Not All SBOMs Are Created Equal

Jeff Williams
Co-founder and CTO
Contrast Security

March 2022

We all blindly trust software with the most important things in life

Social

Elections

Business

Power Grid

Money

Government

We have a right to know some basic security information…

Who built it?
How was it tested?
What versions of libraries are in there?
Does it have known vulnerabilities?
Etc…

“Software Bill of Materials”

SBOMs are incredibly simple.

Myths:

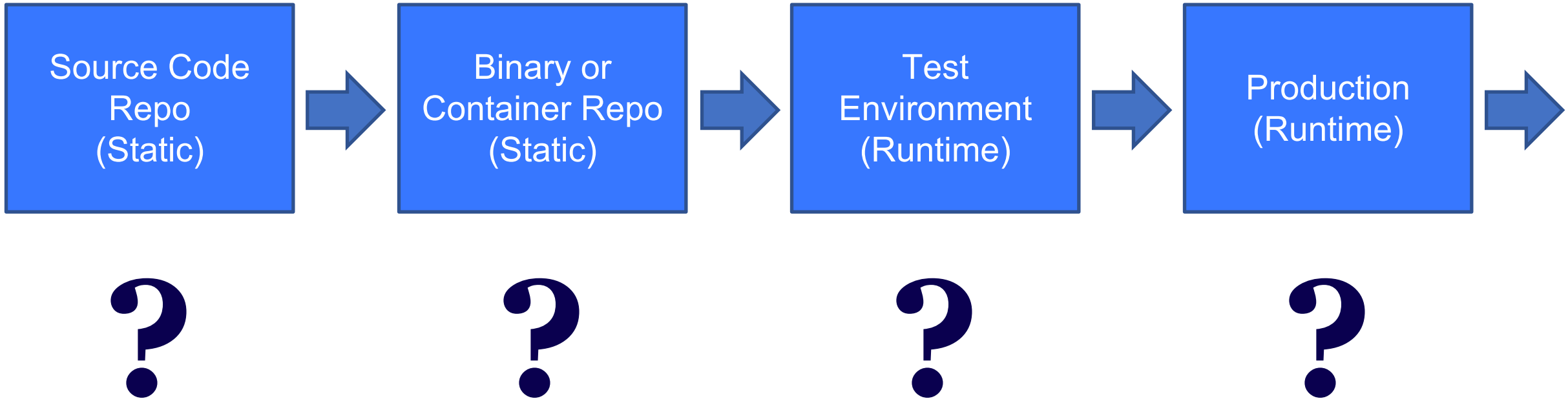
- **SBOMs help attackers - FALSE**
- **SBOMs aren’t actionable - FALSE**
- **SBOMs expose your code - FALSE**
- **SBOMs don’t scale - TBD**

