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

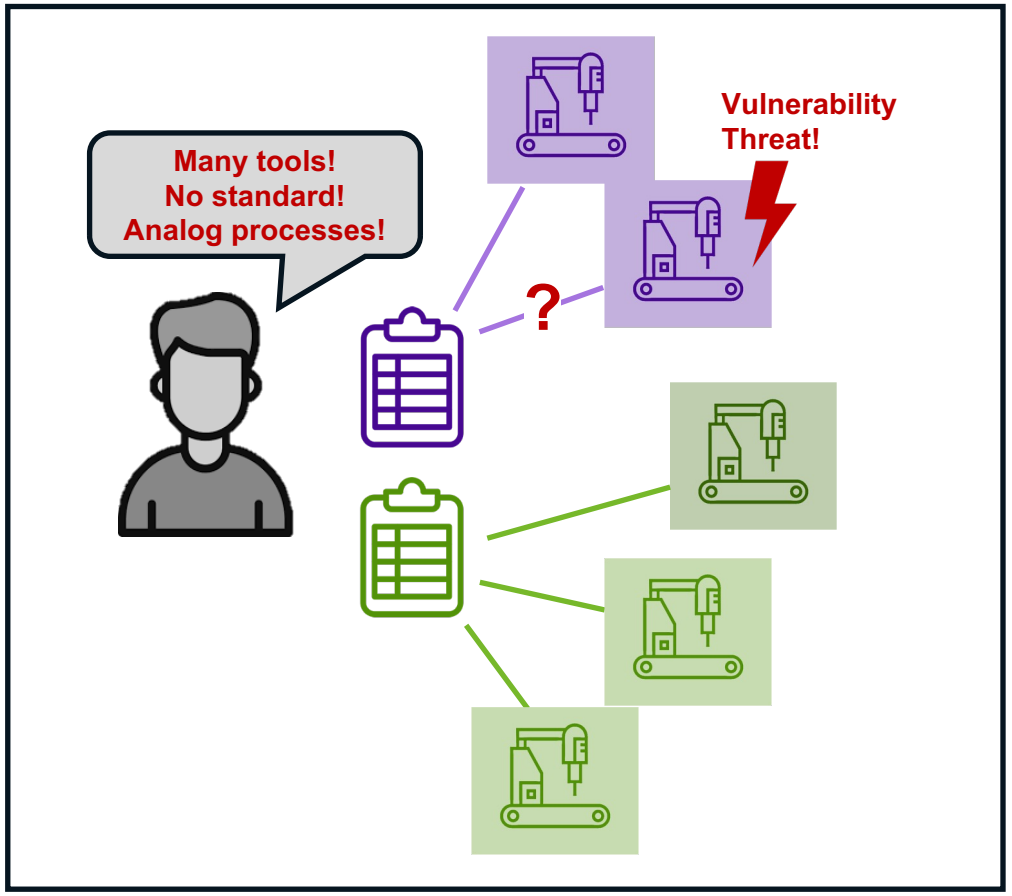
- BSI makes vulnerability patch management based on Software Bill of Material (SBoM) mandatory.

