

A Practical Guide for Unlocking Business Value from Your SBOMs

Developed by the SBOMOps Working Group
of the CISA SBOM Community

Reference to Anita et. al.
presentation at SSCA
Forum

Presentation

Improving Risk Management Decisions with SBOM Data

May 13, 2025



PRESENTERS

Tim Mackey - Black Duck

Anita D'Amico - Cotopaxi Consulting

Ken Zalevsky - Vigilant Ops

DESCRIPTION

This presentation illustrated SBOM lifecycle management and use cases, essentially the insights resulting from the SBOMOps working group. These results highlight the utility of SBOMs for both SBOM producers and consumers.

DOWNLOADS

[Risk Management with SBOM Data](#) (PDF)

<https://csrc.nist.gov/Presentations/2025/improving-risk-management-decisions-with-sbom-data>

Who am I?

04/2017 - 09/2023 □ **Incident handler** at Siemens Product Computer Emergency Response Team (ProductCERT) and Lead Engineer for **Cyber Threat Intelligence for Products**

09/2023 – Present □ Senior Key Expert Vulnerability Management OT technologies @ **Siemens Research**

- Maintain partnerships with various universities and research institutions
- **Represent Siemens** in various public technical working groups and external communities



UNIVERSIDADE FEDERAL
DO RIO DE JANEIRO



TF-CSIRT
Trusted Introducer



Charter
of Trust
charter-of-trust.com

Motivation

- Explore the downstream lifecycle and
- Practical applications of SBOMs across
 - software production,
 - distribution, and
 - consumption phases.



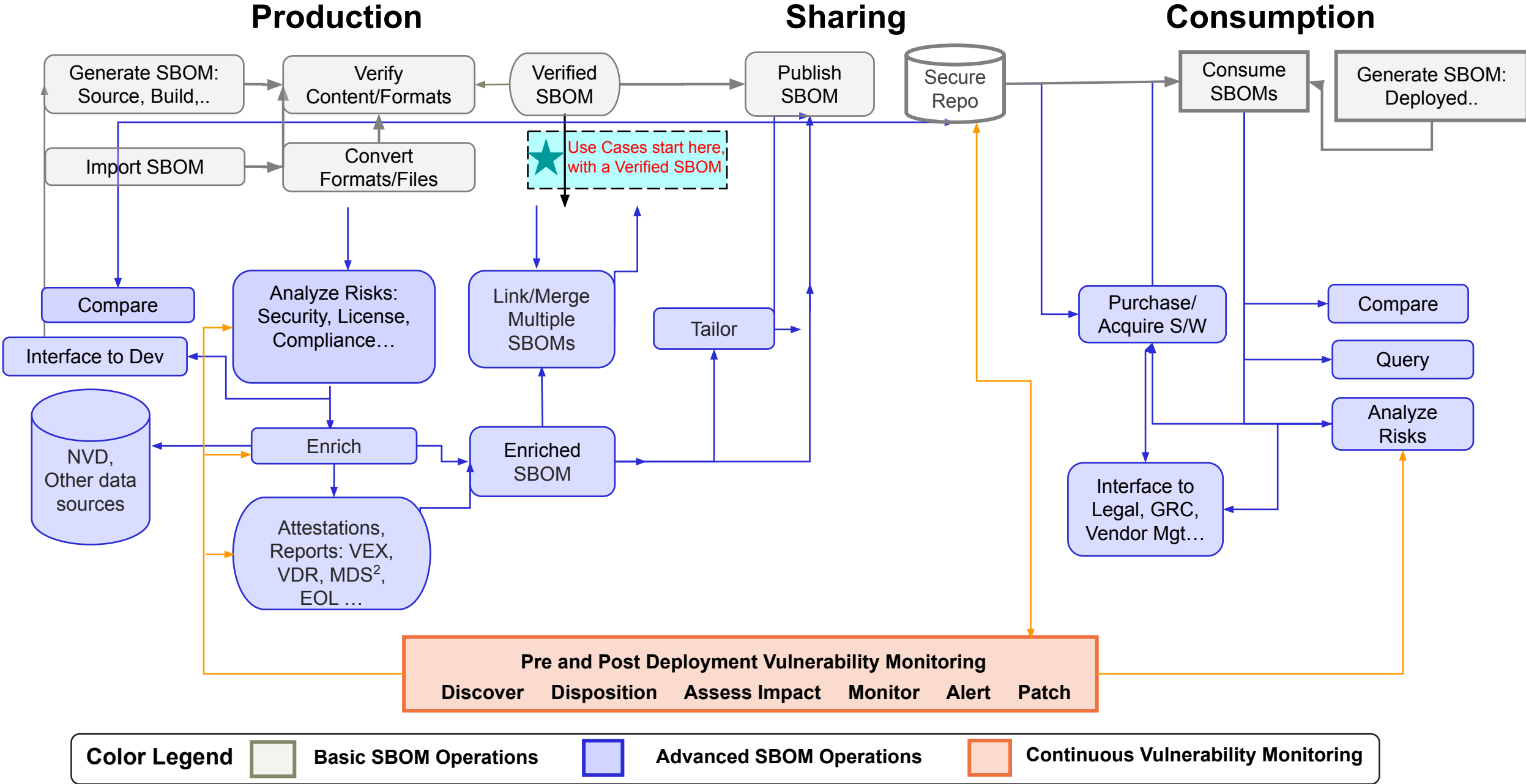
Improving Risk Management Decisions with SBOM Data

