boston MEDevice an MD&M event

SEPTEMBER 30 – OCTOBER 1, 2025

BOSTON CONVENTION &
EXHIBITION CENTER

SBOMs in MedTech:

Ensuring Compliance, Security, and Innovation in a Rapidly Evolving Regulatory Landscape

Tim Mackey
tmackey@blackduck.com

Ken Zalevsky
kzalevsky@vigilant-ops.com

Forces Driving the MedTech SBOM Imperative

- Regulatory pressure continues to escalate (524B, EU NIS2, FDA, EU CRA, etc.)
- Supply chain threats proliferate through third-party components
- Continuous post-market vigilance, timely responses to vulnerabilities expected
- Changing market dynamic with more customers demanding transparency

How MedTech Manufacturers Are Using SBOMs Today

- To improve supply chain visibility by tracking third-party components
- To identify risks by mapping SBOM components to known vulnerabilities
- To provide engineering teams visibility during the product build process
- For premarket submissions as required by FDA
- To respond to customer cybersecurity documentation requests

Where Manufacturers Go Wrong in SBOM Implementation

- Treating SBOMs as one-time artifacts, not evolving SBOMs across lifecycle
- Incomplete or shallow coverage of components
- Format inconsistency hindering interoperability
- Failure to operationalize - not linking SBOM into QMS, CAPA, other workflows
- Lack of post-market process for continuous monitoring and updates

How Leaders Get SBOMs Right

- Move beyond one-time SBOMs to continuous lifecycle management
- Ensure complete visibility across build and runtime components
- Integrate SBOMs into compliance workflows and processes
- Use SBOMs as a strategic enabler, building customer trust
- Measure and demonstrate tangible results, like time to deploy security patches

boston MEDevice an MD&M event

SEPTEMBER 30 – OCTOBER 1, 2025

BOSTON CONVENTION & EXHIBITION CENTER

COMPANY OVERVIEW

Bayer is a global enterprise with core competencies in healthcare and agriculture. Their commitment to innovation and sustainability drives them to develop cutting-edge solutions that address some of the world's most pressing challenges.

As a leader in the life sciences industry, Bayer prioritizes transparency, security, and compliance to maintain trust with stakeholders and meet evolving regulatory requirements.

Case Study: *Bayer*

SOLUTION

Comprehensive SBOM Oversight: Unified data integration from both development and runtime environments to generate complete and actionable SBOMs.

Automated, Scalable Processes: Optimized workflows that minimize manual intervention, accelerating regulatory submissions.

Regulatory-Ready Compliance: Seamless alignment with FDA and international standards, supporting defect density metrics and versatile export formats (e.g., CycloneDX, SPDX, PDF, VEX).

Proactive Risk Management: Continuous risk assessment and prioritization, enabling real-time monitoring of vulnerabilities and their impact on specific products.

COMPANY OVERVIEW

Ascensia Diabetes Care is a global leader in medical device manufacturing, dedicated to improving the health and lives of people with diabetes.

Since its founding in 2016, Ascensia has been at the forefront of healthcare innovation. Headquartered in Basel, Switzerland, the company's commitment to advancing technology and improving patient outcomes sets it apart as a trusted name in diabetes care.

ASCENSIA
Diabetes Care

***Case Study:** Ascensia Diabetes Care*

SOLUTION

Ascensia turned to Vigilant Ops to meet their SBOM management needs.

Holistic SBOM Management: Integration of data from development and runtime environments to create complete, actionable SBOMs.

Automation and Scalability: Streamlined workflows, reducing manual efforts and enabling more efficient regulatory submissions.

Compliance-Ready Capabilities: Alignment with FDA and global regulatory requirements, including defect density metrics and flexible export formats (e.g., CycloneDX, SPDX, PDF, VEX, etc.).

Risk Management: Continuous risk scoring and dispositioning to assess and monitor vulnerabilities' impact on specific products.

