Top three activities for future meetings

Discussion / Panel: A lifecycle of an SBOM - following the tracking of software metadata from generation to use

- Supported by stories and screenshots from other POCs

Discussion / Brainstorm: Use cases for the Energy sector

- What's possible today?
- What is desired for tomorrow?
- Identify unique Energy sector drivers

Discussion: SBOM's for Legacy Equipment

- Overview of the "legacy problem"
- Demonstration of binary analysis and useful tools
- Vendor perspectives on SBOMs for Legacy products

Top 12 Vote-getters

In the voting session, SBOM POC participants identified the following highest overall priorities (in descending order):

118	Demo/Walkthrough of Full SBOM lifecycle from detection, producing, Storage to distribution (12 votes)
10	Develop standard contract clauses to require vendors to provide SBOM (10 votes)
67	Explore the Use Case: Limits/Merits of creating SBOMS for legacy components (8 votes)
122	Produce general SBOM whitepaper and beginner how to get involved document (7 votes)
1	Create SBOMs from open-source products (6 votes)
54	Address SBOM confidentiality: How do vendors and utilities control access to SBOMs to ensure that they are not released publicly and used by bad actors to target systems? An NDA approach does not seem to be adequate if SBOMs are issued to hundreds of utilities each with thousands of employees (6 votes)
2	Develop taxonomy describing information to be included in the SBOM e.g. differentiating between developed software and open source. (5 votes)
25	Address the gap of how to create SBOMs when no source code is available (5 votes)
40	Address the gap that open source & Commercial are part of a single product: an a single SBOM needs to cover both (5 votes)
62	Explore the Use Case: Using SBOMs for vulnerability management. (5 votes)
105	Training on how to maintain an SBOM, including frequency and notifications of updates (5 votes)
106	Training on minimum attributes of the SBOM specific to various grid components (5 votes)

The complete list of ideas generated is listed below, sorted into affinity groups within their associated prompt grouping.

Tasks To Perform

What specific tasks should we perform together?

Create SBOMS and identify key components

1. Create SBOMs from open-source products (6 votes)
2. Some type of taxonomy is needed regarding information to be included in the SBOM e.g. differentiating between developed software and open source. (5 votes)
3. Define or identify existing SBOM format to be used together with clear requirements what information is expected to be exposed (4 votes)
4. Create SBOMs from proprietary source products (4 votes)
5. Identify what a good SBOM MVP example would look like (3 votes)
6. Validate that generated SBOMs are in compliance with various formats (2 votes)
7. There's a lot to learn about SBOMs. That's job no. 1. (2 votes)
8. Define minimum content required in an SBOM (1 vote)
9. Identify any existing similar frameworks that can be leveraged (1 vote)

Define and Incentivize SBOM Compliance

10. Need standard contract clauses to require vendors to provide SBOMs (10 votes)
11. Will the recent Cyber Exec Order incorporate a SBOM approach as a federal requirement for particular systems? (3 votes)
12. Clear ROI examples (3 votes)
13. Create and vet introductory resources to spread the word on value and use of SBOMS (0 votes)
14. To include clauses for timely notification in case of updates or changes to a previously completed SBOM (0 votes)

Develop Security/Privacy Standards

15. Replace Fear with Knowledge to address the concern that publishing SBOMs is not a concern as tools can easily extract a device's firmware to reverse engineer the SBOM. (4 votes)
16. Use of an NDA to have access to the SBOM's from a vendor (1 vote)

What tasks should be performed as a part of SBOM Exchange collaborations?

17. Develop / customize the NDA / information protection instrument (4 votes)
18. Create clear guidance on structure and boundaries for exchanges (3 votes)
19. Decision on publish/subscribe, file folders, or email? How to share (2 votes)
20. Exchange of SBOMs between producers and consumers of SBOM information (2 votes)
21. Need as much automation as possible (0 votes)
22. Define criteria for who can participate (0 votes)
23. Determine parties to exchange information (0 votes)
24. Determine how exchanges will happen. FTP? (0 votes)

Goals Gaps and Activity Planning

Are there any specific gaps in available knowledge or capability that we should address together?

