The Life of an SBOM:

Where does it go and what do people do to it and with it?

Anita D’Amico, PhD

www.cotopaxiconsulting.com

Ken Zalevsky

www.vigilant-ops.com

Cotopaxi Consulting
Cross the Chasm with Confidence

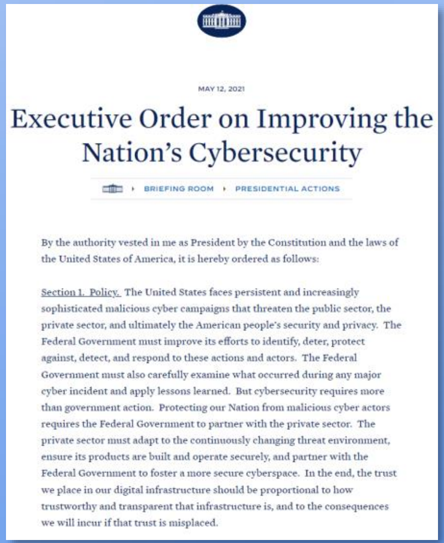
VIGILANTOPS

Introductions

- About the speakers: Ken Zalevsky and Anita D’Amico
    - Background
    - Interest in SBOMs
- About the audience:
    - Interest in SBOMs
    - Verticals
    - What you hope to learn

Motivation for SBOM Generation and Management

- **EO14028**: Executive Order on Improving the Nation's Cybersecurity
  - SBOMs required for all (non-open source) software acquired by US government
- **DHS CISA Attestation**: Mandates for adherence to Secure Software Development Framework (SSDF)
- **FDA Guidelines**: Compliance requirements for medical devices
  - October 2023: FDA's cybersecurity requirements for all cyber device manufacturers seeking FDA approval
- **Emerging U.S. Hospital Regulations:**
  - Anticipated new regulations impacting SBOM management in hospitals



MAY 12, 2021

Executive Order on Improving the Nation's Cybersecurity

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

Software Bill of Materials (SBOM)

- Comprehensive inventory of ingredients in software used in an application or device
- Usually generated by the product's team as part of the software development process (Source or Build SBOMs)
  - Can also be generated post deployment (Deployed SBOM)
- Delivered to consumer of product in SPDX, CycloneDX or SWID standard formats

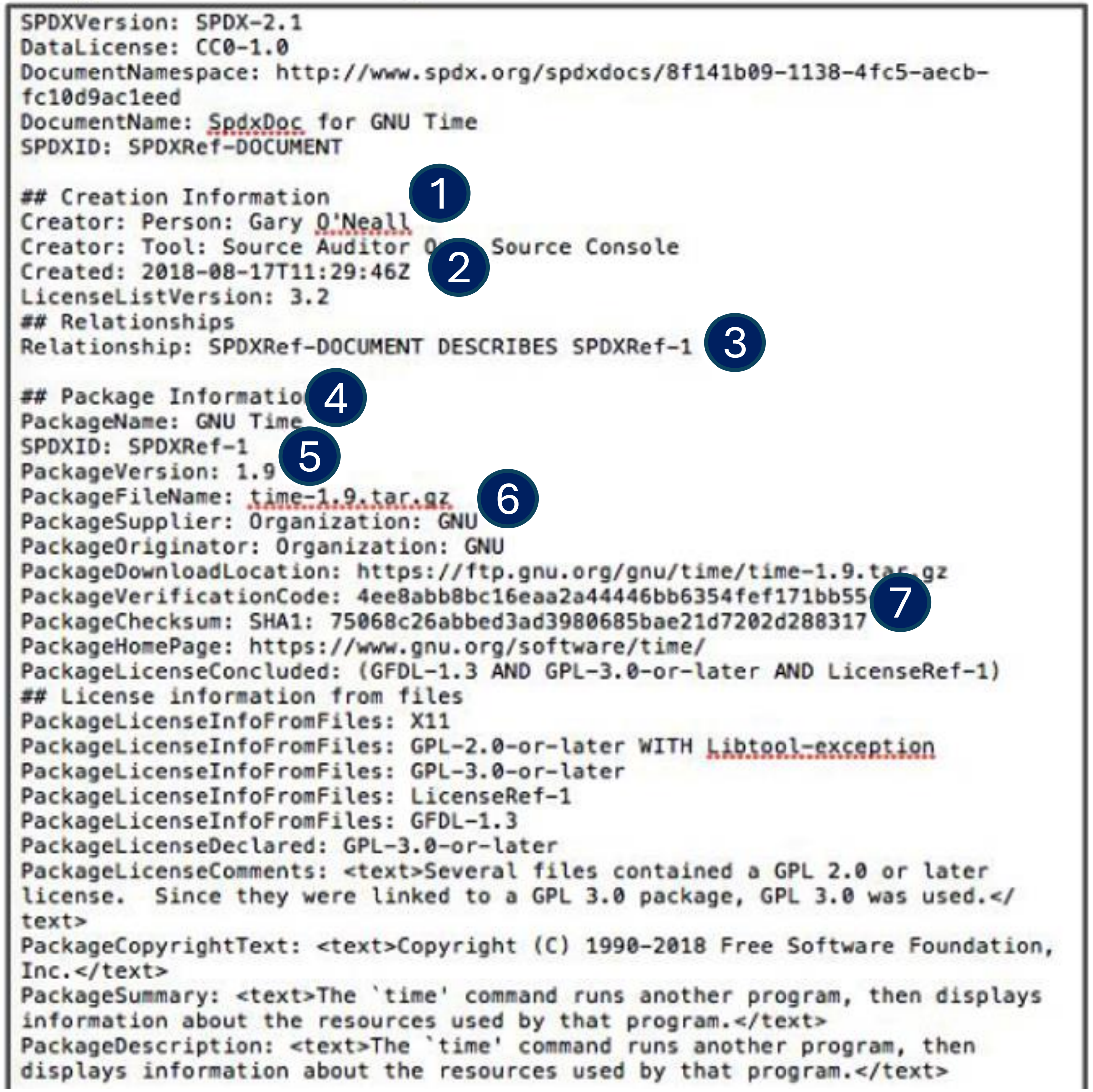
Minimum data in SBOM

- Supplier name
- Component names
- Versions of each component
- Dependencies on each component
- Author of SBOM
- Other unique identifiers
- Time stamp

Types of Software Bill of Material (SBOM) Documents, published by CISA, 2023. https://www.cisa.gov/sites/default/files/2023-04/sbom-types-document-508c.pdf

The Minimum Elements for a Software Bill of Materials (SBOM). Published by US Dept of Commerce and National Telecommunications and Information Administration (NTIA). July 2021. https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

Build SBOM (SPDX)



```
SPDXVersion: SPDX-2.1
DataLicense: CC0-1.0
DocumentNamespace: http://www.spdx.org/spdxdocs/8f141b09-1138-4fc5-aecb-
fc10d9ac1eed
DocumentName: SpdxDoc for GNU Time
SPDXID: SPDXRef-DOCUMENT

## Creation Information
Creator: Person: Gary O'Neall
Creator: Tool: Source Auditor Open Source Console
Created: 2018-08-17T11:29:46Z
LicenseListVersion: 3.2
## Relationships
Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-1

## Package Information
PackageName: GNU Time
SPDXID: SPDXRef-1
PackageVersion: 1.9
PackageFileName: time-1.9.tar.gz
PackageSupplier: Organization: GNU
PackageOriginator: Organization: GNU
PackageDownloadLocation: https://ftp.gnu.org/gnu/time/time-1.9.tar.gz
PackageVerificationCode: 4ee8abb8bc16eaa2a44446bb6354fef171bb55
PackageChecksum: SHA1: 75068c26abbed3ad3980685bae21d7202d288317
PackageHomePage: https://www.gnu.org/software/time/
PackageLicenseConcluded: (GFDL-1.3 AND GPL-3.0-or-later AND LicenseRef-1)
## License information from files
PackageLicenseInfoFromFiles: X11
PackageLicenseInfoFromFiles: GPL-2.0-or-later WITH Libtool-exception
PackageLicenseInfoFromFiles: GPL-3.0-or-later
PackageLicenseInfoFromFiles: LicenseRef-1
PackageLicenseInfoFromFiles: GFDL-1.3
PackageLicenseDeclared: GPL-3.0-or-later
PackageLicenseComments: <text>Several files contained a GPL 2.0 or later
license.  Since they were linked to a GPL 3.0 package, GPL 3.0 was used.</
text>
PackageCopyrightText: <text>Copyright (C) 1990-2018 Free Software Foundation,
Inc.</text>
PackageSummary: <text>The `time' command runs another program, then displays
information about the resources used by that program.</text>
PackageDescription: <text>The `time' command runs another program, then
displays information about the resources used by that program.</text>
```

Minimum data in SBOM

1. Author of SBOM
2. Time stamp
3. Dependencies
4. Component Name
5. Component version
6. Supplier name
7. Unique identifier

SBOM Lifecycle Management aka SBOM Operations

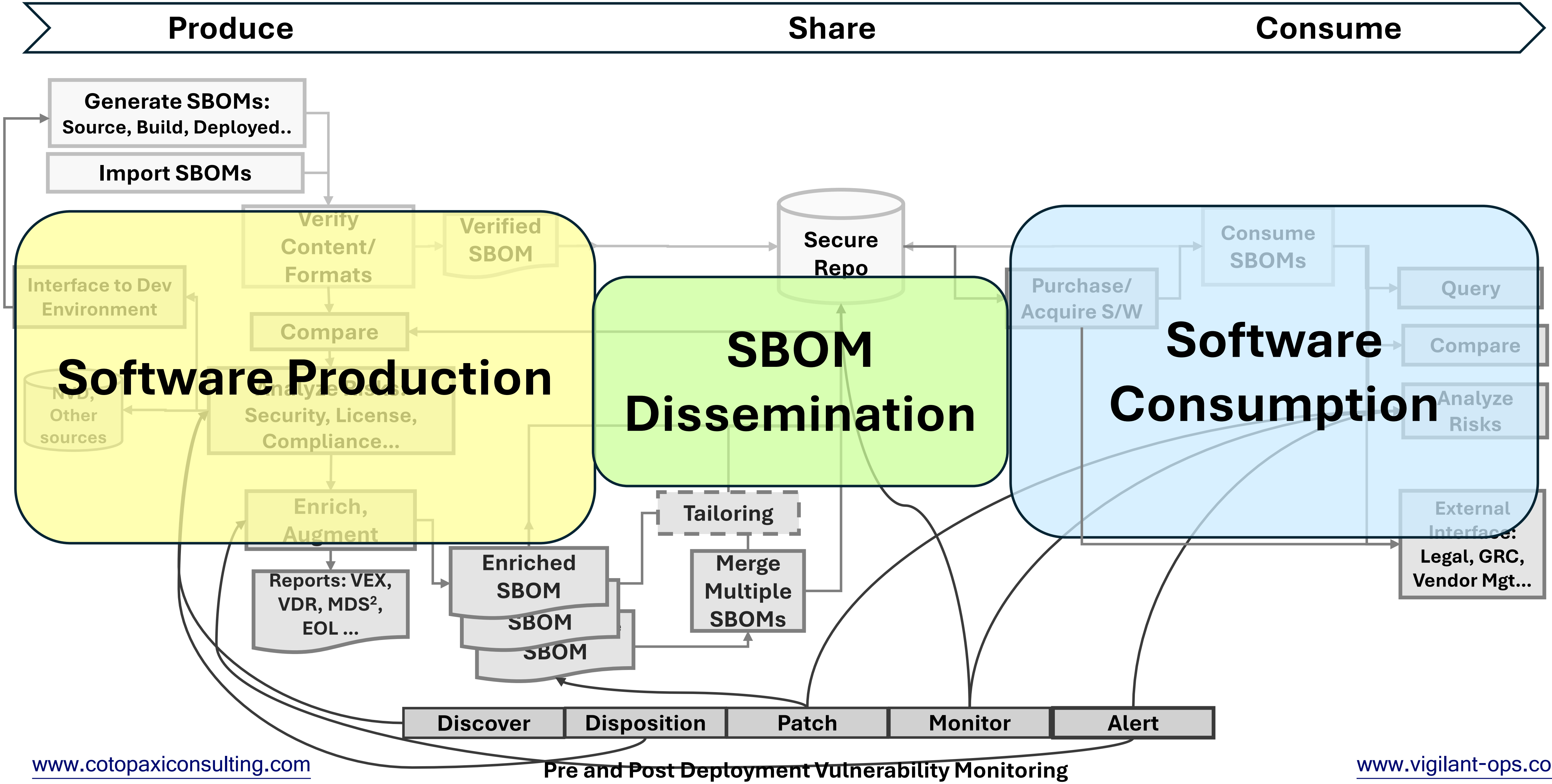
What you do with an SBOM

- Actions taken largely after initial SBOM generation
- By software producer, distributor and consumer
- To impact software security, supply chain transparency, regulatory and license compliance, procurement processes

