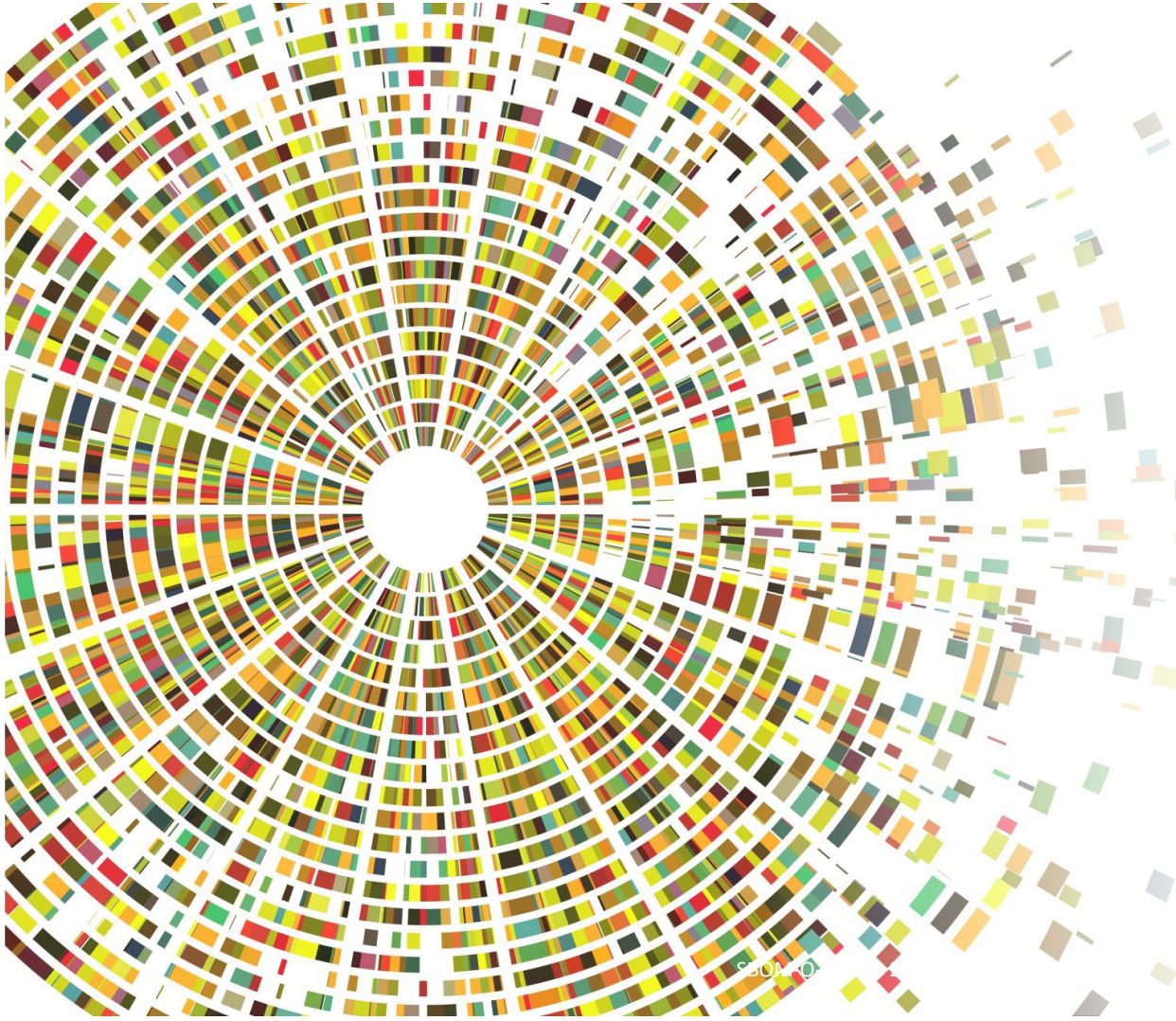


SBOM

Software Bill of Materials

Healthcare Proof of Concept WG

Healthcare SBOM POC

- Established as part of NTIA Software Transparency Effort
- Focus on defining SBOM best practices for Healthcare

Investigate 2018-2019	Exercised primary use cases in creating & ingesting SBOMs for risk management Proved the actionable value of component transparency to the consumer
Iterate 2020-2021	More participants, more use cases, more devices, more data, more tools Proved the viability of standard formats, data, tools Created How-To Guide for SBOM Generation
Integrate 2022 - now	Drive adoption, expanded participation; real-world scenarios & data Vulnerability Exploitability Exchange (VEX), End-to-End workflow Automate SBOM sharing

Current Healthcare SBOM POC Activities

Producing VEX Companion Content for an SBOM

- Focus on **vulnerabilities** in a component **that do Not Impact** the Medical Device (Not Affected)
- Areas of investigation
  - Minimize Software Identification challenges
  - What Vulnerabilities require VEX statements
  - The Role of Cybersecurity Risk Severity Scores
  - Required content for producing VEX statements
- Identify gaps/areas needing further investigation

