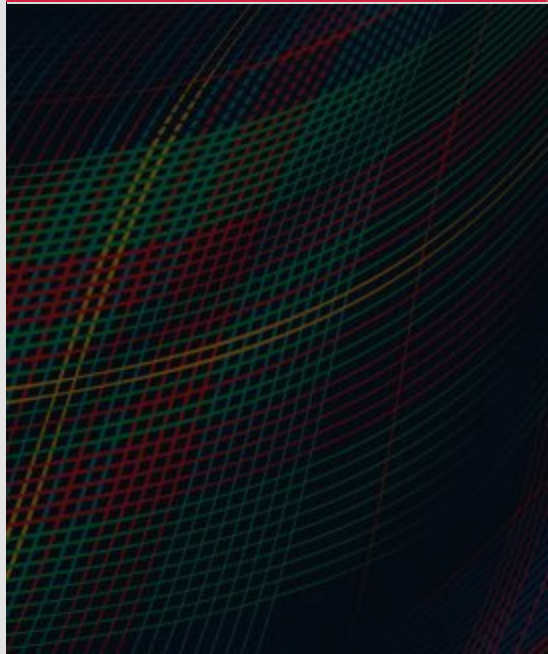
Software Bill of Materials (SBOM) Framework: Informing Risk Reduction

Carnegie Mellon University
Software Engineering Institute



SEPTEMBER 6, 2023

Mike Bandor
Charles M. Wallen
Carol Woody, PHD

© 2023 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

Document Markings

Copyright 2023 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

CERT® and OCTAVE® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM23-0930

Agenda

- Software and Supply Chain – Managing Resilience and Acquisition Challenges
- Leveraging ASF to Inform SBOM Use Cases and Risk Reduction
- SBOM Framework Overview
- Use of SBOM Data to Inform Risk Reduction: Visualizing the Unseen
- Summary

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

ASF: Informing SBOM Use Cases and Risk Reduction

The Challenge and Our Approach to a Solution

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

Carnegie Mellon University
Software Engineering Institute

Supply Chain/Acquisition Risk Is Increasing

More than 230,000 organizations were examined to discover their relationships with third parties. 98% of organizations have a relationship with a third party that has been breached within the last two years.
https://www.securityweek.com/98-of-firms-have-a-supply-chain-relationship-that-has-been-breached-analysis/

- Heartland Payment Systems (2009)
- Silverpop (2010)
- Epsilon (2011)
- New York State Electric and Gas (2012)
- Target (2013)
- Lowes (2014)
- AT&T(2014)
- HAVEX / Dragonfly attacks on energy industry (2014)
- DOD TRANSCOM contractor breaches (2014)
- Equifax (2017)
- Marriott (2018)
- SolarWinds (2020)
- Log4j (2021)
- Medibank (2022)
- MOVEit...(2023)

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

Key Software and Supply Chain Cybersecurity Challenges

Carnegie Mellon University Software Engineering Institute

Systems are increasingly software intensive and complex.

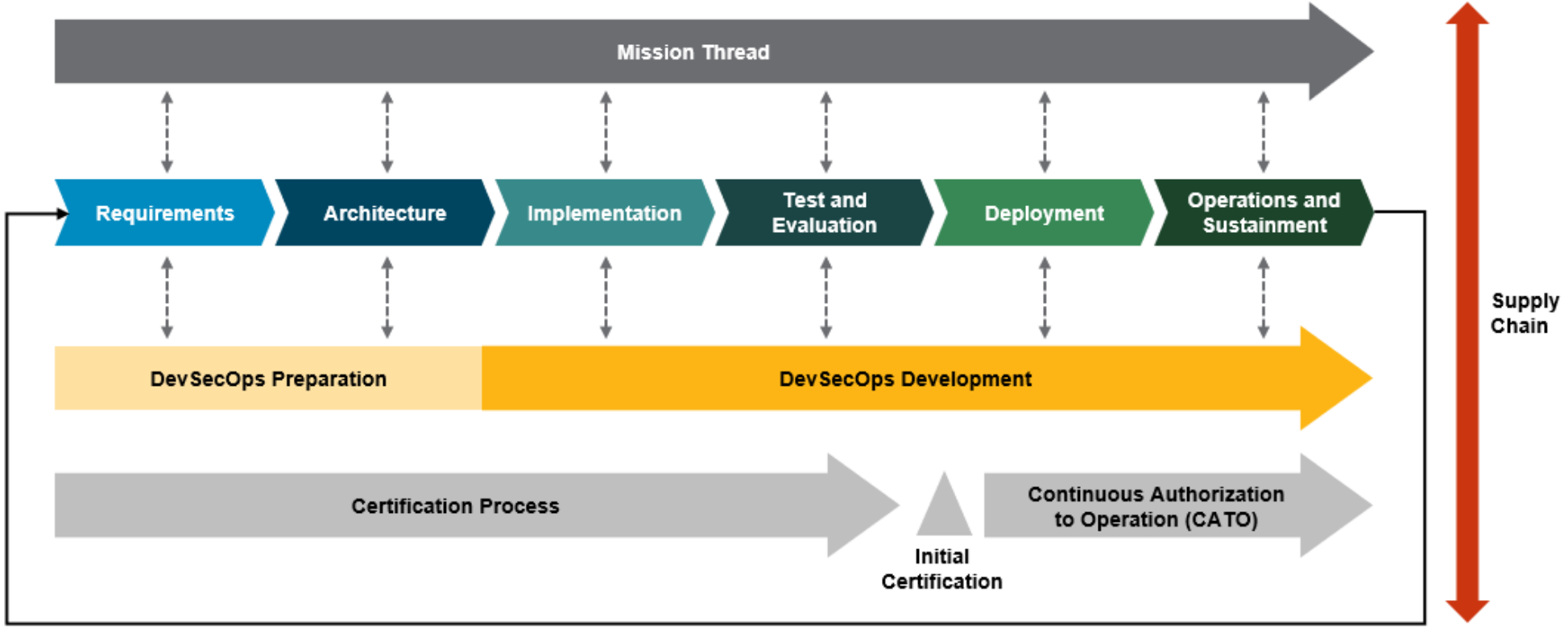
Third-party components are widespread throughout every system and require an integrated acquisition, engineering, development, and operational focus to ensure sufficient security and resilience.

