
timesys

5 Hacks For SBOM Management Mitigate Medical Device Security Risk

SECURITY SERIES

Al Feczko
Timesys Corporation

timesys

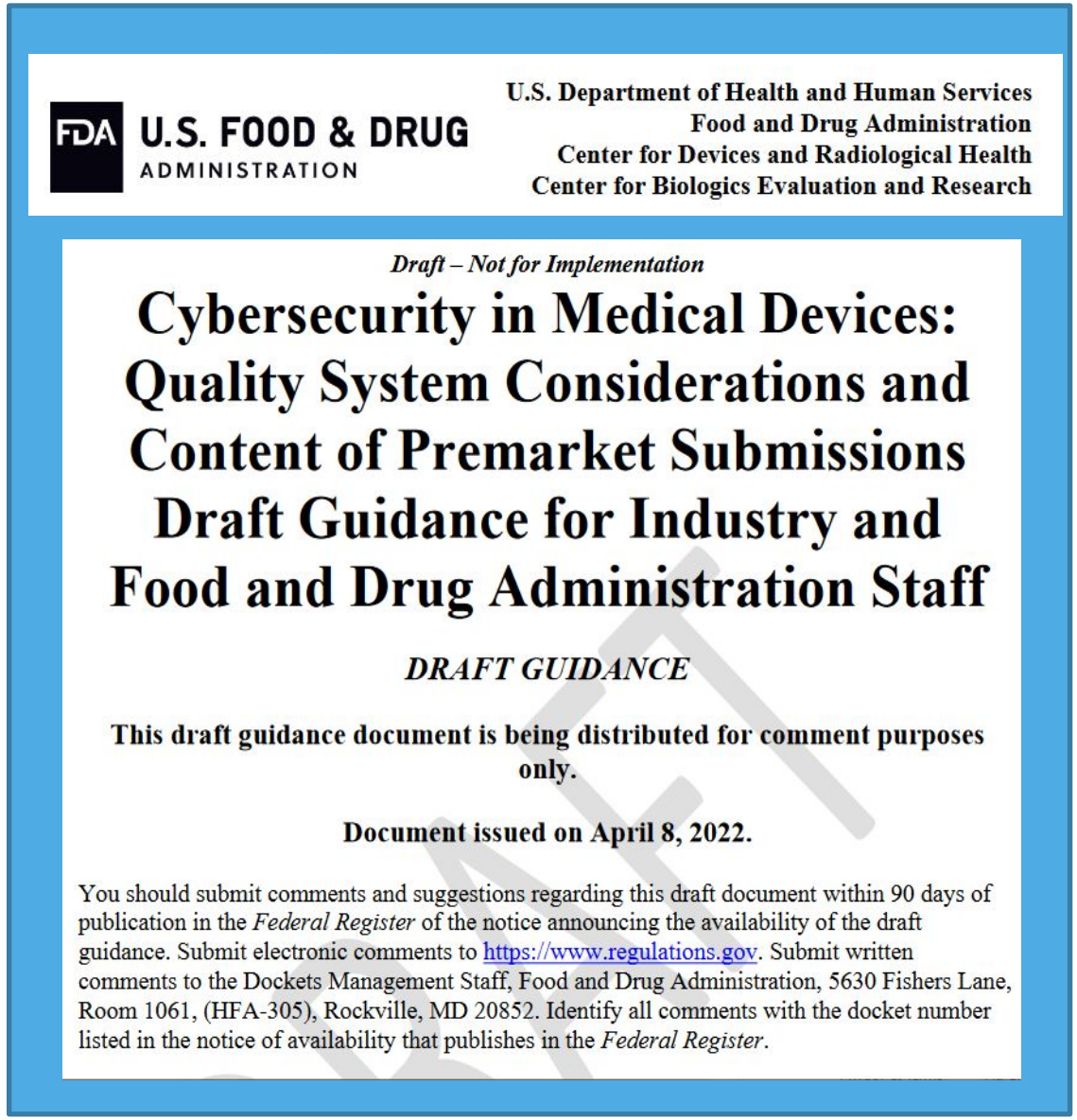
FDA CYBERSECURITY GUIDANCE FOR PREMARKET SUBMISSIONS – UPDATED APRIL 2022

General Principles

- Cybersecurity part of device safety & quality
- Designing for Security is critical
  - Authenticity
  - Authorization
  - Availability
  - Confidentiality
  - Secure and timely updatability and patchability
- Guidelines for transparency & documentation
  - Labeling and User Manuals
  - Vulnerability Management Plan & SBOMs

Use an SPDF (Secure Product Development Framework) to Manage Cyber Risks

- Threat modeling
- Third Party Software Components
- Security Assessment & Risk Management



U.S. FOOD & DRUG ADMINISTRATION

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Center for Biologics Evaluation and Research

Draft – Not for Implementation

Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Draft Guidance for Industry and Food and Drug Administration Staff