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

Remote Device Management – Use Case Vulnerability Management

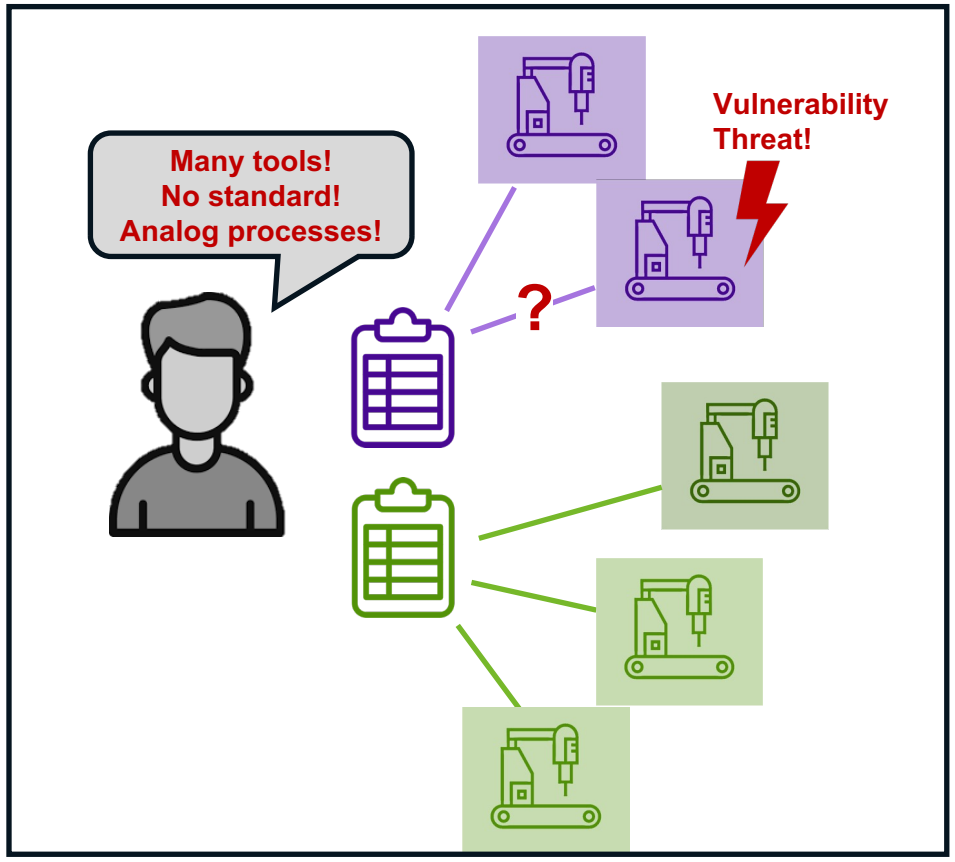
Current Situation

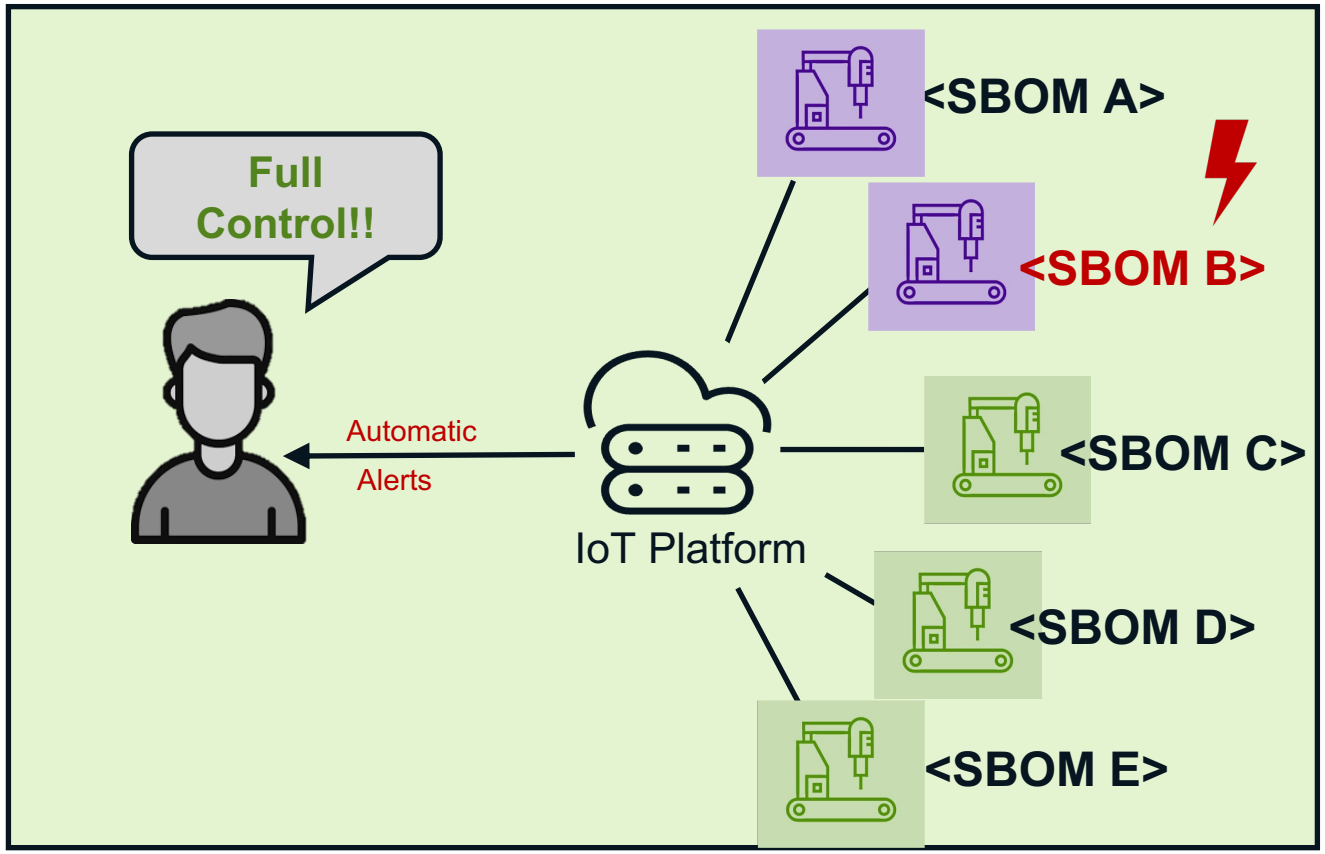
- OT admins typically discover and track devices manually in spreadsheets.
- Patchwork of existing and mostly proprietary vulnerability management tools.
- Tools are normally not connected to management systems like ERP or IT asset management. So, manual update on-site is needed.
- Vulnerability Management: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



