Enhancing Railway Resilience through Secure Software Development

Practical Approach to Cyber Resilience Act Compliance

We make Digitalization easy.

December 2025

tmc

FOUNDED IN	4 SITES	EMPLOYEES	PROFITABLE SINCE
2019	Austria, India, USA	117	Day 1

The IT branch of world market leader Plasser & Theurer: **High-tech in the Niche**

Coming from Austria, the **#4 export country in rail technology**

You are no Beta-Tester: we are doing **Quality Assurance on our machines and tracks**

tmOS for Track machine automation, Track Geometry and Point Clouds – and still keeping the knowledge at the customers

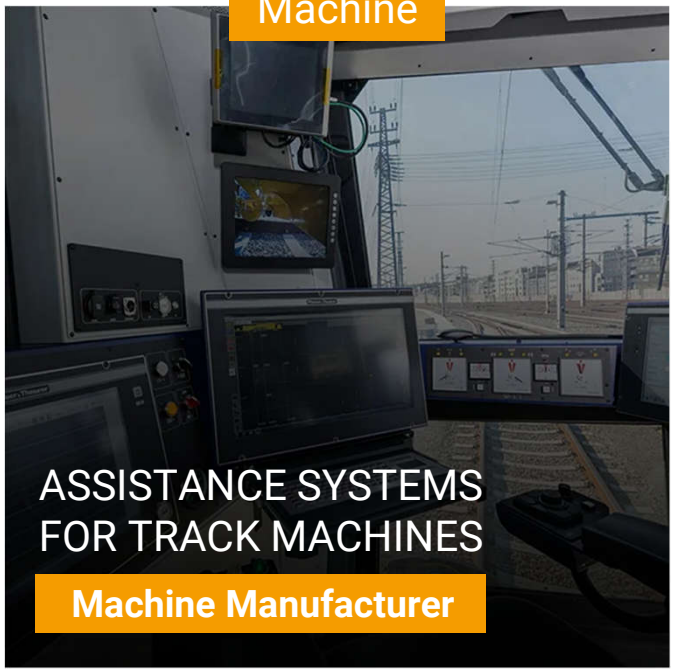
tmOS addresses **Lifecycle Management, Obsolescence and Cybersecurity**