…

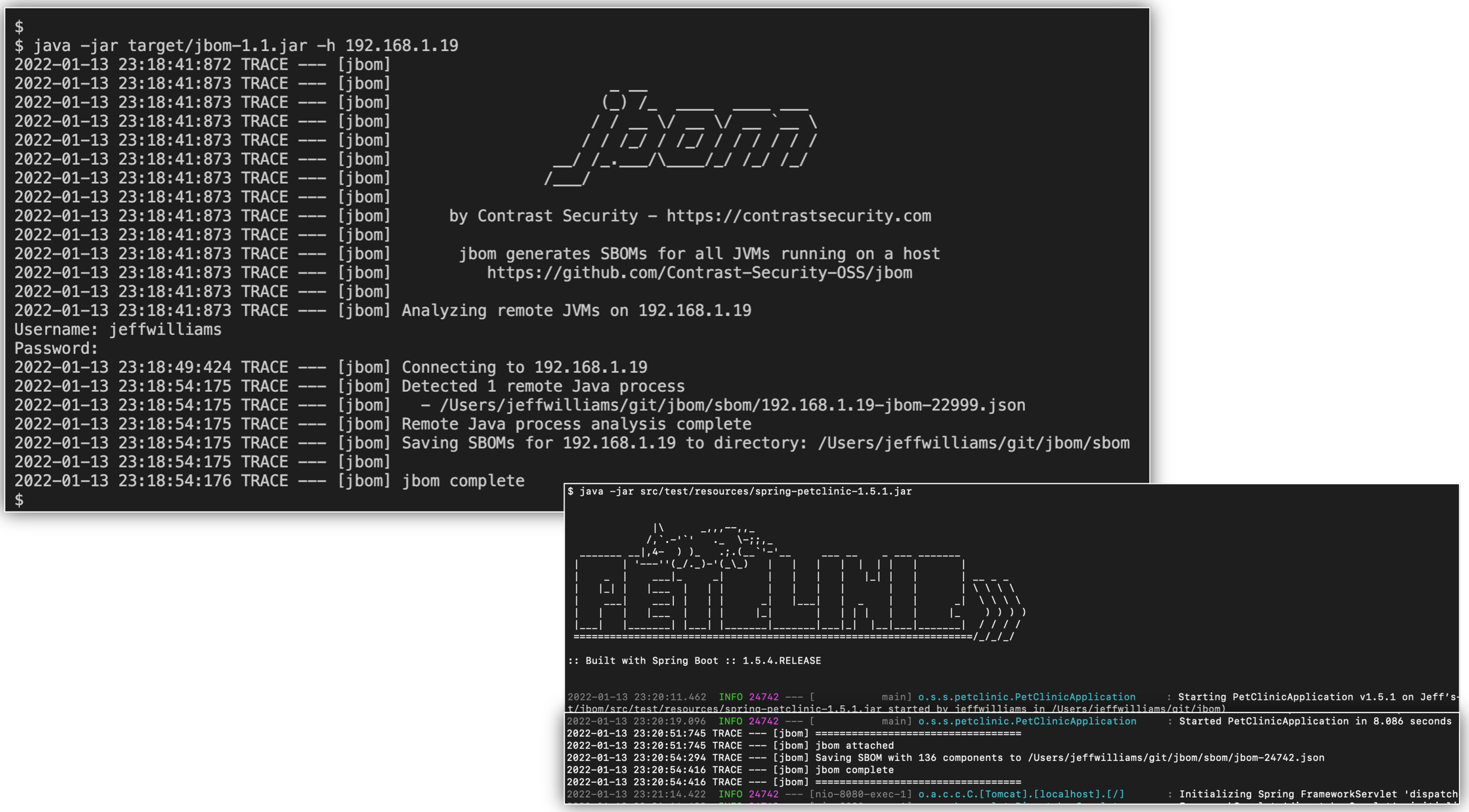
- **SBOMs are accurate - FALSE**

SBOMs must accurately reflect the actual software

Where does SBOM data come from?



JBOM: Free open source SBOM tool for Java!



JBOM creates both…

- **Static SBOMs from both local <u>and remote</u> filesystems**
- **Runtime SBOMs from both local <u>and remote</u> running applications!**

https://github.com/Contrast-Security-OSS/jbom

Issue 1: Basic Finding Libraries

- Scanning filesystems and containers
- Archives – jar, war, ear, zip
- Nested archives
- Repackaging classes into “fat jars”
- Custom structure like Spring Boot
- Shading / relocation
- Unarchived classes?

