

Remote Device Management – Use Case Vulnerability Management



Motivation for cross vendor cooperation in remote device management

Interconnectedness of assets for flexible production exposes production facilities to open networks with **potential for cybersecurity attacks**

Cyber Resilience Act:

- ❖ High pressure to act for all manufacturers of devices that collect or send data.

Vulnerability Patch Management

- ❖ BSI makes vulnerability patch management based on Software Bill of Material (SBoM) mandatory.

Open Industry 4.0 Alliance helps its members to be prepared for the upcoming challenges!



Die Erhöhung der Sicherheit von Lieferketten ist ein Kernanliegen des BSI.

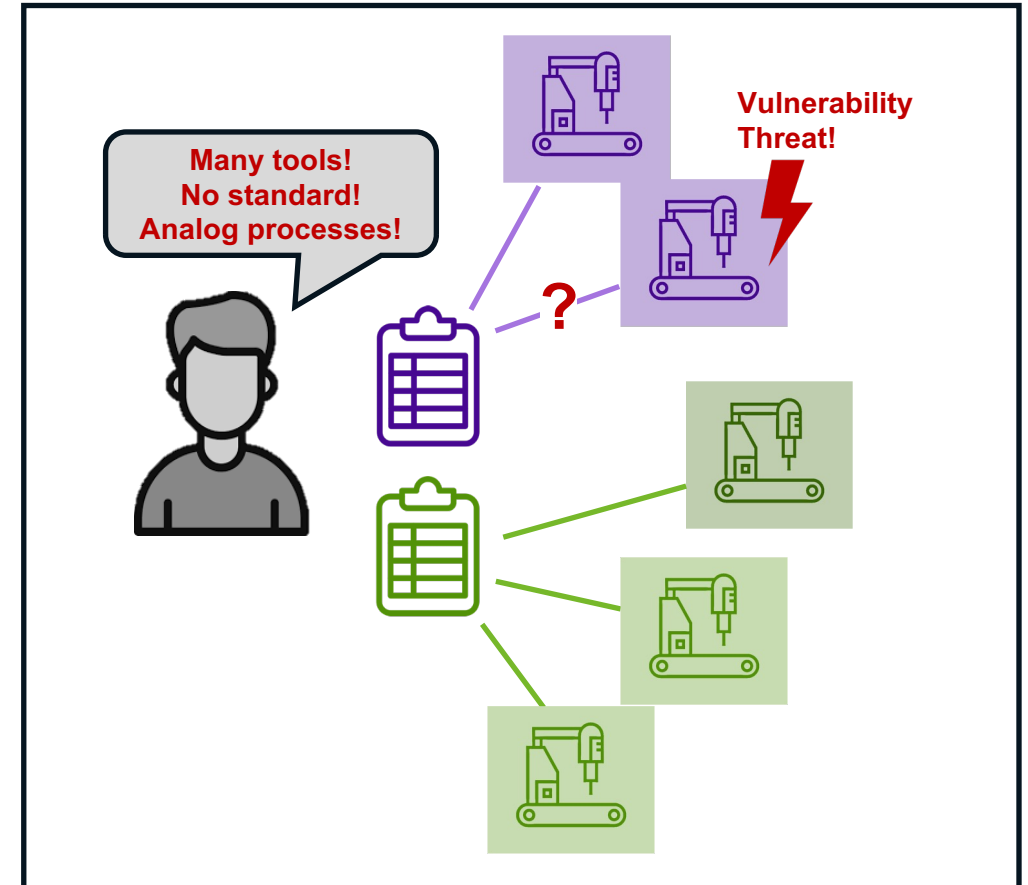
- Dazu gehört ein transparentes und effizientes Schwachstellen- und Patchmanagement auf Basis von „Software Bills of Material (SBoM)“.
- Das „Common Security Advisory Framework (CSAF)“ kann entscheidend dazu beitragen den Überblick von Maßnahmen zur Behebung von Schwachstellen zu behalten.
- Das Format „Vulnerability Exploitability eXchange (VEX)“ als CSAF-Profil vereinfacht es, nicht relevante Schwachstellen schneller zu identifizieren, um Ressourcen nur für wichtige Schwachstellen einzusetzen.
- Maschinelle Verarbeitbarkeit und Automatisierung hilft, diese Aufgabenstellungen effizient zu bearbeiten.



