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

SQUARE D by Schneider Electric

APC by Schneider Electric

AVEVA

Key figures for 2022

5% of revenues devoted to R&D

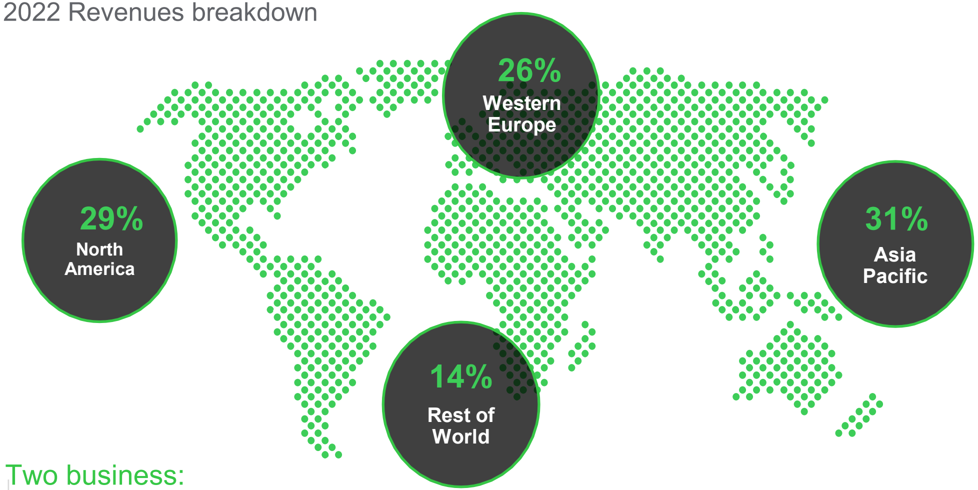
€34 billion
2022 revenues

43%
of revenues in new economies

128,000+
Employees in over 100 countries

A well-balanced global presence

2022 Revenues breakdown



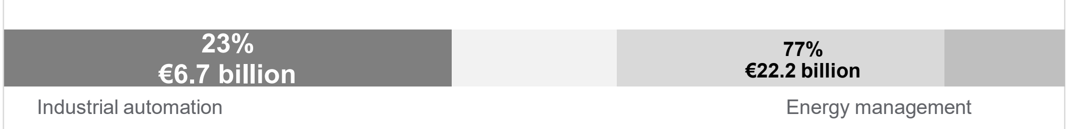
26% Western Europe

29% North America

31% Asia Pacific

14% Rest of World

Two business:



23%
€6.7 billion
Industrial automation

77%
€22.2 billion
Energy management

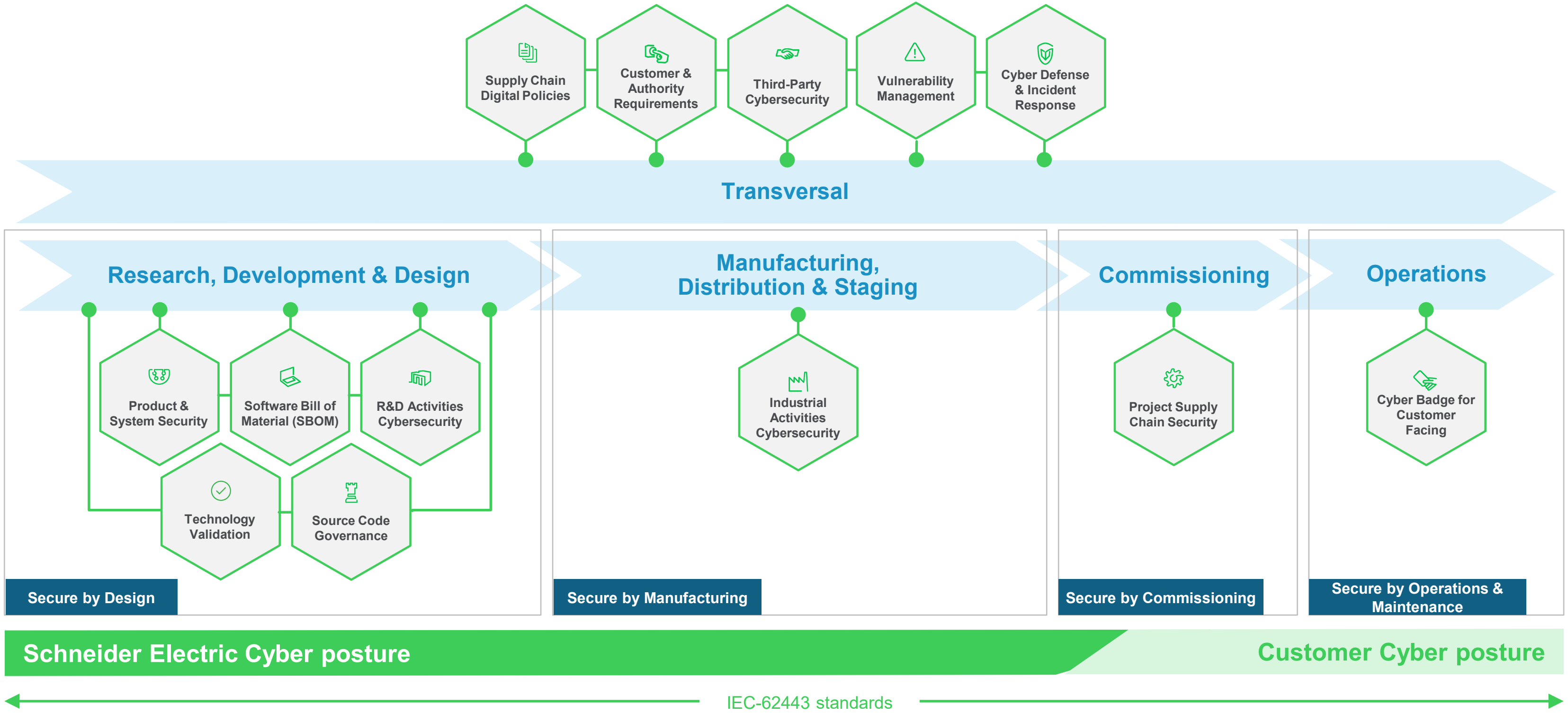
We partner in everything we do

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…



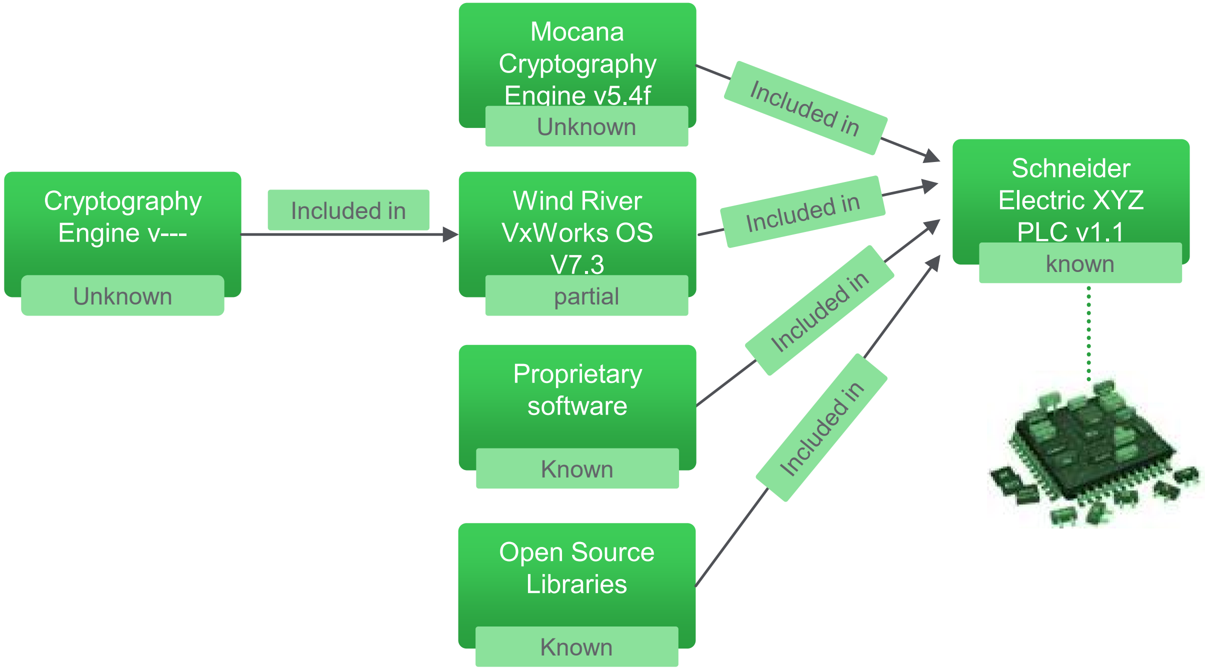
Supply Chain Digital Policies
Customer & Authority Requirements
Third-Party Cybersecurity
Vulnerability Management
Cyber Defense & Incident Response
Transversal
Research, Development & Design
Product & System Security
Software Bill of Material (SBOM)
R&D Activities Cybersecurity
Technology Validation
Source Code Governance
Secure by Design
Manufacturing, Distribution & Staging
Industrial Activities Cybersecurity
Secure by Manufacturing
Commissioning
Project Supply Chain Security
Secure by Commissioning
Operations
Cyber Badge for Customer Facing
Secure by Operations & Maintenance
Schneider Electric Cyber posture
Customer Cyber posture
IEC-62443 standards