Dynamic, Multi-Player Ecosystem

- Spans lifecycle of software: production, release, deployment, maintenance
- SBOM management users: software release engineers, AppSec teams, PSIRTs, risk/compliance teams, procurement, consumer's security team, incident responders

SBOM's Lifecycle: Three Major Stages



Who Cares? Industries and stakeholders most actively managing SBOMs

Produce → Share → Consume

Software Producers

- Medical device manufacturers
- Financial services
- US government suppliers
- B2B enterprise software
- Automotive manufacturers
- IoT, e.g., heating, security sensors

Stakeholders

- Software release engineering
- Product security
- Risk/compliance
- Field service reps

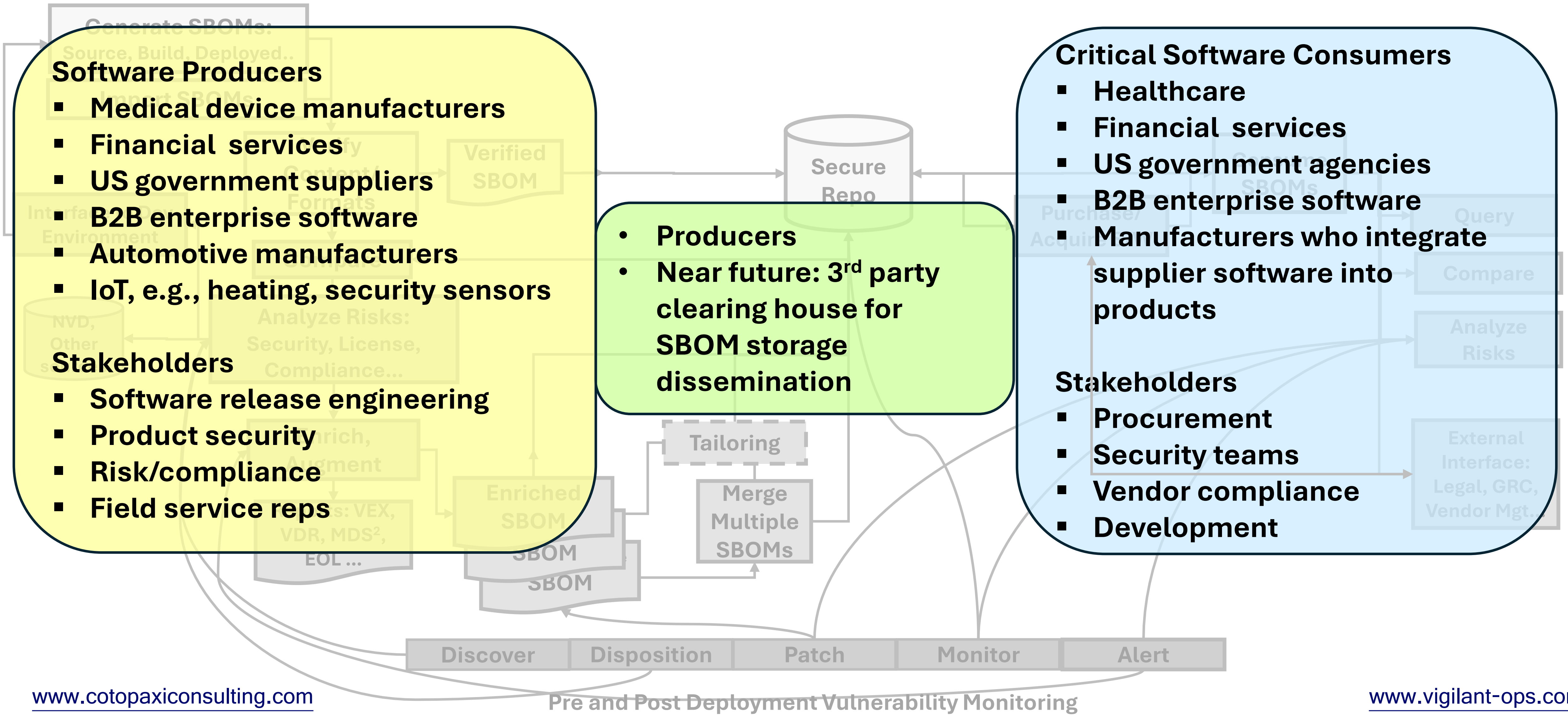
- Producers
- Near future: 3rd party clearing house for SBOM storage dissemination

Critical Software Consumers

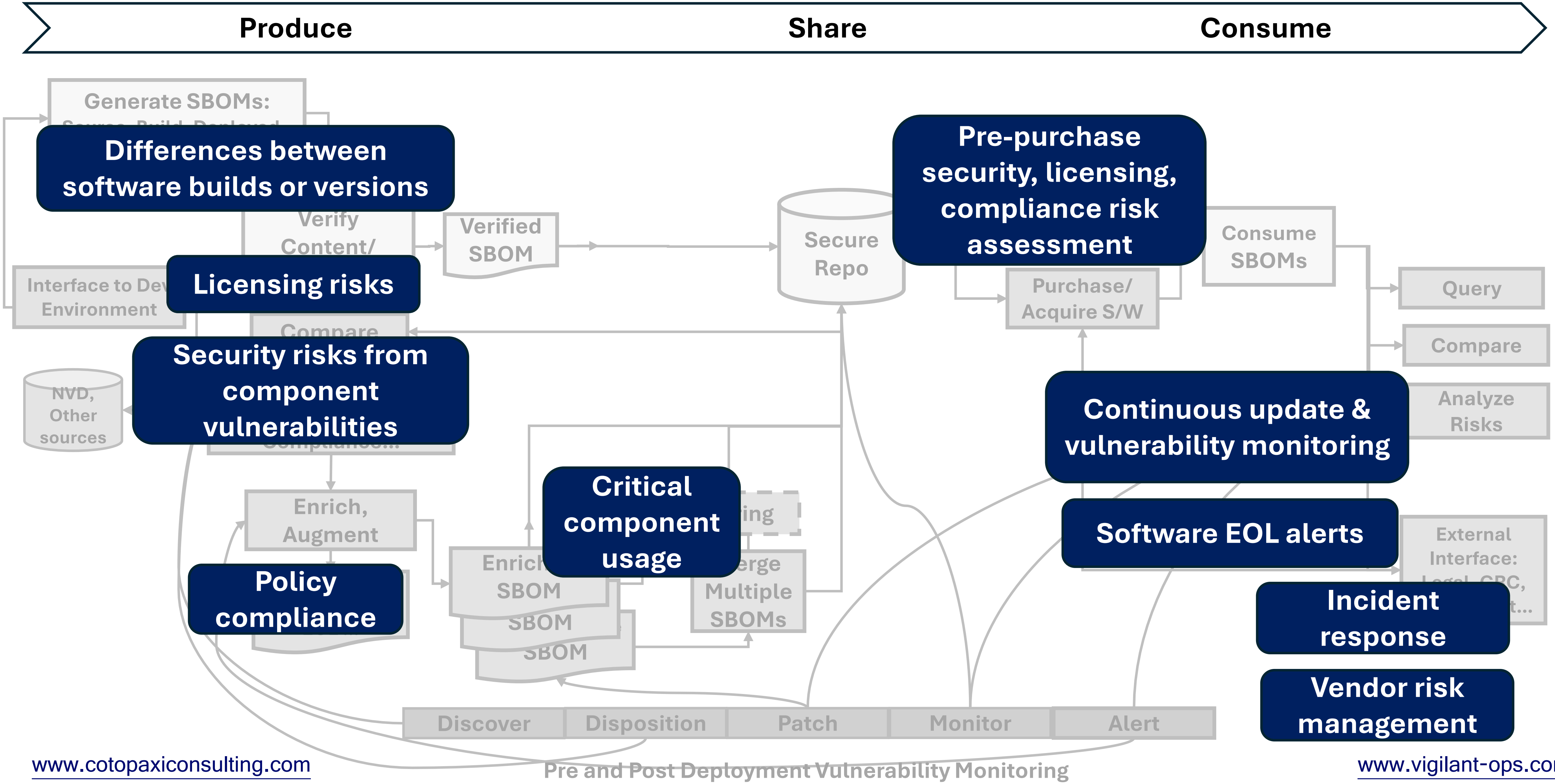
- Healthcare
- Financial services
- US government agencies
- B2B enterprise software
- Manufacturers who integrate supplier software into products

Stakeholders

- Procurement
- Security teams
- Vendor compliance
- Development


Generate SBOMs: Source, Build, Deployed..
Import SBOMs
Verify Content / Formats
Verified SBOM
Interface to Dev Environment
Compare
NVD, Other s...
Analyze Risks: Security, License, Compliance...
Enrich, Augment
...s: VEX, VDR, MDS², EOL ...
Enriched SBOM
SBOM
SBOM
Secure Repo
Tailoring
Merge Multiple SBOMs
Consume SBOMs
Purchase/ Acquire
Query
Compare
Analyze Risks
External Interface: Legal, GRC, Vendor Mgt...
Discover
Disposition
Patch
Monitor
Alert
Pre and Post Deployment Vulnerability Monitoring