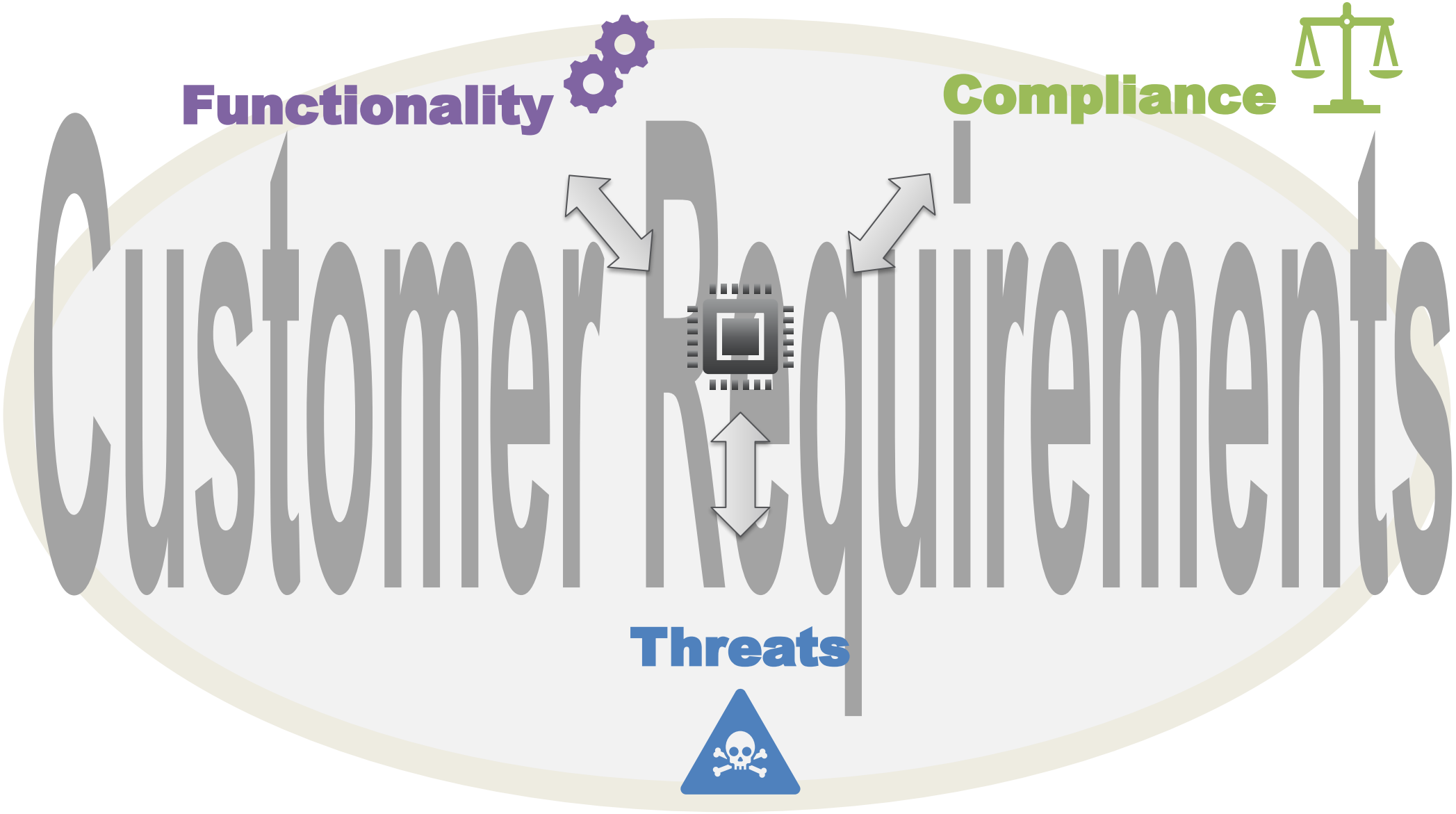
DRAFT GUIDANCE

This draft guidance document is being distributed for comment purposes only.

Document issued on April 8, 2022.

You should submit comments and suggestions regarding this draft document within 90 days of publication in the *Federal Register* of the notice announcing the availability of the draft guidance. Submit electronic comments to https://www.regulations.gov. Submit written comments to the Dockets Management Staff, Food and Drug Administration, 5630 Fishers Lane, Room 1061, (HFA-305), Rockville, MD 20852. Identify all comments with the docket number listed in the notice of availability that publishes in the *Federal Register*.

PRODUCT FORCING FUNCTIONS

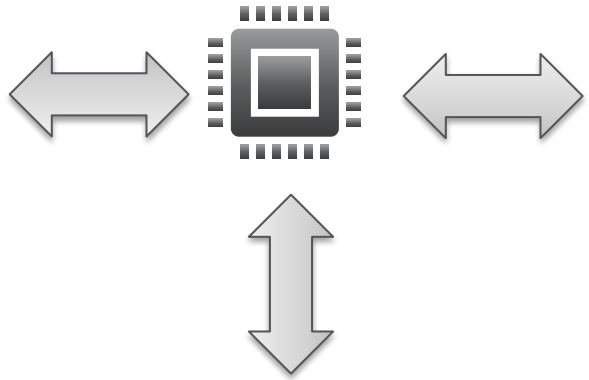


(TECHNICAL) FUNCTIONALITY

Increased attention !

- Product Complexity
- Re-use/modularization
- Quality/Technical Debt
- Feature Completeness

Cost-efficiency and time-to-market are limiting factors



COMPLIANCE

- Legislation/Regulation
- Standards/Certification
- Licensing of open source and external proprietary SW
- Licensing and sales contracts towards customers/partners

! Increased attention

Product compliance is essential

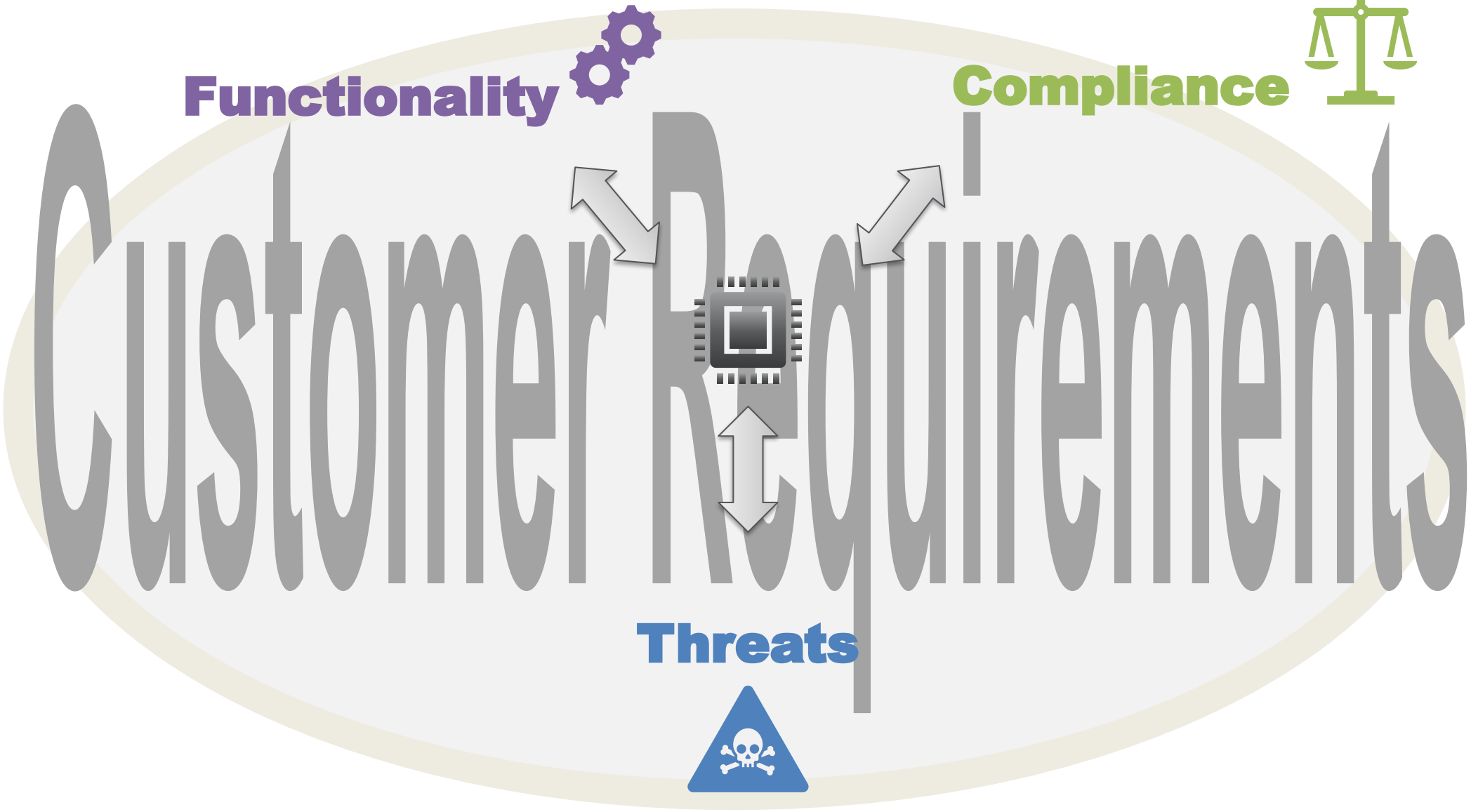
THREATS

- Increasing number of Supply-Chain attacks
- Growing surface for potential attacks
- Managing vulnerability of (sub-)components

! Increased attention

Mitigations required

Do you know what is in your software?