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.



Mocana Cryptography Engine v5.4f

Unknown

Cryptography Engine v---

Unknown

Wind River VxWorks OS V7.3

partial

Proprietary software

Known

Open Source Libraries

Known

Schneider Electric XYZ PLC v1.1

known

Included in

Included in

Included in

Included in

Included in

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

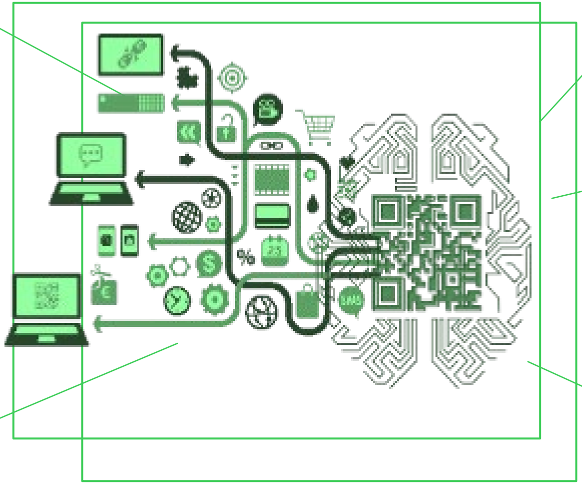
- U.S. Executive Order 14028 for improving cyber security includes a provision for SBOMs)
- U.S. Department of Energy CyTRICS program with Schneider Electric requires the SBOMs for all products
- Cyber Resilience Act (Europe)

Internal compliance

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

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

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

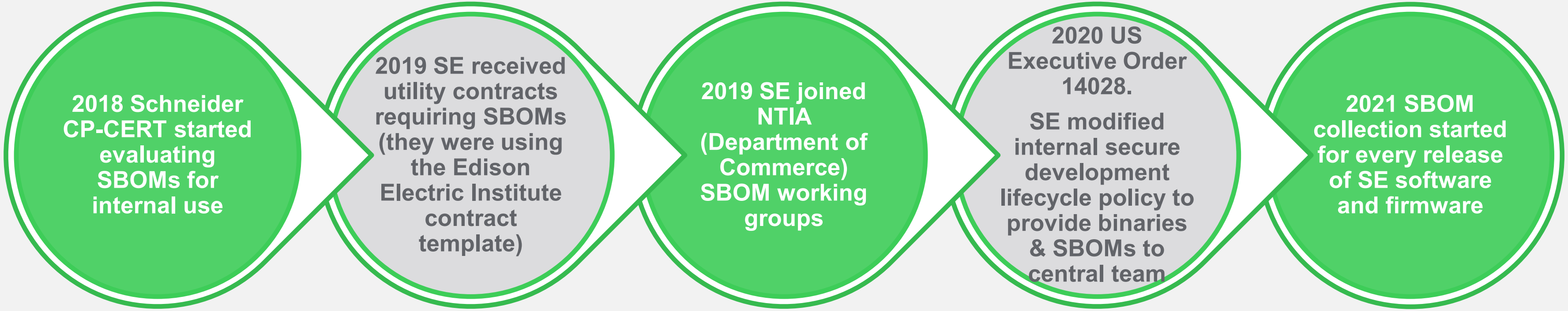
Make informed risk-based decisions

End of life alerts

Support compliance and reporting requirements

Reduction in costs through streamlined and efficient administration

SBOM Storyline: SE SBOM Journey



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.

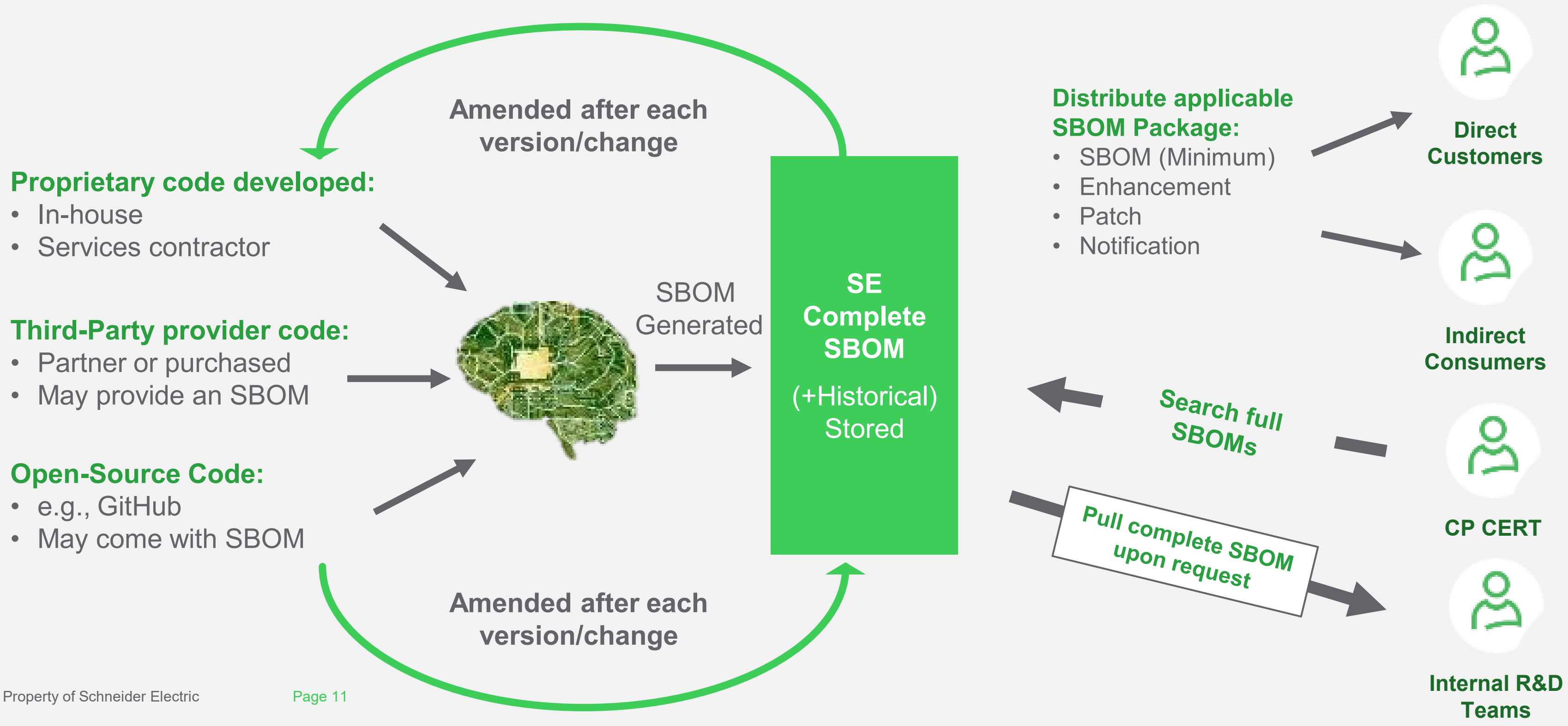
SE modified internal secure development lifecycle policy to provide binaries & SBOMs to central team