Why Do They Care? Sample use cases deriving benefits of SBOM management



Differences between software builds or versions

Licensing risks

Security risks from component vulnerabilities

Policy compliance

Critical component usage

Pre-purchase security, licensing, compliance risk assessment

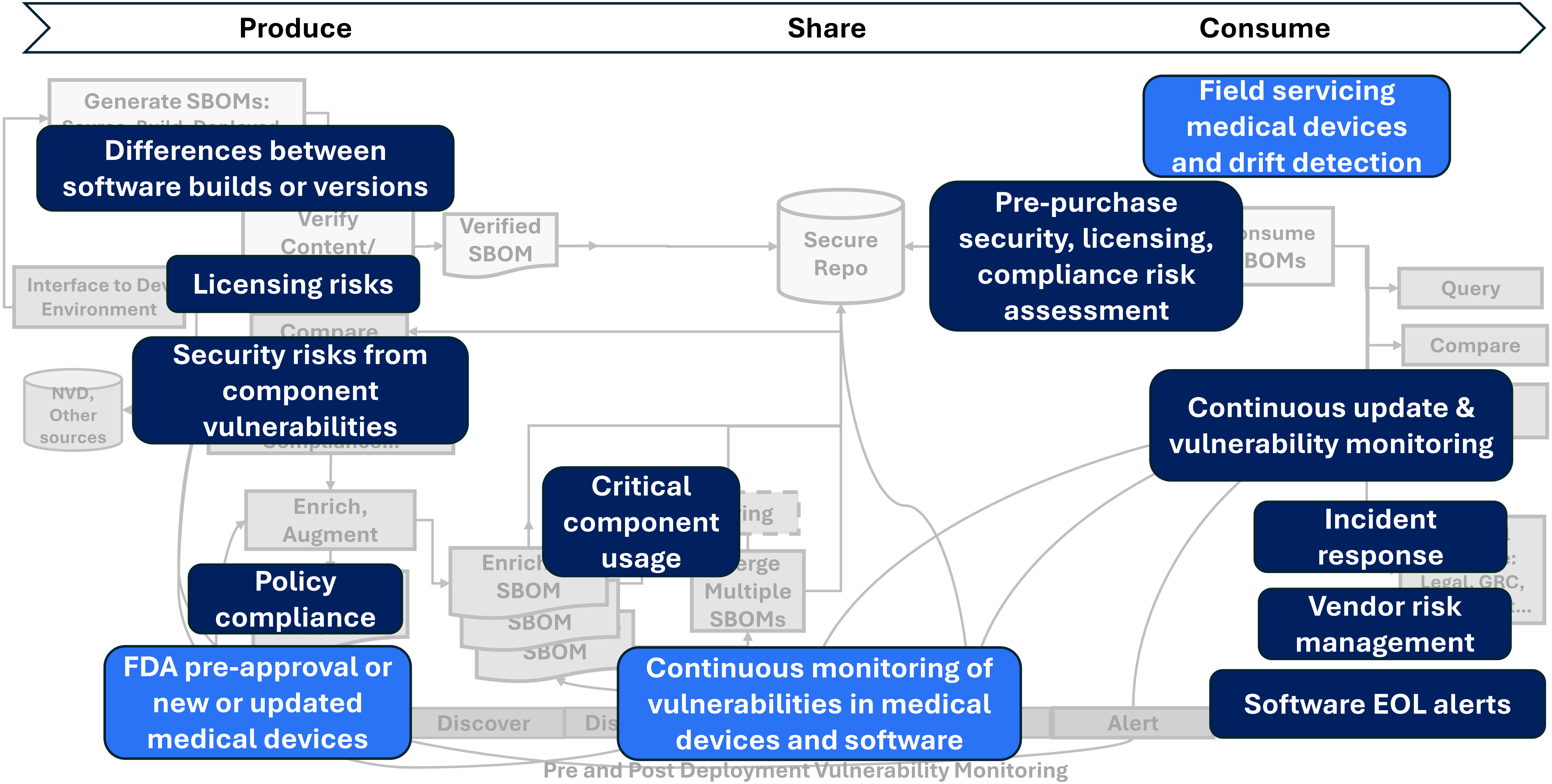
Continuous update & vulnerability monitoring

Software EOL alerts

Incident response

Vendor risk management

Why Do Medical Technology and Healthcare Care? Sample use cases



Differences between software builds or versions

Licensing risks

Security risks from component vulnerabilities

Policy compliance

FDA pre-approval or new or updated medical devices

Critical component usage

Continuous monitoring of vulnerabilities in medical devices and software

Pre-purchase security, licensing, compliance risk assessment

Field servicing medical devices and drift detection

Continuous update & vulnerability monitoring

Incident response

Vendor risk management

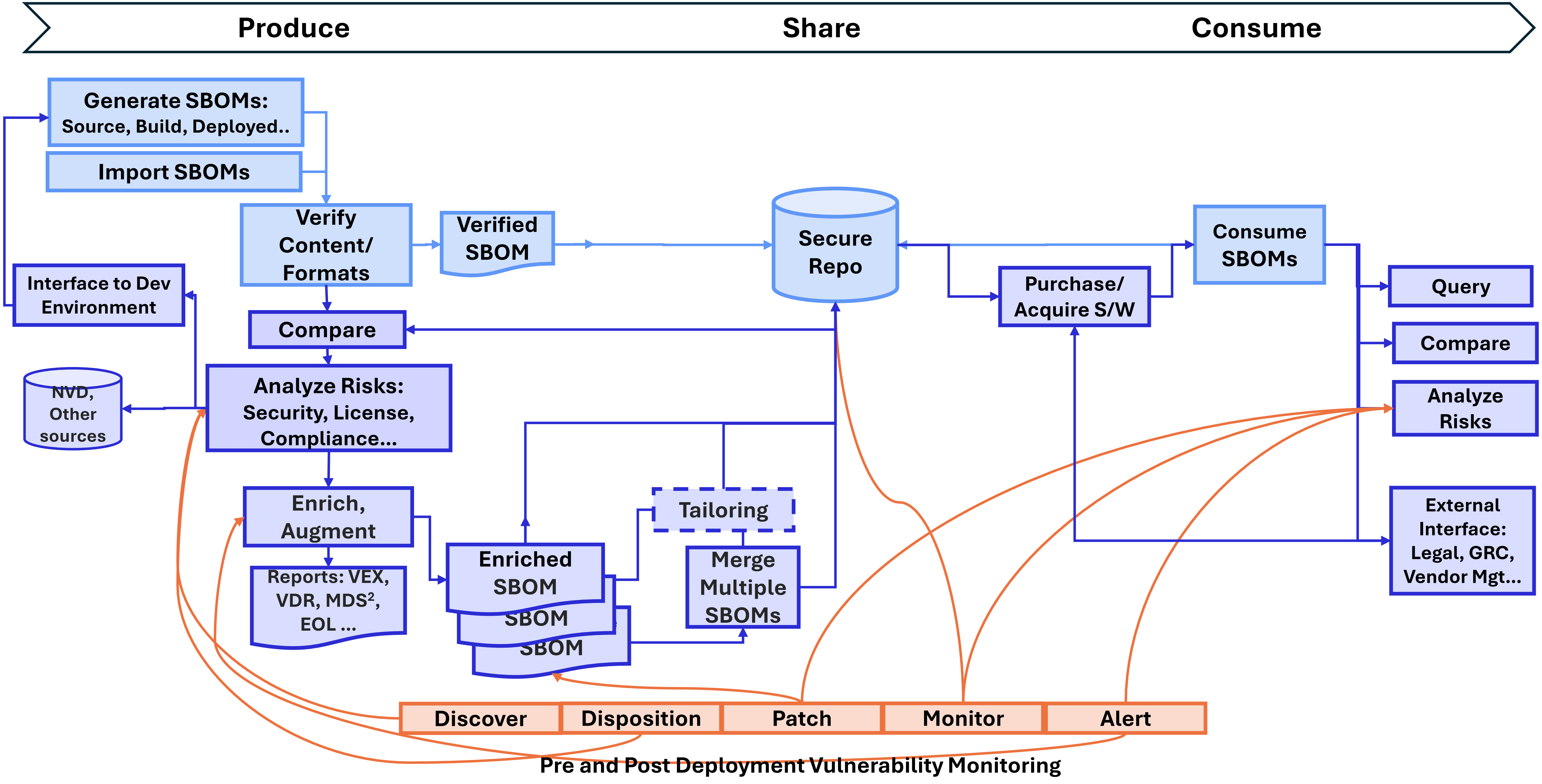
Software EOL alerts

SBOM Management/Operations

Essential SBOM Management

Advanced SBOM Operations

Vulnerability Monitoring/ Management



Produce

Share

Consume

Generate SBOMs: Source, Build, Deployed..

Import SBOMs

Verify Content/ Formats

Verified SBOM

Interface to Dev Environment

Compare

Analyze Risks: Security, License, Compliance…

NVD, Other sources

Enrich, Augment

Reports: VEX, VDR, MDS², EOL …

Enriched SBOM

SBOM

SBOM

Tailoring

Merge Multiple SBOMs

Secure Repo

Purchase/ Acquire S/W

Consume SBOMs

Query

Compare

Analyze Risks

External Interface: Legal, GRC, Vendor Mgt…

Discover

Disposition

Patch

Monitor

Alert

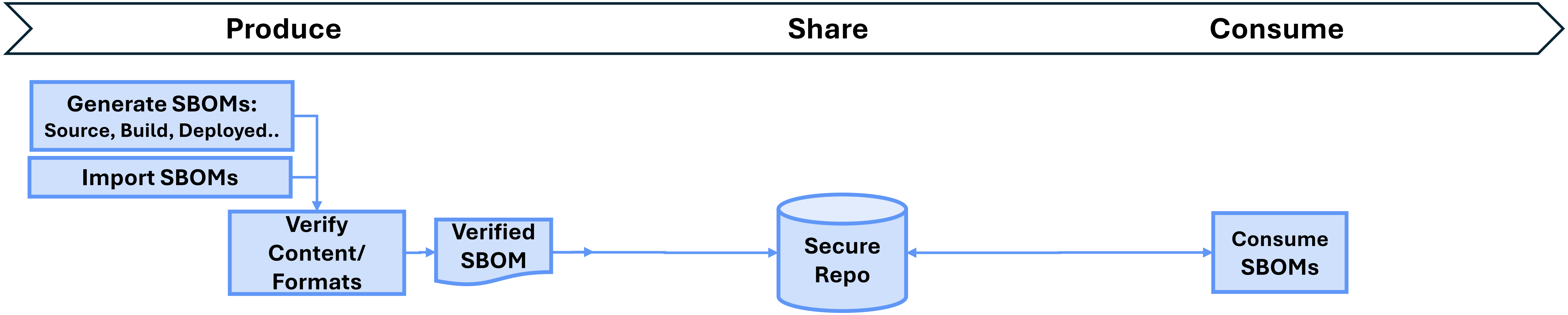
Pre and Post Deployment Vulnerability Monitoring