Our portfolio

tmOS

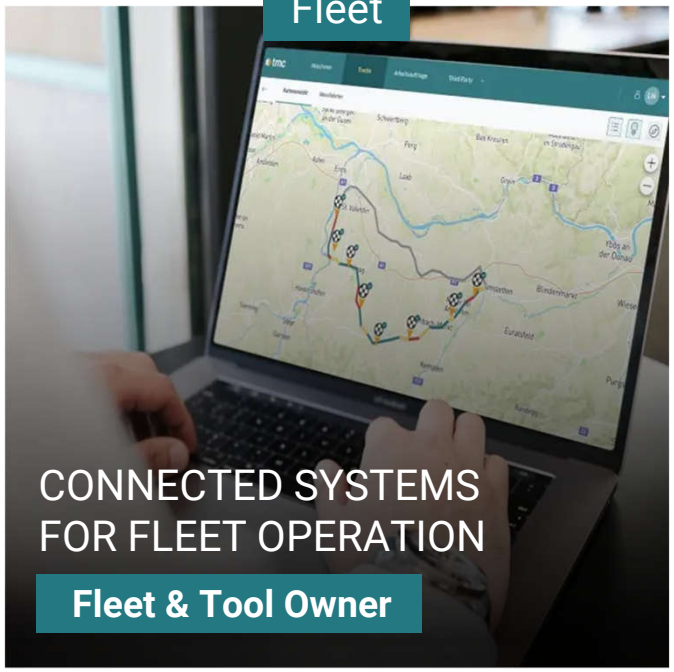
one platform
that covers it all

Machine



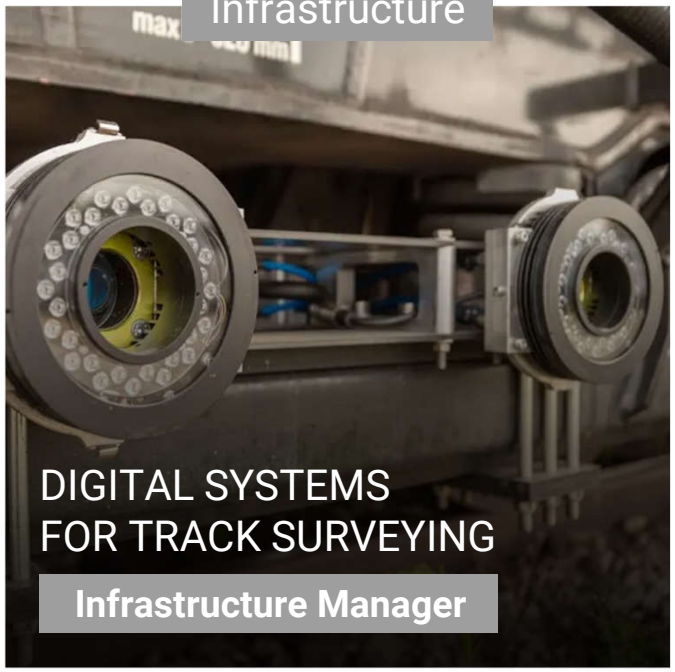
We make digitization easy for you. Our solutions turn the track machines you manufacture into highly efficient machines that give you a competitive edge.

Fleet



Keep an eye on the condition of your track machines with our solutions. This allows for improve operation and maintenance planning, as well as reduced costs.

Infrastructure



We automate track surveying so that you can work more efficiently, precisely and above all, safely. We make track measurement possible, without an impact on operations.

... resulting in

a fully closed Loop

DATA SYNCHRONIZATION

DATA SYNCHRONIZATION

DATA SYNCHRONIZATION

Pre-Measurement

MEASUREMENT CARS, TROLLEYS, FLAT WAGONS

Data Analytics & Work Preparation

BACKOFFICE

Work Execution & Post-Measurement

TRACK WORK MACHINES

Transparent Documentation

BACKOFFICE

tmc is committed to Security

We are ISO 27001 certified

SECURITY CERTIFICATION INFORMATION
ISO 27001:2013
No.00615/0

A Pillar of Success:

"Information Security
is a critical part of the tmc DNA"
Michael Wachert-Rabl, CISO

We are providing compliance with:

- EU Network Information Directive 2
- EU Cyber Resilience Act
- EU Radio Equipment Directive
- EU Data Act
- EU GDPR
- EU AI-Act

tmc products on track for compliance with:

- IEC 62443
- TS 50701

Cyber Resilience Act (CRA)

A path to compliance in software development

1. Product Classification (identify and cluster products)

2. Security Processes

A. Risk Assessment
- SW splitting in security zones
- Risk assessment via Threat Modelling

A.(2) CRA Product Requirements
Reset Function, User Mgmt, Encryption,
Logging, DoS Resilience, Automatic Updates, etc.

B. Design, Development & Production
- Security-by-Default (e.g. V-Cycle and IEC 62443-4-1), Security Zones
- Limit attack surface, increase availability
- Testing: Vulnerability Scans, Fuss Testing, Overloads, Pen-Testing

C. Vulnerability Handling
- Identify & Document SW components & vulnerabilities (via SBOM)
- Standardized process for updates
- Public disclosure of fixed vulnerabilities and incident reporting

3. Documentation

A. Technical Documentation

Product Description:
- Intended purpose
- Essential functionalities
- System architecture
- Drawings and Overview

Functionality & security test reports & vulnerability handling
- Single Point of Contact
- Support End & Lifecycle (min. 5 years)
- Manual for how to install updates & patches
- SBOM (in a stand-alone document)

Cybersecurity risk and measures
- Threat Modelling
- Different client architectures must be considered

B. Information & instructions to the user
An excerpt of the technical documentation must be made available to the customers
- Less comprehensive & less confidential

C. Conformity Assessment
I. Self Assessment:
for most products, a self-assessment confirms CRA compliancy
II. Third-Party Assessment:
High security risk products must be assessed by a 3rd party
III. Declaration of Conformity = CE marking

Cyber Resilience Act (CRA)

Open-Source CRA tools

1. **Risk Assessment:** (STRIDE Methodology)
- Microsoft Threat Modelling Tool
- OWASP Threat Dragon
- Draw.io

