Schneider Electric
SBOMs – The Missing Link
VulnCon – March 2024

Cassie Crossley, VP Supply Chain Security
Who is Schneider Electric?
Schneider Electric provides energy and automation digital solutions for efficiency and sustainability

Key figures for 2022

5% of revenues devoted to R&D

€34 billion
2022 revenues

43% of revenues in new economies

128,000+
Employees in over 100 countries

A well-balanced global presence
2022 Revenues breakdown

Two business:

<table>
<thead>
<tr>
<th></th>
<th>23%</th>
<th>77%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industrial automation</td>
<td>€6.7 billion</td>
<td>€22.2 billion</td>
</tr>
<tr>
<td>Energy management</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
We partner in everything we do

650k service providers & partners

42k+ system integrators & developers

54k+ unique suppliers
We seek to embrace the whole value chain from security by design to secure operations with a comprehensive set of programs…
Schneider Electric’s SBOM Initiative
What is an SBOM?

A Software Bill of Materials (SBOM) is a formal record containing the details and supply chain relationships for the various components used in building software. These components, including libraries and modules, can be open source or proprietary, free or paid, and the data can be widely available or access-Internal.
Why do we need an SBOM application

Understanding the code that makes up our products provides SE with a blueprint for determining cyber security vulnerabilities, licensing implications, potential impacts, and how to respond.

**Regulation compliance**
- U.S. Executive Order 14028 for improving cyber security includes a provision for SBOMs
- U.S. Department of Energy CyTRICS program with Schneider Electric requires the SBOMs for all products
- Cyber Resilience Act (Europe)

**Accelerated Vulnerability Management**
Speed of remediation is affected when you don’t have SBOM data in a centralized system

**Risk Mitigation**
- Through notification in advance of potential attack
- Mitigate brand reputational risk

**Internal compliance**
Compliance to the SE Secure Development Lifecycle policy and ISA/IEC 62443-4-1 certification

**Procurement**
- Required in Edison Electric Institute contract template (used by most utilities)
- RFI - Department of Homeland Security
- U.S. Office of Management and Budget (OMB) Memo M-22-18 and M-23-16
- NIST SP 800-161 C-SCRM
- NIST SP 800-218 Secure Software Development Framework

**Trust Charter**
- Creates an enhanced level of trust between SE and our end consumers
- Early notification of SE products used in critical areas that could be targeted
- Thought leadership in the global Security landscape
SBOM Use Cases

Software Production: SBOM’s can help SE decision what external software should be included in our code base

- Reduce
  - Unplanned/unscheduled work
  - Code Bloat

- Dependencies
  - Understand broader complex links across all code bases

- Compliance
  - License Obligations
  - End of life

- Monitor
  - Components for Vulnerabilities

- Tracking
  - Ease of code review
  - Component usage: Banned/Allowed

Software Selection: SBOM can help Clients and Consumers select what products to purchase

- Identify potential vulnerabilities
- Targeted Security analysis
- End-of-life component(s) awareness

- Verify Source
  - Compliance with internal/regulatory policies
  - Claims verification

- Software integrations
- Pre-purchase/installation planning
- Market Signals

Software Operation: SBOM can help to install, configure, maintain, and administer software

- Quickly evaluate if a component is in use
- Independent mitigations
- Make informed risk-based decisions
- End of life alerts
- Support compliance and reporting requirements
- Reduction in costs through streamlined and efficient administration
2018 Schneider CP-CERT started evaluating SBOMs for internal use

2019 SE received utility contracts requiring SBOMs (they were using the Edison Electric Institute contract template)

2019 SE joined NTIA (Department of Commerce) SBOM working groups

2020 US Executive Order 14028. SE modified internal secure development lifecycle policy to provide binaries & SBOMs to central team

2021 SBOM collection started for every release of SE software and firmware
SBOM: Logical Flow

SBOM Processing and Construction: High-Level End-to-End Flow for each Product (Software and/or Firmware)

SE Product: Software and/or Firmware

Proprietary code developed:
- In-house
- Services contractor

Third-Party provider code:
- Partner or purchased
- May provide an SBOM

Open-Source Code:
- e.g., GitHub
- May come with SBOM

Amended after each version/change

SBOM Generated

SE Complete SBOM
(+Historical) Stored

Distribute applicable SBOM Package:
- SBOM (Minimum)
- Enhancement
- Patch
- Notification

Direct Customers
Indirect Consumers
CP CERT
Internal R&D Teams

Search full SBOMs
Pull complete SBOM upon request
SBOMs and Vulnerability Management
Use Case - Vulnerability

We learn of a vulnerability and want to know if any SE products contain the software or component.

I've heard about the Log4j vulnerability. Do any of your products contain this open source software?

1. Search the SBOM database for SBOMs with the open source component
2. Create a list of all potentially affected products
3. Issue an Impact Analysis (full set of offers or target)
4. Product teams review source code and confirm if or if not affected
Targets

Focus on the Accelerated Vulnerability Management

• Speed of remediation is affected when you don’t have SBOM data in a centralized system.
• Significant effort is needed to identify if our products are impacted by high profile 3rd party components, vulnerabilities, or threats.
• Teams often incorrectly identify a product to be not affected or affected due lack of data quality.