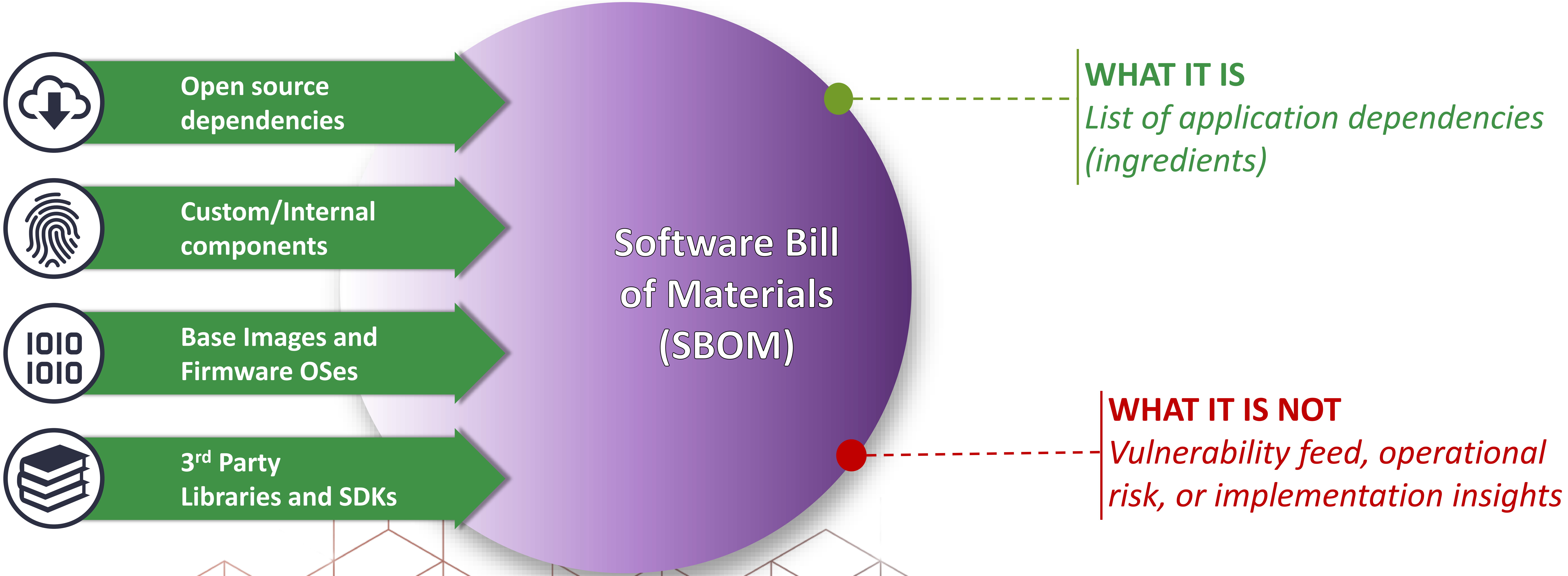
Looking beyond SBOMs to Workflows

boston MEDevice an MD&M event

SEPTEMBER 30 – OCTOBER 1, 2025

BOSTON CONVENTION &
EXHIBITION CENTER

Comprehensive SBOMs identify the origin of all components



Open source dependencies

Custom/Internal components