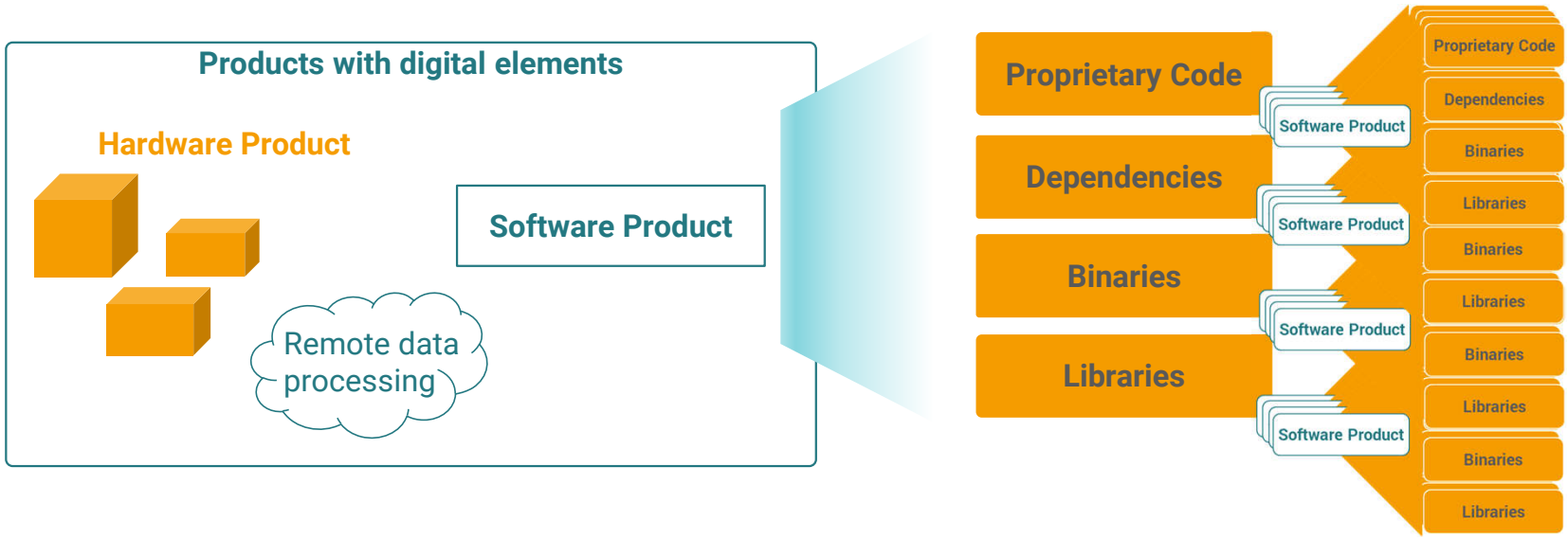
2. **Vulnerability Management:**
- Software Bill of Material creation via: CycloneDX (OWASP)
- Tracking/Analysis of CVSS within SW components via: Dependency-Track (OWASP)

CVSS COMMON VULNERABILITY SCORING SYSTEM

3. **Process Documentation:**
- Documentation Tool (Docmost, BookStack, LibreOffice etc.)
- Technical Documentation
- Information and Instructions to the User

Software Bill of Materials

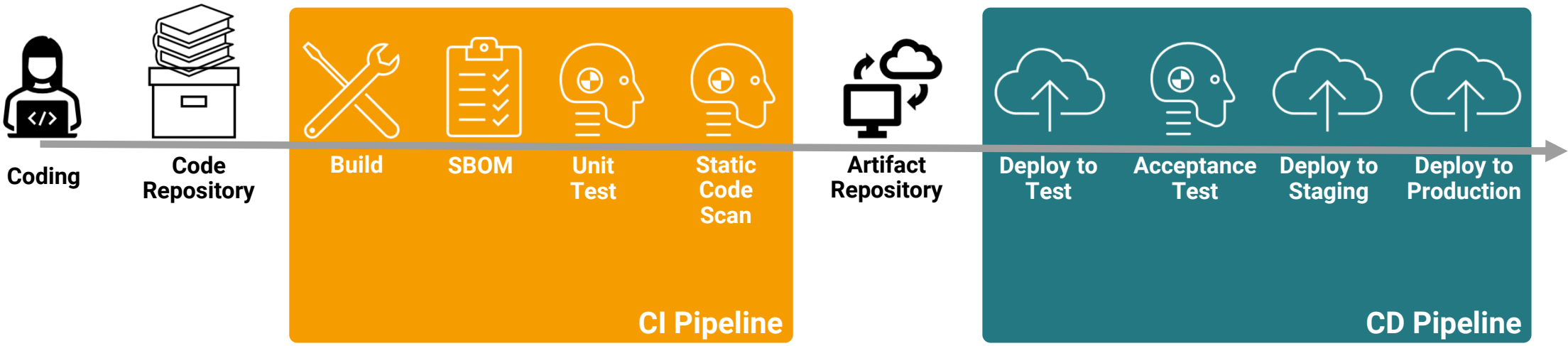
‘software bill of materials’ means a formal record containing details and supply chain relationships of components included in the software elements of a product with digital elements