September 18, 2025

Improving Risk Management Decisions with SBOM Data

https://openssf.org/wp-content/uploads/2025/09/Improving_Risk_Management_Decisions_with_SBOM_Data.pdf

The SBOM Lifecycle



Production

- Generate SBOM: Source, Build,..
- Import SBOM
- Verify Content/Formats
- Convert Formats/Files
- Verified SBOM
- Analyze Risks: Security, License, Compliance...
- Compare
- Interface to Dev
- NVD, Other data sources
- Enrich
- Attestations, Reports: VEX, VDR, MDS², EOL ...
- Link/Merge Multiple SBOMs
- Enriched SBOM

Sharing

- Publish SBOM
- Secure Repo
- Tailor

Consumption

- Consume SBOMs
- Generate SBOM: Deployed..
- Purchase/Acquire S/W
- Interface to Legal, GRC, Vendor Mgt...
- Analyze Risks
- Compare
- Query

Pre and Post Deployment Vulnerability Monitoring

Discover Disposition Assess Impact Monitor Alert Patch

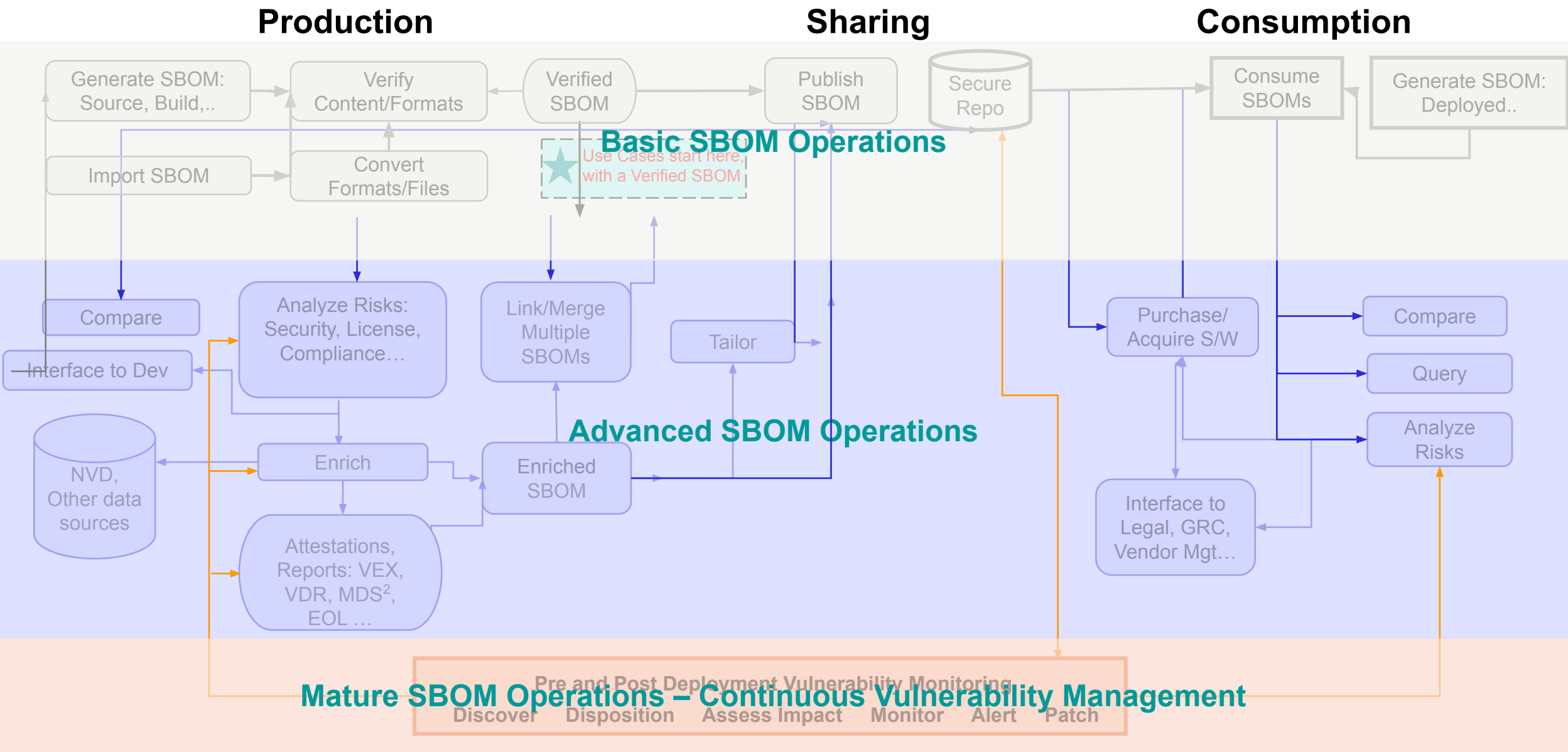
Color Legend Basic SBOM Operations Advanced SBOM Operations Continuous Vulnerability Monitoring