Base Images and Firmware OSes

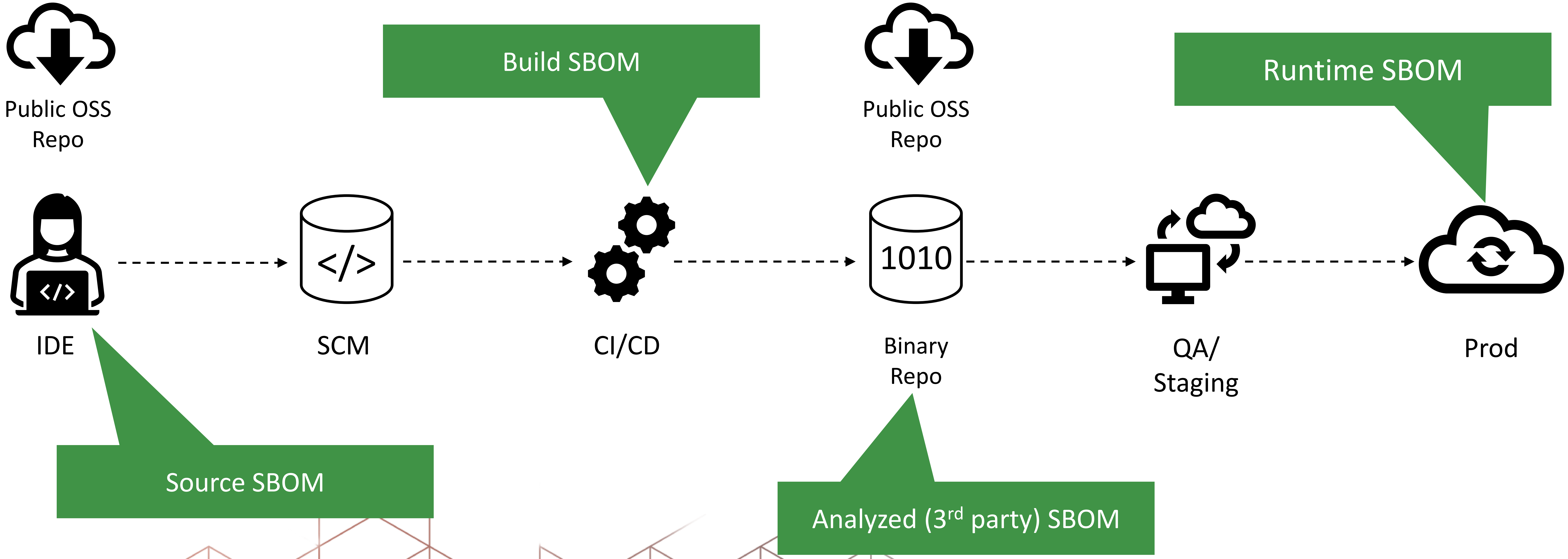
3rd Party Libraries and SDKs

Software Bill of Materials (SBOM)

WHAT IT IS
List of application dependencies (ingredients)

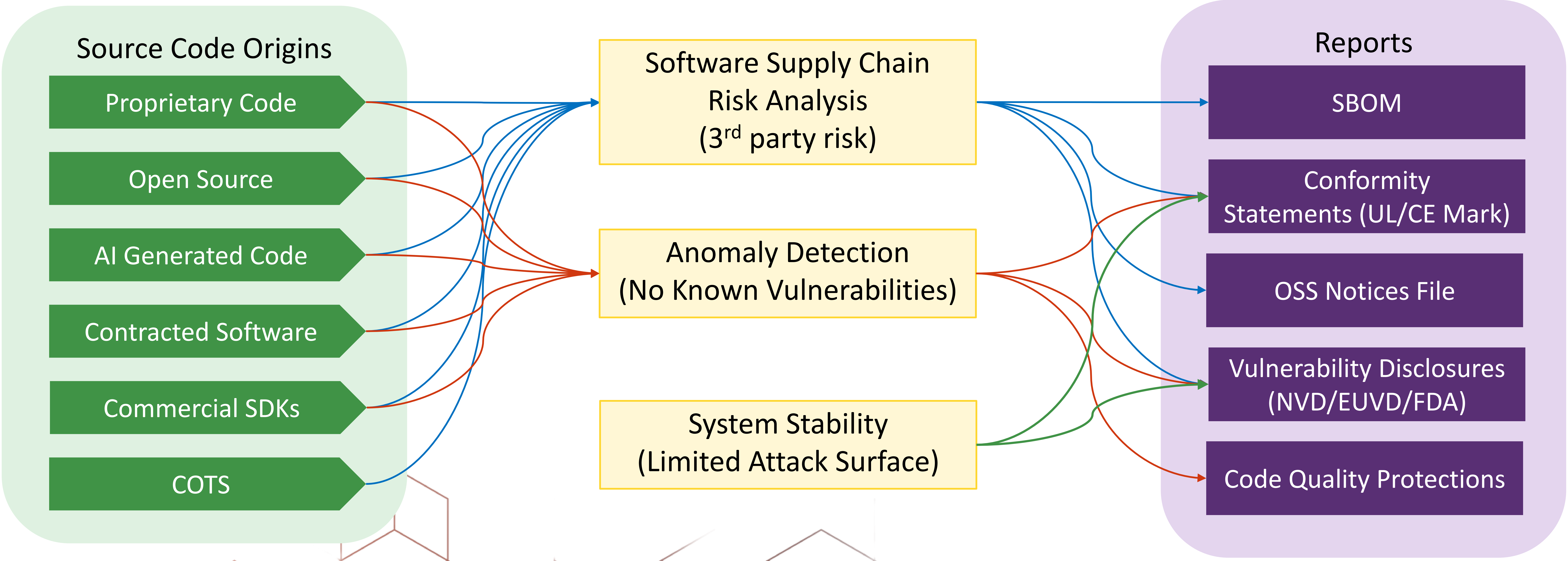
WHAT IT IS NOT
Vulnerability feed, operational risk, or implementation insights