- At least the first level must be documented (direct dependencies)
- Provided in a common machine-readable format (SPDX, CycloneDX etc.)
- Updated during the product lifecycle or for 5 years

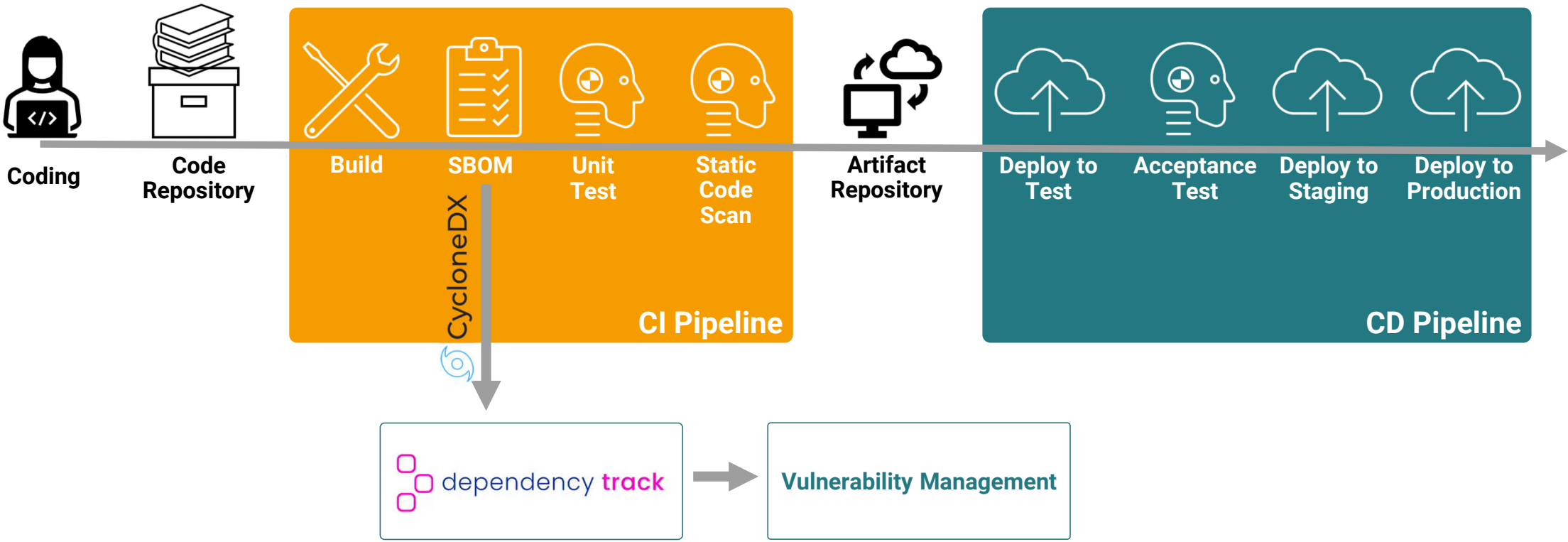
Software Development CI/CD Pipeline

How DevOps work:



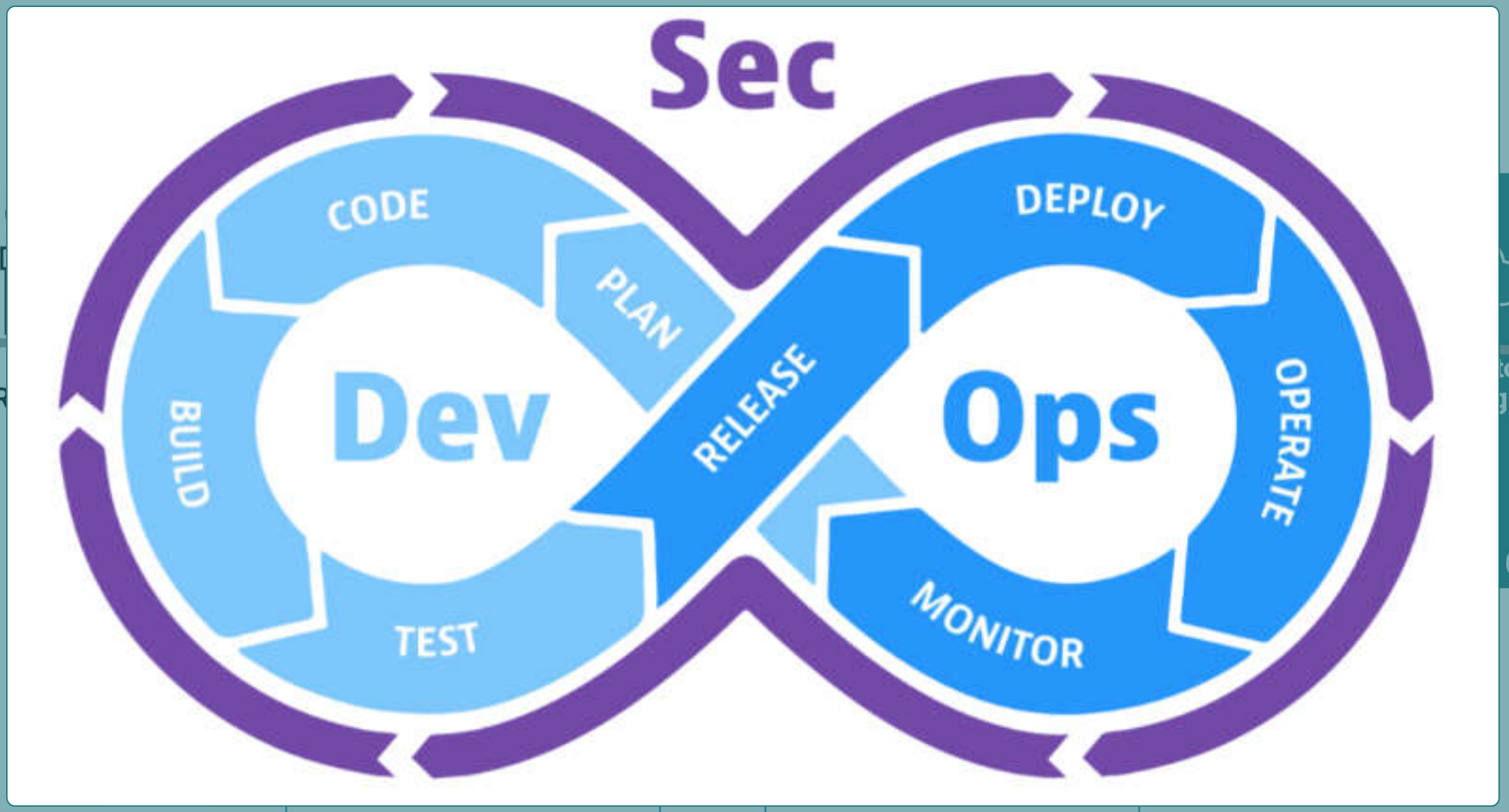
Software Development CI/CD Pipeline

How DevOps work:



Software Development CI/CD Pipeline

How DevOps work:



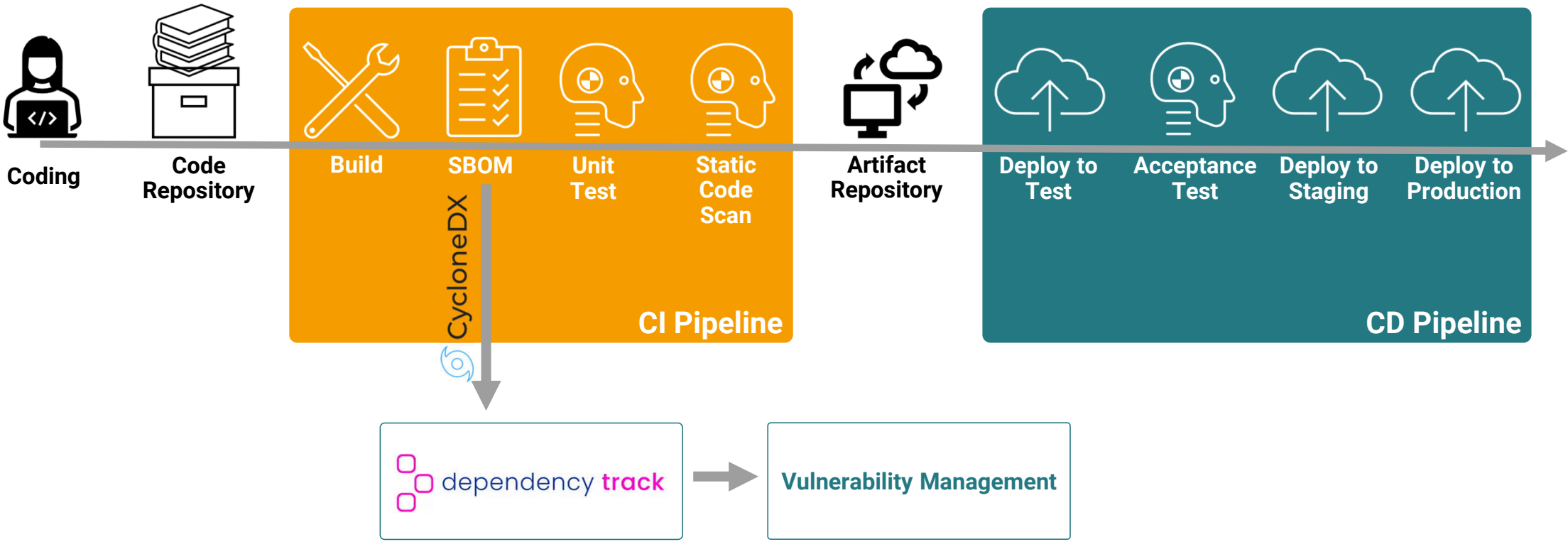
Coding

Deploy to Production

CD Pipeline

Software Development CI/CD Pipeline

How DevOps work:



CycloneDX – A SBOM Format

Open-source developed by OWASP

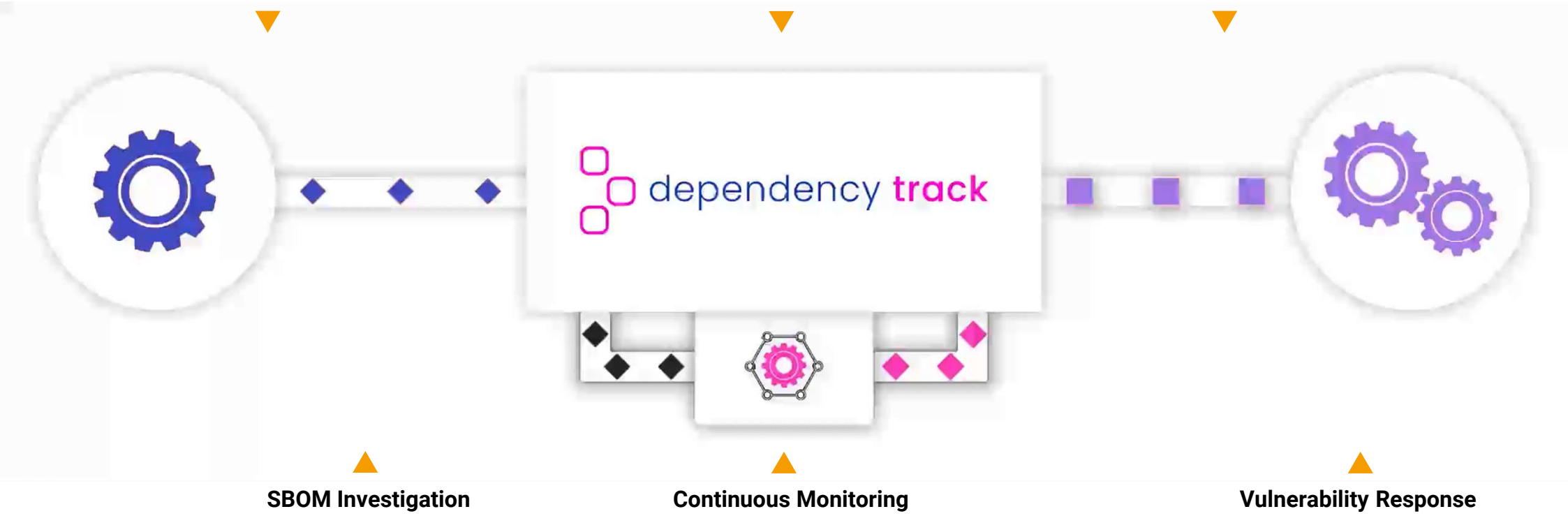
Example of a component identity in CycloneDX (JSON format)


```
{
    "type": "library",
    "group": "com.example",
    "name": "awesome-library",
    "version": "1.0.0",
    "cpe": "cpe:2.3:a:acme:awesome:1.0.0:*:*:*:*:*:*:*",
    "purl": "pkg:maven/com.example/awesome-library@1.0.0",
    "omniborId": [ "gitoid:blob:sha1:261eeb9e9f8b2b4b0d119366dda99c6fd7d35c64" ],
    "swhid": [ "swh:1:cnt:94a9ed024d3859793618152ea559a168bbcbb5e2" ],
    "swid": {
      "tagId": "swidgen-242eb18a-503e-ca37-393b-cf156ef09691_1.0.0",
      "name": "Acme Awesome Library",
      "version": "1.0.0",
      "text": {
        "contentType": "text/xml",
        "encoding": "base64",
        "content": "U1dJRCBkb2N1bWVudCBkb2VzIGhlcmU="
      }
    }
}
```