Color Legend Basic SBOM Operations Advanced SBOM Operations Continuous Vulnerability Monitoring

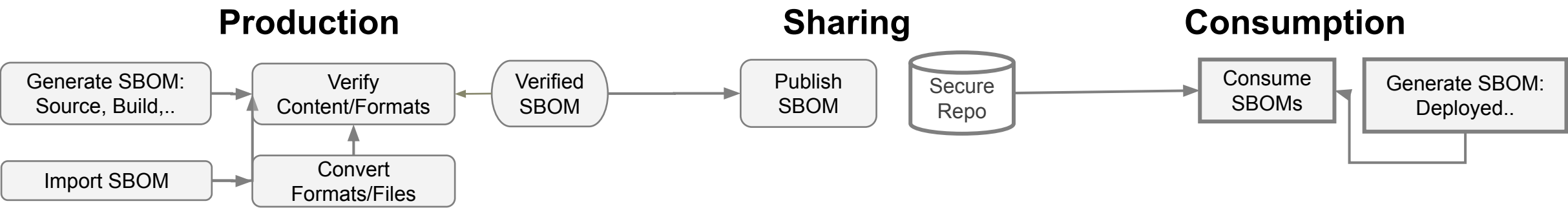
Color Legend Basic SBOM Operations Advanced SBOM Operations Continuous Vulnerability Monitoring

Color Legend Basic SBOM Operations Advanced SBOM Operations Continuous Vulnerability Monitoring

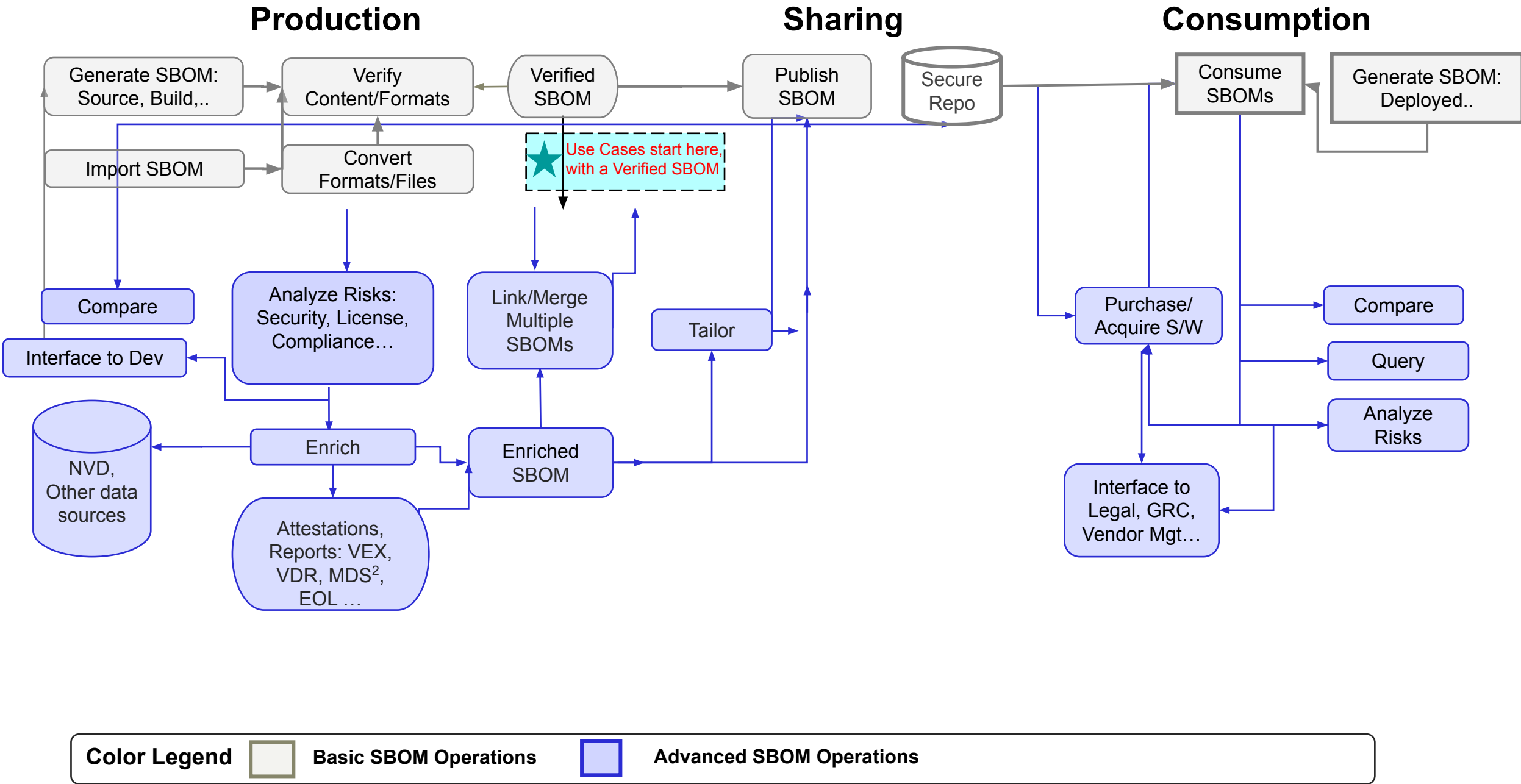
The SBOM Lifecycle: 3 Levels of Maturity



