LOGIIC™

Linking the Oil and Gas (O&G) Industry to Improve Cybersecurity

SBOM Study: Managing ICS software risks to Oil & Gas

In 2021, LOGIIC (Linking the Oil and Gas Industry to Improve Cybersecurity) conducted a study to understand how SBOMs and other vendor capabilities can be used to manage cybersecurity risks to industrial control systems (ICS) software that may be introduced from third-party components that are part of vendor solutions. This study was based on SBOM research conducted by LOGIIC which included Executive Order 14028 (May 12,2021) that President Biden issued on Improving the Nation's Cybersecurity. [#1] The order includes new requirements for software vendors selling software to the U.S. government. One of these requirements consists of providing a U.S. government purchaser a Software Bill of Materials (SBOM) for each product either directly or by other means such as a website.

A Software Bill of Materials (SBOM) is effectively a list of ingredients or a nested inventory. It is a formal record containing the details and supply chain relationships of various components used in building software [#2 p. 10]. SBOMs enable better software security and supply chain risk management [#2 p. 18]. It is critical for each industry sector to establish a common set of practices and market expectations that is viable and reflects the needs of the industry [#2 p.18].

LOGIIC SBOM Study Results Summary

LOGIIC was able to determine that vendors who are critical to our operations are taking steps to improve their software development lifecycle (SDLC) processes to ensure they can quickly respond to vulnerabilities in third party components used in their solutions. These processes along with their inventory of software components help them to achieve the software inventory goals defined for SBOMs. The vendors in this study have varying degrees of maturity that enables them to manage vulnerabilities in their products.

While LOGIIC supports and encourages the use and development of SBOMs, the tools and processes for producers and consumers to obtain value from SBOMs are not sufficiently mature, which may delay adoption:

- Although some vendors have agreed to share their SBOMs with customers (licensed and/or authorized users), the majority of vendors have decided not to support the unlimited public release of their SBOMs because of concerns about loss of their Intellectual Property, exposing vulnerabilities to potential adversaries, and the other challenges in this list.

- Commercial tools are available to securely create, use, store and share SBOMs. But, open source and commercial tool integration needs to mature for SBOMs to be widely used, given that energy sector companies under tight budget constraints may choose to utilize open source tools, while others may be using commercial tools.
- There are a limited number of commercially available solutions to help vendors create and manage SBOMs. In addition, many of the tools are not comprehensive and focus on specific development platforms.
- SBOMs may provide open source or other software subcomponents, but they currently do not identify vulnerabilities.
- Today, asset owners would have to allocate significant funds to staff a team to manage and obtain value from SBOMs as they become available from numerous vendors, until the use and scanning of SBOMs becomes automated and widely used commercial tools become the standard.
    - Many asset owners already have relationships with their key vendors who will perform detailed analysis as vulnerabilities in third party components are identified so the asset owners understand the risks to their operations.
    - The value to the asset owners from SBOMs would need to justify these additional costs
    - Industry Sector collaboration groups, like ISACs might be able to centrally manage SBOMs and perform related functions for a specific industry sector, but those costs would have to be agreed to and justified by all members of the group.

There are actions that can provide significant value in the near term while the SBOM processes mature:

- Asset Owners can work with their vendors to establish processes and agreements to accomplish many of the SBOM goals:
    - Vendors share information with asset owners that achieve the same goals as Vulnerability Exploitability eXchange (VEX) data that cross references data from National Vulnerability Database (NVD) to understand the potential impact to their products.
    - Processes exist for asset owners to obtain status from vendors when they suspect vulnerabilities in vendor products associated with third party components.
- Vendors can strengthen or verify their SDLC processes by:
    - Leveraging ISA 62443 4-1 standards and certification, or other standards that define SDLC processes.
    - Maintaining a comprehensive software component inventory, like the data in SBOMs, and establish processes to quickly identify potential risks associated with 3rd party software components.

LOGIIC will use what we learned from this study to help influence legislation and regulations that may impact the oil & gas industry. LOGIIC is willing to assist the government agencies and standards bodies to develop special use cases that are needed for our industry.

Vendors Pursuing SBOMs

There were five vendors participating in this LOGIIC SBOM study. Of the five, three were pursuing SBOM creation at some level of maturity. These three vendors took different approaches with each either exploring proof-of-concept or selecting a vendor tool to assist with SBOM creation or purchasing and deploying a product for SBOM creation. The other two vendors were not pursuing SBOMs but believe they can accomplish the same goals through traditional software development lifecycle management and vulnerability scanning to inventory components and highlight component vulnerabilities. While

software development lifecycles and manual inventory tracking are important for keeping software secure, they are not always timely in identifying software vulnerabilities. Meanwhile, once fully mature and standardized, SBOMs will be able to scale across the software ecosystem because of their support for automation, which includes automatic generation and machine-readability. Machine-readable SBOMs often accelerate the process of identifying and remediating potentially vulnerable subcomponents once subcomponent vulnerabilities have been identified by using automation. For now, however, until SBOM technology becomes more mature and incorporates automation more broadly, a robust vendor code inventory may provide more details than a SBOM. For example, the vendor would be able to state whether open source code containing a vulnerability was included in a product.