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

Amended after each version/change

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

Direct Customers

Indirect Consumers

Search full SBOMs

CP CERT

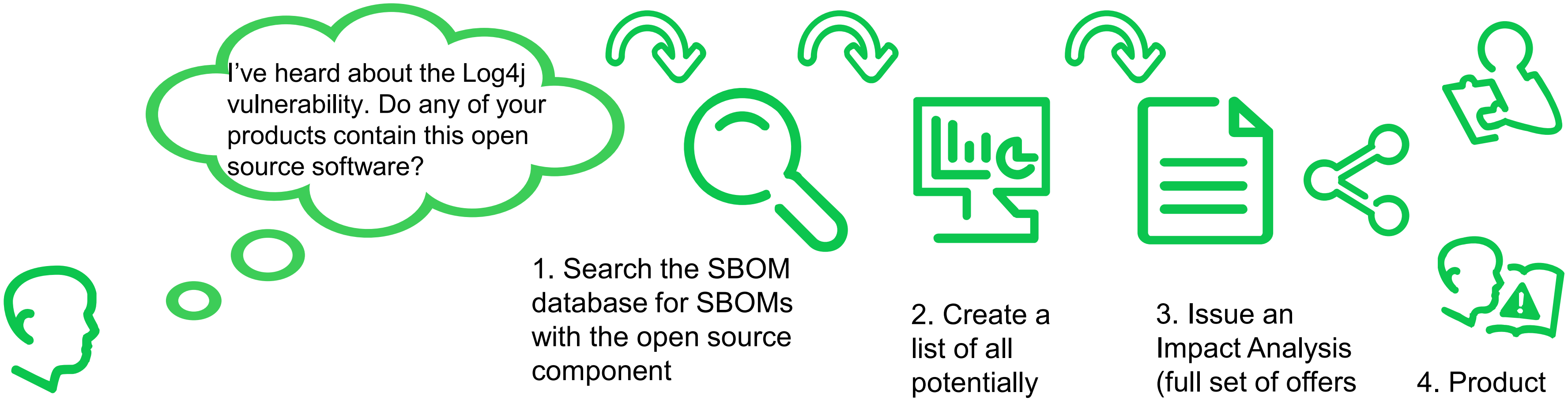
Pull complete SBOM upon request

Internal R&D Teams

SBOMs and Vulnerability Management

Use Case - Vulnerability

We learn of a vulnerability and want to know if any SE products contains 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

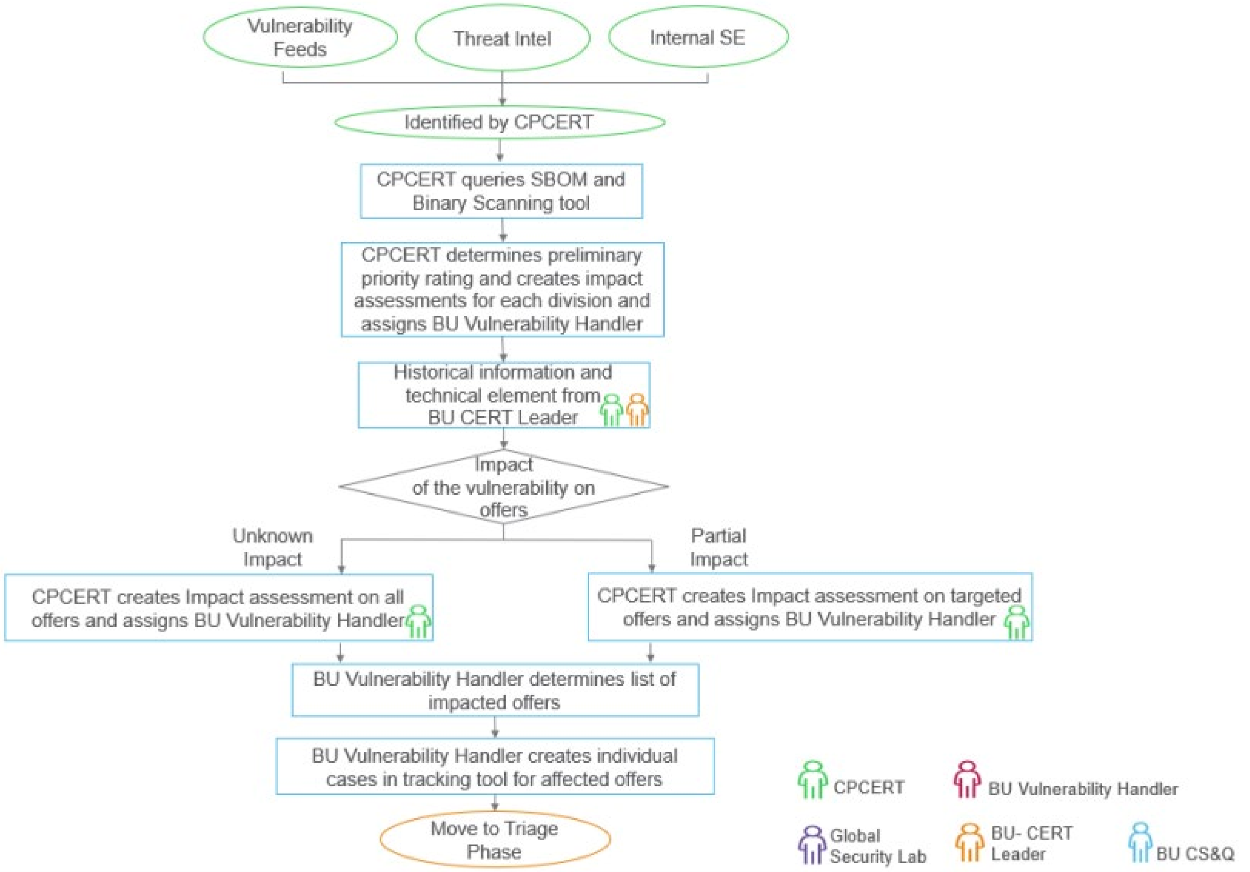
Targets after SBOM initiative

80%
Reduction in staff hours

80%
Reduction in time to identify vulnerable component

Leveraging SBOMs in Impact Assessments

Impact Assessment



Vulnerability Feeds

Threat Intel

Internal SE

Identified by CPCERT

CPCERT queries SBOM and Binary Scanning tool

CPCERT determines preliminary priority rating and creates impact assessments for each division and assigns BU Vulnerability Handler

Historical information and technical element from BU CERT Leader

Impact of the vulnerability on offers

Unknown Impact

Partial Impact

CPCERT creates Impact assessment on all offers and assigns BU Vulnerability Handler

CPCERT creates Impact assessment on targeted offers and assigns BU Vulnerability Handler

BU Vulnerability Handler determines list of impacted offers

BU Vulnerability Handler creates individual cases in tracking tool for affected offers