Essential SBOM Management

Basic Functions for Production, Dissemination and Consumption of SBOMs

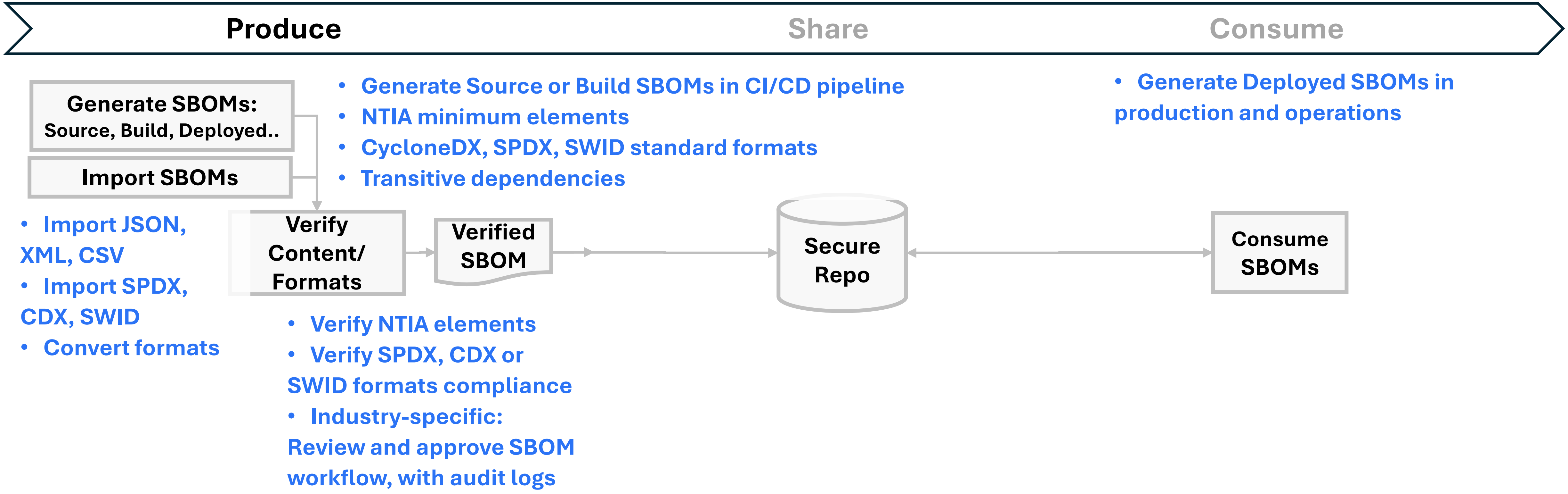
SBOM Management/Operations

Essential SBOM Management



Typical Requirements

Essential SBOM Management



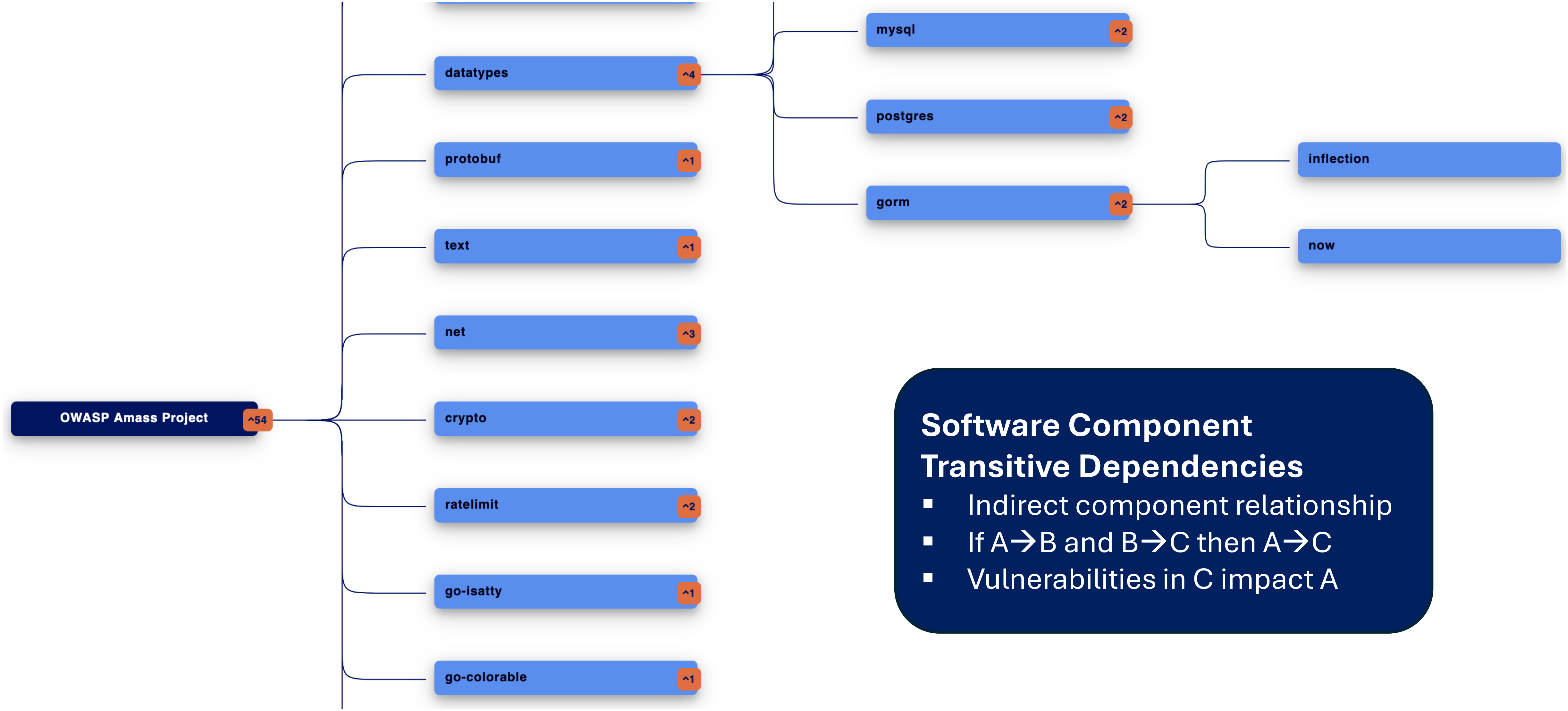
- Generate Source or Build SBOMs in CI/CD pipeline
- NTIA minimum elements
- CycloneDX, SPDX, SWID standard formats
- Transitive dependencies

- Import JSON, XML, CSV
- Import SPDX, CDX, SWID
- Convert formats

- Verify NTIA elements
- Verify SPDX, CDX or SWID formats compliance
- Industry-specific: Review and approve SBOM workflow, with audit logs

- Generate Deployed SBOMs in production and operations

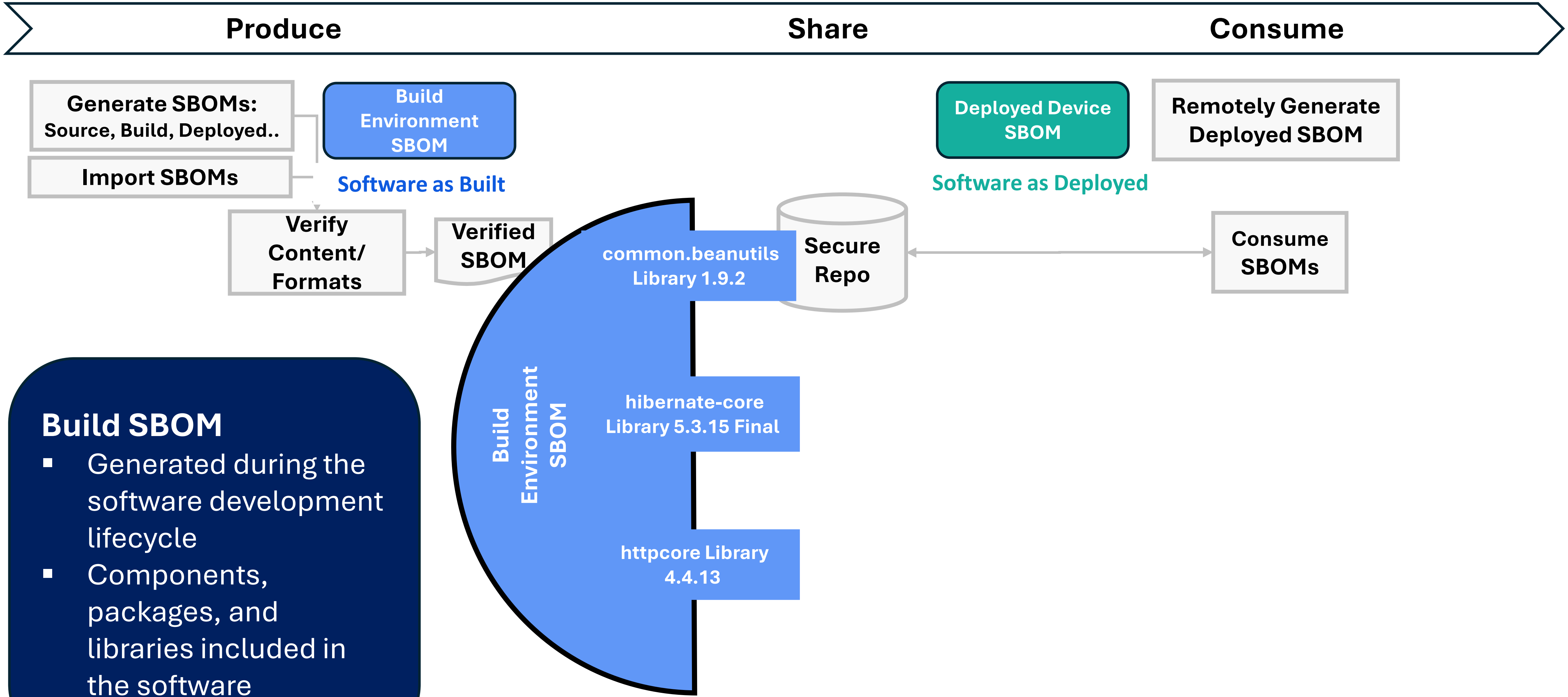
Transitive Dependencies



Software Component Transitive Dependencies

- Indirect component relationship
- If A→B and B→C then A→C
- Vulnerabilities in C impact A

Difference between Build and Deployed SBOMs



Produce

Share

Consume

Generate SBOMs:
Source, Build, Deployed..