SBOM in Special Cases

25. How do we create SBOMs when no source code is available (5 votes)
26. Who will produce fully qualified SBOMs for Open-Source Software? (3 votes)
27. Legacy product challenges (2 votes)

28. We need to include third parties can/cannot provide for SBOMs - is it feasible (0 votes)
29. Trust verification of foreign-produced SBOMs from critical systems (0 votes)
30. What about exemptions? A vendor does not want to participate due to inability or trade secret claims? (0 votes)

Understanding and Utilizing SBOM

31. How does a vendor collect the data for the SBOM? (2 votes)
32. Limits and appropriate and inappropriate uses and goals of SBOMS (2 votes)
33. Difference between initial SBOM requirements and 2nd, 3rd, etc. iterations of future SBOM requirements/components (1 vote)
34. Customer facing SBOM vs. build SBOM (1 vote)
35. What tools are available for end users? What tools are needed? (3 votes)
36. Cross-domain links (energy + comms, energy + transport, etc.) (2 votes)
37. HBOM (2 votes)
38. How does a consumer link together the security implications associated with multiple SBOMS for each component but implemented as a system (2 votes)
39. It is very difficult to determine if a vulnerability in an included subcomponent is exploitable in the implementing product. (0 votes)

SBOM Components and Requirements

40. Open source & Commercial are part of a single product: an a single SBOM needs to cover both (5 votes)
41. Format/Structure of SBOM + HBOM (i.e., Firmware connection to hardware) (2 votes)
42. Should SBOMs include everything in the install package (config files) or just binaries & libraries (2 votes)
43. Are there levels of SBOM granularity that are essentially TLP: White (1 vote)
44. Assigning software components unique IDs before consumption (1 vote)
45. Determine level of granularity to drill down. e.g., how far do we need to drill to call it done? (1 vote)
46. Alignment of SBOM data with Vulnerability repository search functions (1 vote)
47. Initial SBOM components vs. 2nd, 3rd iterations of SBOM (0 votes)
48. How to incorporate cloud applications associated with product into SBOM (0 votes)

SBOM Integrity

49. Who certifies the SBOM's (3 votes)
50. Use of SBOM in regulated environments (CIP vs non-CIP) (3 votes)
51. How to address Errors in an SBOM (2 votes)
52. Should an SBOM have a (mandatory) review/renewal date like a policy (1 vote)
53. Neutral self-assessment criteria for tools (1 vote)

Security and Information Sharing

54. SBOM CONFIDENTIALITY: How do vendors and utilities control access to SBOMs to ensure that they are not released publicly and used by bad actors to target systems? An NDA approach does

not seem to be adequate if SBOMs are issued to hundreds of utilities each with thousands of employees (6 votes)

55. How will SBOMS be used in liability/legal cases? (4 votes)
56. Will there be the development of a SBOM Global Directory for vendors, software components, products? (4 votes)
57. How do vendors avoid unnecessary queries about SBOM details when vulnerabilities are not applicable to their integrated use in a vendor product? (2 votes)
58. Verify authorized digital signer -> Supplier relationships (1 vote)
59. How will the SBOMs be shared with end users (0 votes)
60. will there be a central organization monitoring and managing the SBOM community and updating guidance documents? who will oversee and maintain the integrity of the creation, exchange process? (0 votes)

Challenges to Adoption

61. How to address the pushback on time to prepare an SBOM (1 vote)

Use Cases to Explore

What Use cases pertinent to SBOM Consumers should we explore?

SBOM utilization

62. Using SBOMs for vulnerability management. (5 votes)
63. Analyzing SBOMS and taking actions based on the analysis (3 votes)
64. Process for requesting SBOMs (Specific product and version). It's not possible to know what version of the product is installed at the customer site (2 votes)
65. Leveraging SBOM or lack of SBOM for contracting/procurement processes, how to reference in procurement and contract language (2 votes)
66. Software supply chain risk assessment (1 vote)

SBOM in specific applications/special cases

67. Limits/Merits of creating SBOMS for legacy components (8 votes)
68. SBOMS relative to energy interdependent infrastructures (4 votes)
69. Tying an SBOM to a specific HBOM (4 votes)
70. If a vendor is ISO 27001, should it be required to provide SBOM's? (3 votes)
71. What changes need to be made to config & vulnerability management tools, so they can utilize SBOM info. (2 votes)
72. Which internal depts & BU's can derive the most value from SBOMS? (1 vote)
73. Public/Private partnership lessons learned (1 vote)
74. connected vs not connected vs Windows vs iOS vs Android, etc. (1 vote)
75. Using SBOMs for license management (0 votes)
76. Industry Specific software not in the ICS area (0 votes)
77. Explore use of SBOM with Application Control Solutions (0 votes)
78. Explore use of SBOM with MUD (ports & service declaration) (0 votes)
79. Cloud (0 votes)
80. manufacture, and operations of PV inverters, along with lifecycle updates in the field (0 votes)