Issue 2 – Identifying Libraries

- **By name?**
- **By hash?**
- **From dependency tool config?**

Issue 3: Excluding Build and Test Libraries

- Test cases
- Test frameworks
- Tools and utilities
- Build and deploy tools

Issue 4: Finding Server/Platform Libraries

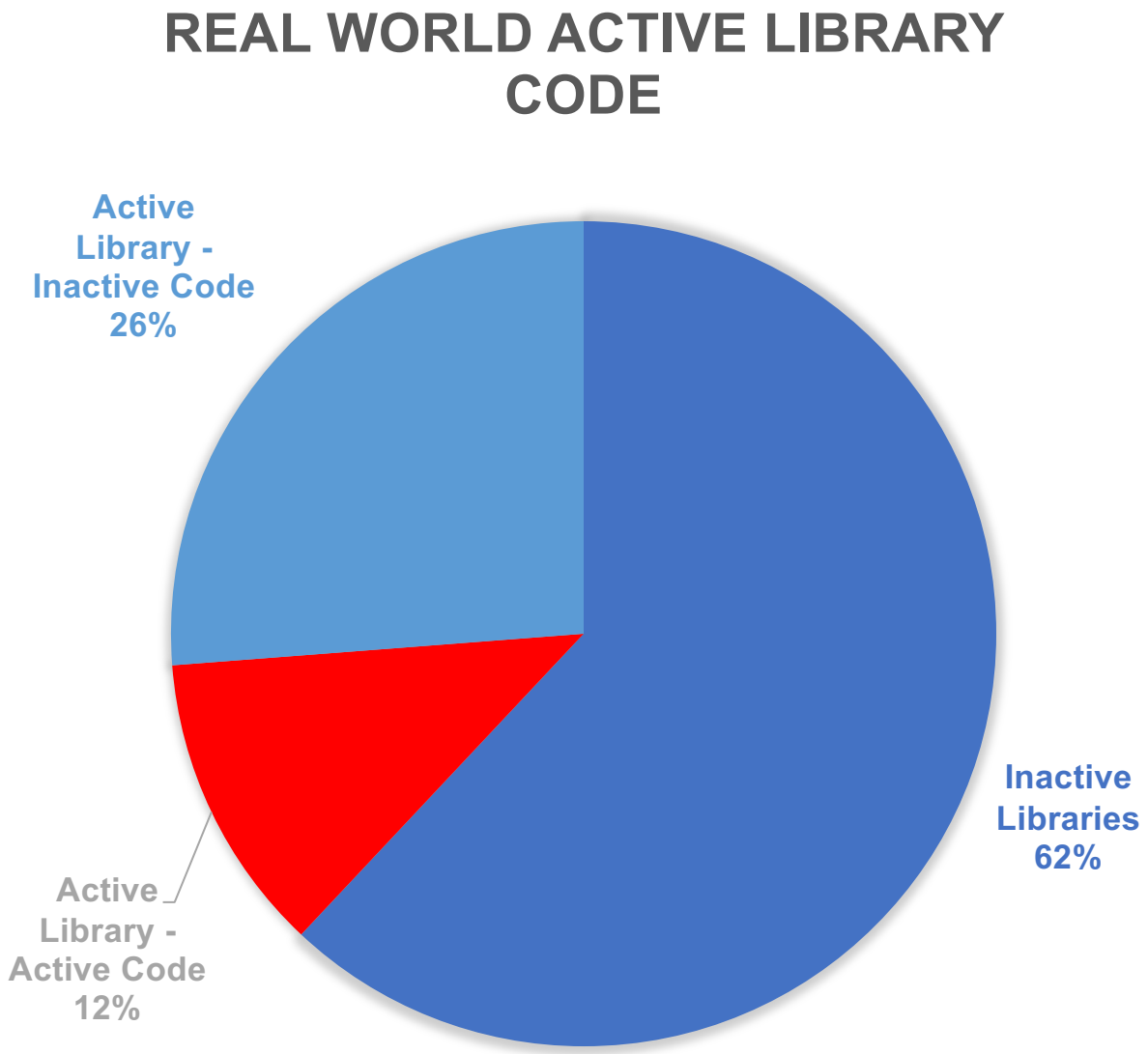
- App server libraries
- Platform libraries

Issue 5: Finding Hidden Libraries

- Dynamic classloading
- Remote classloading
- Custom classloading – encrypted lib?
- Plugins
- Instrumentation
- Compiler
- Native code