Move to Triage Phase

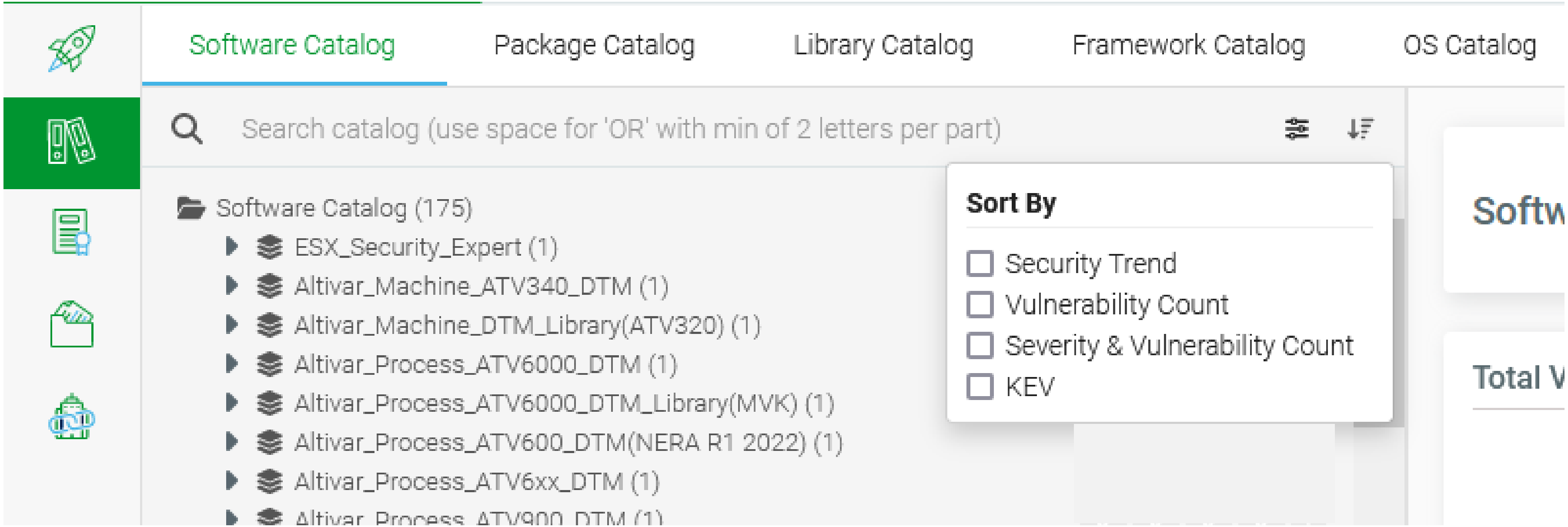
CPCERT

BU Vulnerability Handler

Global Security Lab

BU- CERT Leader

BU CS&Q

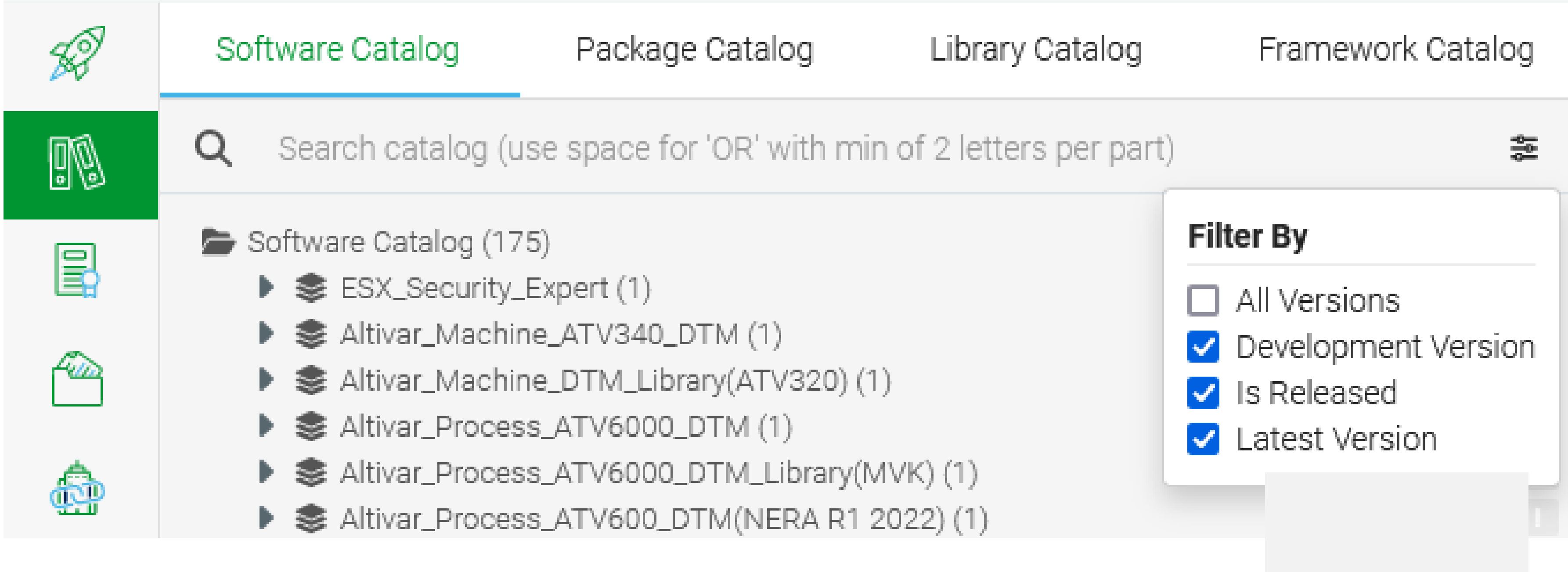


Software Catalog (175)

- ESX_Security_Expert (1)
- Altivar_Machine_ATV340_DTM (1)
- Altivar_Machine_DTM_Library(ATV320) (1)
- Altivar_Process_ATV6000_DTM (1)
- Altivar_Process_ATV6000_DTM_Library(MVK) (1)
- Altivar_Process_ATV600_DTM(NERA R1 2022) (1)
- Altivar_Process_ATV6xx_DTM (1)
- Altivar_Process_ATV900_DTM (1)

Sort By

□ Security Trend
□ Vulnerability Count
□ Severity & Vulnerability Count
□ KEV



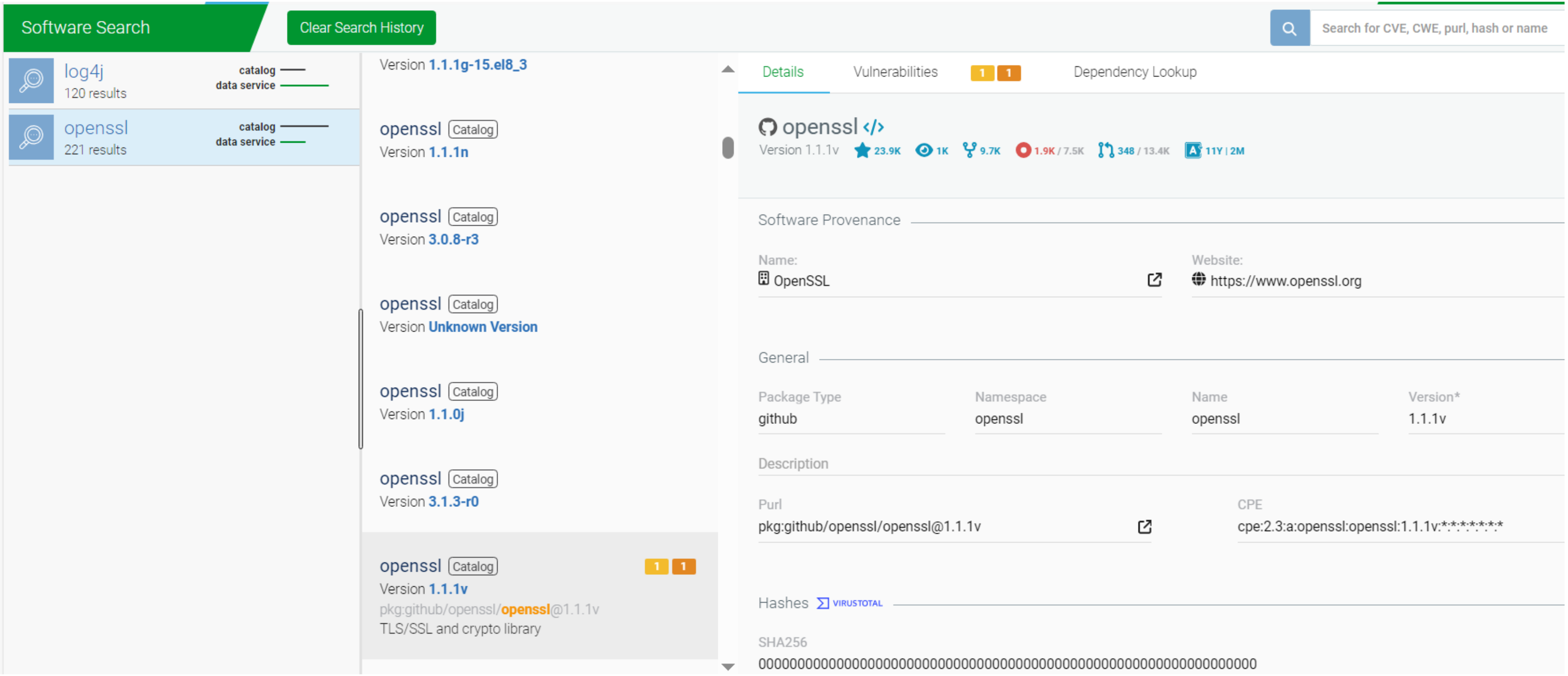
Software Catalog
Package Catalog
Library Catalog
Framework Catalog
Search catalog (use space for 'OR' with min of 2 letters per part)