AGENDA

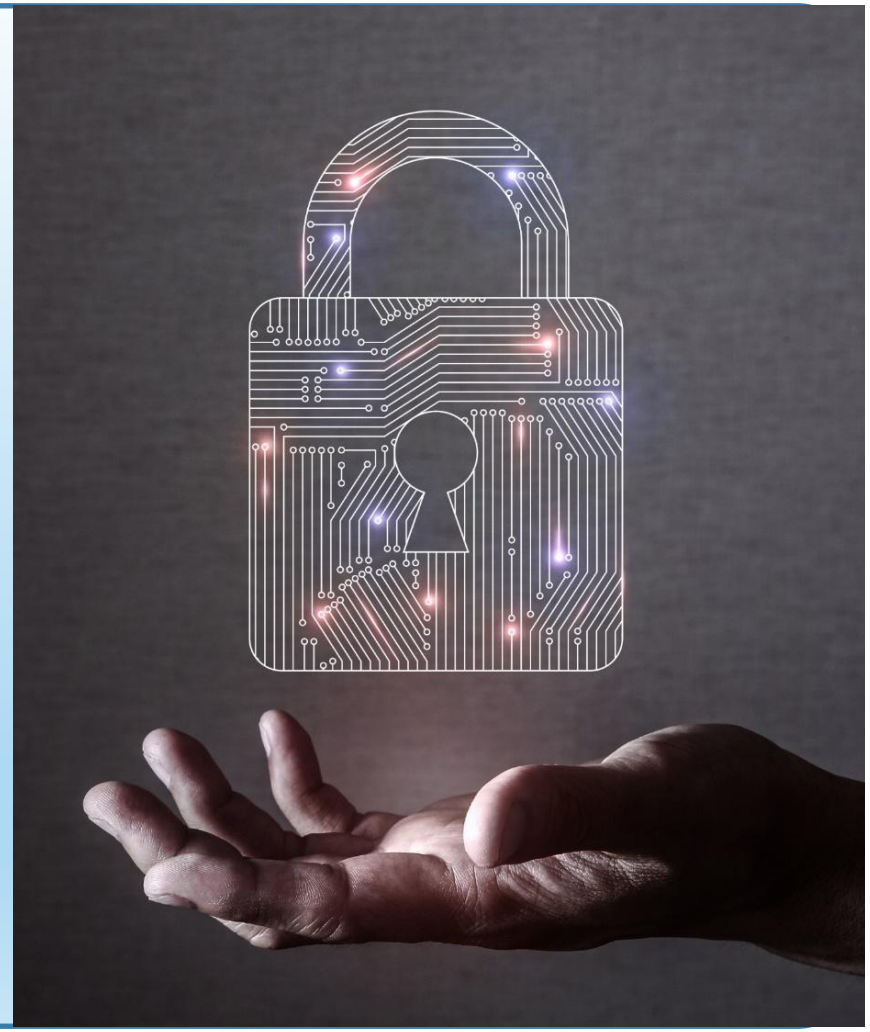
Software Bill of Materials

SBOM standards

Automating SBOM generation

Monitoring SBOM for Security Vulnerabilities

Integrating tools with the engineering process

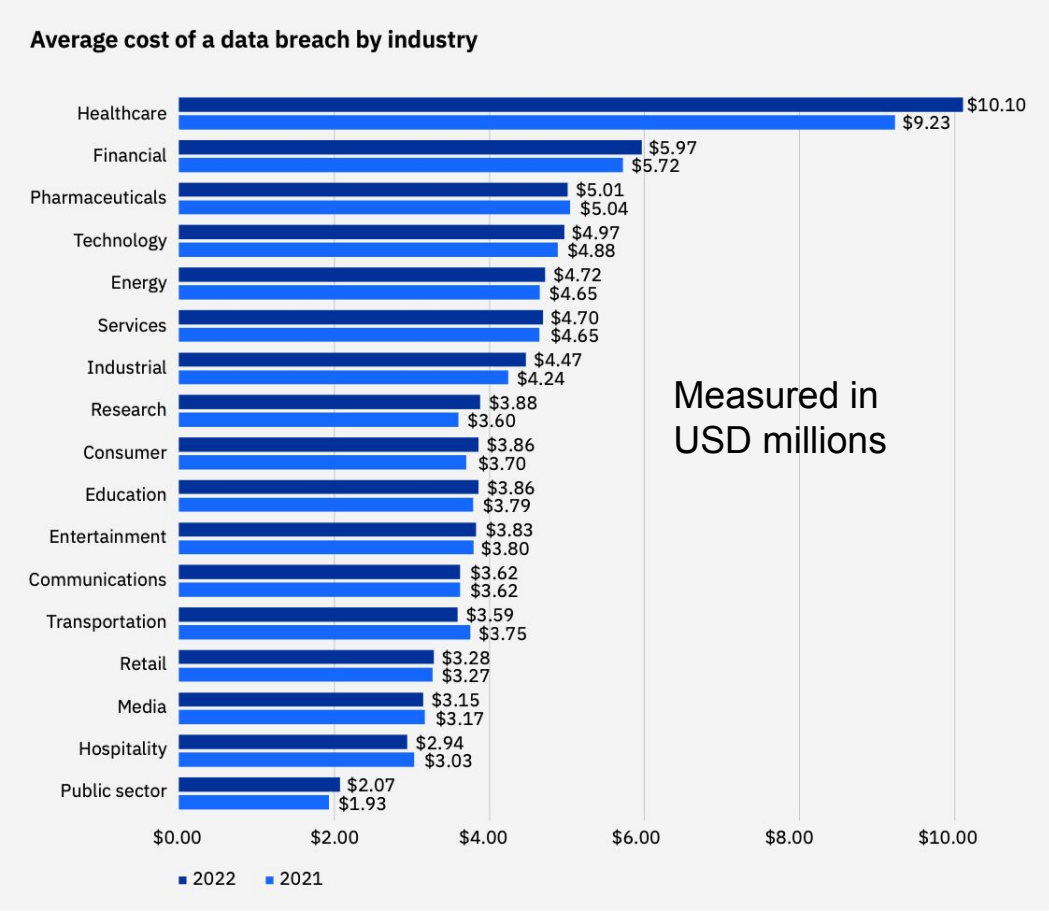


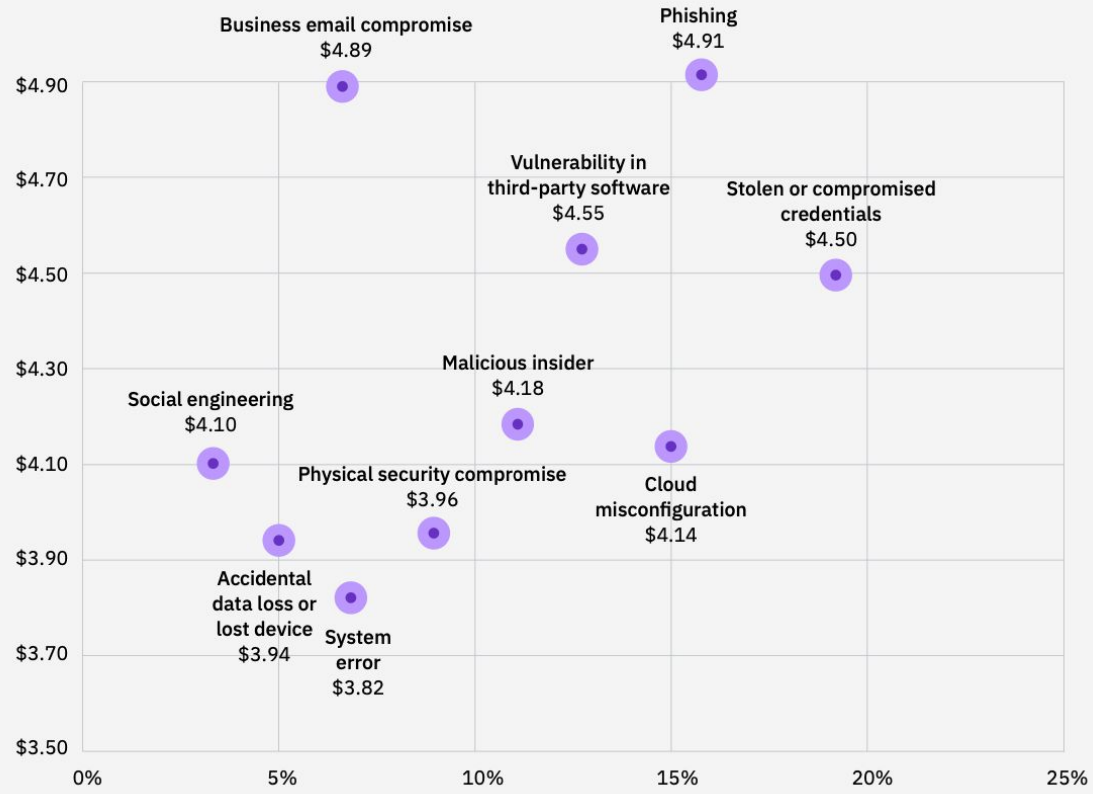
“Security is not our highest priority…

We will look into it later…”

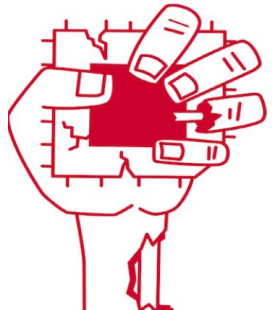
… after an incident??

WHY SHOULD YOU CARE – AND NOW, NOT LATER!!





Source: IBM – Cost of Data Breach 2022 Report



timesys

WHERE WILL ATTACKERS FOCUS THEIR EFFORTS?

🔮 **55.7 billion connected IoT devices; 80B ZB data**

📱 **embedded products = larger and more vulnerable attack surface**

🔒 **air gaps can't provide adequate security** – for critical data

Good news and bad news

👍 Attacks focused on **widely used/downloaded packages** – which are not installed on most *properly designed* embedded systems

👎 As IT systems gets harder to attack, **hackers will focus on devices**


Hack #1
use monetary and reputation risk
to secure the budget that you need