Remote Device Management – Use Case Vulnerability Management

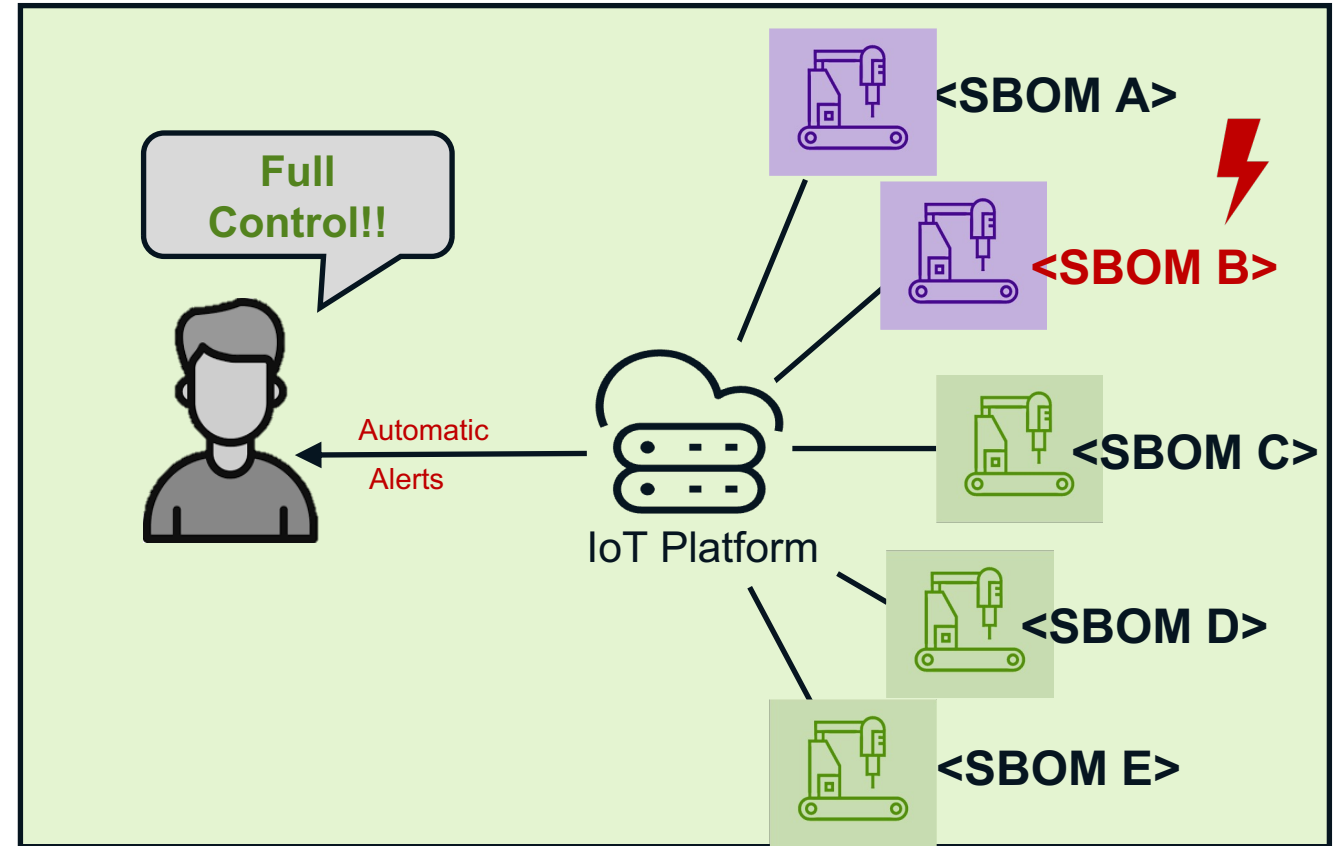
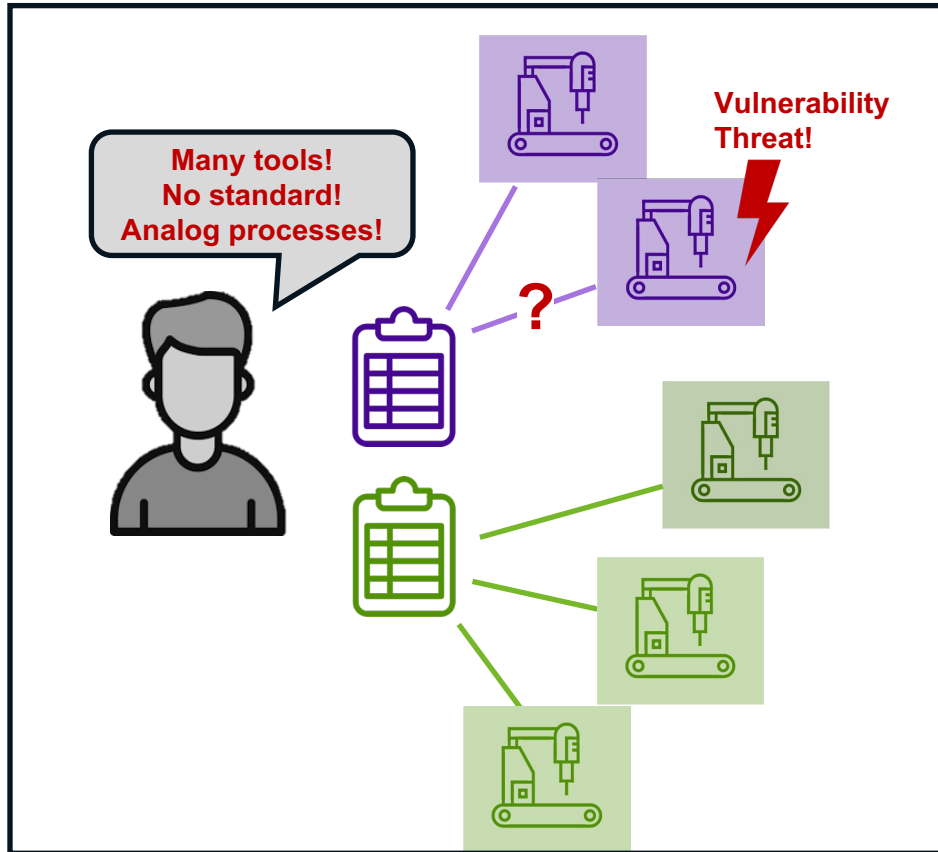
Current Situation