Knowing where an SBOM is created within the SDLC matters



Source: *Terms used are consistent with [CISA SBOM Types April 2023]*

SBOMs are part of a "Secure by Default" cyber-hazard analysis



Source Code Origins

- Proprietary Code
- Open Source
- AI Generated Code
- Contracted Software
- Commercial SDKs
- COTS

Software Supply Chain
Risk Analysis
(3rd party risk)

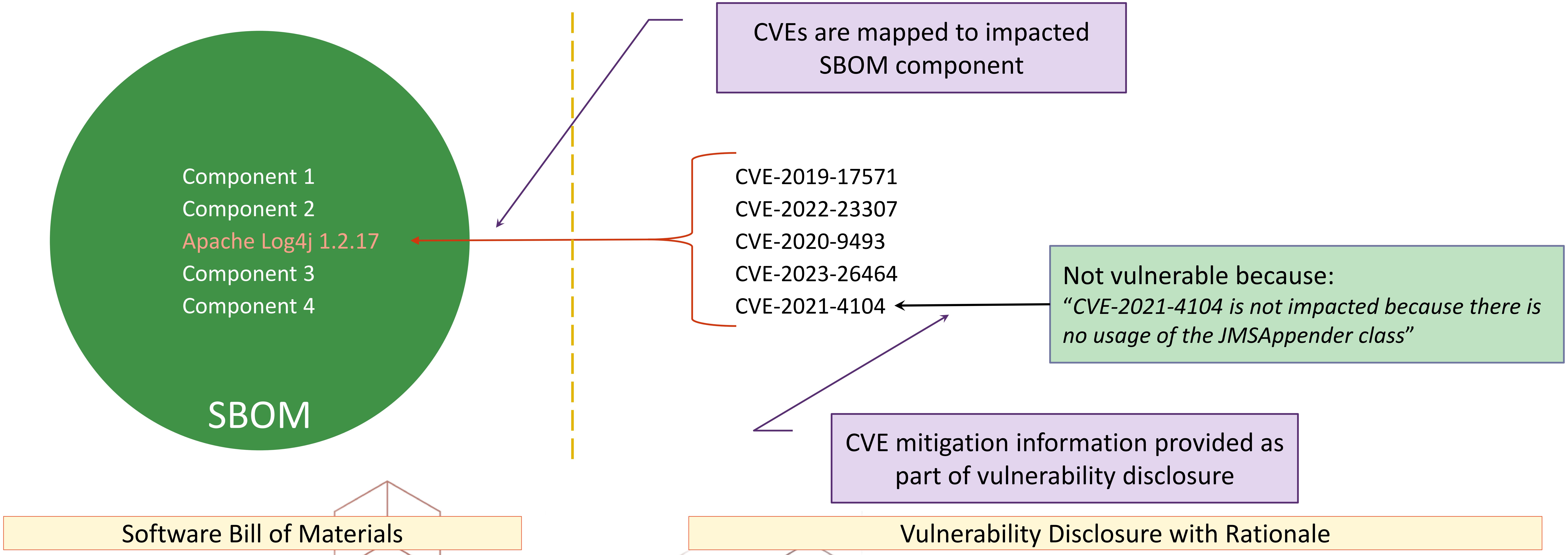
Anomaly Detection
(No Known Vulnerabilities)

System Stability
(Limited Attack Surface)

Reports

- SBOM
- Conformity Statements (UL/CE Mark)
- OSS Notices File
- Vulnerability Disclosures (NVD/EUVD/FDA)
- Code Quality Protections

Disclosing unpatched CVEs present at release or post-market



CVEs are mapped to impacted SBOM component

Component 1
Component 2
Apache Log4j 1.2.17
Component 3
Component 4

SBOM

CVE-2019-17571
CVE-2022-23307
CVE-2020-9493
CVE-2023-26464
CVE-2021-4104

Not vulnerable because:
“CVE-2021-4104 is not impacted because there is no usage of the JMSAppender class”