- cpe: A CPE (Common Platform Enumeration) identifier used for vulnerability matching.
- purl: A Package URL (purl) that uniquely identifies the component in package ecosystems.
- omniborId A GitOID reference for source code integrity (hash of a Git blob).
- swhid A Software Heritage ID, pointing to archived source code in the Software Heritage archive.
- swid A SWID (Software Identification) tag, another standard for identifying software.
  - tagId: Unique identifier for the SWID tag.
  - text: Contains SWID XML data encoded in Base64.

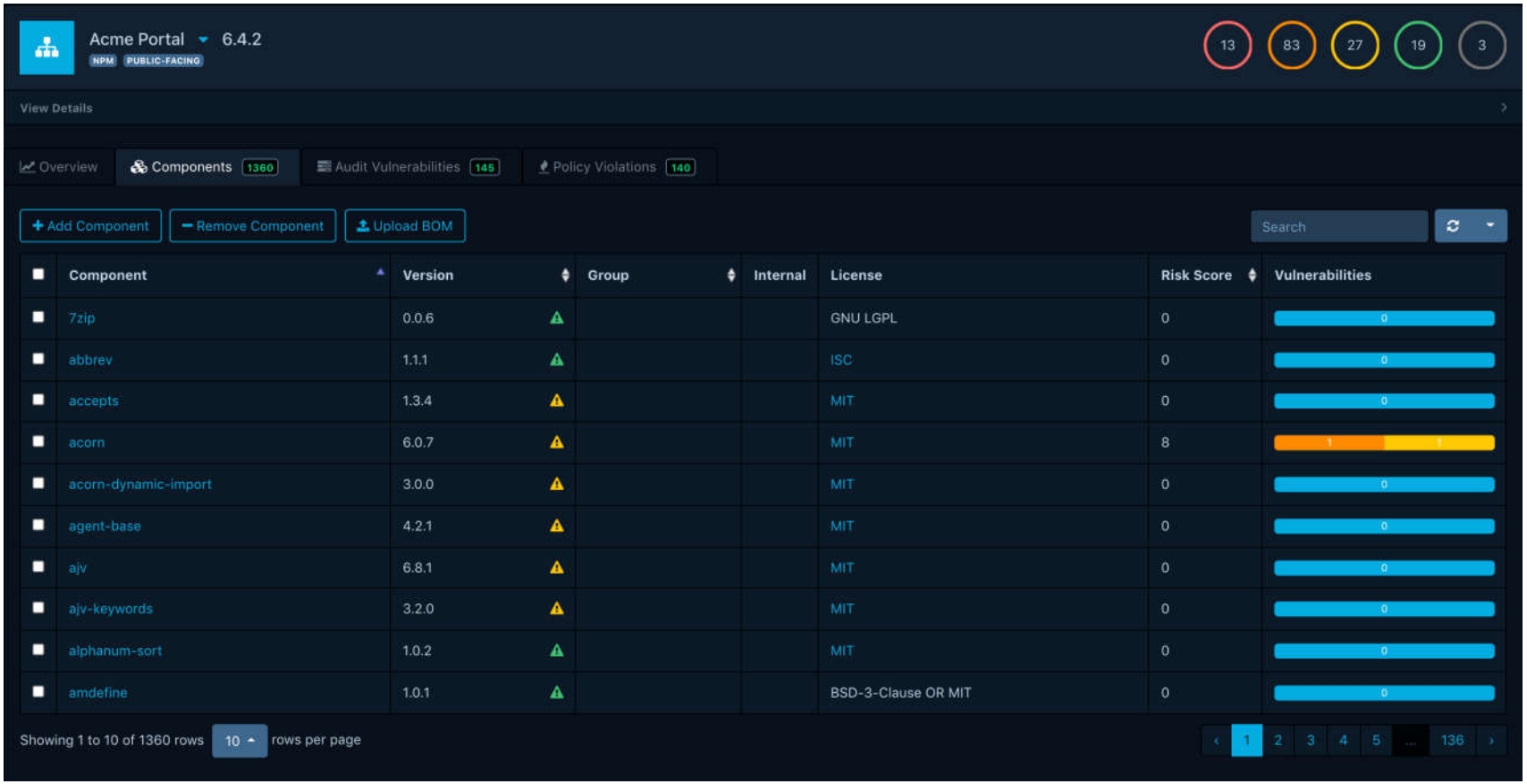
SBOM Platform & Vulnerability Management