Managing relationships with third parties is a critical success factor.

- A program cannot effectively manage cyber risks alone.
- Supply chain risk management requires collaboration.
- Data-driven

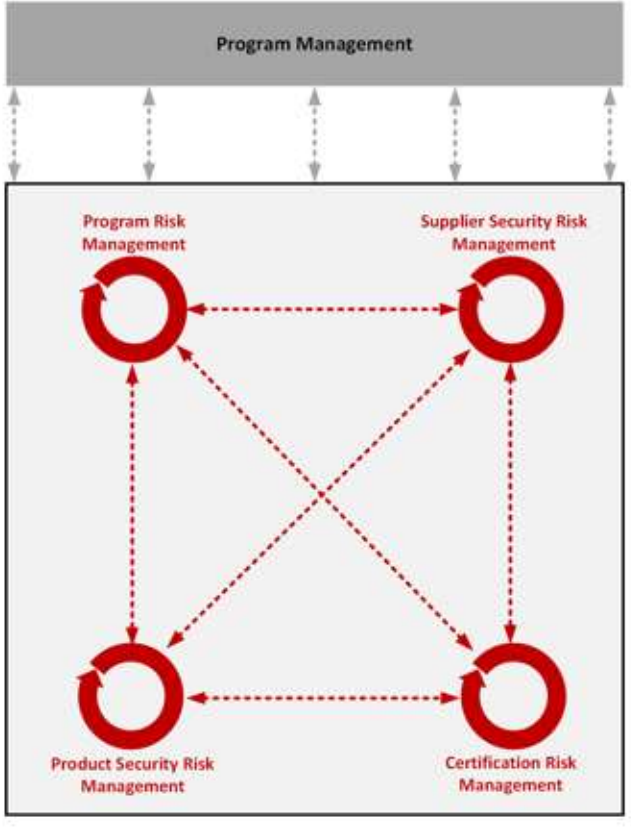
© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

Acquisition Cybersecurity Problem Space



© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

Challenge: Integrating Security and Supplier Risk Management across the Organization



Security and supplier risk management are typically outside of the program risk management.

Information is scattered in many documents such as Program Protection Plan (PPP), Cybersecurity Plan, System Development Plan, Supply Chain Risk Management Plan, etc.

Many activities across the organization are critical to managing cyber risks and must be addressed collaboratively across the lifecycle and supply chain and integrated with program risk management.

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

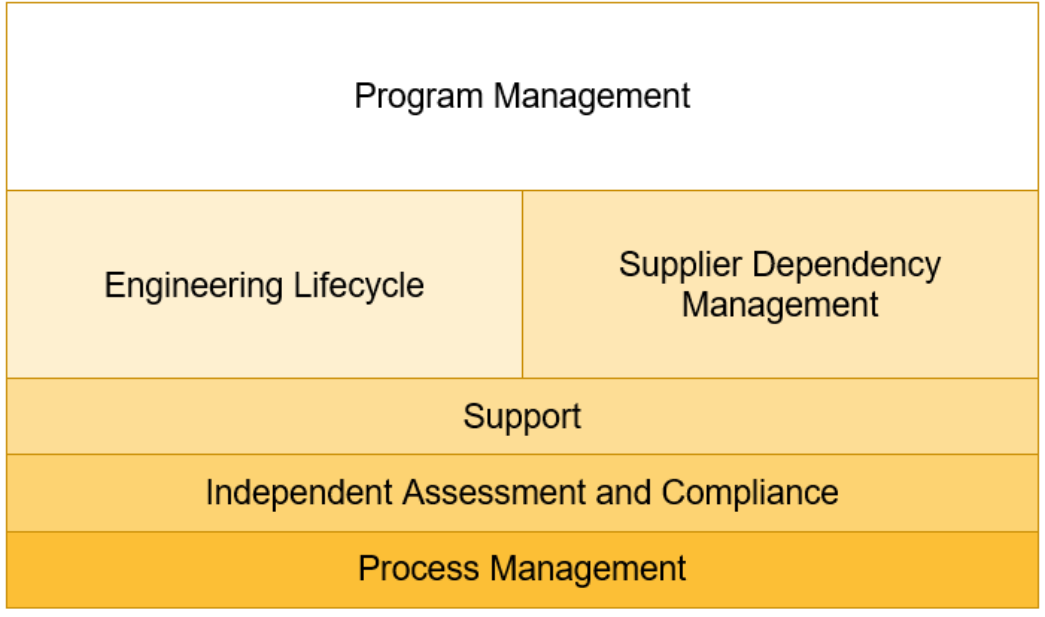
What is the Acquisition Security Framework (ASF)?

The ASF is a collection of leading practices for building and operating secure and resilient software-reliant systems.

The ASF is designed to proactively enable system security and resilience engineering across the lifecycle and supply chain.

It provides a roadmap for building security and resilience into a system rather than "bolting it on" after deployment.