Software Catalog (175)

- ESX_Security_Expert (1)
- Altivar_Machine_ATV340_DTM (1)
- Altivar_Machine_DTM_Library(ATV320) (1)
- Altivar_Process_ATV6000_DTM (1)
- Altivar_Process_ATV6000_DTM_Library(MVK) (1)
- Altivar_Process_ATV600_DTM(NERA R1 2022) (1)

Filter By

□ All Versions
☑ Development Version
☑ Is Released
☑ Latest Version



log4j
120 results
catalog
data service

openssl
221 results
catalog
data service

Version **1.1.1g-15.el8_3**

openssl Catalog
Version **1.1.1n**

openssl Catalog
Version **3.0.8-r3**

openssl Catalog
Version **Unknown Version**

openssl Catalog
Version **1.1.0j**

openssl Catalog
Version **3.1.3-r0**

openssl Catalog 1 1
Version **1.1.1v**
pkg:github/openssl/**openssl**@1.1.1v
TLS/SSL and crypto library

openssl </>
Version 1.1.1v 23.9K 1K 9.7K 1.9K / 7.5K 348 / 13.4K 11Y | 2M

Software Provenance

Name:
OpenSSL

Website:
https://www.openssl.org

General

Package Type	Namespace	Name	Version*
github	openssl	openssl	1.1.1v

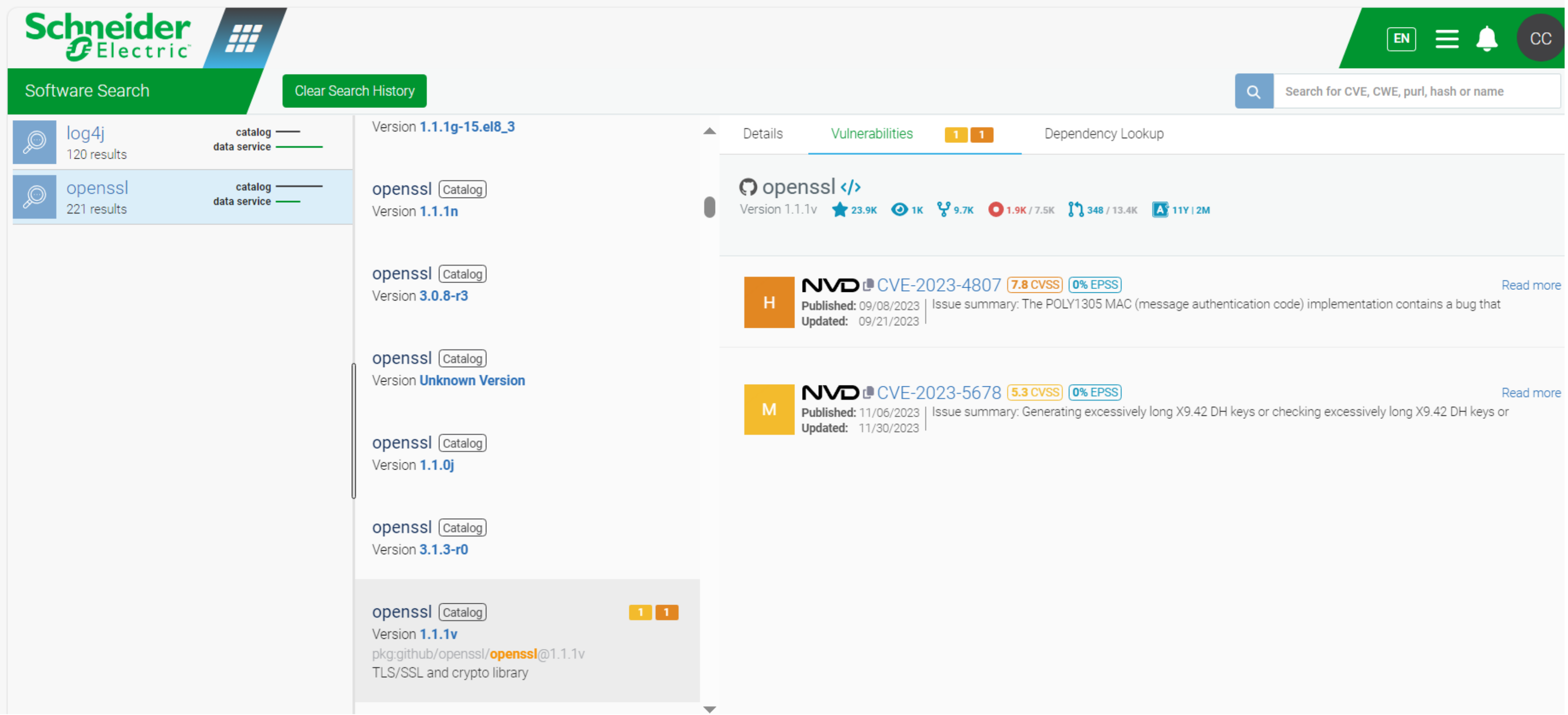
Description

Purl
pkg:github/openssl/openssl@1.1.1v

CPE
cpe:2.3:a:openssl:openssl:1.1.1v:*:*:*:*:*:*:*

Hashes VIRUSTOTAL

SHA256
0000000000000000000000000000000000000000000000000000000000000000



log4j
120 results
catalog
data service

openssl
221 results
catalog
data service

Version 1.1.1g-15.el8_3

openssl Catalog
Version 1.1.1n

openssl Catalog
Version 3.0.8-r3

openssl Catalog
Version Unknown Version

openssl Catalog
Version 1.1.0j

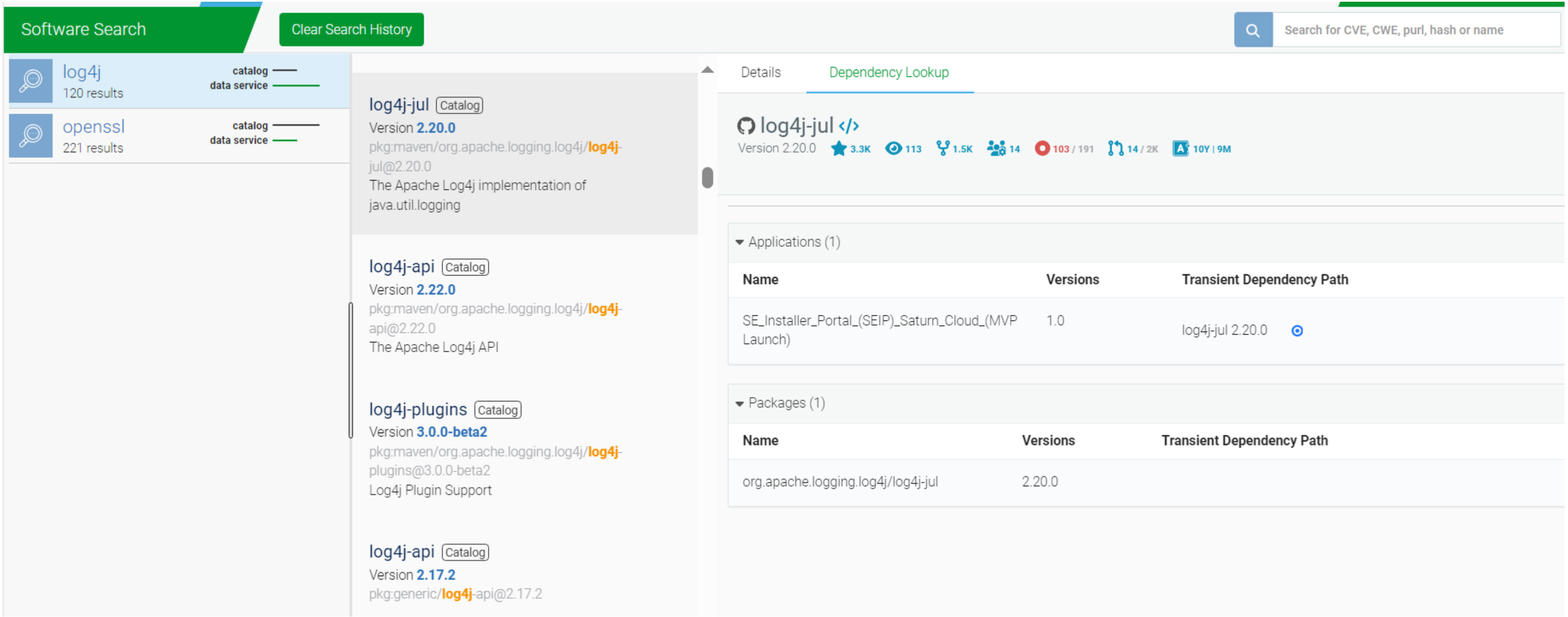
openssl Catalog
Version 3.1.3-r0

openssl Catalog 1 1
Version 1.1.1v
pkg:github/openssl/openssl@1.1.1v
TLS/SSL and crypto library

openssl </>
Version 1.1.1v 23.9K 1K 9.7K 1.9K / 7.5K 348 / 13.4K 11Y | 2M

H NVD CVE-2023-4807 7.8 CVSS 0% EPSS
Published: 09/08/2023
Updated: 09/21/2023
Issue summary: The POLY1305 MAC (message authentication code) implementation contains a bug that

M NVD CVE-2023-5678 5.3 CVSS 0% EPSS