- ❖ OT admins typically discover and track devices manually in spreadsheets.
- ❖ Patchwork of existing and mostly proprietary vulnerability management tools.
- ❖ Tools are normally not connected to management systems like ERP or IT asset management. So, manual update on-site is needed.
- ❖ **Vulnerability Management:**
Standardized, cloud-based solution for industrial assets is missing!



Remote Device Management – Use Case Vulnerability Management

Challenges & Way Forward



OI4 drives standardized, digital Vulnerability Management

Remote Device Management – Use Case Vulnerability Management

Demo Utilization of Software-BOM via Cumulocity IoT Platform (1)



The screenshot displays the Cumulocity IoT Device Management interface for a device named 'sag/MyDevice'. The left sidebar contains navigation options such as Home, Devices, Registration, All devices, Map, Simulators, Availability, Overviews, Groups, Device types, SmartREST templates, Device protocols, LWM2M post-operatio..., and Management. The main content area is divided into several sections: Info, Measurements, Alarms, Control, Software (highlighted), Availability, Events, and Identity. The 'Software' section is active, showing a list of installed software components. A search bar and a filter dropdown are present above the list. The list includes the following items:

| Component Name | Version |
|----------------|---------------|
| actix-codec | VERSION 0.5.1 |
| actix-http | VERSION 3.3.1 |
| actix-macros | VERSION 0.2.4 |
| actix-router | VERSION 0.5.1 |
| actix-rt | VERSION 2.8.0 |
| actix-server | VERSION 2.2.0 |
| actix-service | VERSION 2.0.2 |
| actix-utils | VERSION 2.0.1 |

To the right of the installed software list is a 'Software changes' section, which currently displays 'No software changes. Selected actions will be displayed here.' A dashed green box highlights the installed software list, with a dotted line pointing from it to the caption below.

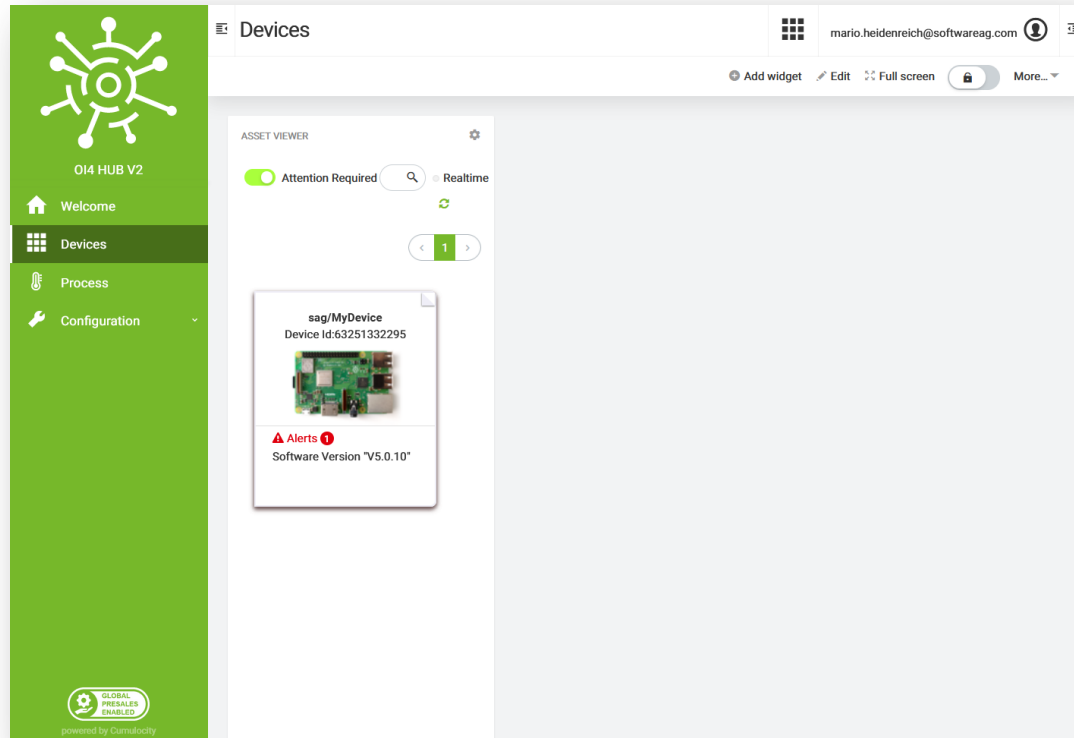
SBOM imported into Cumulocity IoT Device Management