to proactively deal with the problem
timesys

2008 Gartner report on the state of *open source software*:

"if you don't think you use it, then you use it; and

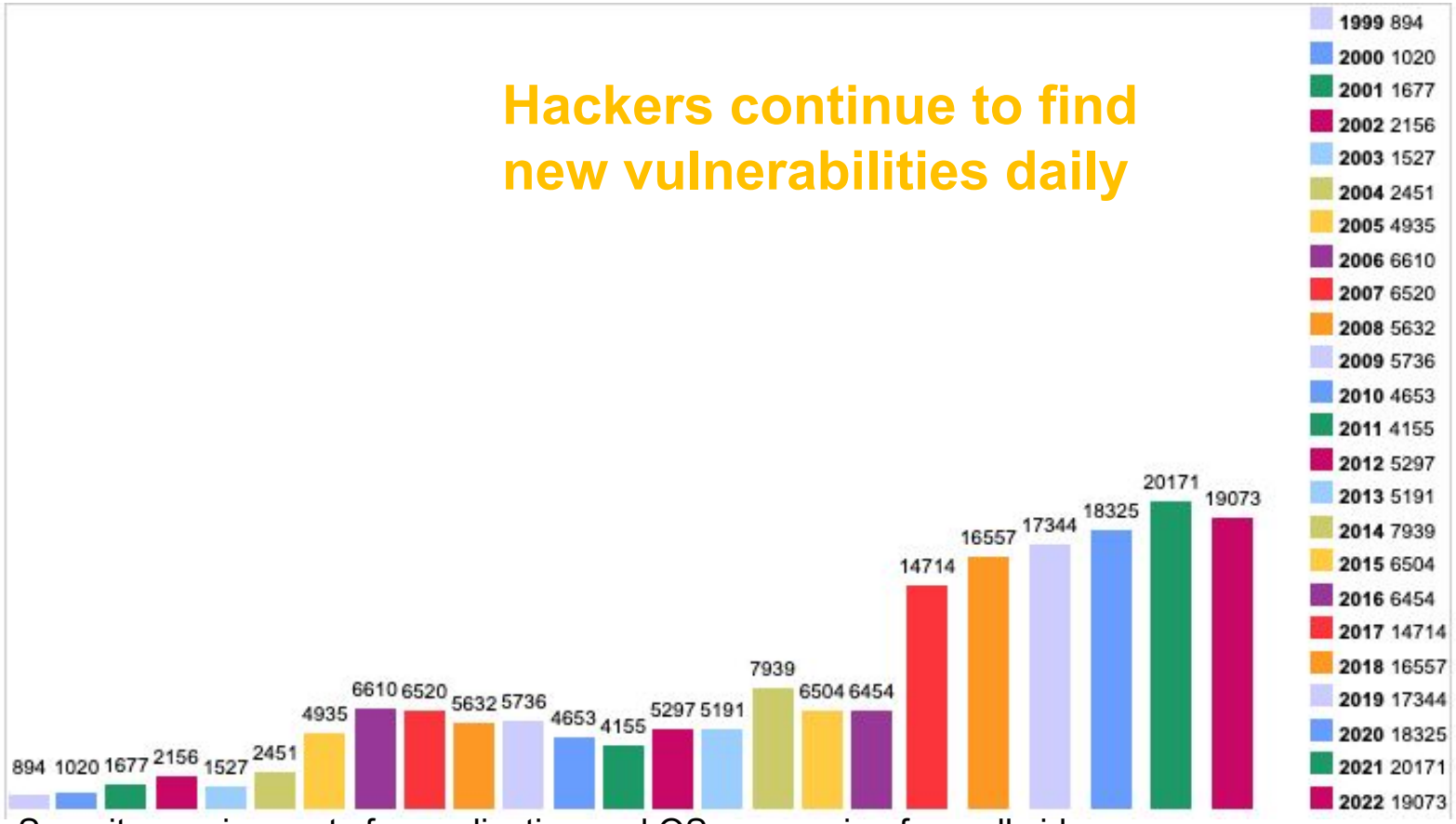
if you think you do use it, then you use lots more of it than you know."

The Hidden & Exponential Challenges of Dependencies:

- direct: libraries code is directly calling into
- transitive: libraries that your dependencies are linked against (dependencies of dependencies)

Example: sqlite requires dependencies like readline & zlib; readline requires glibc & ncurses, etc.

DEVICE SECURITY AND MAINTENANCE IS KEY



Reported vulnerabilities
> 19,000 in 2022
(avg > 350 per week)

Source: cvedetails.com

Security requirements for application and OS are coming from all sides

- End device users are reporting problems
- You need to meet industry compliance requirements
- Your company has internal cybersecurity guidelines

WHAT DO I NEED TO KNOW?

What products do I have?

What software do I have in my products?

Which software comes from suppliers?

What are the known issues with my product software?