Published: 11/06/2023
Updated: 11/30/2023
Issue summary: Generating excessively long X9.42 DH keys or checking excessively long X9.42 DH keys or



log4j
120 results
catalog
data service

openssl
221 results
catalog
data service

log4j-jul Catalog
Version 2.20.0
pkg:maven/org.apache.logging.log4j/log4j-jul@2.20.0
The Apache Log4j implementation of java.util.logging

log4j-api Catalog
Version 2.22.0
pkg:maven/org.apache.logging.log4j/log4j-api@2.22.0
The Apache Log4j API

log4j-plugins Catalog
Version 3.0.0-beta2
pkg:maven/org.apache.logging.log4j/log4j-plugins@3.0.0-beta2
Log4j Plugin Support

log4j-api Catalog
Version 2.17.2
pkg:generic/log4j-api@2.17.2

log4j-jul </>
Version 2.20.0 ★ 3.3K 113 1.5K 14 103 / 191 14 / 2K 10Y | 9M

Applications (1)

Name	Versions	Transient Dependency Path
SE_Installer_Portal_(SEIP)_Saturn_Cloud_(MVP Launch)	1.0	log4j-jul 2.20.0 ⊙

Packages (1)

Name	Versions	Transient Dependency Path
org.apache.logging.log4j/log4j-jul	2.20.0	

Summary and Q&A

Summary of our SBOM Journey

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

Strengths

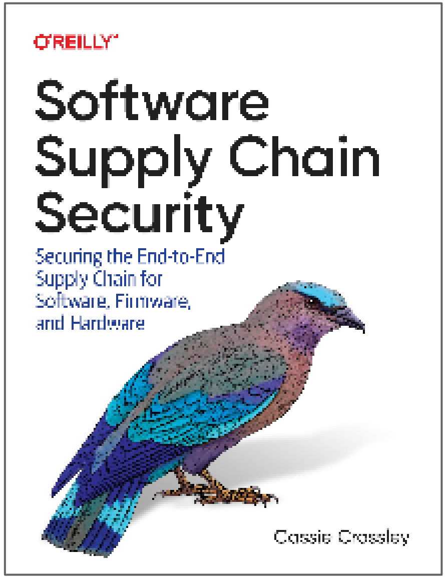
- 4000+ SBOMs for internal products
- Valuable learnings and **improved speed** to generate security notices by leveraging SBOMs during Log4j, OpenSSL, and other critical open-source CVEs
- Increased **awareness** in R&D teams regarding third party dependencies
- Stronger transparency and **trust** with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



O'REILLY

Software Supply Chain Security

Securing the End-to-End Supply Chain for Software, Firmware, and Hardware

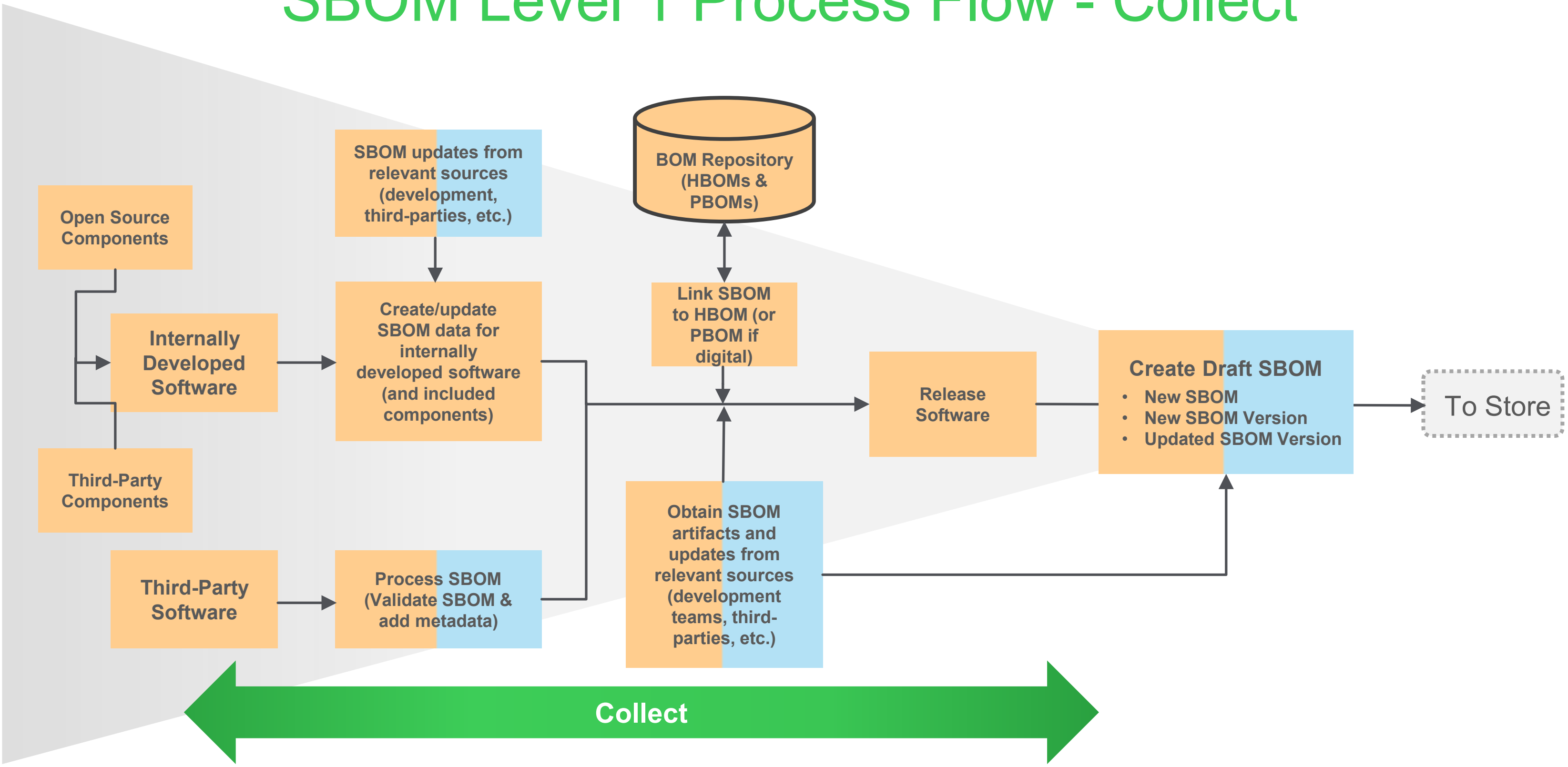
Cassie Crossley

Life Is On

Schneider Electric

Appendix

SBOM Level 1 Process Flow - Collect



Open Source Components

Internally Developed Software

Third-Party Components

Third-Party Software

SBOM updates from relevant sources (development, third-parties, etc.)