CVE mitigation information provided as part of vulnerability disclosure

Software Bill of Materials

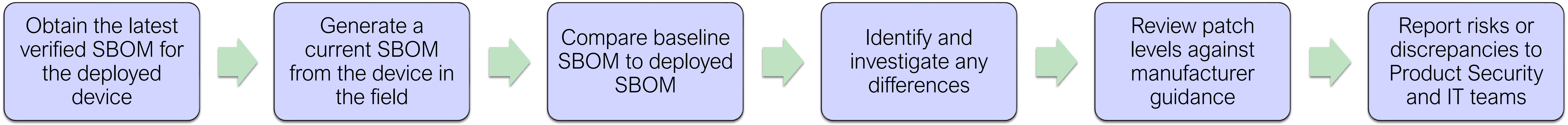
Vulnerability Disclosure with Rationale

Scenario: Field servicing of software-enabled devices

Overview ◆ Use SBOMs to maintain, troubleshoot, and verify deployed devices over their operational life.

Key Actors ◆ Product Security ◆ Field Service ◆ Consumer IT ◆ Consumer Security

Process Steps



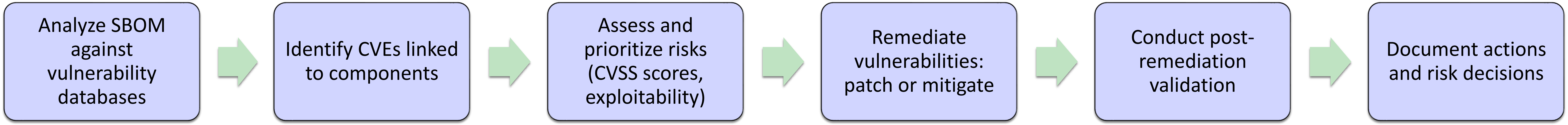
Obtain the latest verified SBOM for the deployed device → Generate a current SBOM from the device in the field → Compare baseline SBOM to deployed SBOM → Identify and investigate any differences → Review patch levels against manufacturer guidance → Report risks or discrepancies to Product Security and IT teams

Scenario: Pre-deployment vulnerabilities and exposures

Overview ◆ Identify and mitigate vulnerabilities in software components before product release to minimize risk, compliance, and enhance trust

Key Actors ◆ Procurement ◆ Regulatory ◆ Engineering ◆ Product Security (PSIRT)

Process Steps



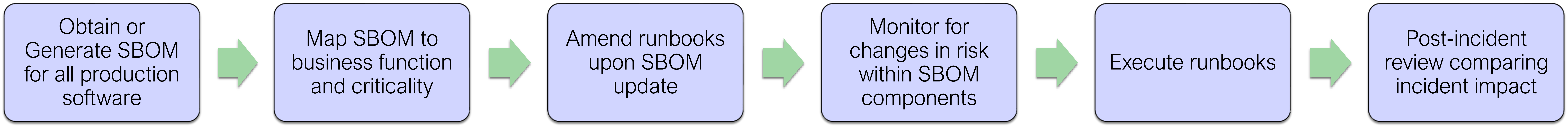
Analyze SBOM against vulnerability databases → Identify CVEs linked to components → Assess and prioritize risks (CVSS scores, exploitability) → Remediate vulnerabilities: patch or mitigate → Conduct post-remediation validation → Document actions and risk decisions

Scenario: Incident response

Overview ◆ Enhance incident response processes by enabling faster identification, containment, and remediation of incidents (e.g. Log4J)

Key Actors ◆ IT/DevSecOps ◆ Risk and Compliance ◆ Legal ◆ Engineering

Process Steps



Obtain or Generate SBOM for all production software → Map SBOM to business function and criticality → Amend runbooks upon SBOM update → Monitor for changes in risk within SBOM components → Execute runbooks → Post-incident review comparing incident impact

Questions

boston MEDevice an MD&M event

SEPTEMBER 30 – OCTOBER 1, 2025

BOSTON CONVENTION &
EXHIBITION CENTER

Thank You!

Tim Mackey
Head of Software Supply Chain Strategy
Black Duck, Inc.
tmackey@blackduck.com
linkedin.com/in/mackeytim/

Ken Zalevsky
CEO
Vigilant Ops, Inc.
ken.zalevsky@vigilant-ops.com
linkedin.com/in/ken-zalevsky/