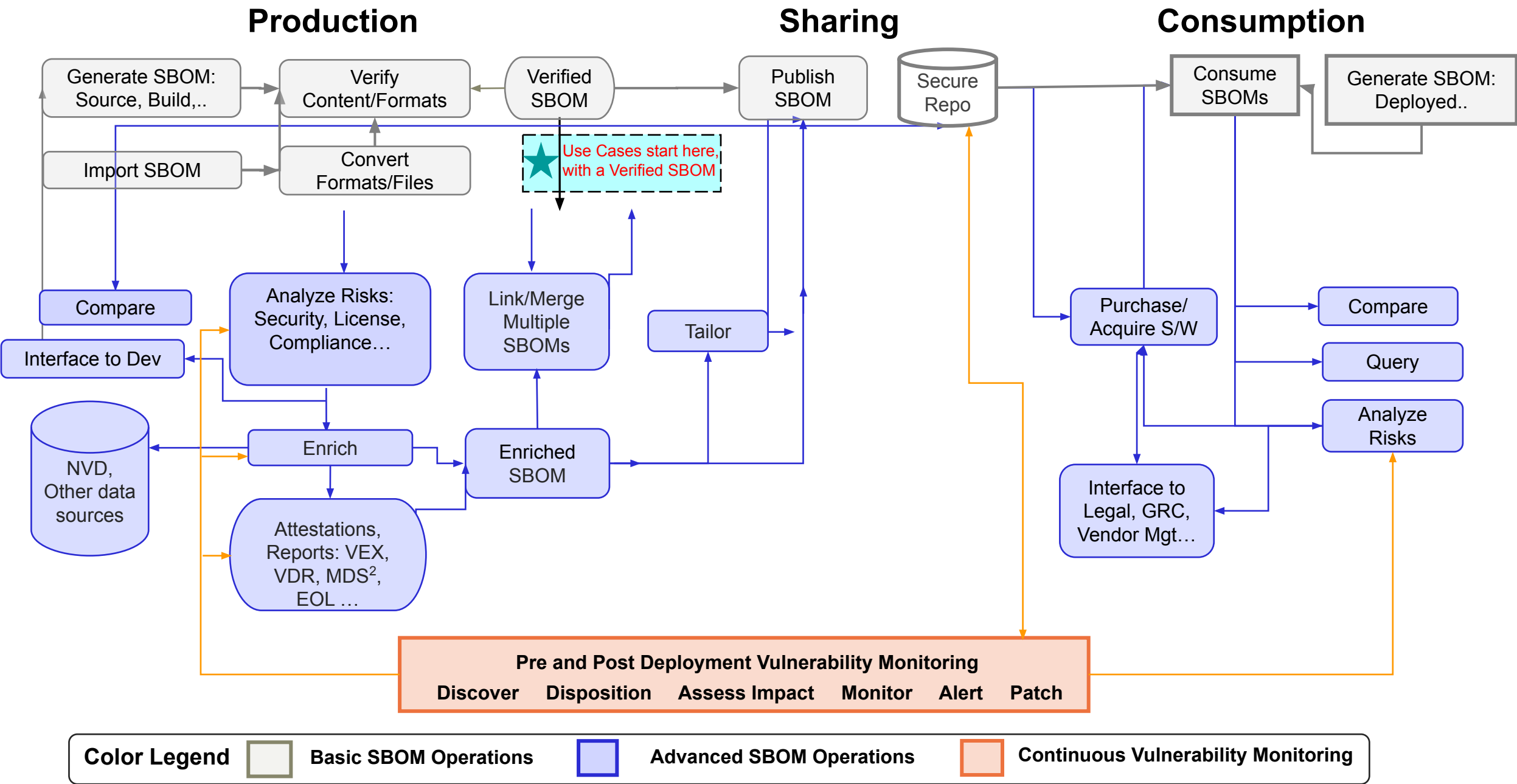
Basic SBOM Operations



Advanced SBOM Operations

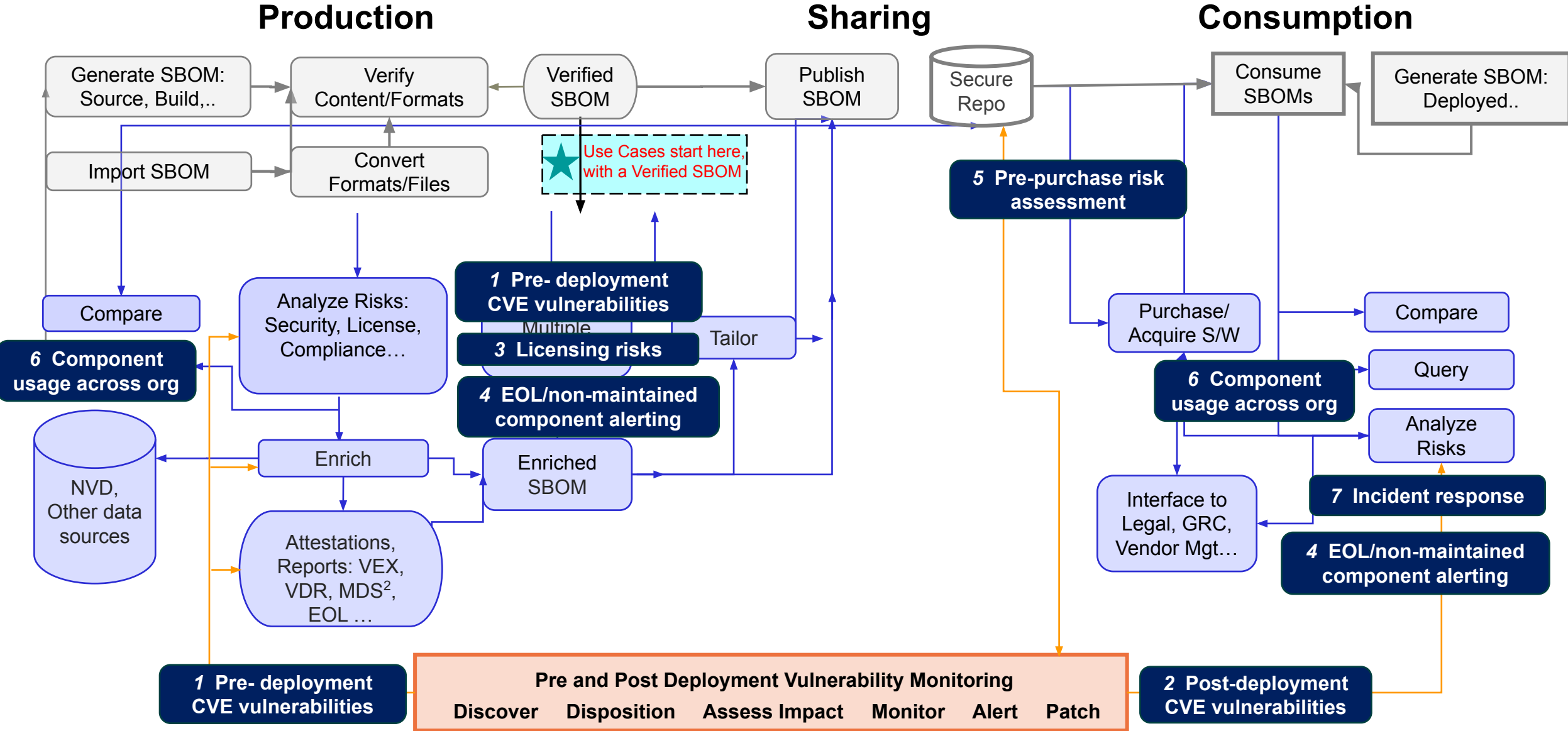


Mature Operations – Continuous Monitoring

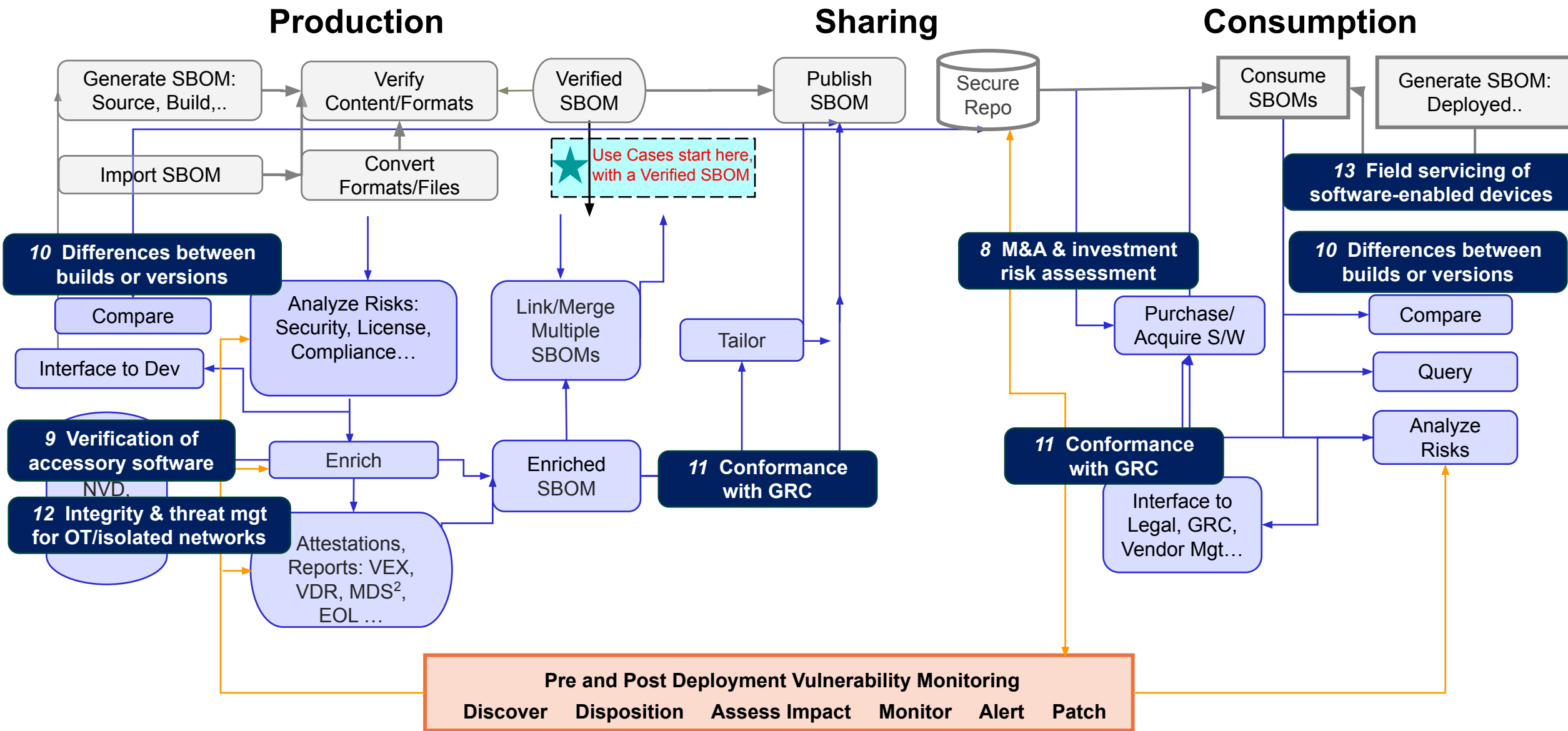


Use Cases that Illustrate Insights and Value Gained from SBOM

Use Cases Cover the Entire SBOM Lifecycle



Use Cases Cover the Entire SBOM Lifecycle



Use Cases Grouped by Maturity/Applicability and Stakeholder Role

Use Case #	Maturity/Applicability	Role	
	Most Mature / Broadest Applicability	Produce	Consume
1	Pre-Deployment CVE Vulnerabilities	✗	
2	Post-Deployment CVE Vulnerabilities		✗
3	Licensing Risks	✗	✗
4	EOL and Non-maintained Component Alerting	✗	✗
5	Pre-purchase Risk Assessment		✗
6	Component Usage Across an Organization	✗	✗
	Moderately Mature / Moderate Applicability		
7	Incident Response		✗
8	M&A and Investment Risk Assessment		✗
9	Verification of Accessory Software		✗
10	Differences in Components Between Build or Versions	✗	✗
	Least Mature / Focused Applicability		
11	Conformance with Disparate GRC Specifications	✗	✗