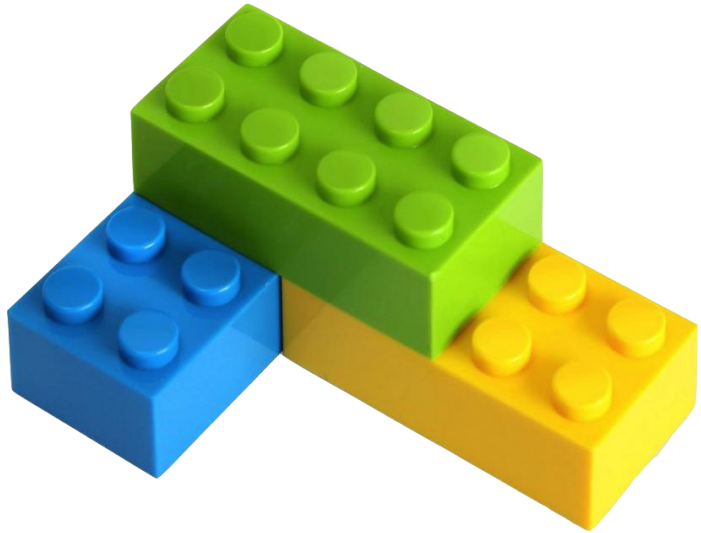
What are mitigation measures?


Hack #2
Understand and Validate
Provenance and Integrity of Your Software Components
timesys

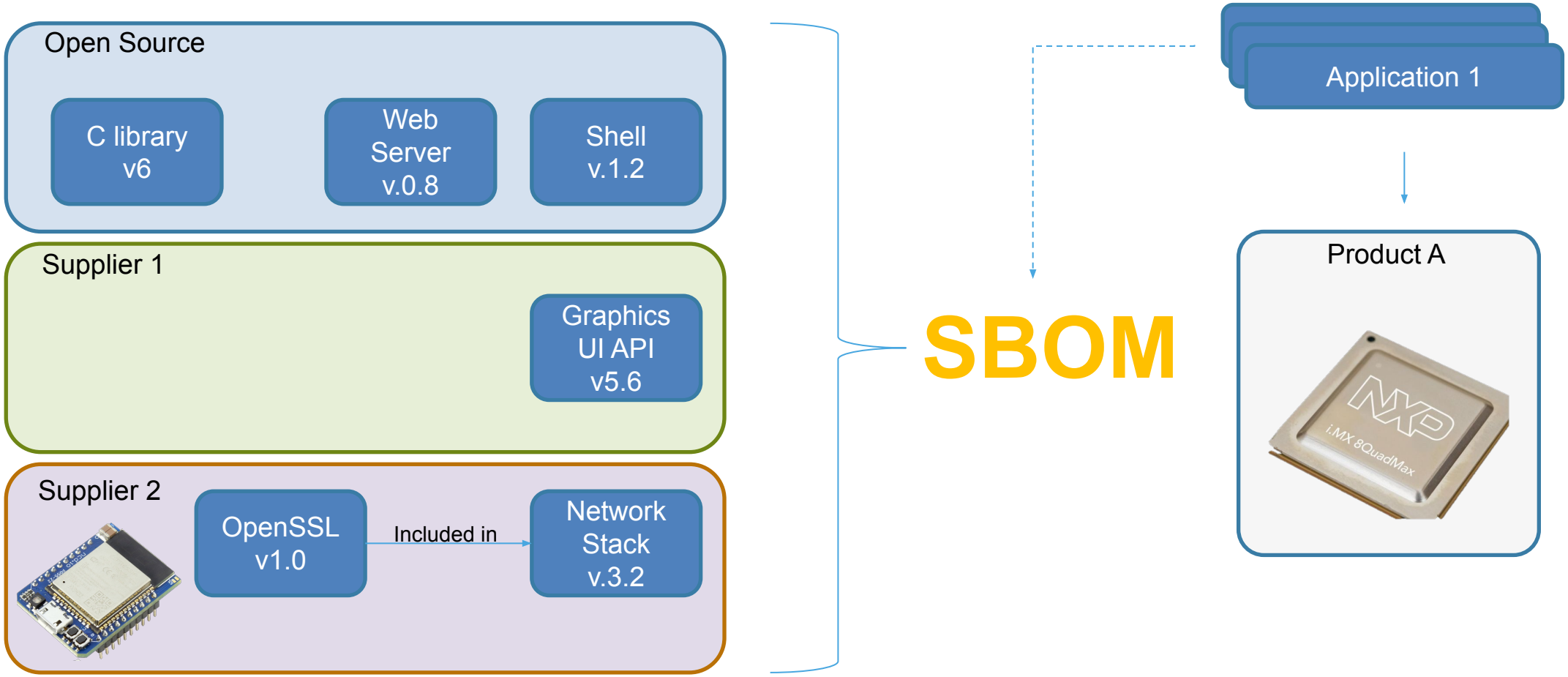
- Start with a “vetted” release
- Verify signatures, or, at a minimum, verify hash
- Other Recommendations:
  - Have commit signing as a mandatory configuration.
  - Enable static code scanning and open source scanning across your repositories.
  - Before any software is updated, run the changes through a code checking review and signing process by another party; this can guard against unintentional oversights and insider threats.

PRIORITY 1 – KNOW WHAT SOFTWARE RUNS IN YOUR PRODUCTS!

- Would you eat something that you don't recognize? (maybe ☺)
  - We like to know the ingredients
- Historically, all products know their Hardware **Bill of Materials**
  - Determines large chunk of the product cost
  - Helps with business decisions
- Increasing number of products are build from other hardware/software components
  - How do we know what we are getting?



WHAT SOFTWARE IS IN YOUR PRODUCT?



DEFINES SBOM

Section 4 Excerpts: Enhancing Software Supply Chain Security

- NTIA defines the “minimum elements” of SBOM
- Commerce and USG defines guidance on providing a purchaser a Software Bill of Materials for each product

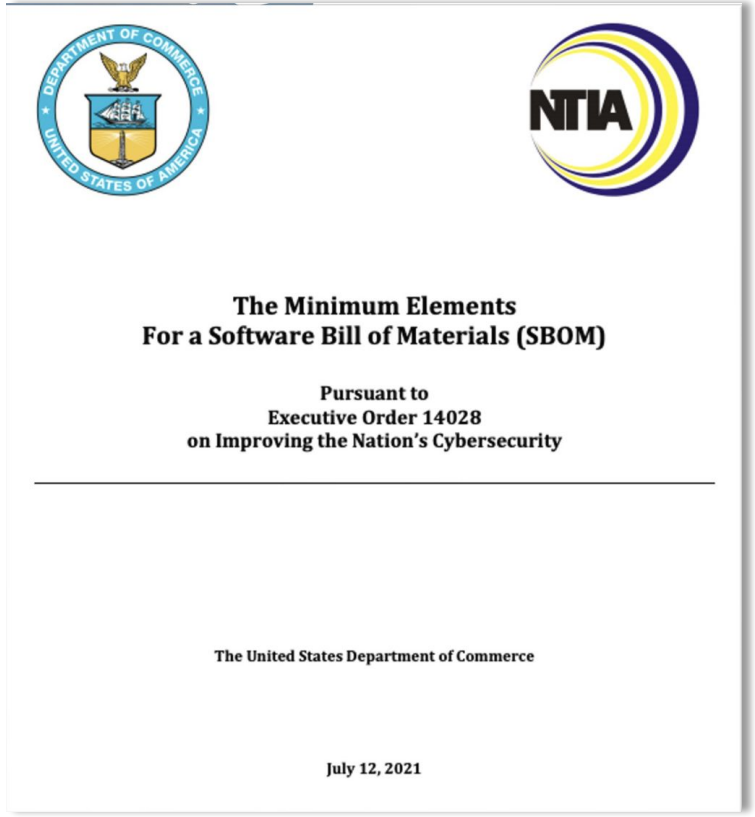
THE WHITE HOUSE

BRIEFING ROOM

Executive Order on Improving the Nation’s Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

(e) Within 90 days of publication of the preliminary guidelines pursuant to subsection (c) of this section, the Secretary of Commerce acting through the Director of NIST, in consultation with the heads of such agencies as the Director of NIST deems appropriate, shall issue guidance identifying practices that enhance the security of the software supply chain. Such guidance may incorporate the guidelines published pursuant to subsections (c) and (i) of this section. Such guidance shall include standards, procedures, or criteria regarding:



The Minimum Elements For a Software Bill of Materials (SBOM)

Pursuant to Executive Order 14028 on Improving the Nation’s Cybersecurity

The United States Department of Commerce

July 12, 2021

WHERE IS SBOM AFTER THE EXECUTIVE ORDER?