Dependency Track (SBOM Platform ➔ Vulnerability Management)



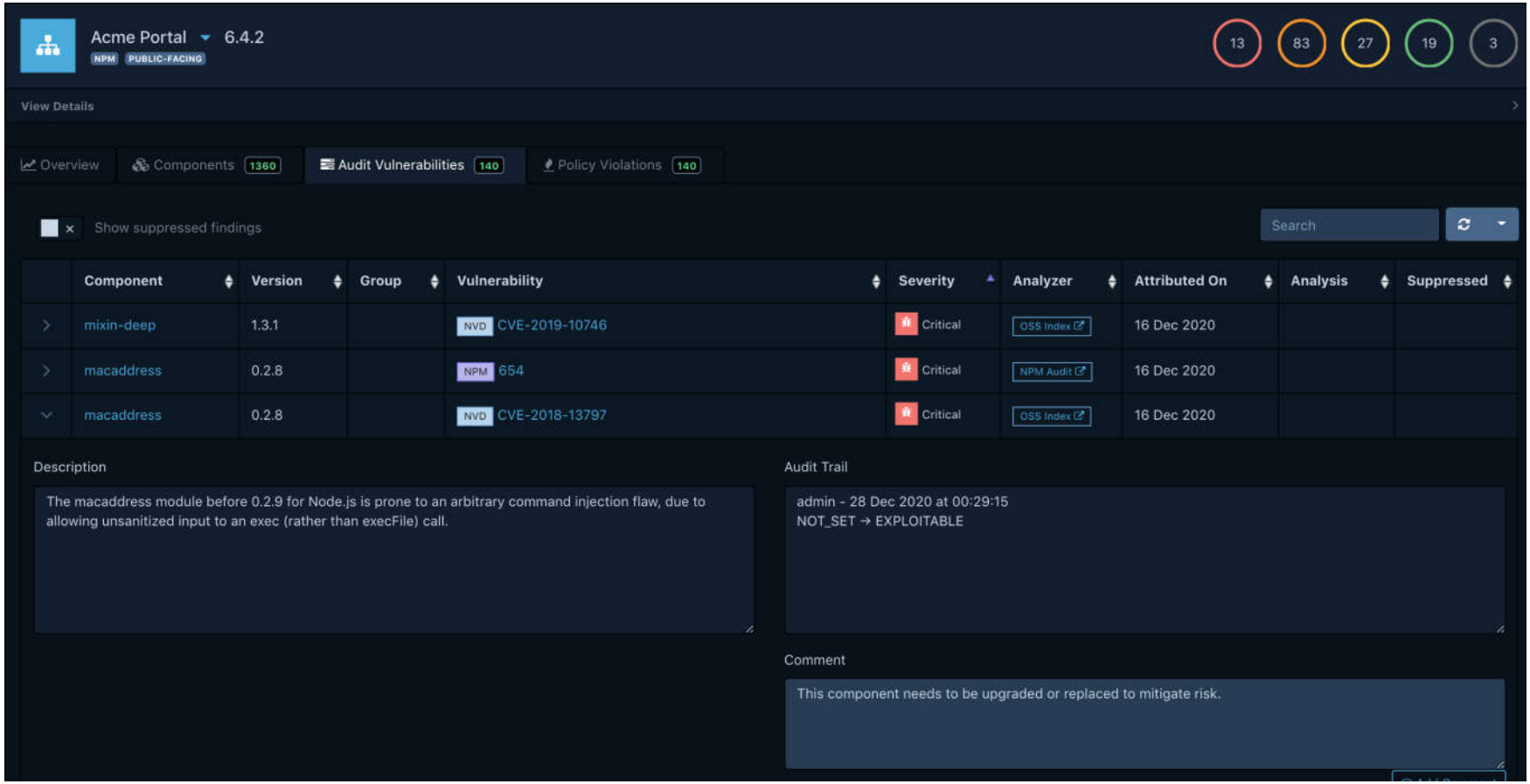
SBOM Generation & Vulnerability Management

Dependency-Track OWASP



SBOM Generation & Vulnerability Management

Dependency-Track OWASP



SBOM Generation & Vulnerability Management

Dependency-Track OWASP

Vulnerabilities must actively be tracked and alerted throughout the whole DevOps cycle.

How can manufacturers guarantee vulnerability management over the whole product lifecycle?

100% accurate SBOMs are extremely challenging - what SBOM quality is sufficient?


tmc
We make digitalization of railway track maintenance easy.
Power to the railways.