Remote Device Management – Use Case Vulnerability Management

Challenges & Way Forward

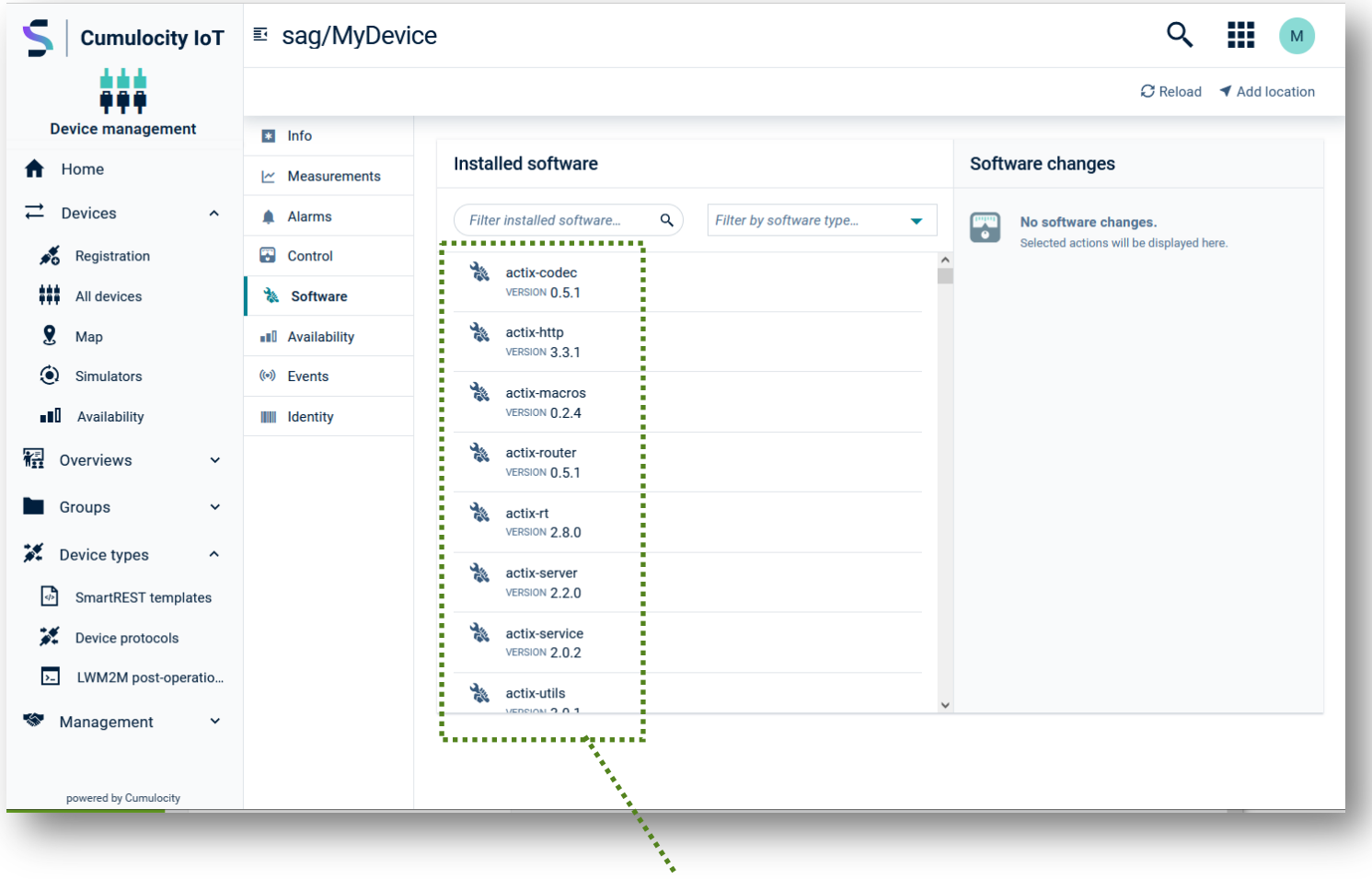




OI4 drives standardized, digital Vulnerability Management

Remote Device Management – Use Case Vulnerability Management

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

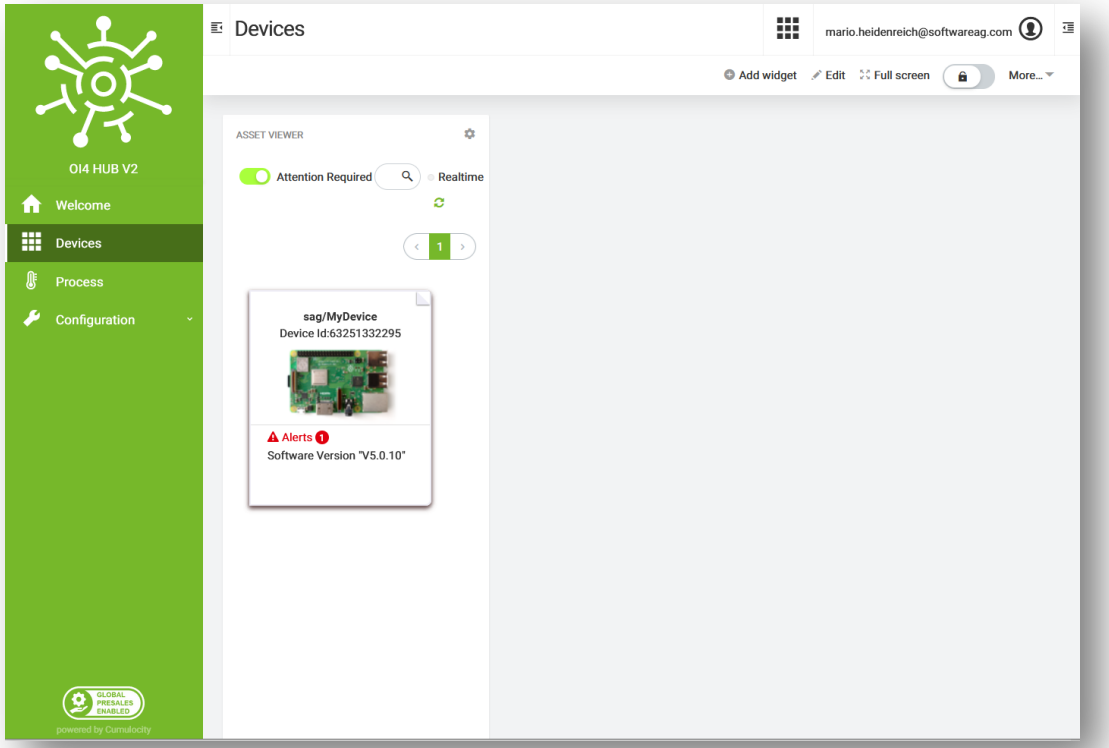


SBOM imported into Cumulocity IoT Device Management