- Multiple standards emerged as leaders for SBOM
  - SPDX (http://spdx.dev)
  - CycloneDX (http://cyclonedx.org)
  - SWID (https://www.iso.org/standard/65666.html)
- Standards drive sharing and exchanging
- Multiple tools emerge
  - Mostly consuming SBOMs
- SBOM automation progressing slowly
- SBOMs contain multiple information and can be linked to Vulnerability Exploitability eXchange (VEX) data

Hack #3

Start Small

timesys

MINIMUM SBOM INFORMATION ACCORDING TO NTIA

Component Field	Description
Name	Software component name
Version	Installed component version
Unique identifier	Unique identifier can be a CPE, PURL, SWID. All identifier formats have their own specifications for the way an identifier is generated, so organizations must choose the format that's right for their business.
Relationship with other dependencies	Brief description of the way the component interacts with the software, including if it interacts with other dependencies
Developer name	Individual's name or business name of the developer that created the component
Author of SBOM data	The individual or company/tool that generated the SBOM
Document Creation Date/Time	timestamp for when the SBOM document was generated

Component Identity Matters!

SBOM STANDARDS

	CycloneDX	SPDX	SWID
Supported by	OWASP	Linux Foundation	NIST
Format Standard	No standard format, but OWASP defines specifications.	ISO/IEC 5962:2021	ISO/IEC 19770-2:2015
Unique Identifiers Supported	SWID, CPE, PURL	CPE, PURL	SWID
Target Audience	Developers and security teams	Developers and administrators	Governments and developers working for governments
Output formats supported	json, xml, protobuf	xls, rdf, json, yml	xml

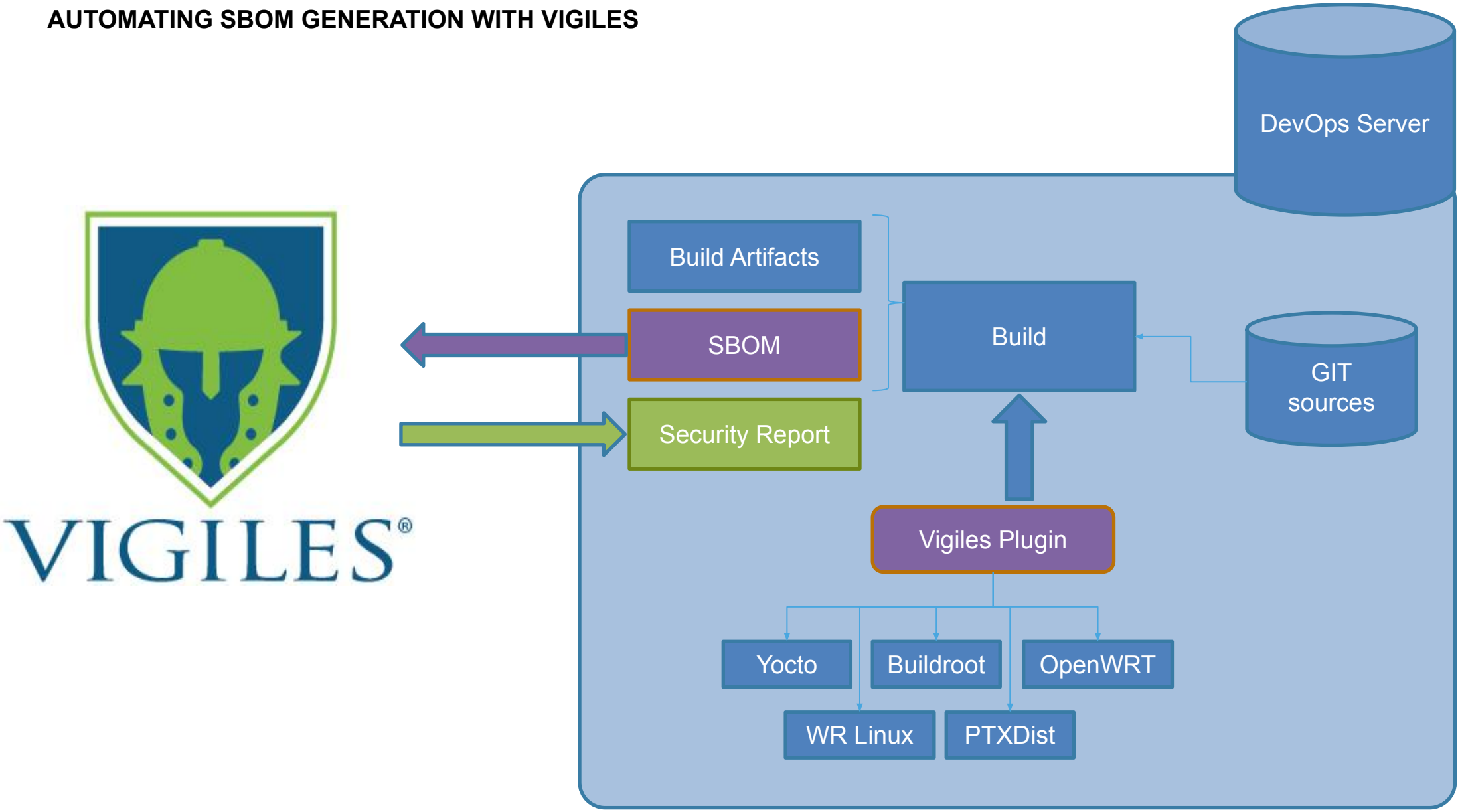
STANDARDS EXAMPLES

```
{
  "bomFormat": "CycloneDX",
  "specVersion": "1.4",
  "serialNumber": "urn:uuid:3e671687-395b-41f5-a30f-a58921a69b79",
  "version": 1,
  "components": [
    {
      "type": "application",
      "name": "Acme Application",
      "version": "9.1.1",
      "cpe": "cpe:/a:acme:application:9.1.1",
      "swid": {
        "tagId": "swidgen-242eb18a-503e-ca37-393b-cf156ef09691_9.1.1",
        "name": "Acme Application",
        "version": "9.1.1",
        "text": {
          "contentType": "text/xml",
          "encoding": "base64",
          "content": "PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0idXRmLTgiID8+
        }
      }
    },
```