Import SBOMs

Build Environment SBOM

Software as Built

Verify Content/ Formats

Verified SBOM

Build Environment SBOM

common.beanutils Library 1.9.2

hibernate-core Library 5.3.15 Final

httpcore Library 4.4.13

Secure Repo

Deployed Device SBOM

Software as Deployed

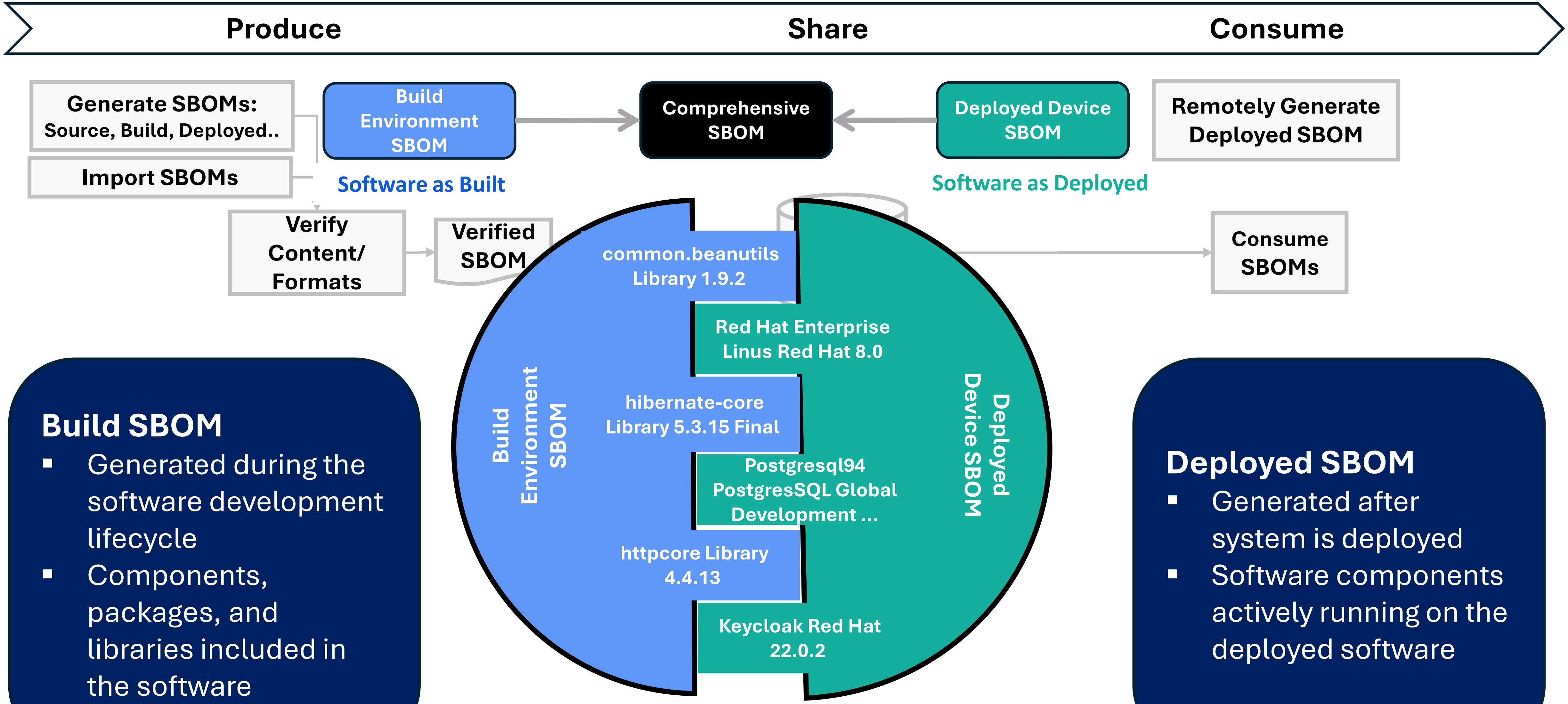
Remotely Generate Deployed SBOM

Consume SBOMs

Build SBOM

- Generated during the software development lifecycle
- Components, packages, and libraries included in the software

Difference between Build and Deployed SBOMs



Produce

Share

Consume

Generate SBOMs: Source, Build, Deployed..

Import SBOMs

Build Environment SBOM

Software as Built

Comprehensive SBOM

Deployed Device SBOM

Software as Deployed

Remotely Generate Deployed SBOM

Verify Content/ Formats

Verified SBOM

Consume SBOMs

Build Environment SBOM

Deployed Device SBOM

common.beanutils Library 1.9.2

Red Hat Enterprise Linus Red Hat 8.0

hibernate-core Library 5.3.15 Final

Postgresql94 PostgresSQL Global Development ...

httpcore Library 4.4.13

Keycloak Red Hat 22.0.2

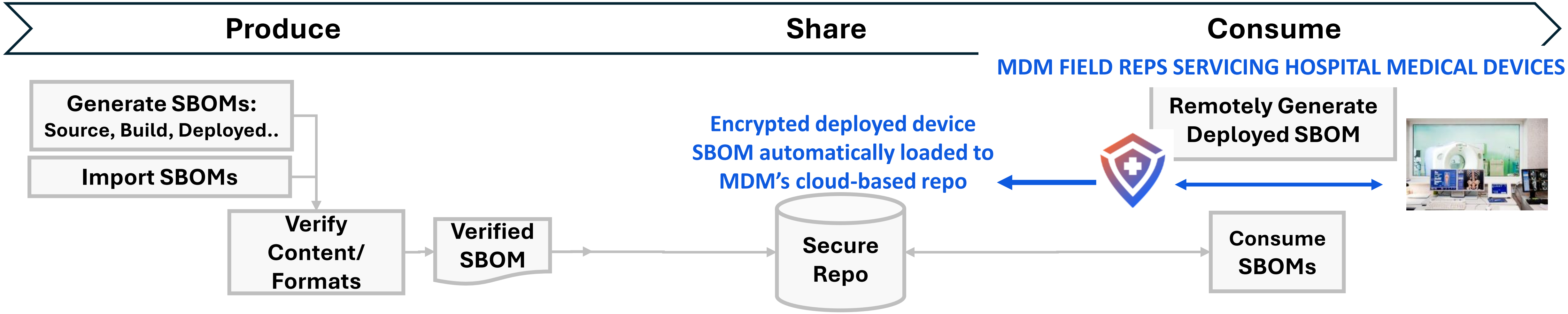
Build SBOM

- Generated during the software development lifecycle
- Components, packages, and libraries included in the software

Deployed SBOM

- Generated after system is deployed
- Software components actively running on the deployed software

Medical Device Manufacturer (MDM) Use Case for Build + Deployed SBOMs



Encrypted deployed device SBOM automatically loaded to MDM's cloud-based repo

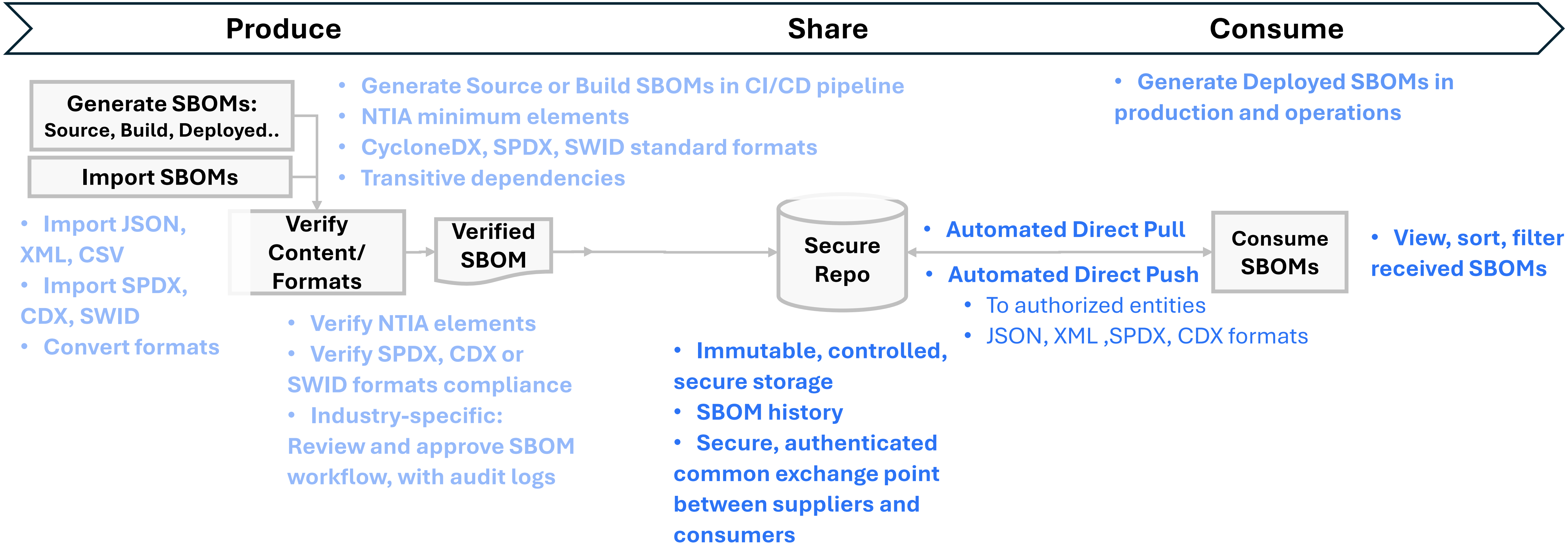
Repo updated with *Comprehensive* SBOM

BENEFITS

- Accurate device profile
- Targeted patching
- History of device updates
- Real-time system comparison to pinpoint *drift* between built and deployed device

Typical Requirements

Essential SBOM Management



Produce

Share

Consume

Generate SBOMs:
Source, Build, Deployed..

- Generate Source or Build SBOMs in CI/CD pipeline
- NTIA minimum elements
- CycloneDX, SPDX, SWID standard formats
- Transitive dependencies

Import SBOMs

- Import JSON, XML, CSV
- Import SPDX, CDX, SWID
- Convert formats

Verify Content/ Formats

- Verify NTIA elements
- Verify SPDX, CDX or SWID formats compliance
- Industry-specific: Review and approve SBOM workflow, with audit logs

Verified SBOM

Secure Repo

- Immutable, controlled, secure storage
- SBOM history
- Secure, authenticated common exchange point between suppliers and consumers

- Automated Direct Pull
- Automated Direct Push
  - To authorized entities
  - JSON, XML ,SPDX, CDX formats

