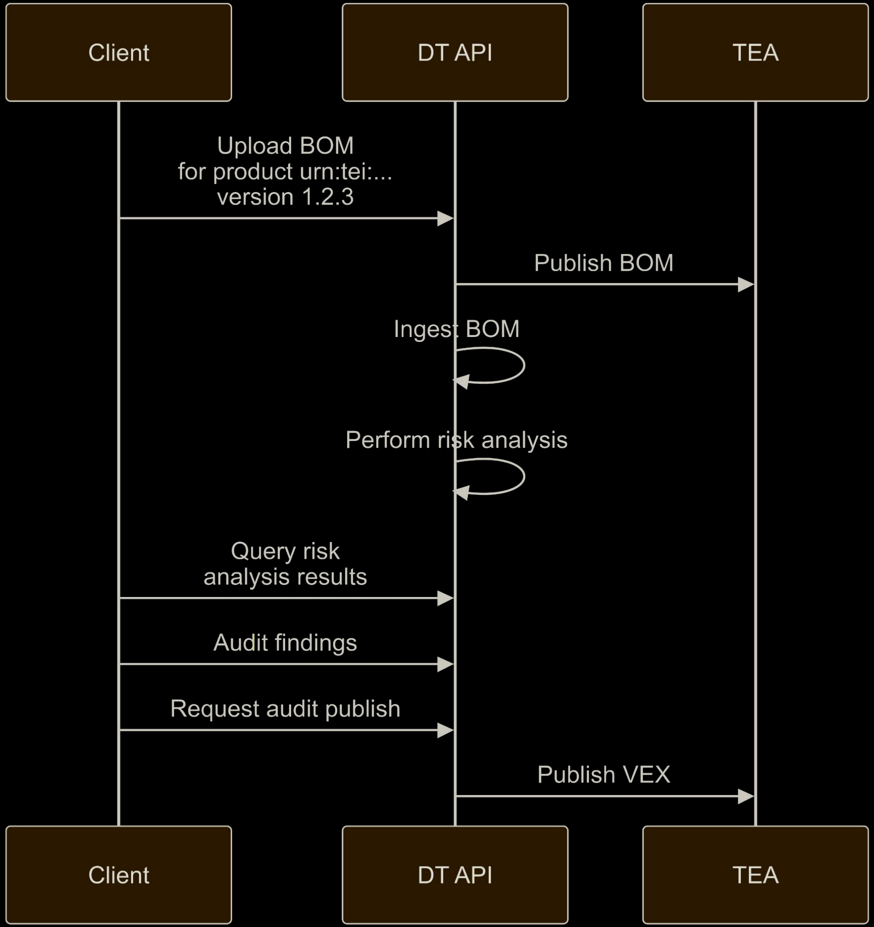
admin - 24 Nov 2024 at 13:18:10
Vendor Response: NOT_SET → WILL_NOT_FIX

Comment

Analysis: Not Affected

Justification: Code not reachable

Vendor Response (project): Will not fix


Client
DT API
TEA
Upload BOM
for product urn:tei:...
version 1.2.3
Publish BOM
Ingest BOM
Perform risk analysis
Query risk
analysis results
Audit findings
Request audit publish
Publish VEX
Client
DT API
TEA

# Eating our own dogfood.