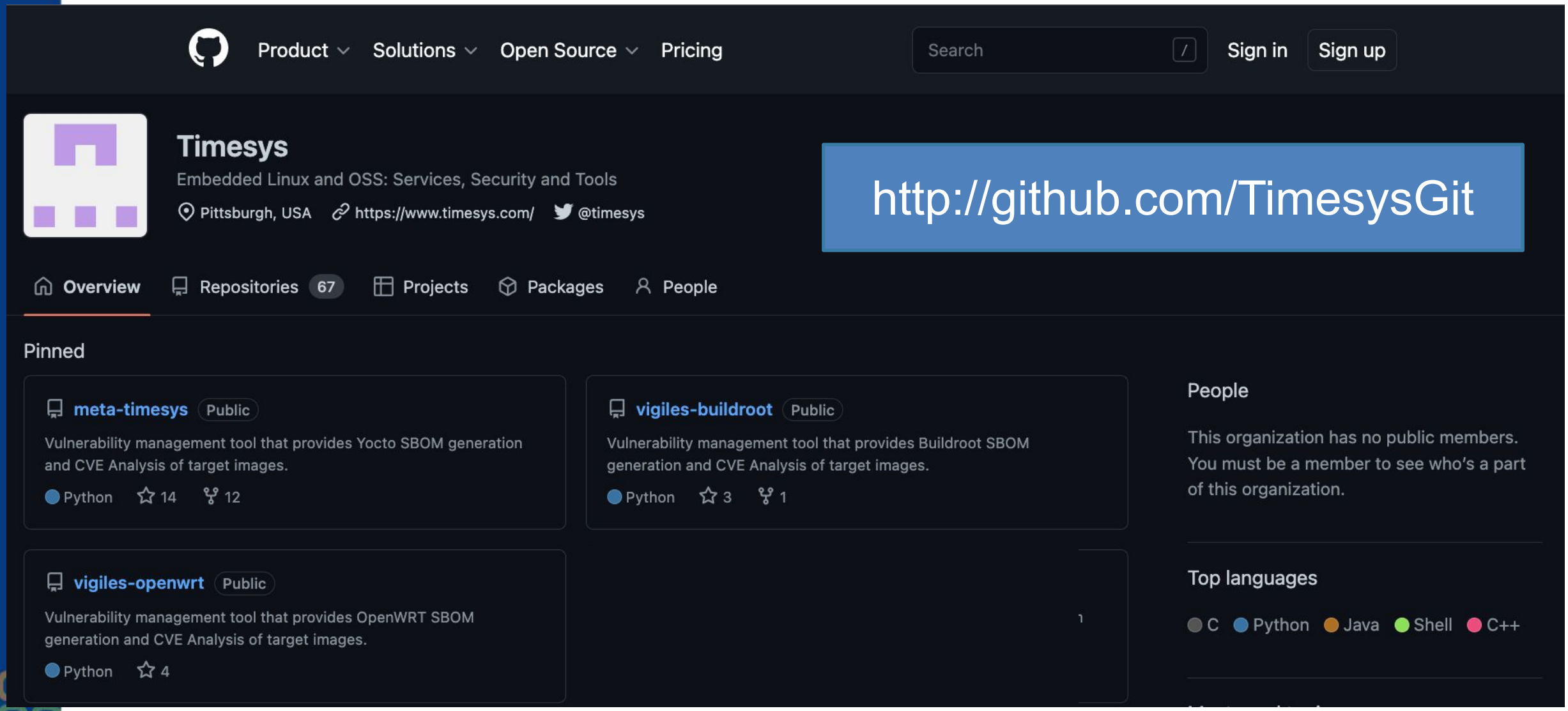
```
SPDXVersion: SPDX-2.2
DataLicense: CC0-1.0
SPDXID: SPDXRef-DOCUMENT
DocumentName: imx-image-core
DocumentNamespace:
https://linuxlink.timesys.com/vigiles/spdxdocs/imx-image-core-18044d5f-999d-4
94c-a6e9-c399b57f41a9
LicenseListVersion: 3.13
Creator: Organization: Timesys Corporation
Creator: Tool: VigilesManifestExporter-1.0
Created: 2022-05-03T19:08:38Z
CreatorComment: <text>This document was auto-generated by
VigilesManifestExporter tool.</text>

PackageName: busybox
SPDXID: SPDXRef-busybox-1.33.1
PackageVersion: 1.33.1
PackageDownloadLocation:
https://busybox.net/downloads/busybox-1.33.1.tar.bz2;name=tarball
FilesAnalyzed: false
PackageLicenseConcluded: NOASSERTION
PackageLicenseDeclared: GPLv2 AND bzip2-1.0.4
PackageCopyrightText: NOASSERTION
ExternalRef: SECURITY cpe23Type
cpe:2.3:a:busybox:busybox:1.33.1:*:*:*:*:*:*:*
PackageSupplier: Organization: OpenEmbedded ()
```


Hack #4
Automate!
Integrate SBOM tools into your CI/CD pipelines
timesys

AUTOMATING SBOM GENERATION WITH VIGILES



VIGILES PLUGINS ARE ON GITHUB



VIGILES®

- Vigiles generates:
  - an SBOM in SPDX format
  - a license manifest
  - a list of vulnerability patches that have been applied
  - a list of vulnerabilities that have been triaged and whitelisted
- Easily used with Yocto Project, Buildroot, and OpenWRT
  - e.g., Yocto metalayer (https://github.com/TimesysGit/meta-timesys)

```
RELEASE=krogoth
git clone https://github.com/TimesysGit/meta-timesys.git -b
$RELEASE
```

GENERATING AN SBOM FROM YOCTO PROJECT WITH VIGILES

VIGILES®

Step 1: Configure your Yocto build for scanning with Vigiles (in conf/local.conf)

```
INHERIT += "vigiles"
VIGILES_KEY_FILE = "/tools/timesys/linuxlink_key"
```