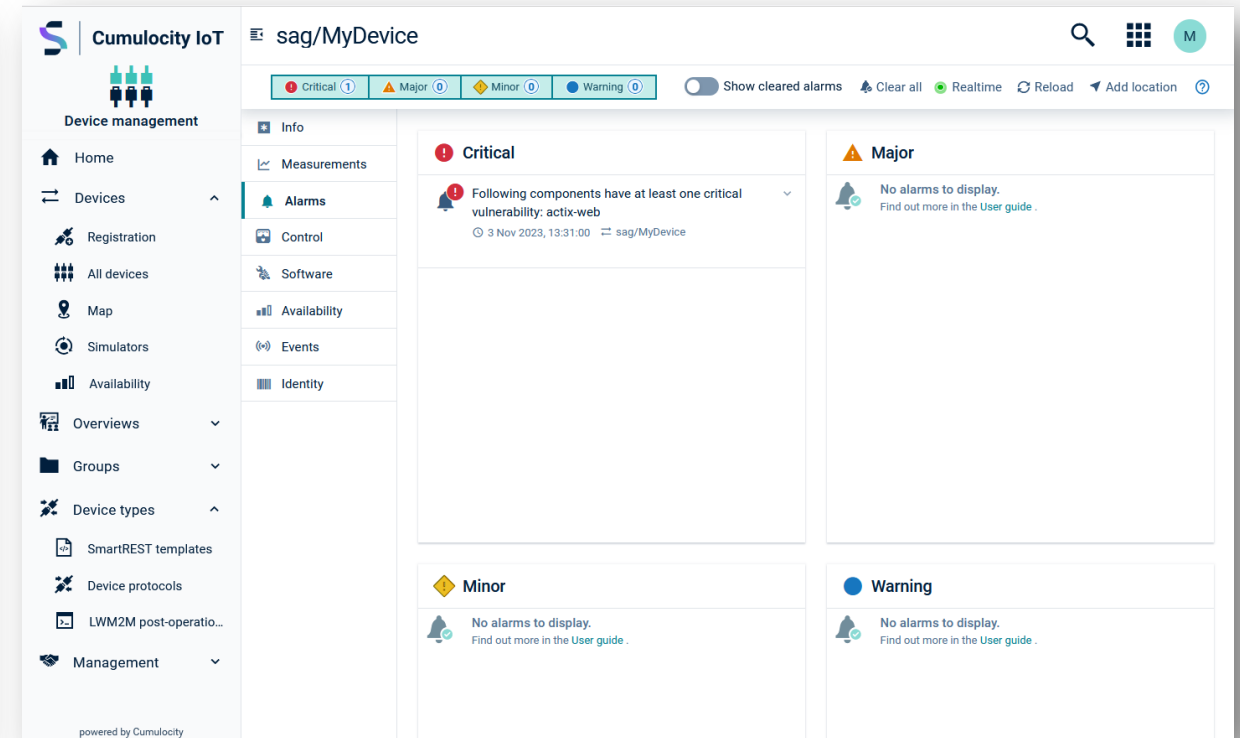
Remote Device Management – Use Case Vulnerability Management



Utilization of Software-BOM via Cumulocity IoT Platform (2)