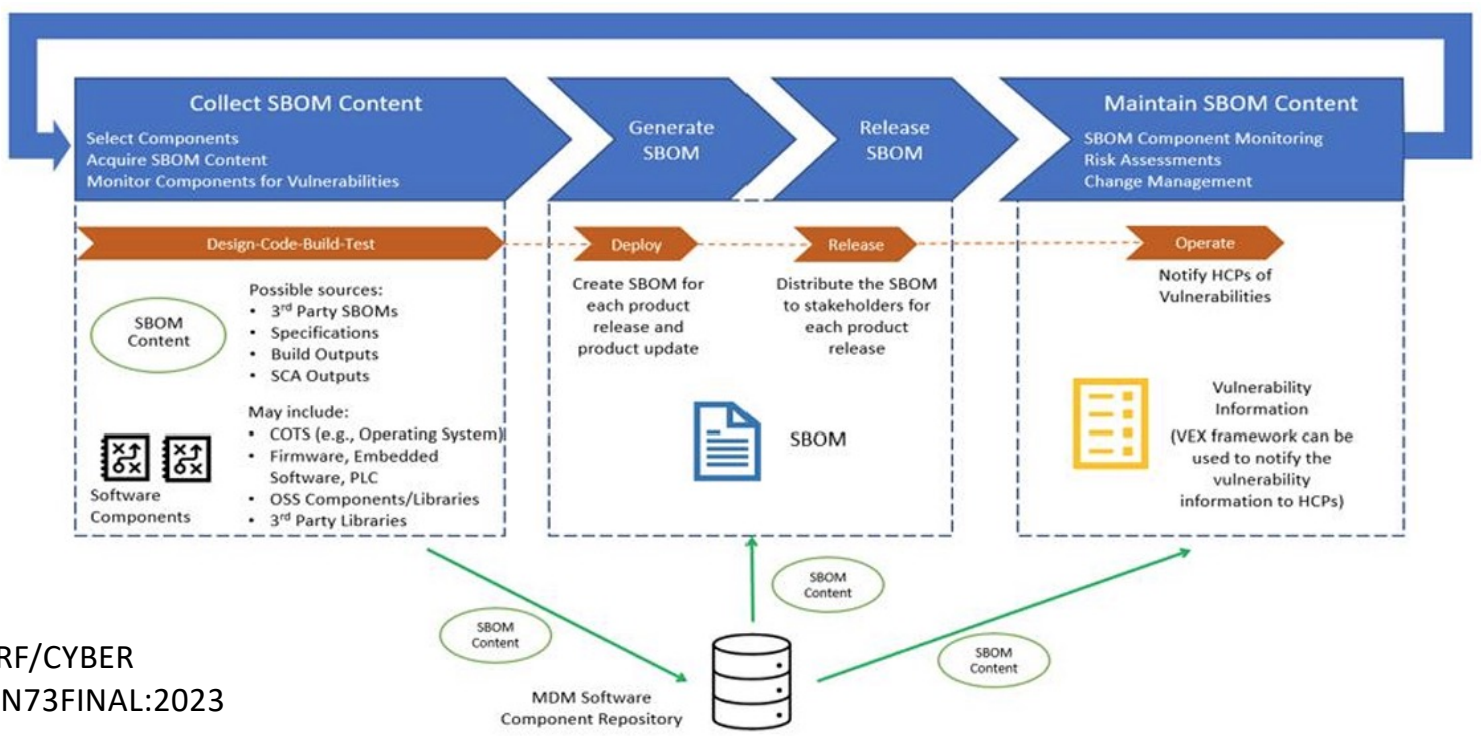
Evaluate end-to-end generation, sharing, consumption, and usage of SBOM/VEX content

SBOM Content Sharing

- Initial approach was controlled access via a shared folder
- Collaborating with H-ISAC on sharing through a central repository