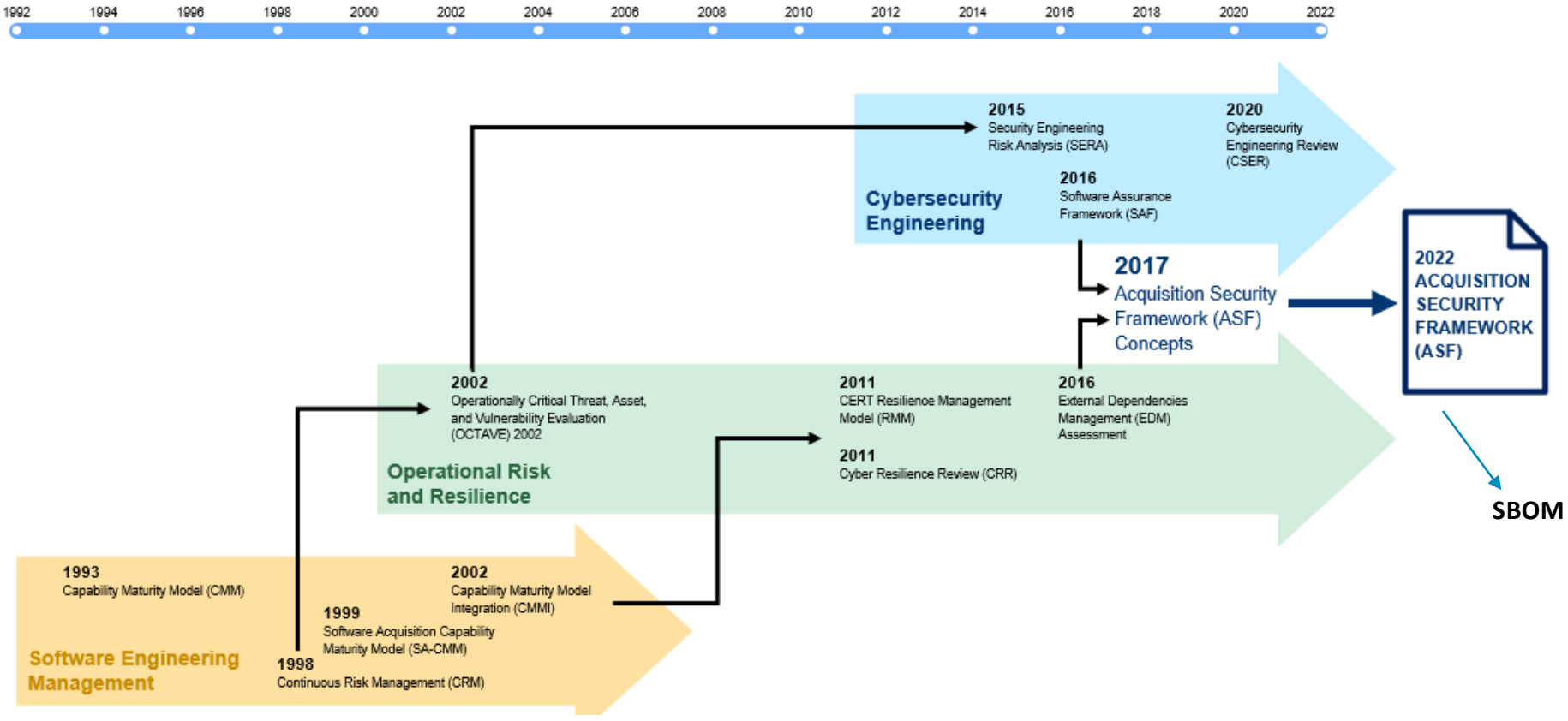
ASF principles and concepts facilitate efficient and predictable systems environments and more manageable delivery and risk outcomes.



© 2023 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

ASF Research Lineage



© 2023 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

Tailored Risk Frameworks

ASF principles and concepts enable effective management of security and resilience risks across a range of challenges areas.

Frameworks consistent with ASF principles and concepts can be tailored based on problem space and scope:

- SBOM Framework (prototype completed)
- Cybersecurity Engineering Framework (in progress)
- Zero Trust Framework (proposed)

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

ASF: Informing SBOM Use Cases and Risk Reduction

SBOM Framework: Use Cases and Risk Reduction Practices

Carnegie Mellon University
Software Engineering Institute

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

What is a Software Bill of Materials (SBOM)

An SBOM is a formal record containing the details and supply chain relationships of various components used in building software. In addition to establishing these minimum elements, this report defines the scope of how to think about minimum elements, describes SBOM use cases for greater transparency in the software supply chain, and lays out options for future evolution.[1]

SBOMs are mandated under a federal directive EO 14028, *Executive Order on Improving the Nation's Cybersecurity*[2]

1 *The Minimum Essential Elements of a Software Bill of Materials*, United States Department of Commerce, July 12, 2021, https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf
2 *Executive Order on Improving the Nation's Cybersecurity*, White House, 12 May 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

SBOM Framework – Our Approach

1. Survey of SBOM perspectives and use cases - reveal a strong emphasis on defining the content and format
2. Expanded on existing practices – utilized a lifecycle approach
3. Outlined key activities – requirements, build, deploy, use
4. Determined practices – enable ongoing use and management
5. Codified SBOM Framework – five goal areas

Requirements, Planning, Build/Construct, Deploy/Use, Manage/Support, and Infrastructure

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

Perspectives on SBOM and Use Cases

Carnegie Mellon University Software Engineering Institute

The Department of Commerce noted in the "Minimum Elements" document that:

"…these are the initial steps and requirements needed to support the basic use cases. There is more work to be done to expand transparency in the software supply chain and to support visibility for securing software."

Source: Department of Commerce The Minimum Elements For a Software Bill of Materials (SBOM), 2021

Common SBOM Use Cases:

- Build an SBOM for a system
- Receive and manage third-party SBOMs
- Manage known vulnerabilities
- Manage software versions
- Manage code reuse
- Manage software components that reach end of life
- Manage software licenses

Source: National Telecommunications and Information Administration (NTIA) Use Cases Working Group, 2019.