Create/update SBOM data for internally developed software (and included components)

Process SBOM (Validate SBOM & add metadata)

BOM Repository (HBOMs & PBOMs)

Link SBOM to HBOM (or PBOM if digital)

Obtain SBOM artifacts and updates from relevant sources (development teams, third-parties, etc.)

Release Software

Create Draft SBOM
- New SBOM
- New SBOM Version
- Updated SBOM Version

To Store

Collect

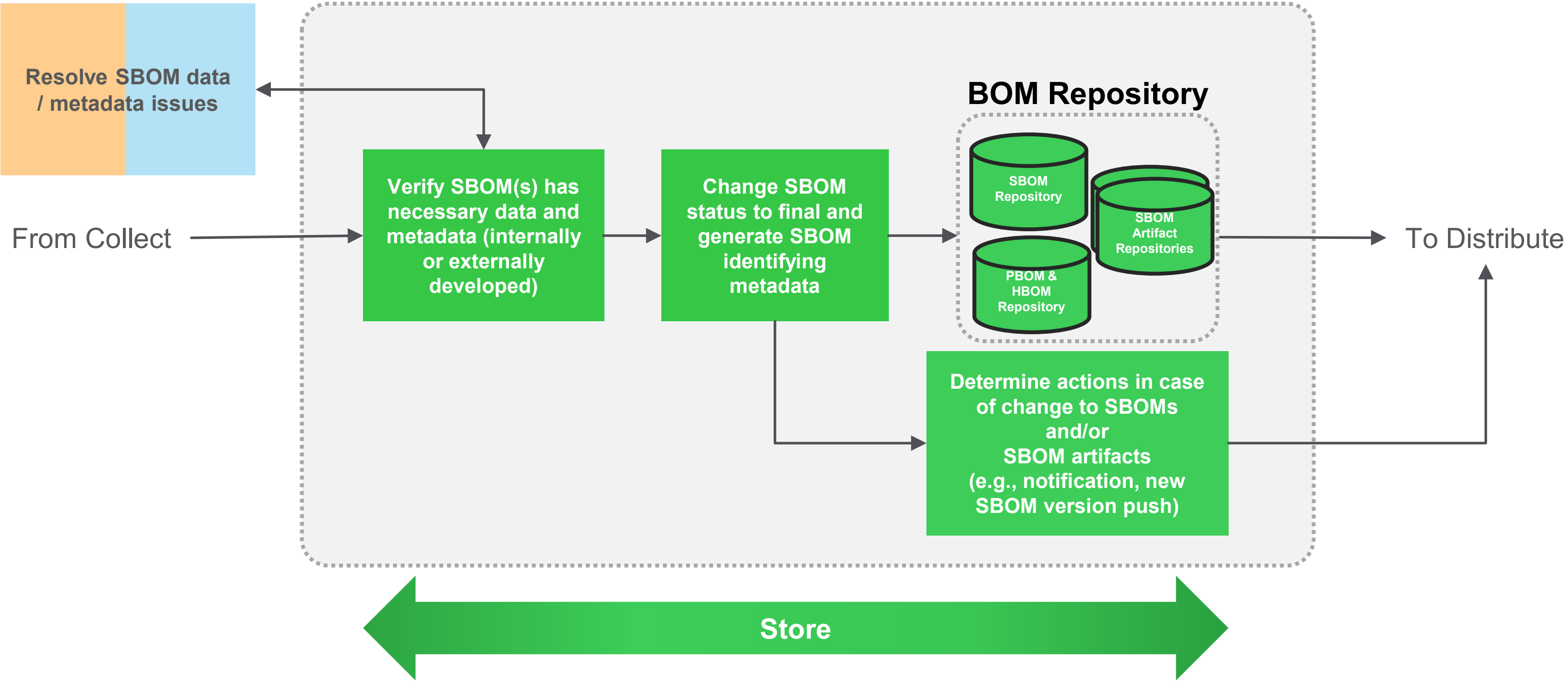
● SBOM Consumer

🟩 Schneider Electric SBOM Solution

▨ Schneider Electric Product Teams

▨ Schneider Electric Non-IT Users

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
BOM Repository
SBOM Repository
SBOM Artifact Repositories
PBOM & HBOM Repository
To Distribute
Determine actions in case of change to SBOMs and/or SBOM artifacts (e.g., notification, new SBOM version push)
Store