Consume SBOMs

- View, sort, filter received SBOMs

- Generate Deployed SBOMs in production and operations

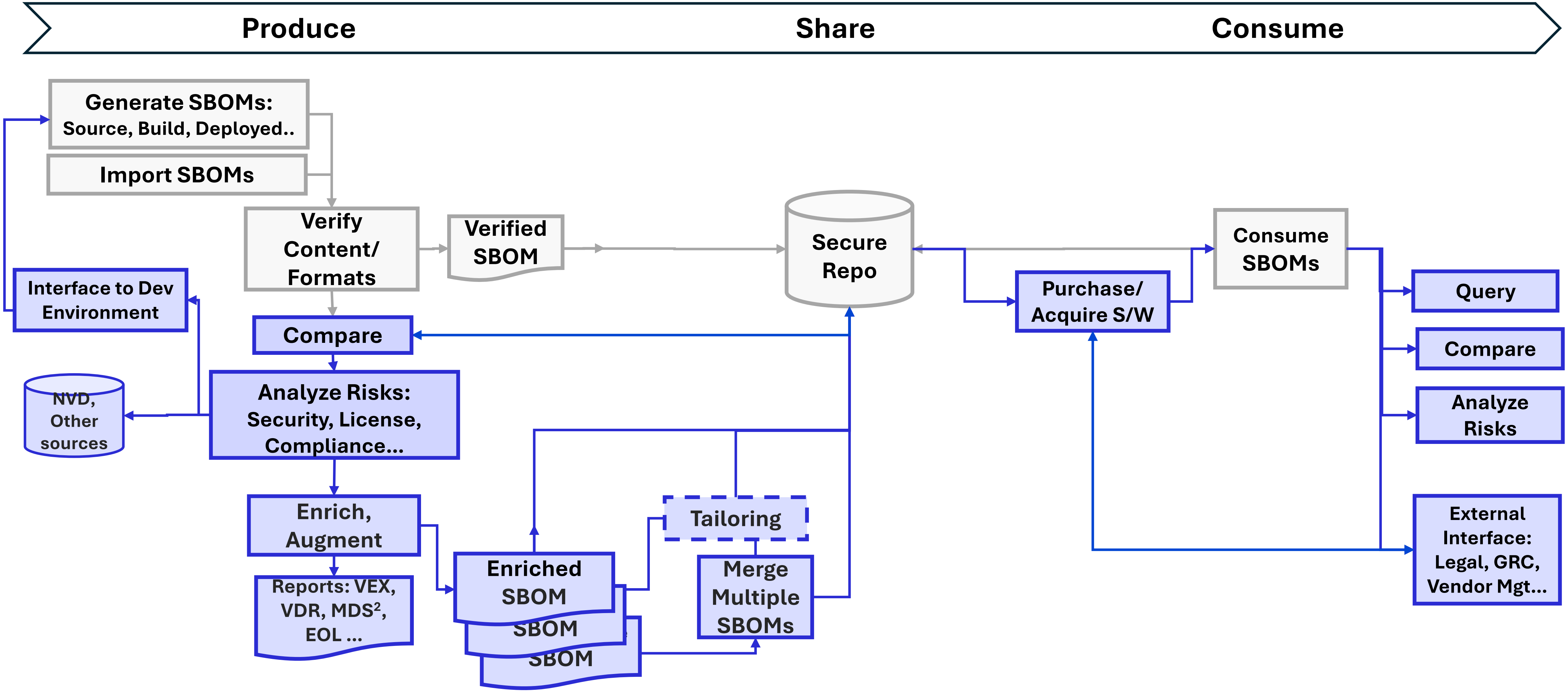
Advanced SBOM Operations

What Organizations Do To SBOMs to Increase Their Value

SBOM Management/Operations

Essential SBOM Management

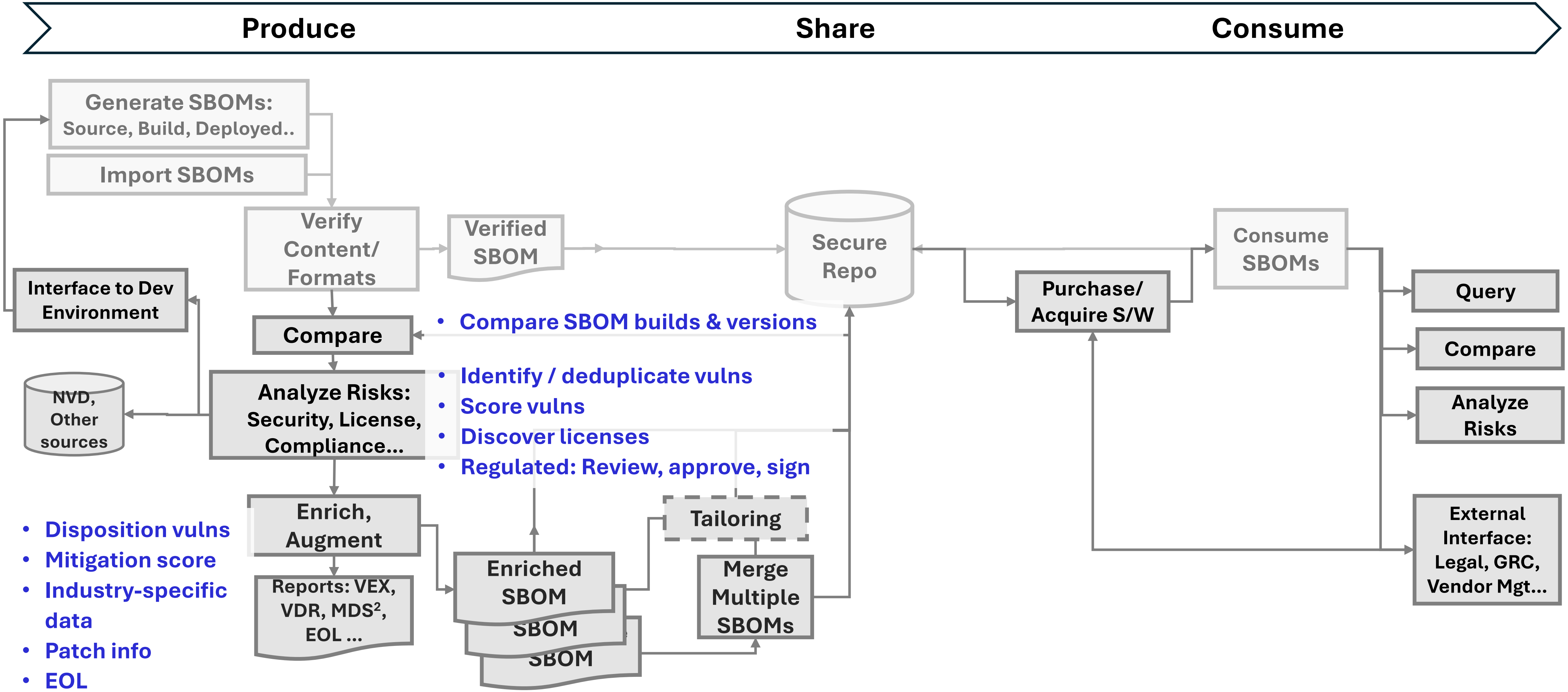
Advanced SBOM Operations



Typical Requirements

Essential SBOM Management

Advanced SBOM Operations



- Compare SBOM builds & versions

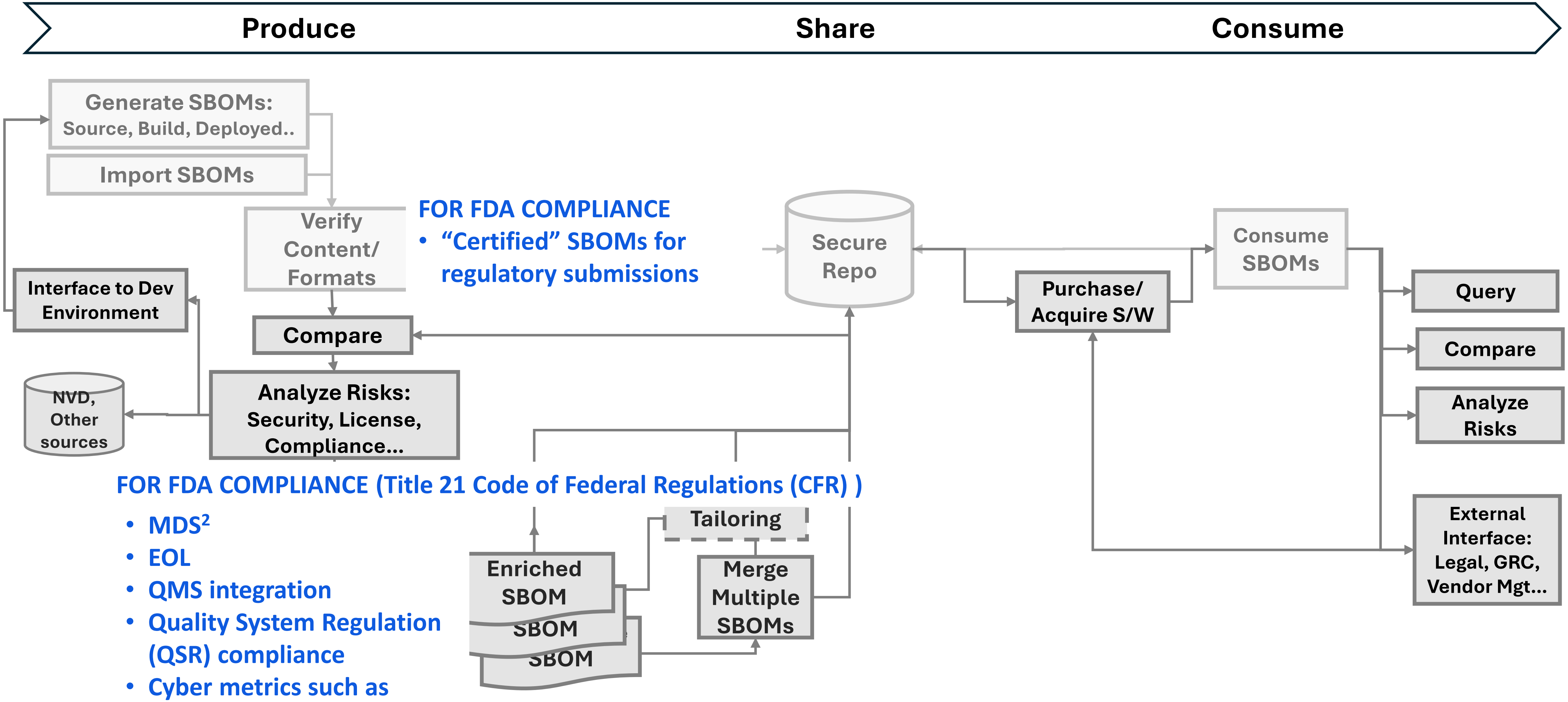
- Identify / deduplicate vulns
- Score vulns
- Discover licenses
- Regulated: Review, approve, sign

- Disposition vulns
- Mitigation score
- Industry-specific data
- Patch info
- EOL
- Custom notes

- Custom Reports
- Regulated: Compliance reporting

- Enriched SBOM incorporates supplemental data and documents

Product Documentation Required to Supplement SBOMs of Medical Device Software



Produce

Share

Consume

Generate SBOMs: Source, Build, Deployed..

Import SBOMs

Verify Content/ Formats

Interface to Dev Environment

Compare

Analyze Risks: Security, License, Compliance...

NVD, Other sources

FOR FDA COMPLIANCE

- “Certified” SBOMs for regulatory submissions

Secure Repo

Purchase/ Acquire S/W

Consume SBOMs

Query

Compare

Analyze Risks

External Interface: Legal, GRC, Vendor Mgt...