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

ASF Concepts Applied to SBOM: Setting the Scope

Carnegie Mellon University Software Engineering Institute

To set the scope, we developed a scenario for implementing an SBOM that includes the following:

- *Build / construct* an SBOM
- *Use the SBOM* to support identification of known vulnerabilities and risk reduction

SBOM practices were established based on this scenario

- expanded by considering a lifecycle perspective (goals):
- Requirements, Planning, Build/Construct, Deploy/Use, Manage/Support, and Infrastructure

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

Leveraging ASF to Inform Common SBOM Use Cases

Carnegie Mellon University Software Engineering Institute

Activity	Use Case
Requirements	
Plan	
Build / Construct	*Build SBOM for system* *Receive and manage third-party SBOMs*
Deploy / Use	*Manage known vulnerabilities*
Manage / Support	
Infrastructure	

44 practices were developed for activities in the lifecycle that enable and support operational use of the SBOM data

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

SBOM Framework Goals -- Requirements

Carnegie Mellon University Software Engineering Institute

Goal 1—SBOM requirements for the program are identified and managed.

The purpose of this goal is to ensure that SBOMs are integrated with the program's security/resilience activities.

1. Are program goals (e.g., reducing risk, managing system security/resilience)established for using SBOMs?
2. Are program requirements (e.g., required and desired data elements)established for SBOM content?
3. Are program requirements established for using SBOMs to support risk reduction and security/resilience activities?
4. Are criteria/triggers in place for reviewing SBOM requirements?
5. Are SBOM requirements updated periodically based on reviews and lessons learned?
6. Are baseline (i.e., boilerplate) SBOM requirements that apply to all program and system suppliers identified and documented?
7. Are criteria used to evaluate each supplier's ability to meet the program's SBOM requirements?
8. Are SBOM requirements included in formal agreements?

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

SBOM Framework Goals -- Plan

Carnegie Mellon University Software Engineering Institute

Goal 2—A plan for developing and using SBOMs is developed.

The purpose of this goal is to ensure that the programs have a plan for using SBOMs to manage software security/resilience risks.

1. Are standards, guidelines, and policies for implementing SBOM practices and artifacts established?
2. Are requirements established for implementing SBOM practices and artifacts to support risk management across the program or system?
3. Is sufficient funding allocated for implementing SBOM practices and artifacts across the program or system?
4. Are staff members assigned to implement SBOM practices and artifacts across the program or system?
5. Are roles and responsibilities established for SBOM practices?
6 Do stakeholders understand their roles in implementing, managing, and supporting SBOM practices?
7. Is SBOM training for technical and program staff members provided as needed?
8 Is a plan developed to manage SBOM practices and artifacts across the program or system?
9. Is the SBOM plan monitored and adjusted as needed?

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

SBOM Framework Goals – Build / Construct

Carnegie Mellon University Software Engineering Institute

Goal 3—SBOM data is created for the system, subsystems, and components.

The purpose of this goal is to ensure that accurate and complete SBOM data is created and validated for the system, subsystems, and components.

1. Does the program's SBOM format meet specified requirements?
2. Is architecture information that identifies software components for each system and subsystem available?
3. Are information sources (e.g., engineering data, licensing data, results of software composition analysis) for creating an SBOM specified and used?
4. Are SBOMs for the system's commercial off-the-shelf (COTS) software, government off-the-shelf (GOTS) software, and open-source software (OSS) available?
5. Is an SBOM created or identified for each software component?
6. Are multiple SBOMs integrated to construct dependency trees for the system?
7. Is SBOM data validated for completeness and accuracy?

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

SBOM Framework Goals -- Deploy / Use

Carnegie Mellon University Software Engineering Institute

Goal 4—Vulnerabilities are identified and managed in SBOM software components, leading to reduced system risk.

The purpose of this goal is to ensure that SBOMs are used to manage vulnerabilities in the system's software components.

1. Are known vulnerabilities and available updates monitored for software components identified in the system's SBOM?
2. Are vulnerabilities in SBOM components identified?
3. Is the mission risk of each SBOM component assessed?
4. Are software updates prioritized based on their potential impact to mission risk?
5. Are software component reviews/updates conducted based on their mission-risk priorities?
6. Are vulnerability management status, risks, and priorities tracked for each software component?

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

SBOM Framework Goals -- Manage / Support

Carnegie Mellon University Software Engineering Institute

Goal 5—SBOM risks are managed for system components.

The purpose of this goal is to ensure that accurate, complete, and timely SBOM data is available for system components to effectively manage risk.

1. Are the suppliers for system components identified?
2. Is supplier data reviewed periodically and updated as needed?
3. Are SBOMs for system components identified, analyzed, and tracked?
4. Are SBOMs managed to ensure they are current?
5. Are the risks related to incomplete or missing SBOM data identified and mitigated?
6. Are risks and limitations related to managing and redistributing SBOM information identified and managed?
7. Is the provenance of SBOM data established and maintained?

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

SBOM Framework Goals -- Infrastructure

Carnegie Mellon University Software Engineering Institute

Goal 6—SBOM practices, software, and tools are selected, implemented, and managed.

The purpose of this goal is to ensure that SBOM practices, software, and tools are integrated into the program's infrastructure.

1. Are technical requirements for the SBOM infrastructure developed and documented?
2. Are SBOM practices, software, and tools selected and implemented?
3. Are SBOM practices, software, and tools monitored and managed?
4. Is the security/resilience of SBOM practices, software, and tools managed?
5. Are the integrity and authenticity of SBOM data validated and managed?
6. Is each SBOM and its related artifacts managed across the organization?
7. Is each SBOM and its related artifacts managed for each system?