12	Integrity and Threat Management for OT and isolated networks	✗	
13	Field Servicing of Software-enabled Devices	✗	✗

NTIA Minimum Elements Used by Use Case

Use Cases	NTIA Fields Used						
	Supplier	Component	Version	Other Unique Identifiers	Dependency Relationship	Author	Timestamp
Pre-Deployment CVE Vulnerabilities	X	X	X	X	X		
Post-Deployment CVE Vulnerabilities	X	X	X	X	X		
Licensing Risks	X	X	X	X	X		
EOL and Non-maintained Component Alerting	X	X	X		X		X
Pre-purchase Risk Assessment	X	X	X	X	X	X	X
Component Usage Across an Organization	X	X	X	X	X		
Incident Response	X	X	X	X		X	X
M&A and Investment Risk Assessment	X	X	X	X	X	X	X
Verification of Accessory Software	X	X	X	X	X	X	X
Differences in Components Between Build or Versions	X	X	X	X	X	X	X
Conformance with Disparate GRC Specifications	X	X	X	X		X	
Integrity and Threat Management for OT and isolated networks	X	X	X	X	X	X	X
Field Servicing of Software-enabled Devices	X	X	X	X	X	X	X

Data Added or Cross Linked to SBOMs to Meet Use Case Objectives

Use Cases	Added or Cross Linked Data
Pre-Deployment CVE Vulnerabilities	Vulnerability Source (Database, Supplier); Licenses
Post-Deployment CVE Vulnerabilities	Vulnerability Source (Database, Supplier); Runtime Data
Licensing Risks	Licenses
EOL and Non-maintained Component Alerting	Vulnerability Source (Database); EOL
Pre-purchase Risk Assessment	Vulnerability Source (Database); Licenses; EOL; Ownership; Sanctioned Entity
Component Usage Across an Organization	Vulnerability Source (Database); Licenses; EOL; Runtime Data
Incident Response	Vulnerability Source (Database, Supplier); Multiple SBOM Types
M&A and Investment Risk Assessment	Attestations; Sanctioned Entity; Vendor Documentation
Verification of Accessory Software	Vulnerability Source (Database); Licenses
Differences in Components Between Build or Versions	Vulnerability Source (Database); Licenses; EOL; Runtime Data
Conformance with Disparate GRC Specifications	Attestations; Ownership; Sanctioned Entity; Vendor Documentation
Integrity and Threat Management for OT and isolated networks	Vulnerability Source (Database); Licenses; Sanctioned Entity; Integrity
Field Servicing of Software-enabled Devices	Integrity; Vendor Documentation