IoT Cockpit: Overview on devices with vulnerabilities



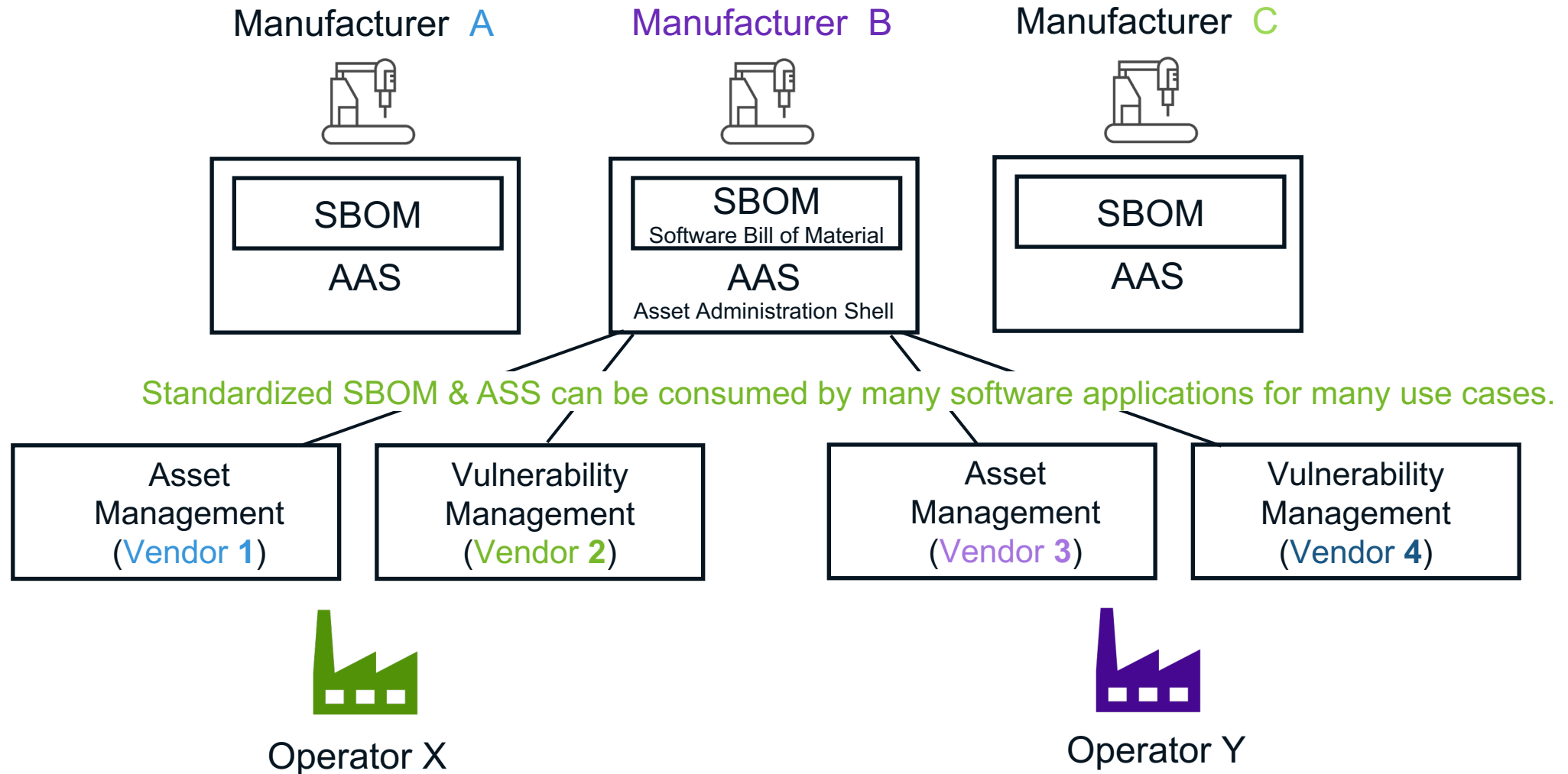
IoT Device Management: Details on vulnerabilities



Remote Device Management – Use Case Vulnerability Management



Standardization drives Automation of Vulnerability Management Across all Stakeholders



Remote Device Management – Use Case Vulnerability Management



There are so many software packages and vulnerabilities to be tracked. It is simply impossible to handle this task manually!

The only way forward:

Automate the handling of data

No need to start from scratch: Learn from the IT domain and reuse best practice, tools and standards, such as Cyclone-Dx or SPDX.

OI4 Approach: Implement interoperable cross-vendor standards based on SBOM and Asset Administration Shell.

Let's Get in Contact

We are looking forward discussing your vulnerability use cases.



Dr. Florian Probst

Director IoT Portfolio Strategy



Linked 

florian.probst@softwareag.com



Cumulocity IoT

Daniel Bitzer

Manager Industrial Security



daniel.bitzer@ifm.com



ifm electronic

Sebastian Fischer

Produktmanager



Linked 

sebastian.fischer@complement.de



omnect

Device Management