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

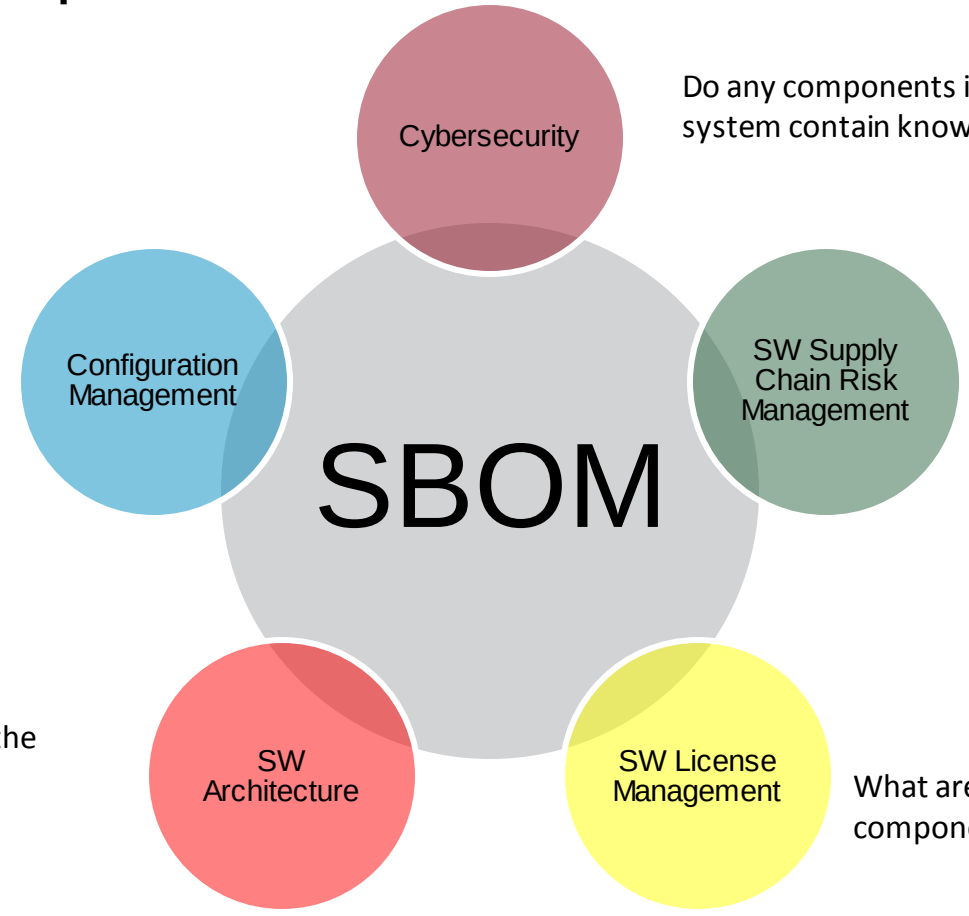
ASF: Informing SBOM Use Cases and Risk Reduction

Software Bill of Materials: Visualizing the Unseen

Carnegie Mellon University
Software Engineering Institute

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

SBOM Relationships with Other Areas



Do any components in or used by the system contain known vulnerabilities?

What components are included/needed in my system?

What are the third-party components in the system and the source of the component information?

Where are the components in the system architecture?

What are the licensing/data rights to components in my system?

© 2023 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

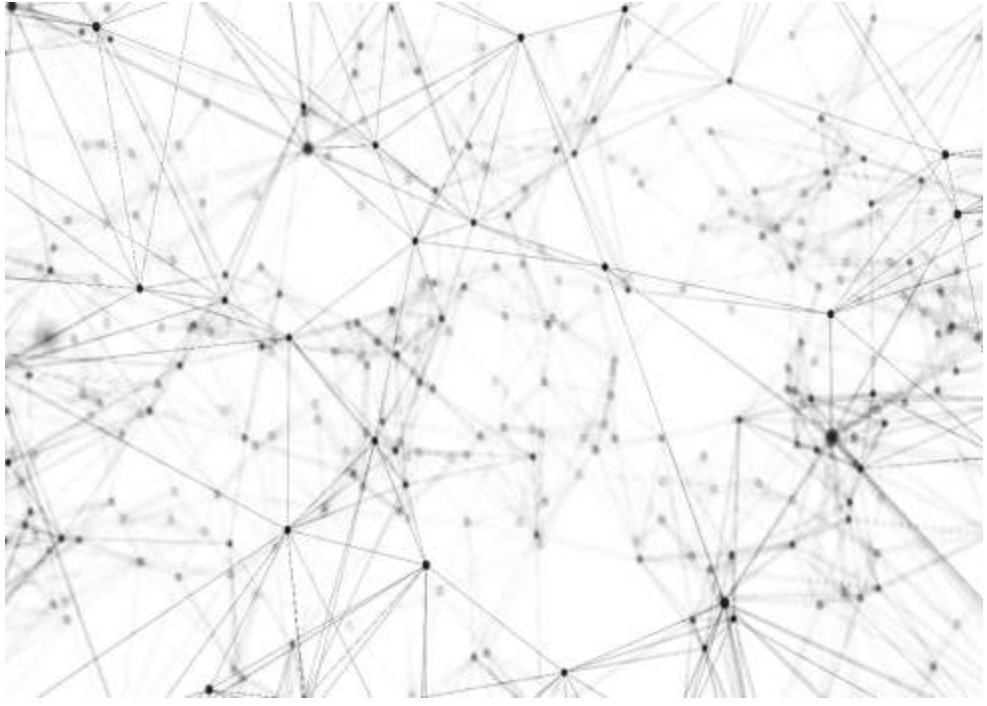
SBOMs at Many Levels

Organizations tend to focus on the product(s) coming through their development pipeline(s)

- What about the tools in the pipeline(s)? Do you know what is there?
- What about the other software used to support the product?
- How do you get complete situational awareness across the entire program?