SBOM Standards

There are three standards for SBOM development:

1. Software Package Data Exchange (SPDX) is an open standard for software bill of materials (SBOM). SPDX allows the expression of components, licenses, copyrights, security references and other metadata relating to software. The SPDX specification is developed by the SPDX workgroup, which is hosted by The Linux Foundation. [#2 p.20]
2. CycloneDX is a software bill of materials (SBOM) standard, purpose-built for software security contexts and supply chain component analysis. The specification is maintained by the CycloneDX Core working group, with origins in the OWASP community [#2 p.20]
3. Software Identification (SWID) tags record unique information about an installed software application, including its name, edition, version, whether it is part of a bundle and more. SWID tags support software inventory and asset management initiatives. The structure of SWID tags is specified in international standard ISO/IEC 19770-2:2015 [#2 p.20]

A tool to convert among the three standards may be found at the following link.

- https://github.com/CycloneDX/cyclonedx-cli#convert-command

The three vendors in this study who were pursuing SBOMs said they could support SPDX or SWID.

SBOM Fields

As a result of Executive Order 14028, the National Telecommunications and Information Administration (NTIA) released a definition of the minimum elements to establish the baseline technology and practices for provisioning SBOMs, which may be considered the SBOM field requirements.

The core of an SBOM is a consistent, uniform structure that captures and presents information used to understand the components that make up software. Data fields contain baseline information about each component that should be tracked and maintained. The goal of these fields (standard SBOM structure) is to enable sufficient identification of these components to track them across the software supply chain and map them to other beneficial sources of data, such as vulnerability databases or license databases. The minimum data fields are contained in Table 1. [#3 p. 8]

Data Field	Description
Supplier Name	The name of an entity that creates, defines, and identifies components.
Component Name	Designation assigned to a unit of software defined by the original supplier.
Version of the Component	Identifier used by the supplier to specify a change in software from a previously identified version.
Other Unique Identifiers	Other identifiers that are used to identify a component or serve as a look-up key for relevant databases.
Dependency Relationship	Characterizing the relationship that an upstream component X is included in software Y.
Author of SBOM Data	The name of the entity that creates the SBOM data for this component.
Timestamp	Timestamp Record of the date and time of the SBOM data assembly.

Table 1. Core SBOM Data Fields

In addition to the data fields described in the minimum elements above, the following data fields are recommended for consideration, especially for efforts that are planned over several years or that require higher levels of security. These recommended elements are contained in Table 2. [#3 p. 14]

Data Field	Description
Hash of the Component	A cryptographic hash offers confidence that a specific component was used. It also provides a foundational element to assist in this mapping software components to vulnerability sources.
Lifecycle Phase	The data about software components can be collected at different stages in the software lifecycle, including from the software source, at build time, or after build through a binary analysis tool.
Other Component Relationships	Other types of dependency relationships can be captured and have been implemented in some SBOM standards. One approach that can be captured today beyond direct dependencies is “derivation” or “descendancy”. This can indicate that a component is similar to some other known component, but that some changes have been made.
License Information	License management was an early use case for SBOM, helping organizations with large and complex software portfolios track the licenses and terms of their diverse software components, especially for open-source software. SBOMs can convey data about the licenses for each component.

Table 2. Recommended SBOM Data Fields

The vendors in this study had the following suggestions that could be included in the unique identifier data field in the minimum data field set, or could be included as separate fields in the SBOM structure

1) Multiple vendors noted that Package URLs (PURLS) may assist in identifying software components
2) One of the vendors noted that the number one need was a list of hashes of components on platforms to allow for whitelisting.
3) Another vendor noted that there are several unique identifier types that work for different classes of software (PURL, Hash, CPE string). It would be helpful to determine a single unique identifier.
    a. The CPE String (Common Platform Identifier), which defines standard methods for assigning names to IT product classes, may be considered, but it does have its challenges. The following CPE 2.3 Naming Specification example represents Microsoft Internet Explorer 8.0.6001 Beta. [#4] The CPE string has no concept of a product component. So, if a vulnerability is buried in a rarely used feature or component, such as the Groove GFS Helper in the Internet Explorer in this example, there is no way to use CPE to express this.

        ```
        wfn:[part="a",vendor="microsoft",product="internet_explorer",
        version="8\.0\.6001",update="beta"]
        ```

SBOM Practices and Processes

An SBOM is more than a structured set of data; to integrate it into the operations of the secure development life cycle avendor organization should follow certain practices and processes that focus on the mechanics of SBOM use. [#3 p. 11]

Practice/Process	Description
Frequency	If the software component is updated with a new build or release, a new SBOM must be created to reflect the new version of the software.
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.
Known Unknowns	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.
Distribution and Delivery	SBOMs should be available in a timely fashion to those who need them and must have appropriate access permissions and roles in place.
Access Control	Many suppliers, including open source maintainers and those with widely available software, may feel their interests are best served by making SBOM data public. Other organizations, especially at first, may wish to keep this data confidential, and limit access to specific customers or users.
Accommodation of Mistakes	Accommodation of mistakes, should be built into the initial implementation phase of SBOM, allowing for omissions and errors. While internal management of supply chain data may be a best practice, it is still evolving. Starting today is better than waiting for perfection.