SBOM Integrity

81. Multiple layers of software. E.g., vendor A vats and provides OS and middleware. This can nest several layers deep. Who provides each SBOM? (3 votes)
82. Ways to determine SBOM completeness (2 votes)
83. What requirements are necessary to ensure that build systems produce authentic and verified SBOMs. (2 votes)
84. Could legacy SBOMs be more accurate than build SBOM? Changes/configurations since procurement (1 vote)
85. Concept of a confidence level for an SBOM element. known vs unknown is binary, there may be gray areas. (1 vote)
86. Process for vendors to support and respond to SBOM questions in a secure manner (0 votes)
87. hierarchical SBOMs (0 votes)

What use cases pertinent to SBOM producers should we explore?

Version Control:

88. How do we know that a given SBOM actually corresponds to the artifacts used to produce a software artifact? (3 votes)
89. how will SBOMS be updated - will there be required standards outlining frequency and accuracy of timeliness of info in an SBOM (1 vote)
90. How will published SBOMs be version controlled? (1 vote)
91. Implications on vendor on providing an incomplete SBOM (unknowingly)? (1 vote)
92. IEC 62443 patching exchange formats in conjunction with SBOM describing the patch (1 vote)
93. Will SBOMs have unique and immutable identifiers (think URI)? (0 votes)
94. Will updating version controlled SBOMs be allowed? If so, will the changes be tracked? (0 votes)

SBOM Production

95. Determine ways to generate SBOMs as a part of the build process (4 votes)
96. Produce for legacy products (4 votes)
97. How will (non-artisanal) SBOMs be produced automatically? (2 votes)
98. Any specific SBOM items key to the Energy/Grid use cases focus? Anything tied to NERC/CIP, etc.? (1 vote)
99. Multiple levels of software (vendor A vets and provides OS and middleware) (0 votes)
100. How to differentiate between vendor-supported/created SBOM and a non-vendor (consultant) created SBOM (0 votes)

Information Sharing

101. Should there be restrictions for who can receive the SBOM? Concern regarding misuse of the documents (4 votes)
102. How SBOMs will be distributed, including legal restrictions (3 votes)
103. How to provide more context around some component usage in SBOM to customers? (1 votes)

104. Gathering required info from upstream library producers, and also their upstream suppliers (0 votes)

Topics for Training

What training opportunities could this POC provide that would hasten SBOM adoption for you?

105. How to maintain an SBOM? Frequency and notifications of updates? (5 votes)
106. Minimum attributes of the SBOM specific to various grid components (5 votes)
107. Training Utilities how to read the SBOM and look for any risks. (4 votes)
108. How to leverage an SBOM for vulnerability handling (3 votes)
109. What are VEXs and how are they used? (2 votes)
110. Once there are use cases, walking through the application of the use cases (2 votes)
111. Overview of guidance documents explaining what is an SBOM and how to customize an SBOM or build on a baseline SBOM (2 votes)
112. How to validate an SBOM for acceptance (2 votes)
113. How can I use an SBOM to help identify and manage risk? (2 votes)
114. Best practices for applying hash values for a specific purpose - integrity, identification, etc. (2 votes)
115. HBOM, SBOM: how to leverage these to assess risk within an organization? (2 votes)
116. SBOM integration into product pipelines: how to get there with no effort ;-) (1 vote)
117. How much should we rely on/follow, from earlier SBOM use cases? (0 votes)

Hands-on Opportunities

What sorts of hands-on opportunities would hasten SBOM opportunities for you?

118. Demo/Walkthrough of Full SBOM lifecycle from detection, producing, Storage to distribution (12 votes)
119. How to manage and protect SBOM data from extraction for nefarious uses (4 votes)
120. Should we have an in-person workshop? (0 votes)
121. Online Videos to demonstrate the use of SBOM (0 votes)

Reports, Publications, and Written Products

What written products and reports should this group generate?

122. General SBOM whitepaper and beginner how to get involved document (7 votes)
123. SBOM Maturity Framework/Checklist (4 votes)
124. Playbooks - Manufacturer vs. End User (4 votes)
125. Potentially: defining energy-specific use cases, with some kind of prioritization of feasibility (3 votes)
126. How to incorporate VEX (1 vote)
127. Lessons learned from generating an SBOM (0 votes)
128. Challenges in using SBOMS and case studies of solutions (0 votes)

Questions:

129. How do we continuously update practices, recommendations, etc.? And not have updating overwhelm users. (3 votes)

130. Where do we publish products? Does this include journals, presentations at conferences, online reports, SBOM energy sector website, etc.? (0 votes)