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

Using Graphs to Visualize the Unknown



Everything is naturally connected, networks of people, transactions, supply chains

> *"Graphs form the foundation of modern data and analytics techniques, with capabilities to enhance and improve user collaboration, Machine Learning models, and explainable Artificial Intelligence." – Gartner, "Top 10 Tech Trends in Data and Analytics," 16 Feb 2021*[1]

Using graphs encodes relationships that cut across data elements and exposes their critical aspects that would not otherwise be visible

A graph lets the problem be represented through **Nodes** and **Relationships** of the nodes to each other

[1] https://www.gartner.com/smarterwithgartner/gartner-top-10-data-and-analytics-trends-for-2021

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

SBOMs and Graphs: A Closer Look

A closer review of the guidance reveals the following (highlighting added for emphasis):

> ***Depth**. An SBOM should contain all primary (top level) components, with all their **transitive dependencies** listed. At a minimum, all top-level dependencies must be listed with enough detail to **seek out the transitive dependencies recursively.***
>
> ***Going further into the graph will provide more information.** As organizations begin SBOM, depth beyond the primary components may not be easily available due to existing requirements with subcomponent suppliers. Eventual adoption of SBOM processes will enable access to additional depth through deeper levels of transparency at the subcomponent level. **It should be noted that some use cases require complete or mostly complete graphs, such as the ability to "prove the negative" that a given component is not on an organization's network.**[1]*

1 *The Minimum Essential Elements of a Software Bill of Materials*, United States Department of Commerce, July 12, 2021, https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

SBOMs and Graphs: A Closer Look

Carnegie Mellon University Software Engineering Institute

Guidance review (continued):

***Known Unknowns**. **For instances in which the full dependency graph is not enumerated in the SBOM, the SBOM author must explicitly identify "known unknowns."** That is, the dependency data draws a clear distinction between a component that has no further dependencies, and a component for which the presence of dependencies is unknown and incomplete...*

***Other Component Relationships**. **The minimum elements of SBOM are connected through a single type of relationship: dependency. That is, X is included in Y. This relationship is implied in the SBOM graph structure…**[1]*

1 *The Minimum Essential Elements of a Software Bill of Materials*, United States Department of Commerce, July 12, 2021, https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

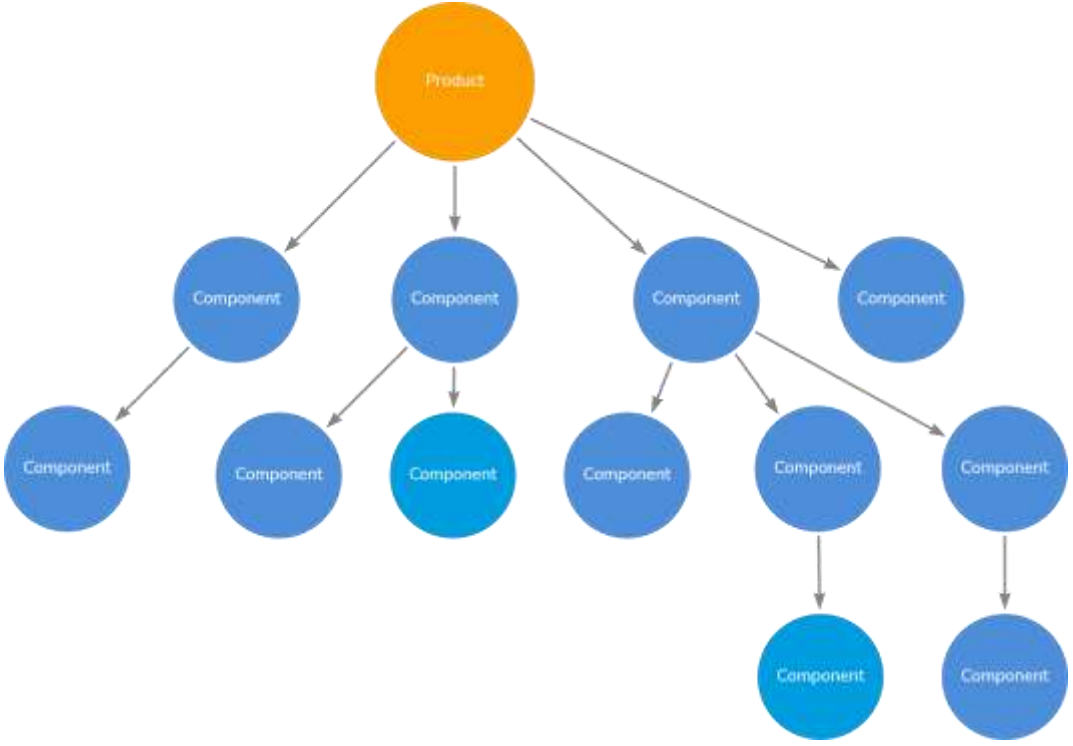
Software Bill of Materials: Visualizing the Unseen