Table 3. SBOM Practices and Processes

One of the vendors had a process recommendation, suggesting two-person control for any SBOM changes.

Automation

Of the vendors pursuing SBOM, only one of the vendors had automated the production of SBOMs. The other two vendors have the intention of pursuing automation as a long-term goal. Today, these vendors rely on spreadsheets and manual processes for tracking software.

Commercial SBOM Tools

The vendors pursuing SBOMs had either purchased or were in the process of evaluating tools that could be used for generating and tracking SBOMs.

A list of commercial tools that generate the SPDX format of SBOMs is at the link below.

Commercial Tools - Software Package Data Exchange (SPDX)

For those interested in using CycloneDX, their tool set is available at the link below.

CycloneDX Tool Center

One of the vendors commented that the value of some commercial SBOM tools is that they provide the ability to quickly scan across all software and see which software may be impacted by a particular vulnerability or other finding. The tools allow the user to look across platforms and see the common components.

Vulnerability Management

VEX, which stands for Vulnerability Exploitability eXchange, is what the NTIA describes as a "companion artifact" to an SBOM. NTIA is working on standards for sharing vulnerability information. SBOMs provide insight into the composition of the product, but they do so at a high level that does not convey the extent to which a known vulnerability can be exploited in the product. This lack of "exploitability" results in many "false positives" being represented in the SBOM data and thus obscures the high-risk exploitable vulnerabilities. [#5]

VEX documents currently have just one standardized format: the Common Security Advisory Framework (CSAF). This format is released by OASIS Open, which is a European-based not for-profit dedicated to producing open-source standards for cybersecurity and related topics. [#6]

Of the five automation vendors in this study, only one was seriously pursuing VEX.

SBOM Sharing

None of the vendors in this study were amenable to unlimited public release of SBOMs. The vendors stated that they may be open to sharing SBOMs through a customer portal for authorized or licensed users.

One of the vendors stated that their legacy system SBOMs are available upon request since those are manually generated and human-readable. The same vendor noted that automated SBOMs are available to their customers as subscribers to their SBOM utility or by request. They noted that there is a large benefit for SBOMs being stored in a global SBOM managed service repository that system integrators may access.

For the Oil and Natural Gas (ONG) Industry, the ONG Information Sharing and Analysis Center (ISAC) should be considered as a possible aggregator/collector of SBOMs. The organization would be well-positioned to scan SBOMs as it is notified of threat information, indicators of compromise, etc.

Timeframe

The automation vendors noted that creating SBOMs for all their products is a multi-year exercise. For some legacy products, SBOM creation may be a manual process, depending on the systems and languages used.

For some vendors, the real challenge may not be the creation of SBOMs but the quantity of products requiring SBOMs. If an automation vendor has hundreds of versions of software deployed in the field, they will need to create hundreds of SBOMs. So, automated creation of SBOMs is critical.

In addition, there may be additional rigor applied for SBOMs created for safety systems over traditional OT systems, that may delay the creation of SBOMs for safety systems.

Study Recommendations

This study brought awareness of the maturity of the SBOM processes at automaton vendors. Automation vendors are at varying stages of maturity in SBOM development. As SBOM processes and tools mature and the vendors move forward with SBOM creation, LOGIIC and API have the following recommendations for our industry:

1) All ONG automation vendors should pursue the creation of SBOMs for tracking software components.
2) ONG automation vendors should use SBOM tools to automate the creation of SBOMs.
3) The industry should continue to observe SBOM adoption to determine if one is dominant for our sector (SPDX, Cyclone DX, SWID)
4) SBOMs produced by automation vendors should include the core and recommended SBOM fields.
5) SBOM creation should require a minimum of two-person control.
6) Automation vendors should plan to pursue VEX for vulnerability information sharing once the standard has been finalize by NTIA.
7) The SBOMs should be available to customers through a customer portal or a SBOM platform/tool.
8) The Unique Identifier field may be used to include Package URLs, Hashes or CPE string.
9) All software components should have hashes to allow for whitelisting.
10) Ideally, a single identifier should be named by CISA for all software components.
11) The ONG ISAC should be considered as a possible aggregator/collector of SBOM information.

[#1] Executive Order on Improving the Nation's Cybersecurity | The White House

[#2] ntia_sbom_energy_jan2021overview_0.pdf (doc.gov)

[#3] sbom_minimum_elements_report.pdf (doc.gov)

[#4] CPE - Common Platform Enumeration: CPE Specifications (mitre.org)

[#5] VEX one-page summary (ntia.gov)

[#6] Understanding Vulnerability Exploitability eXchange (VEX)