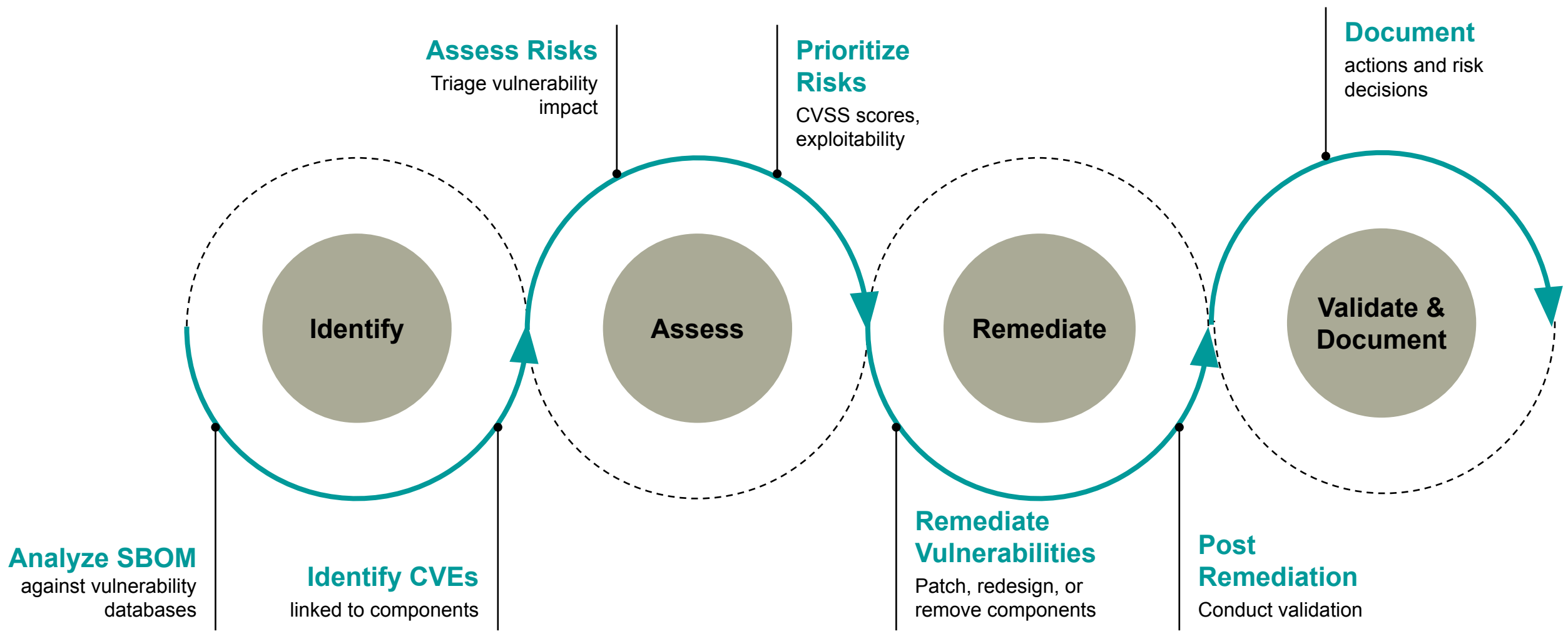
Deeper Dive into Use Case #1

**Pre-deployment Common Vulnerabilities and
Exposures (CVE) vulnerabilities**

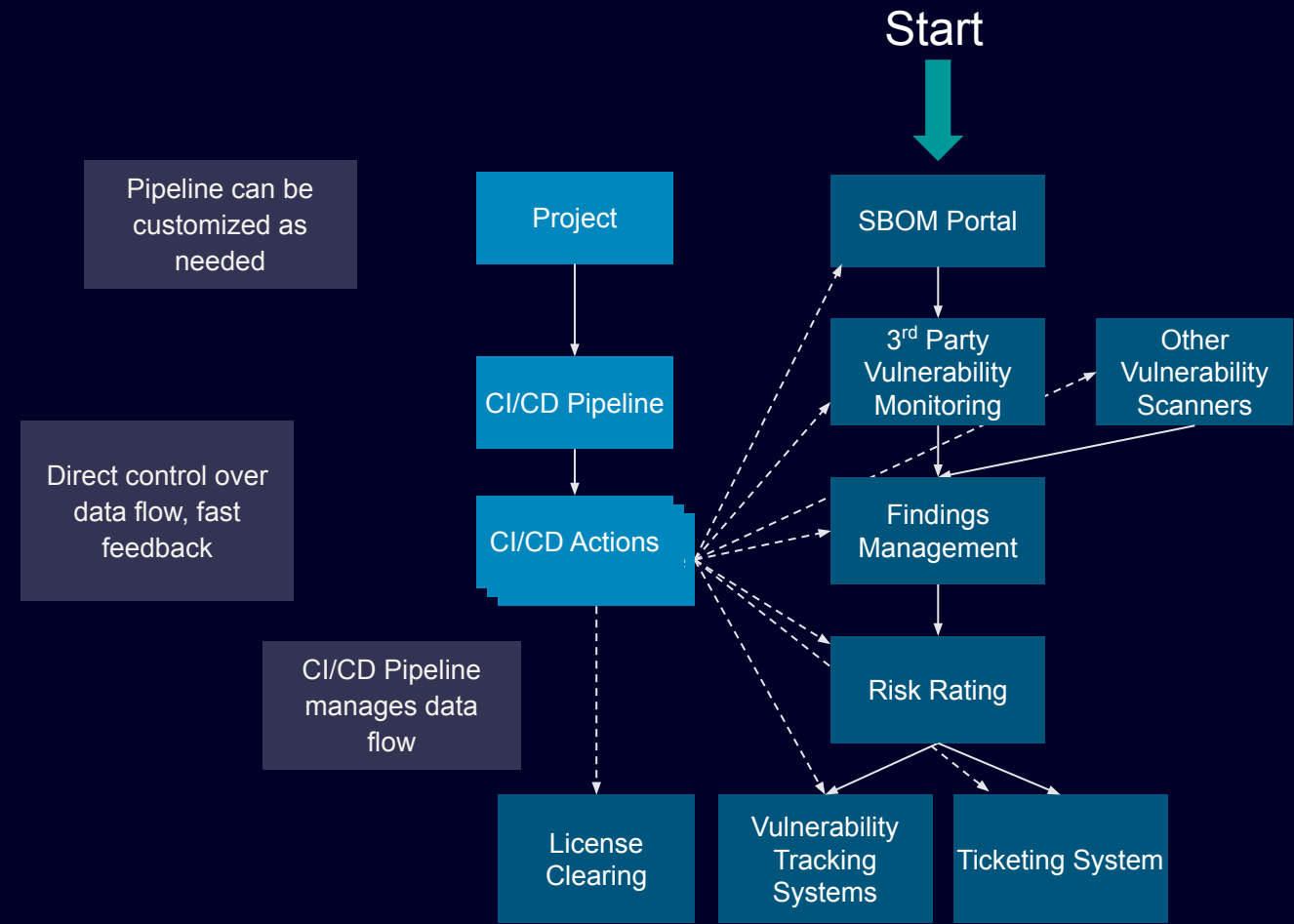
Use Case #1: Pre-deployment CVE vulnerabilities

[1] General Services Administration (GSA) Office of Government-wide Policy. (2024, May 14). Acquisition Letter MV-2023-02 Supplement 2.

Use Case #1: Pre-deployment CVE vulnerabilities



Integration of Vulnerability Management into the CI/CD Pipeline enabled by SBOMs



Key Take-aways

1. **Many different stakeholders** analyze SBOMs across the lifecycle
 - Software Producers, Distributors and Consumers
 - Engineering, Security, Regulatory, Procurement, Legal, IT, Vendor Management
2. SBOM data, combined with external intelligence, greatly improves security and vulnerability management.
 - Most common data: **Vulnerabilities, Licenses, Sanctioned Entities, EOL/EOS**
 - SBOM-drive workflows reduce **security, licensing, compliance and maintainability** risks
3. Supply chain transparency and trust increase when SBOMs are enriched with key operational data.
4. SBOM lifecycle management is becoming a specialized practice — but a shared responsibility.



Most importantly !!
Please read the paper
and share feedback

Improving Risk Management Decisions with SBOM Data