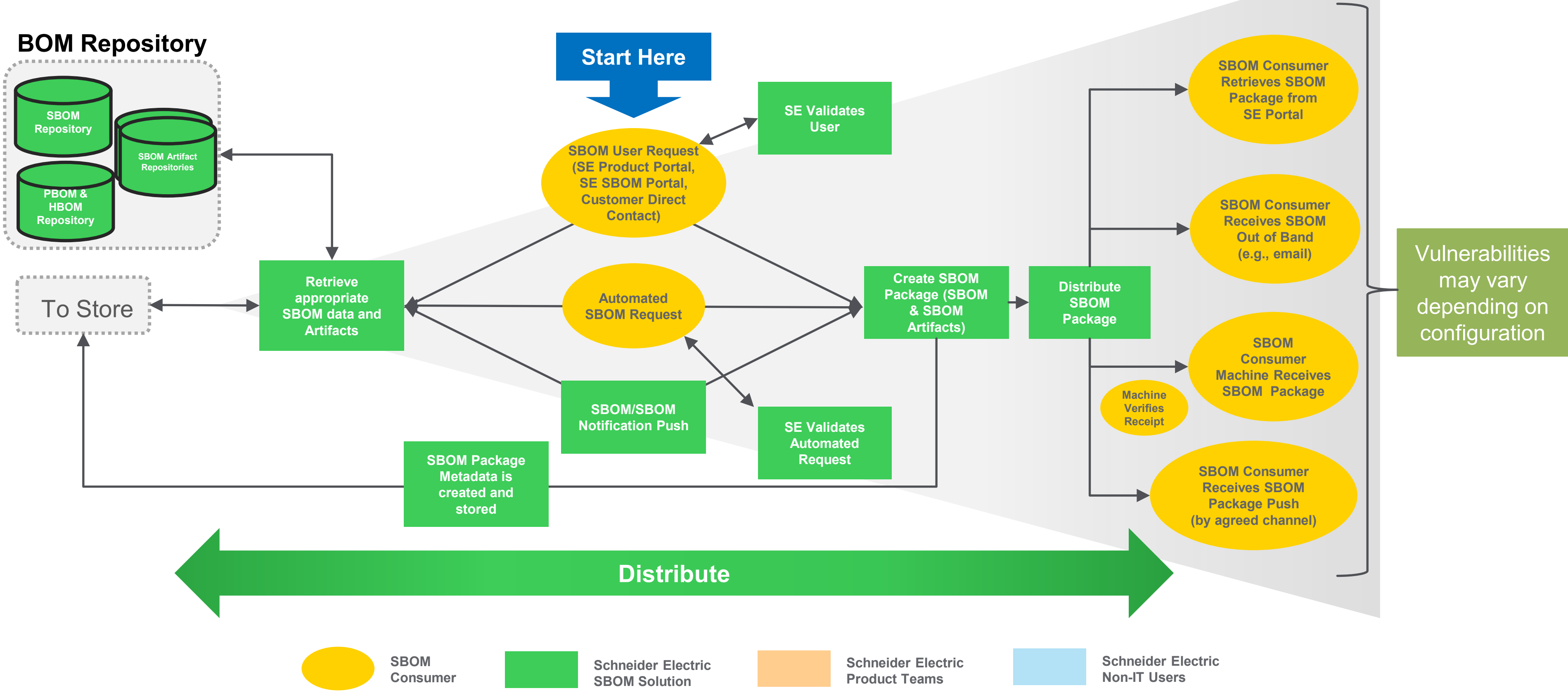
● SBOM Consumer

🟩 Schneider Electric SBOM Solution

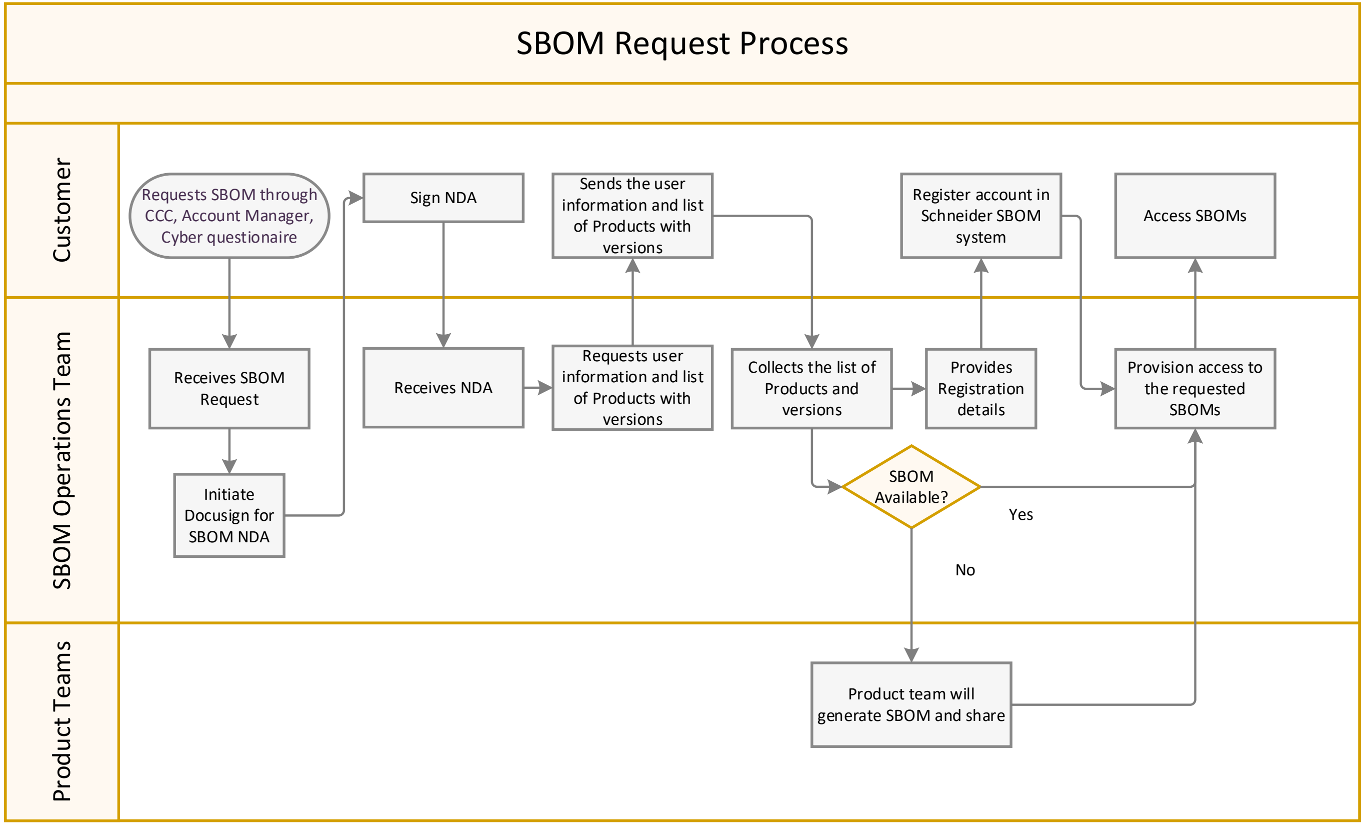
🟧 Schneider Electric Product Teams

🟦 Schneider Electric Non-IT Users

SBOM Level 1 Process Flow - Distribute

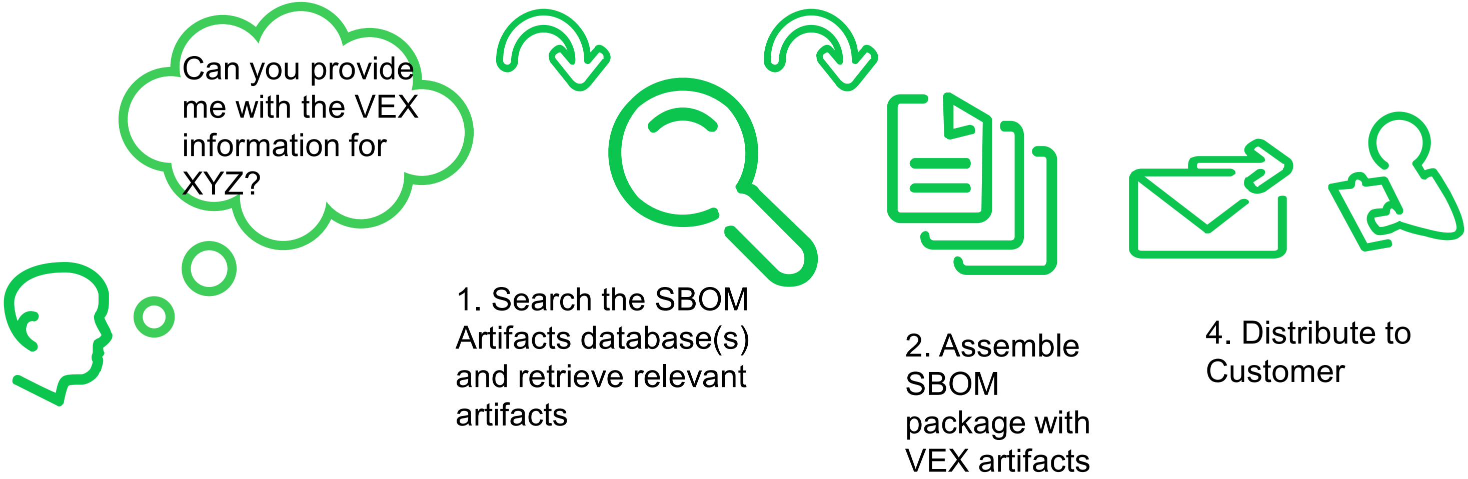

BOM Repository
SBOM Repository
SBOM Artifact Repositories
PBOM & HBOM Repository
To Store
Start Here
SBOM User Request (SE Product Portal, SE SBOM Portal, Customer Direct Contact)
SE Validates User
Retrieve appropriate SBOM data and Artifacts
Automated SBOM Request
SBOM/SBOM Notification Push
SE Validates Automated Request
SBOM Package Metadata is created and stored
Create SBOM Package (SBOM & SBOM Artifacts)
Distribute SBOM Package
SBOM Consumer Retrieves SBOM Package from SE Portal
SBOM Consumer Receives SBOM Out of Band (e.g., email)
SBOM Consumer Machine Receives SBOM Package
Machine Verifies Receipt
SBOM Consumer Receives SBOM Package Push (by agreed channel)
Vulnerabilities may vary depending on configuration
Distribute
SBOM Consumer
Schneider Electric SBOM Solution
Schneider Electric Product Teams
Schneider Electric Non-IT Users

Customer Request: Internal SBOM Process


SBOM Request Process
Customer
SBOM Operations Team
Product Teams
Requests SBOM through CCC, Account Manager, Cyber questionaire
Sign NDA
Sends the user information and list of Products with versions
Register account in Schneider SBOM system
Access SBOMs
Receives SBOM Request
Receives NDA
Requests user information and list of Products with versions
Collects the list of Products and versions
Provides Registration details
Provision access to the requested SBOMs
Initiate Docusign for SBOM NDA
SBOM Available?
Yes
No
Product team will generate SBOM and share

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