Enriched SBOM

SBOM

SBOM

Tailoring

Merge Multiple SBOMs

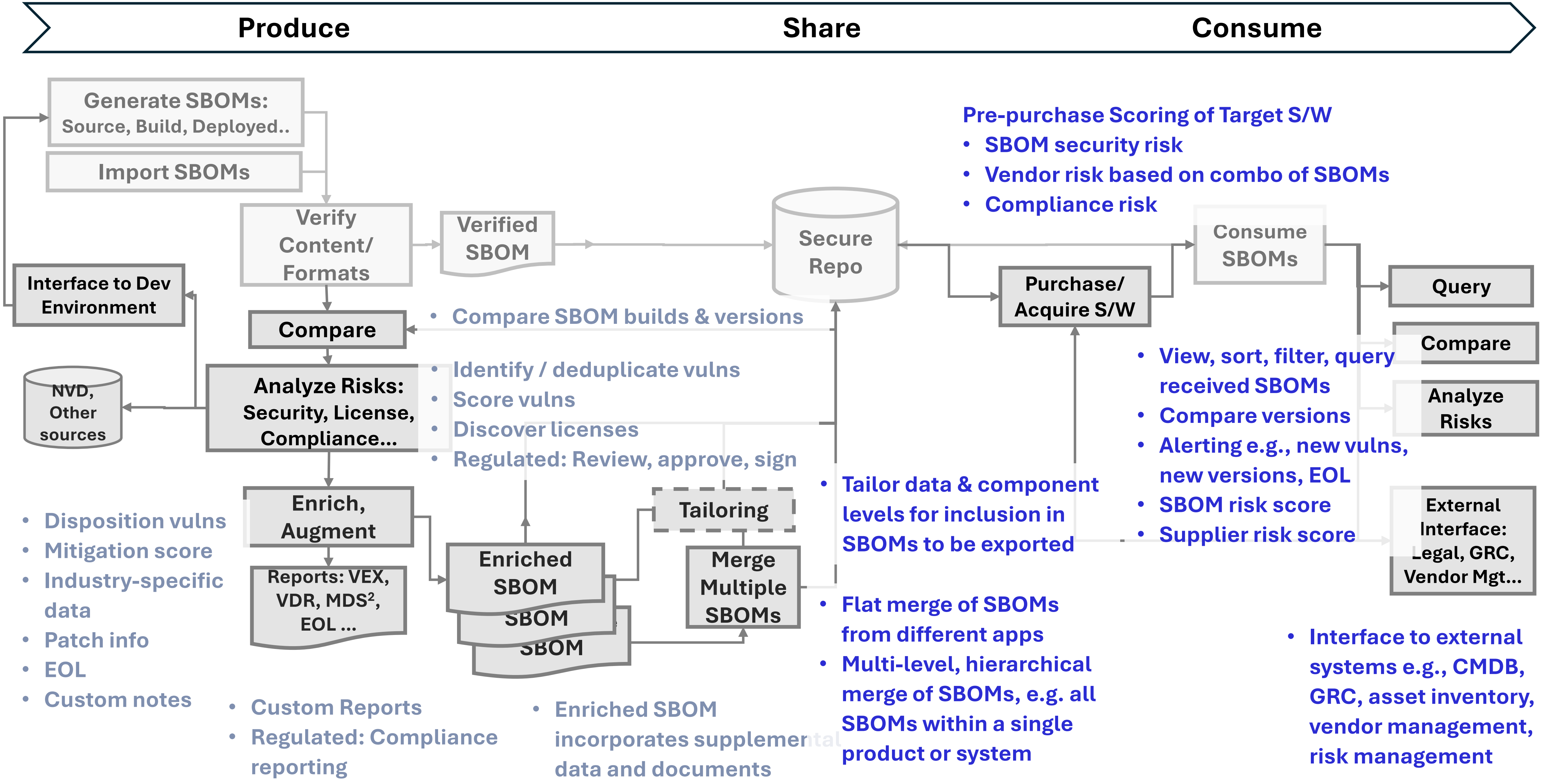
FOR FDA COMPLIANCE (Title 21 Code of Federal Regulations (CFR))

- MDS^2
- EOL
- QMS integration
- Quality System Regulation (QSR) compliance
- Cyber metrics such as patch ratio and patch velocity

Typical Requirements

Essential SBOM Management

Advanced SBOM Operations



Produce

Share

Consume

Generate SBOMs: Source, Build, Deployed..

Import SBOMs

Verify Content/ Formats

Verified SBOM

Secure Repo

Interface to Dev Environment

Compare

- Compare SBOM builds & versions

NVD, Other sources

Analyze Risks: Security, License, Compliance…

- Identify / deduplicate vulns
- Score vulns
- Discover licenses
- Regulated: Review, approve, sign

Enrich, Augment

- Disposition vulns
- Mitigation score
- Industry-specific data
- Patch info
- EOL
- Custom notes

Reports: VEX, VDR, MDS^2, EOL …

- Custom Reports
- Regulated: Compliance reporting

Enriched SBOM

SBOM

SBOM

- Enriched SBOM incorporates supplemental data and documents

Tailoring

Merge Multiple SBOMs

- Tailor data & component levels for inclusion in SBOMs to be exported

- Flat merge of SBOMs from different apps
- Multi-level, hierarchical merge of SBOMs, e.g. all SBOMs within a single product or system

Pre-purchase Scoring of Target S/W

- SBOM security risk
- Vendor risk based on combo of SBOMs
- Compliance risk

Purchase/ Acquire S/W

Consume SBOMs

Query

Compare

Analyze Risks

- View, sort, filter, query received SBOMs
- Compare versions
- Alerting e.g., new vulns, new versions, EOL
- SBOM risk score
- Supplier risk score

External Interface: Legal, GRC, Vendor Mgt…

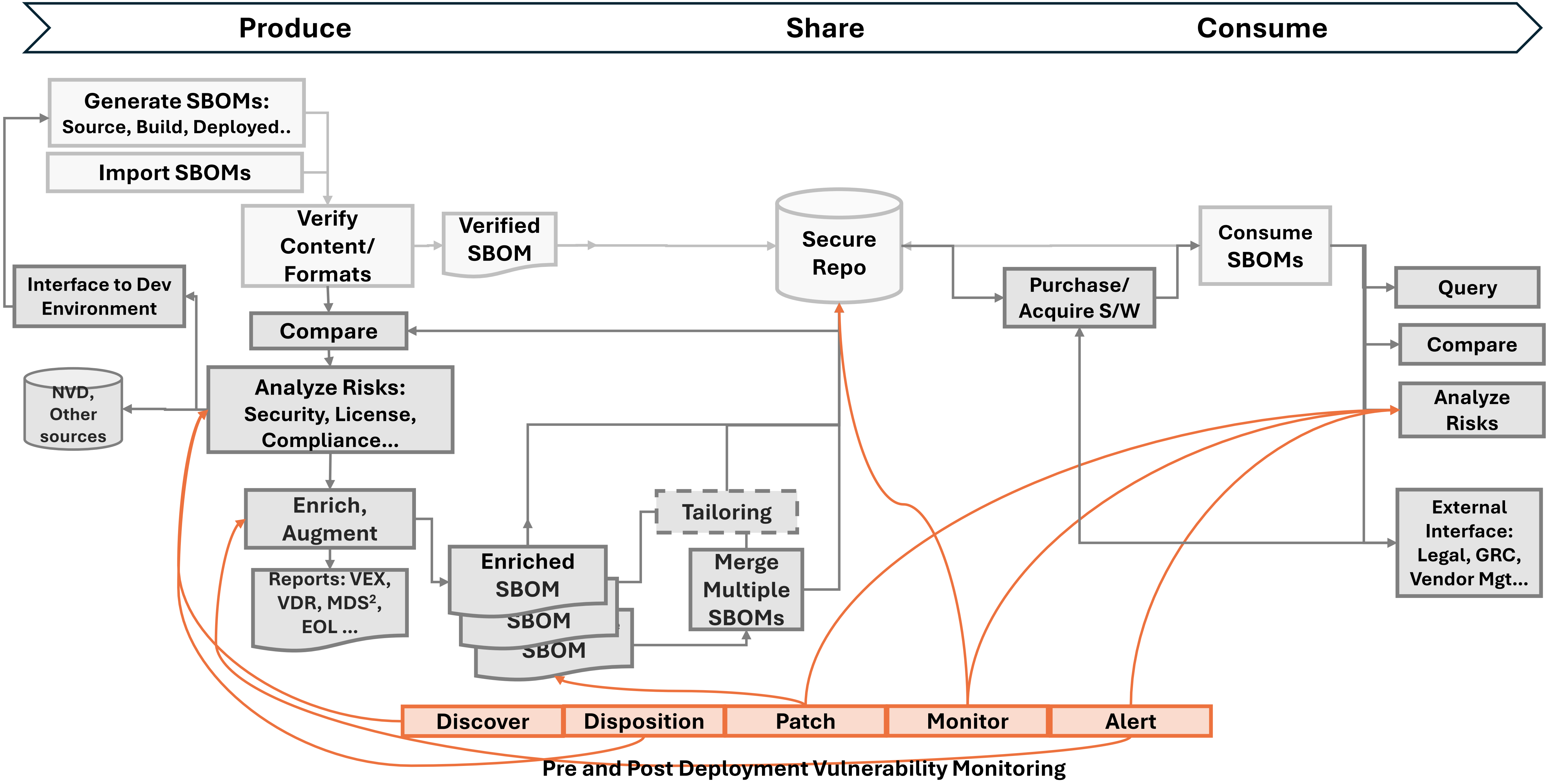
- Interface to external systems e.g., CMDB, GRC, asset inventory, vendor management, risk management

Typical Requirements

Essential SBOM Management

Advanced SBOM Operations

Vulnerability Monitoring/ Management



Produce

Share

Consume

Generate SBOMs: Source, Build, Deployed..

Import SBOMs

Interface to Dev Environment

Verify Content/ Formats

Verified SBOM

Secure Repo

Consume SBOMs

Purchase/ Acquire S/W

Query

Compare

Compare

Analyze Risks

NVD, Other sources

Analyze Risks: Security, License, Compliance…

Enrich, Augment

Reports: VEX, VDR, MDS[2], EOL …

Enriched SBOM

SBOM

SBOM

Tailoring

Merge Multiple SBOMs

External Interface: Legal, GRC, Vendor Mgt…

Discover

Disposition

Patch

Monitor

Alert

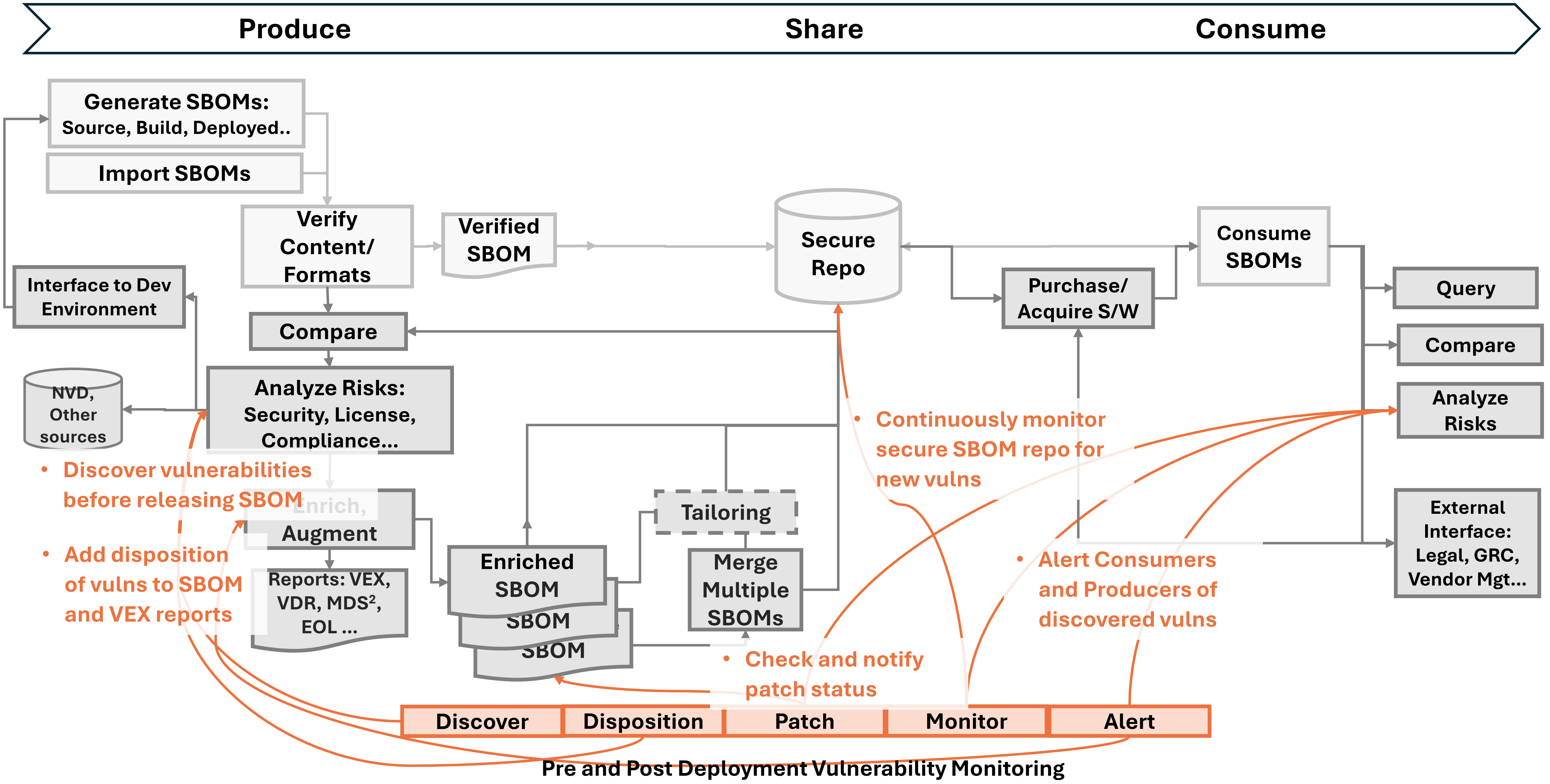
Pre and Post Deployment Vulnerability Monitoring

Typical Requirements

Essential SBOM Management

Advanced SBOM Operations

Vulnerability Monitoring/ Management



Produce

Share

Consume

Generate SBOMs: Source, Build, Deployed..