KPIs

XX days
Avg time to complete an impact assessment

XX
Impact Assessments issued in a year

Targets after SBOM initiative

80%
Reduction in staff hours

80%
Reduction in time to identify vulnerable component
Leveraging SBOMs in Impact Assessments
Vulnerabilities

**openssl**

Version 1.1.1n

- **CVE-2023-4807**
  - Published: 09/06/2023
  - Issue summary: The POLY1305 MAC (message authentication code) implementation contains a bug that

- **CVE-2023-5678**
  - Published: 11/06/2023
  - Issue summary: Generating excessively long X9.42 DH keys or checking excessively long X9.42 DH keys or

Other versions:

- **openssl**
  - Version 3.0.8-r3

- **openssl**
  - Version Unknown Version

- **openssl**
  - Version 1.1.0j

- **openssl**
  - Version 3.1.3-r0

- **openssl**
  - Version 1.1.1v

pkg.github/openssl@1.1.1v

TLS/SSL and crypto library
Summary of our SBOM Journey

3+ years in our SBOM program – mandatory for all products since January 2021

Strengths

• 4000+ SBOMs for internal products
• Valuable learnings and improved speed to generate security notices by leveraging SBOMs during Log4j, OpenSSL, and other critical open-source CVEs
• Increased awareness in R&D teams regarding third party dependencies
• Stronger transparency and trust with customers

Opportunities

• Over half of active development projects don’t have CI/CD pipelines → requires SBOM collection to be manual
• Binary scanning tools designed for open source; cannot identify commercial or proprietary libraries without additional information → requires manual creation of SBOMs and validation of all generated SBOMs
• Many suppliers not prepared yet to provide machine-readable SBOMs
Q&A and Thank you

- Cassie Crossley, VP Supply Chain Security – Cybersecurity & Product Security Office
- Email: cassie.crossley@se.com
- LinkedIn: https://www.linkedin.com/in/cassiecrossley/
- Book Author, *Software Supply Chain Security: Securing the End-to-End Supply Chain for Software, Firmware, and Hardware*
SBOM Level 1 Process Flow - Collect

- **Collect Process SBOM**: Validate SBOM & add metadata
- **SBOM updates from relevant sources**: (development, third-parties, etc.)
- **Obtain SBOM artifacts and updates from relevant sources**: (development teams, third-parties, etc.)
- **Create Draft SBOM**: New SBOM, New SBOM Version, Updated SBOM Version
- **SBOM Consumer**: Schneider Electric SBOM Solution, Schneider Electric Product Teams, Schneider Electric Non-IT Users
- **To Store**
SBOM Level 1 Process Flow - Store

Resolve SBOM data / metadata issues

From Collect

Verify SBOM(s) has necessary data and metadata (internally or externally developed)

Change SBOM status to final and generate SBOM identifying metadata

Determine actions in case of change to SBOMs and/or SBOM artifacts (e.g., notification, new SBOM version push)

BOM Repository

SBOM Repository

PBOM & HBOM Repository

SBOM Artifact Repositories

To Distribute

Store

SBOM Consumer

Schneider Electric SBOM Solution

Schneider Electric Product Teams

Schneider Electric Non-IT Users
SBOM Level 1 Process Flow - Distribute

Start Here

SBOM User Request
(SE Product Portal, SE SBOM Portal, Customer Direct Contact)

Create SBOM Package (SBOM & SBOM Artifacts)

Distribute SBOM Package

SE Validates User

Automated SBOM Request

Retrieve appropriate SBOM data and Artifacts

SBOM Package Notification Push

SBOM Consumer

SBOM Consumer Retrieves SBOM Package from SE Portal

SBOM Consumer Receives SBOM Out of Band (e.g., email)

SBOM Consumer Receives SBOM Package Push (by agreed channel)

SBOM/SBOM Notification Push

SBOM Package Metadata is created and stored

SBOM Consumer Receiving SBOM Package

To Store

Vulnerabilities may vary depending on configuration

SBOM Repository

PBOM & HBOM Repository

BOM Repository

SBOM Repository

SBOM Artifact Repositories

Schneider Electric SBOM Solution

Schneider Electric Product Teams

Schneider Electric Non-IT Users

SBOM Consumer

Property of Schneider Electric

Page 29
Customer Request: Internal SBOM Process

SBOM Request Process

Customer
- Requests SBOM through CCC, Account Manager, Cyber questionnaire
- Receives SBOM Request
- Initiates DocuSign for SBOM NDA
- Signs NDA
- Sends user information and list of Products with versions
- Receives NDA
- Requests user information and list of Products with versions
- Collects the list of Products and versions
- Provides registration details
- Receives NDA
- Collects the list of Products and versions
- Provision access to the requested SBOMs
- Access SBOMs
- SBOM Available?
  - Yes
    - Product team will generate SBOM and share
  - No
    - SBOM Request Process

SBOM Operations Team
- Receives SBOM Request
- Receives NDA
- Signs NDA
- Sends user information and list of Products with versions
- Register account in Schneider SBOM system
- Provides registration details
- Provides registration details
- Access SBOMs
- SBOM Available?
  - Yes
    - Product team will generate SBOM and share
  - No
    - SBOM Request Process

Product Teams
- Receives SBOM Request
- Receives NDA
- Requests user information and list of Products with versions
- Collects the list of Products and versions
- Provides registration details
- Receives NDA
- Collects the list of Products and versions
- Provision access to the requested SBOMs
- Access SBOMs
- SBOM Available?
  - Yes
    - Product team will generate SBOM and share
  - No
    - SBOM Request Process
External Use Case – Additional Artifacts

A customer wants to know additional information included in an SBOM Package (e.g. VEX, VDR, CVE, release notes, etc). This would trigger pulling an SBOM artifact into an SBOM package.

Can you provide me with the VEX information for XYZ?

1. Search the SBOM Artifacts database(s) and retrieve relevant artifacts
2. Assemble SBOM package with VEX artifacts
4. Distribute to Customer