Introducing Health-ISAC SBOM Repository

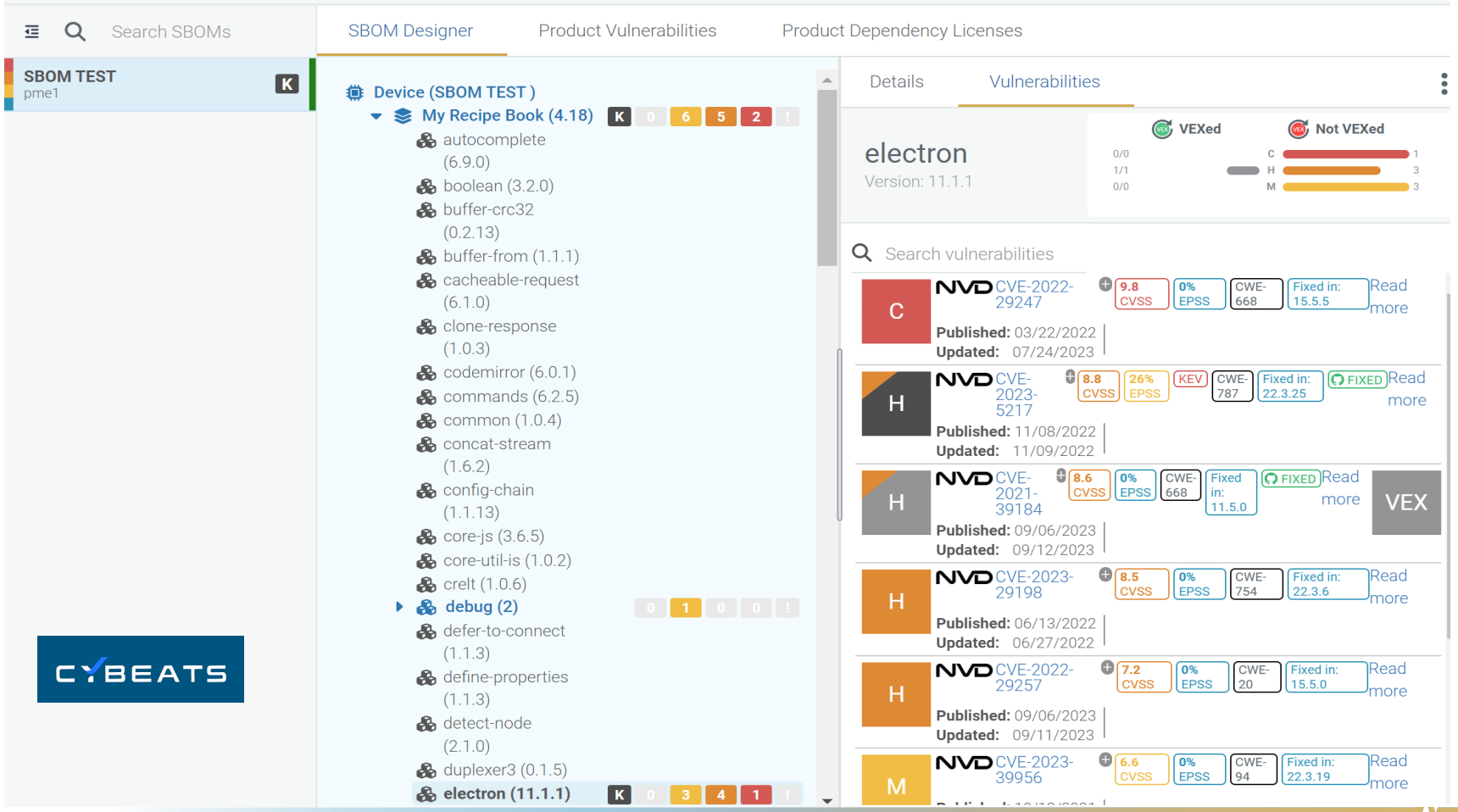
1. 1st of its' kind SBOM repository
2. Improve software transparency
3. Fee-free access for HDO staff (members & non-members)
4. FDA "Manufacturers should provide or make available SBOM information to users on a continuous basis."
5. MDMs can upload and share SBOMs with customers
6. MDMs manage customer's (SBOM users) access
7. Two MDM Use cases
    1. MDM uploads and publishes SBOMs
    2. MDM uploads SBOMs and leverages SBOM Studio correction and enrichment functionality before publishing
8. SBOM studio refreshes CVE correlation hourly



IMDRF/CYBER WG/N73FINAL:2023

Figure 2: SBOM management across the software development life cycle (SDLC)

SBOM Studio - High-Level Architecture


Search SBOMs
SBOM Designer
Product Vulnerabilities
Product Dependency Licenses
SBOM TEST
pme1
Device (SBOM TEST)
My Recipe Book (4.18)
autocomplete (6.9.0)
boolean (3.2.0)
buffer-crc32 (0.2.13)
buffer-from (1.1.1)
cacheable-request (6.1.0)
clone-response (1.0.3)
codemirror (6.0.1)
commands (6.2.5)
common (1.0.4)
concat-stream (1.6.2)
config-chain (1.1.13)
core-js (3.6.5)
core-util-is (1.0.2)
crelt (1.0.6)
debug (2)
defer-to-connect (1.1.3)
define-properties (1.1.3)
detect-node (2.1.0)
duplexer3 (0.1.5)
electron (11.1.1)
Details
Vulnerabilities
electron
Version: 11.1.1
VEXed
Not VEXed
Search vulnerabilities
CVE-2022-29247
CVE-2023-5217
CVE-2021-39184
CVE-2023-29198
CVE-2022-29257
CVE-2023-39956
VEX
CYBEATS