Import SBOMs

Verify Content/ Formats

Verified SBOM

Secure Repo

Consume SBOMs

Interface to Dev Environment

Compare

Purchase/ Acquire S/W

Query

Compare

NVD, Other sources

Analyze Risks: Security, License, Compliance…

Analyze Risks

- Discover vulnerabilities before releasing SBOM

Enrich, Augment

- Continuously monitor secure SBOM repo for new vulns

Tailoring

External Interface: Legal, GRC, Vendor Mgt…

- Add disposition of vulns to SBOM and VEX reports

Enriched SBOM

SBOM

SBOM

Reports: VEX, VDR, MDS², EOL …

Merge Multiple SBOMs

- Alert Consumers and Producers of discovered vulns

- Check and notify patch status

Discover

Disposition

Patch

Monitor

Alert

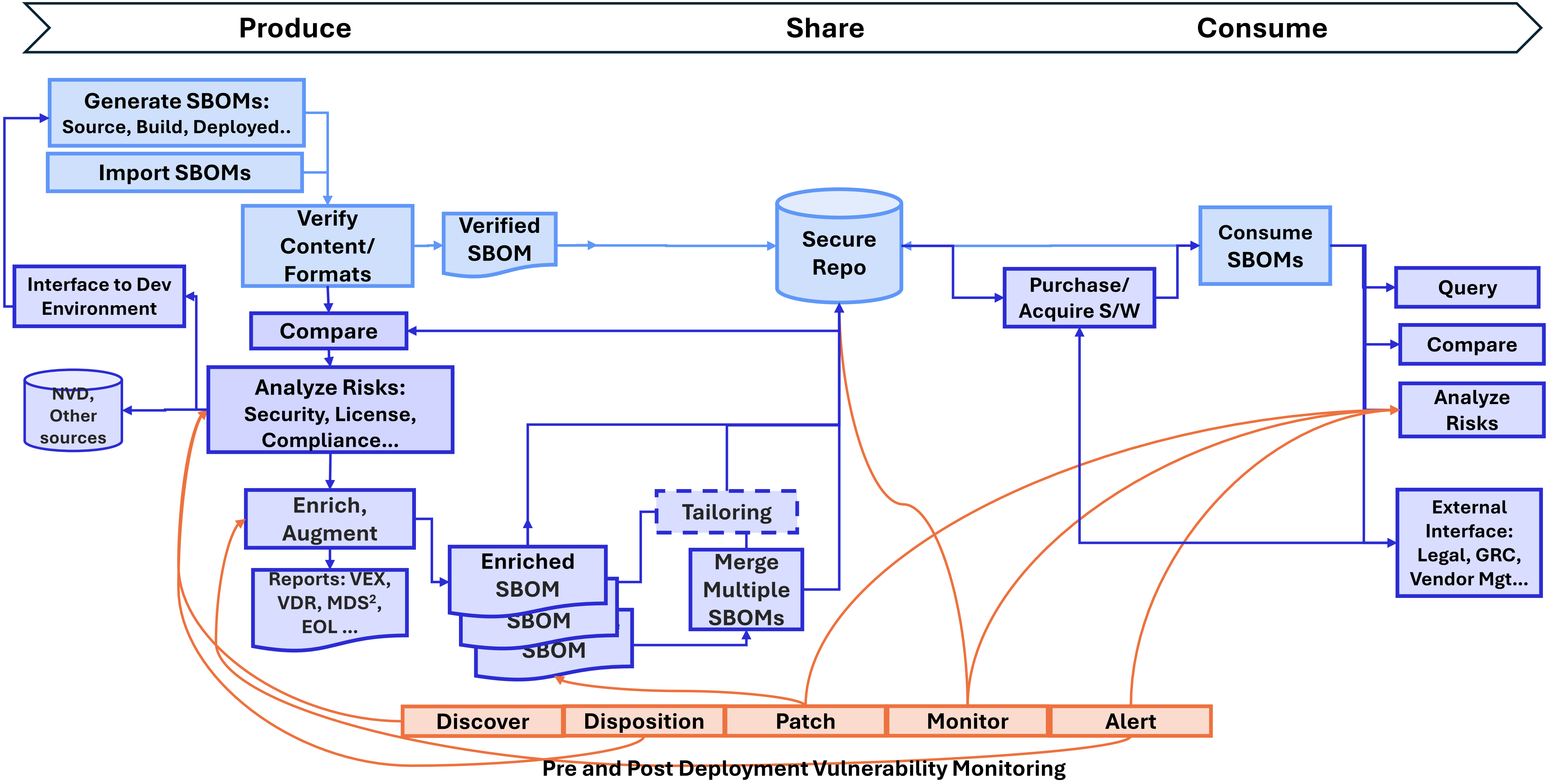
Pre and Post Deployment Vulnerability Monitoring

SBOM Management/Operations

Essential SBOM Management

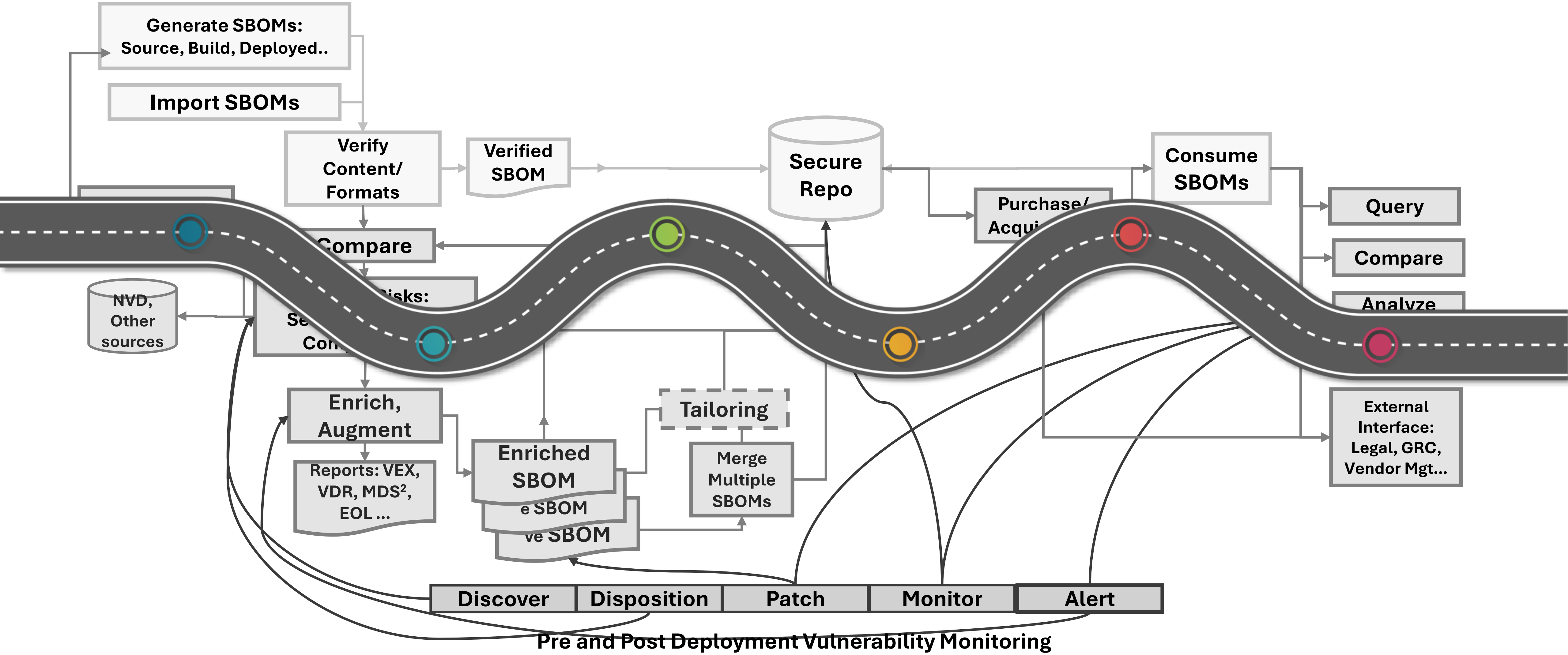
Advanced SBOM Operations

Vulnerability Monitoring/ Management



SBOM Management and Operations Is a Journey:

Each organization is at a different place based on their needs



PRESENTERS

Anita D’Amico, Ph.D.
President, Cotopaxi Consulting LLC
Board Member, Vigilant Ops
anitacodedx@gmail.com
https://www.linkedin.com/in/anita-damico/
www.cotopaxiconsulting.com

Ken Zalevsky
CEO, Vigilant Ops

ken.zalevsky@vigilant-ops.com
https://www.linkedin.com/in/ken-zalevsky/
www.vigilant-ops.com

References

- Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions
- Executive Order on Improving the Nation's Cybersecurity https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
- The Minimum Elements for a Software Bill of Materials (SBOM). Published by US Dept of Commerce and National Telecommunications and Information Administration (NTIA). July 2021. https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf
- NTIA Multistakeholder Process on Software Component Transparency | ntia.gov/sbom SBOM Options and Decision Points, sbom_options_and_decision_points_20210427-1_0.pdf (ntia.gov)
- NTIA (2021) "Sharing and Exchanging SBOMs," National Telecommunications and Information Administration, February 2021, https://ntia.gov/files/ntia/publications/ntia_sbom_sharing_exchanging_sboms-10feb2021.pdf
- Recommendations for Software Bill of Materials (SBOM) Management. Published by NSA. December 2023. CSI-SCRM-SBOM-MANAGEMENT.PDF (defense.gov)
- SBOM Tool Classification Taxonomy NTIA SBOM Formats & Tooling Working Group – March 30, 2021. ntia_sbom_tooling_taxonomy-2021mar30_0.pdf
- Software Bill of Materials (SBOM) Sharing Lifecycle Report. Issued by CISA and US DoE. April 2023 Software Bill of Materials (SBOM) Sharing Lifecycle Report | CISA
- Types of Software Bill of Material (SBOM) Documents, published by CISA, 2023. https://www.cisa.gov/sites/default/files/2023-04/sbom-types-document-508c.pdf