SBOM Dependencies – Expectations vs. Reality

Carnegie Mellon University
Software Engineering Institute

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

SBOM Dependencies – Expectations vs. Reality



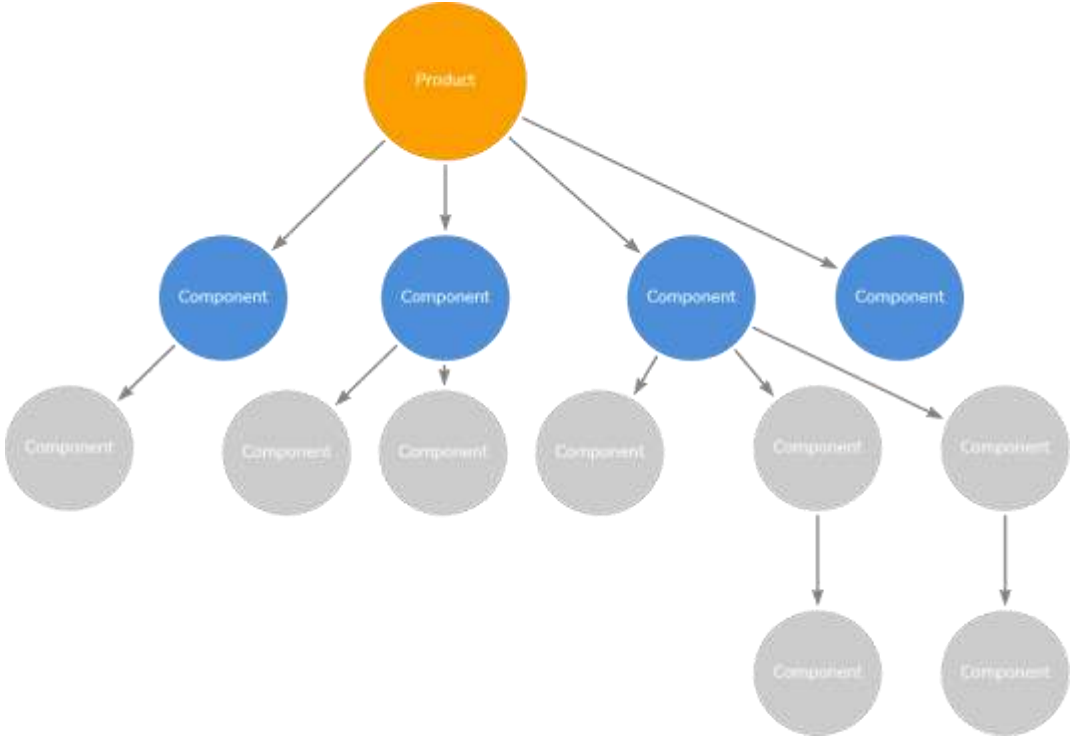
SBOM Dependencies – Organizational Expectations

Many organizations think of their generated SBOM data looks this way

- Assuming the secondary and tertiary dependencies are ingested from their respective suppliers

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

SBOM Dependencies – Expectations vs. Reality



SBOM Dependencies – Organizational Expectations & Missing Data

An organization can currently control what they use

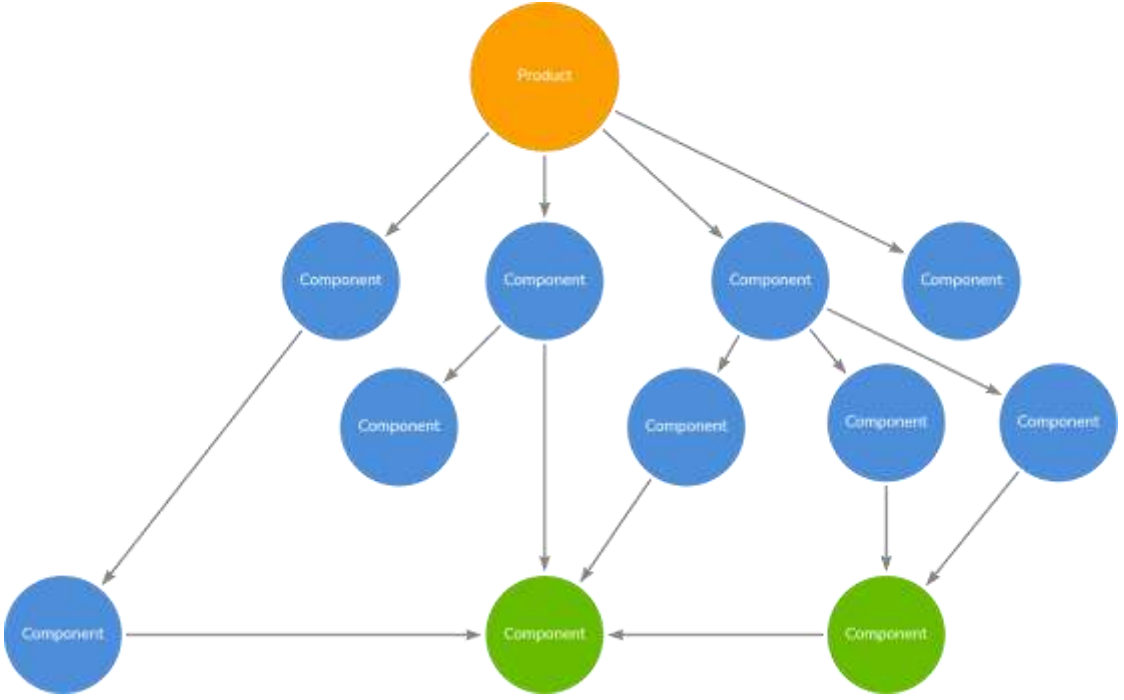
- What are the first level components?
- What are the risks of the unknown components (secondary & tertiary)?

Adding the information to the dependencies is the responsibility of the organization