Step 2: Run the scan

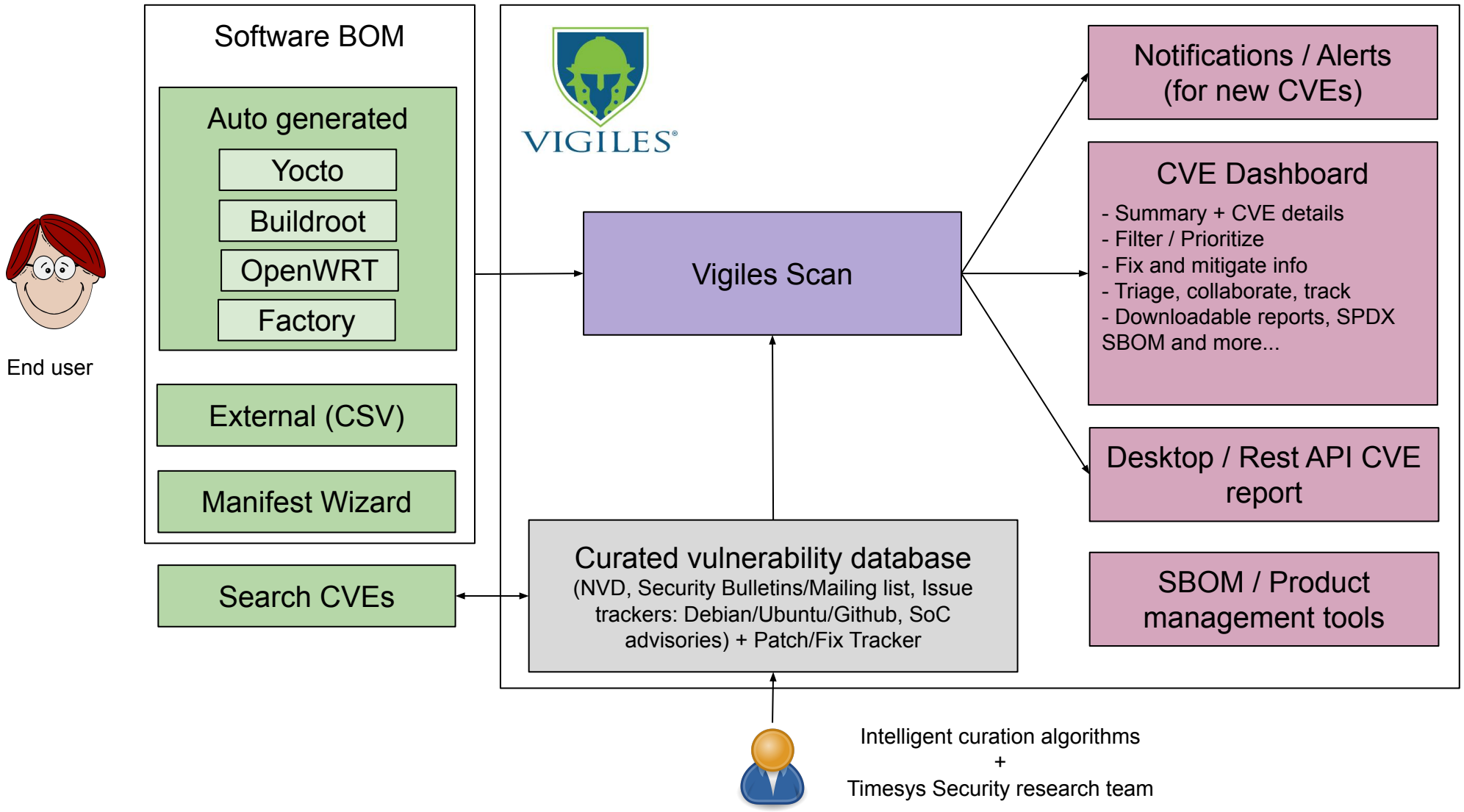
```
$ bitbake -c vigiles_check core-image-minimal
```

Step 3: Look at the report locally

Step 4: Look at the details, analyze and triage using Vigiles online UI


Hack #5
Use a curated database
timesys

VIGILES HIGH-LEVEL ARCHITECTURE OVERVIEW



ATTACK SURFACE VS. DATE LAST UPDATED

2019

sqlite3	3.14.2	3	7	5	0	0
busybox	1.26.2	2	13	3	0	0
lighttpd	1.4.45	1	1	0	0	0
zlib	1.2.11	0	1	0	0	0
dropbear	2019.77	0	1	0	0	0
light_httpd	1.4.45	0	0	0	0	0

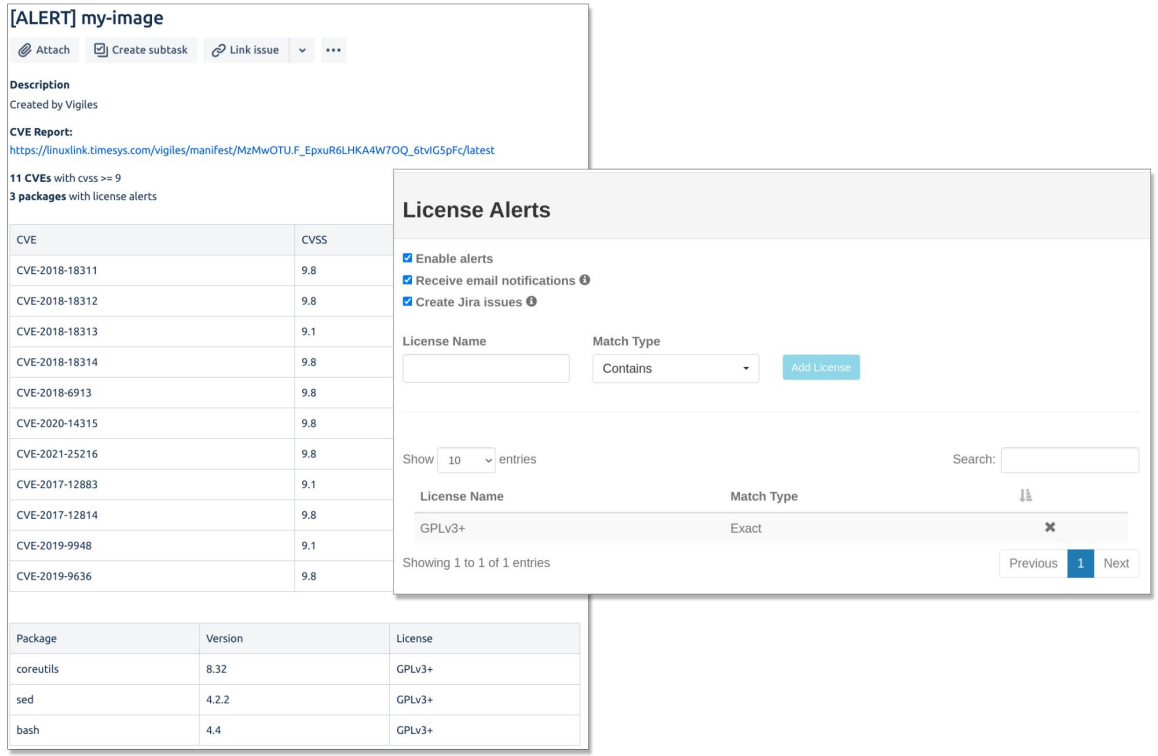
Updated in 2022

busybox	1.35	1	0	0	0	0
dropbear	2022.82	0	0	0	0	0
light_httpd	1.4.64	0	0	0	0	0
lighttpd	1.4.64	0	0	0	0	0
sqlite3	3.38.2	0	0	0	0	0
zlib	1.2.12	0	0	0	0	0

NOTIFICATIONS AND ALERTS

- **Notifications** - allow you to stay on-top of new vulnerabilities reported for already uploaded SBOMs.
  - Email sent with vulnerability digest
  - Selectable cadence: Daily, Weekly, Monthly

- **Policy violation alerts**
  - CVEs exceeding CVSS score threshold — alert on specific score CVEs (e.g. high and critical)
  - Non-authorized license types — alert when new/updated software in SBOM violates company security policy
  - Raise a Jira issue for alerts to help engineering stay on-top of security issues



ENGINEERING PROCESS INTEGRATION

- Separate process possibly involving separate team

- Jira is a commonly used system for tracking issues
- Vigiles offers Jira integration
  - Automatic reporting of CVE issues as Jira issues
  - Brings visibility to security issues to engineering team
  - Becomes part of the engineering sprint planning

- Vigiles API (Python toolkit)
  - Integration with company's CI system for automation including, e.g.:
    - Create a new folder
    - Set folder name
    - Associate SBOM with release tag/version
    - Run a scan and download security report as a PDF
  - Custom dashboard for all security information in one place approach

Hackers Quick Reference Guide

Hack # 1 Use monetary and reputation risk to secure the budget that you need

Hack # 2 Understand and Validate the provenance and Integrity of Your Software Components

Hack # 3 Start Small

Hack # 4 Automate! Integrate SBOM tools into your CI/CD pipelines

Hack # 5 Use a curated database

timesys

Q&A

Timesys is a longtime embedded open source software security expert

To discuss your project or for more information
& to become more secure, please contact us at **sales@timesys.com**

Al Feczko
al.feczko@timesys.com
Timesys Corporation

THANK YOU

timesys