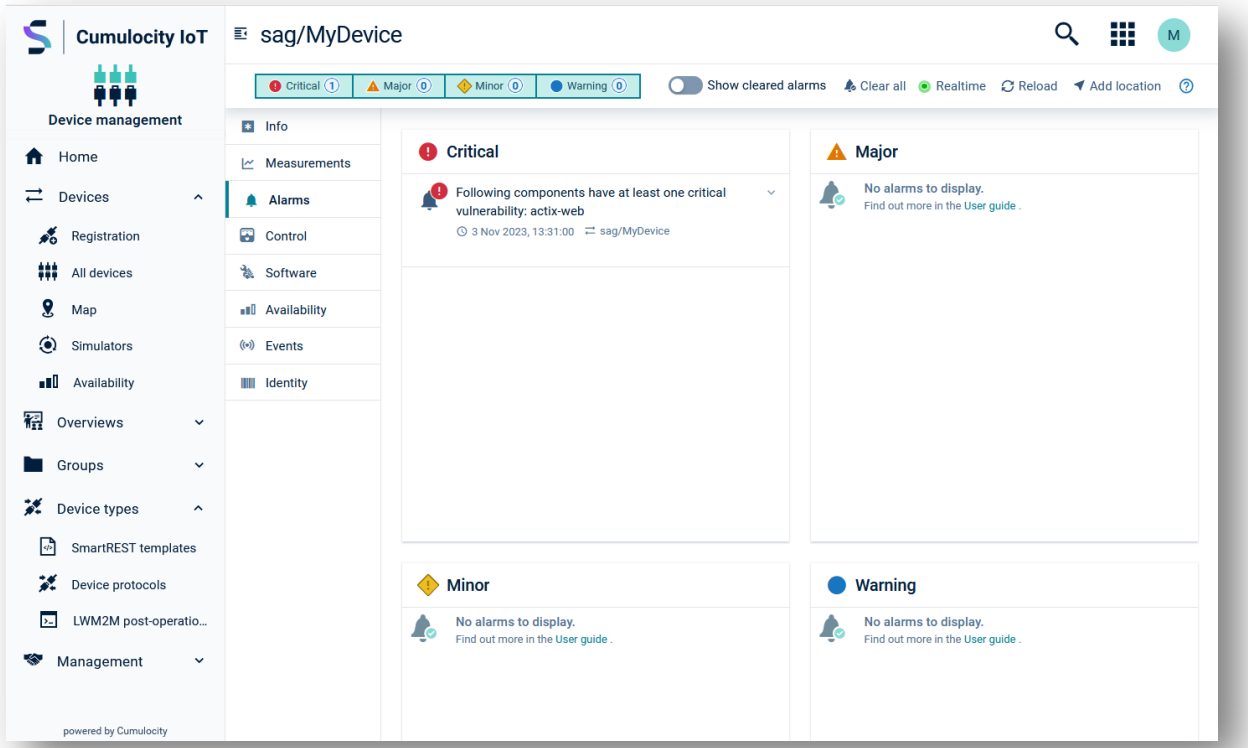
Cumulocity IoT

Remote Device Management – Use Case Vulnerability Management

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



IoT Cockpit: Overview on devices with vulnerabilities

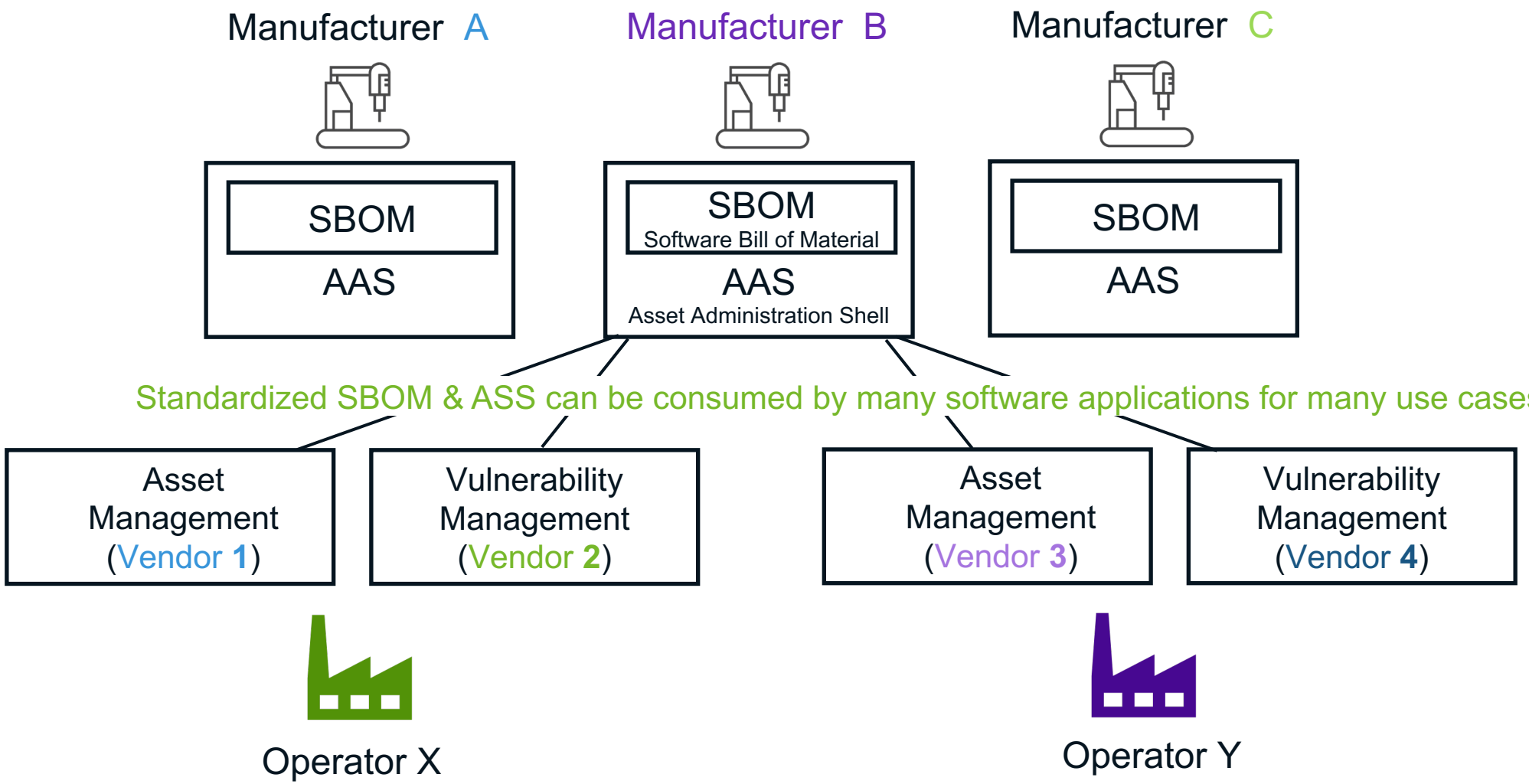


IoT Device Management: Details on vulnerabilities

Cumulocity IoT

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 re-use 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.

OPEN INDUSTRY 4.0 ALLIANCE

Dr. Florian Probst

Director IoT Portfolio Strategy

Linked in

florian.probst@softwareag.com

Cumulocity IoT

Daniel Bitzer

Manager Industrial Security

daniel.bitzer@ifm.com

ifm electronic

Sebastian Fischer

Produktmanager

Linked in

sebastian.fischer@conplement.de

omnect Device Management