- Potentially a full-time responsibility for individual(s) to monitor & maintain

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

SBOM Dependencies – Expectations vs. Reality



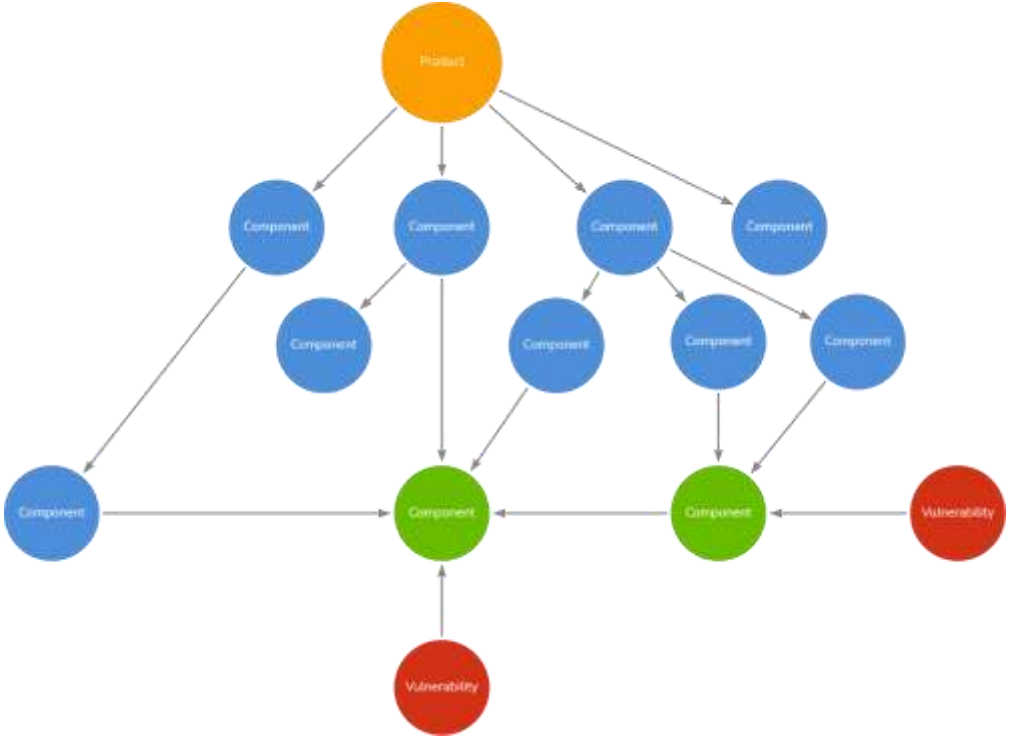
SBOM Dependencies – Reality of the Dependencies

The reality is the component dependencies are not a clean as most organizations think

© 2023 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

SBOM Dependencies – Expectations vs. Reality



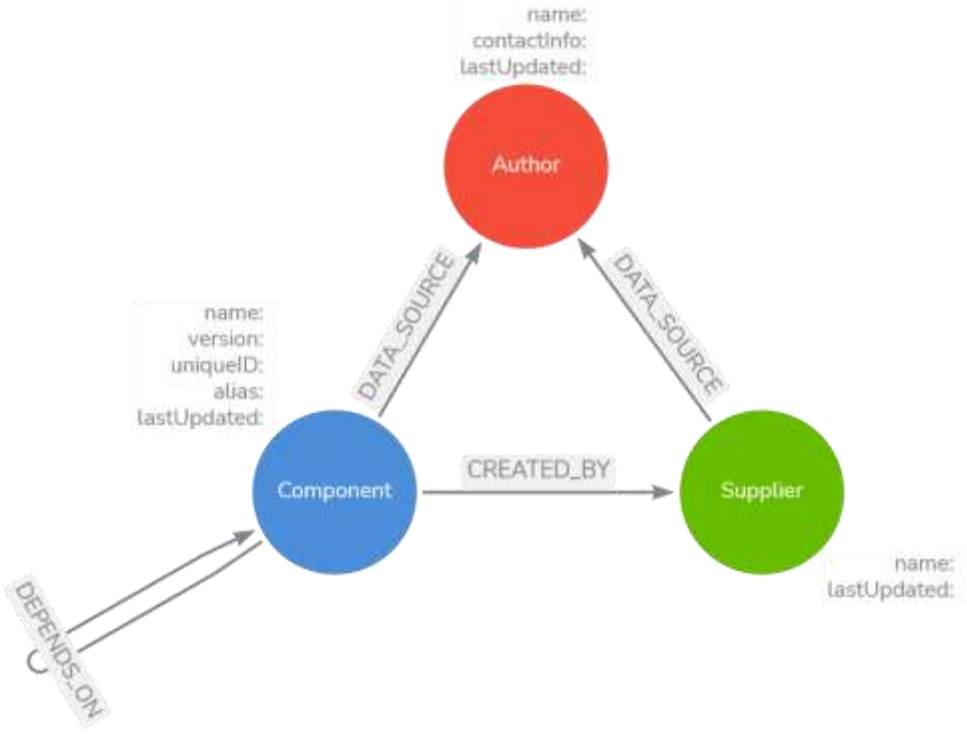
SBOM Dependencies and Vulnerabilities

Adding the vulnerabilities to the data, the system impacts and risks become more apparent!

- Vulnerabilities tend to be managed independently

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

Further Research – Graphing SBOM Data



Basic SBOM Graph Model

Using data exported from an SBOM tool:

- Ingest the data to create the graph prototype (start with SDPX format)
- Develop the scripts and processes to ingest and refine (update) the data
- Identify vulnerability data and add it to the graph
- Use the basic use cases from the SBOM guidance to prove out the model and prototype

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

In Summary

Systems are increasingly software intensive and complex.

Third-party components are widespread throughout every system and require an integrated acquisition, engineering, development, and operational focus to ensure sufficient security and resilience.

The SBOM Framework leverages ASF principles and concepts to inform practices to build, deploy, and use SBOMs to reduce risk programmatically and systematically.

SBOMs and their activities offer expanded data analytic/mining opportunities – visualizing the unseen/unknown to provide innovative new methods and insights to inform risk reduction.

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

Questions

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

The Team

Carol Woody
Principal Researcher
CERT Division

Email: cwoody@cert.org

Christopher Alberts
Principal Cyber Security Analyst
CERT Division

Charles M. Wallen
Information and Infrastructure Security Analyst
CERT Division

Mike Bandor
Senior Software Engineer
Software Solutions Division

.

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

SBOM and Supporting ASF Reference Materials

Carnegie Mellon University Software Engineering Institute

White Paper – *Software Bill of Materials Framework: Leveraging SBOMs for Risk Reduction* https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=982283

White Paper - *Acquisition Security Framework (ASF): An Acquisition and Supplier Perspective on Managing Software-Intensive Systems' Cybersecurity Risk* https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=887698

Technical Note - Alberts, Christopher; Bandor, Michael; Wallen, Charles; & Woody, Carol. *Acquisition Security Framework (ASF): Managing Systems Cybersecurity Risk.* CMU/SEI-2022-TN-003. Software Engineering Institute, Carnegie Mellon University. 2022. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=889215

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]