https://openssf.org/wp-content/uploads/2025/09/Improving_Risk_Management_Decisions_with_SBOM_Data.pdf

Acknowledgements

Authors

Bunny Hernández Banowsky (SHE BASH)
Anita D'Amico (Cotopaxi Consulting, Vigilant Ops)
Ian Dunbar-Hall (Lockheed Martin)
Bill Hansen (Hansen Enterprises LLC))
JC Herz (Exiger)
Nisha Kumar (Oracle)
Tim Mackey (Black Duck)
Mike Lieberman (Kusari)
Victoria Ontiveros (CISA)
Anusha Penumacha (Splunk)
Ricardo Reyes (Chainguard)
Ken Zalevsky (Vigilant Ops)

Designated Technical Reviewers

Bunny Hernández Banowsky (SHE BASH)
Cassie Crossley (Schneider Electric)
Anita D'Amico (Cotopaxi Consulting, Vigilant Ops)
JC Herz (Exiger)
Nisha Kumar (Oracle)
Tim Mackey (Black Duck)
Mike Lieberman (Kusari)
Bob Martin (MITRE)
John Nuckles (ODNI)
Victoria Ontiveros (CISA)
Kayra Otaner (Roche)
Animesh Pattanayak (PNNL)
Vijaya Ramamurthi (Accenture Federal Services)
Ricardo Reyes (Chainguard)
Ria Schalnat (HPE)
Anant Shrivastava (Cyfinoid Research)
Gaurav Srivastava (Siemens)
Ken Zalevsky (Vigilant Ops)

Other Contributors

Ralph Bean (Red Hat)
John Cavanaugh (ProCap360)
Brindusa Curcaneanu (NeuroPace)
Anthony Harrison (APH10)
Charlie Hart (Hitachi America, Ltd.)
Syed Zaeem Hosain (Aeris Communications, Inc.)
Philippe Ombredanne (AboutCode.org, Package-URL, and nexB Inc.)
Melissa Rhodes (Medtronic)
Duncan Sparrell (sFractal)