Issue 6: Determining Active Libraries

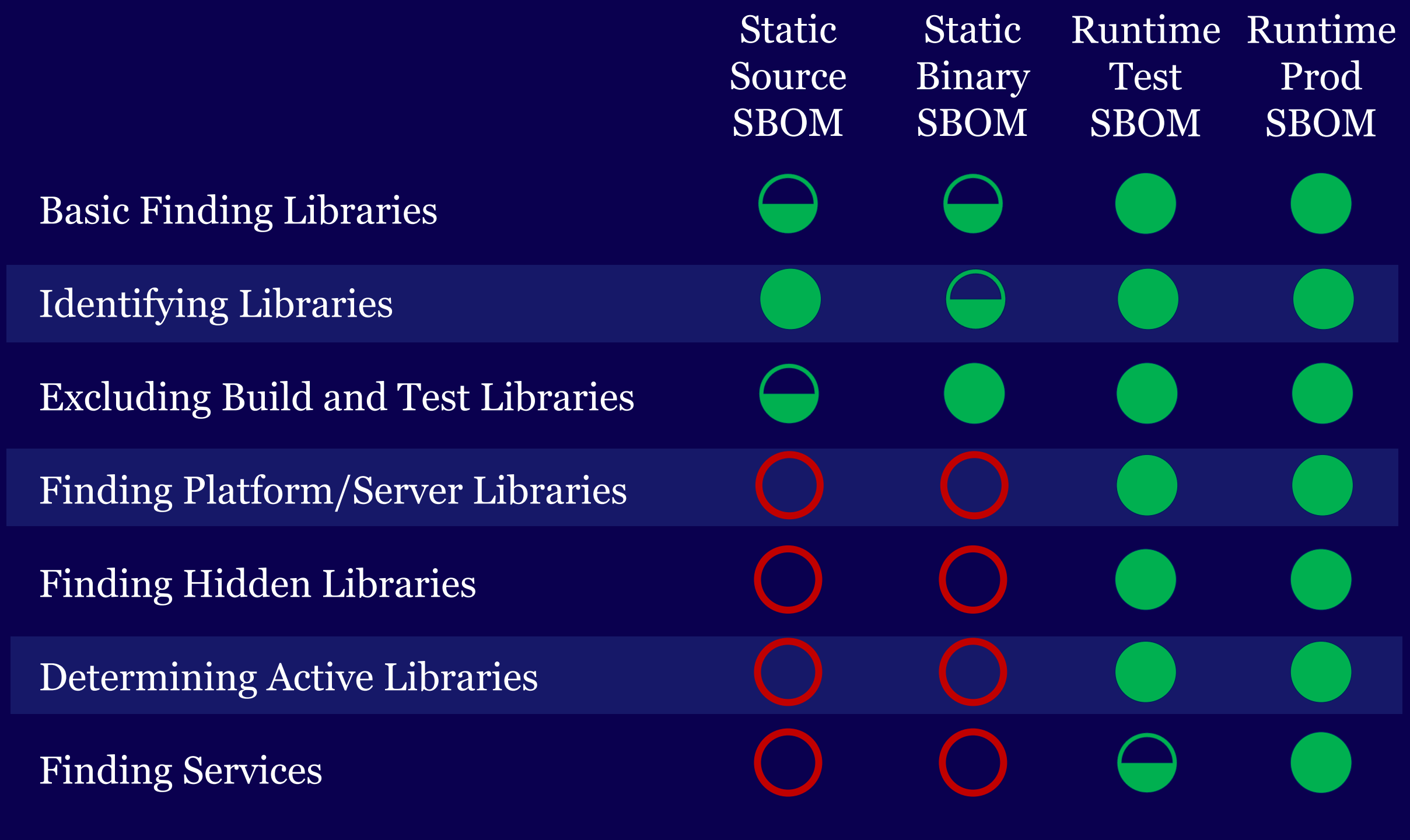
- 62% of libraries are inactive
- 69% of active library code never runs
- FALSE POSITIVES



Contrast State of Open Source (OSS) Security Report 2021

Issue 7: Finding Services

- APIs
- Queues
- Databases
- Serverless Functions
- Mainframe
- Etc…


Static Source SBOM
Static Binary SBOM
Runtime Test SBOM
Runtime Prod SBOM
Basic Finding Libraries
Identifying Libraries
Excluding Build and Test Libraries
Finding Platform/Server Libraries
Finding Hidden Libraries
Determining Active Libraries
Finding Services

You Need a Database!

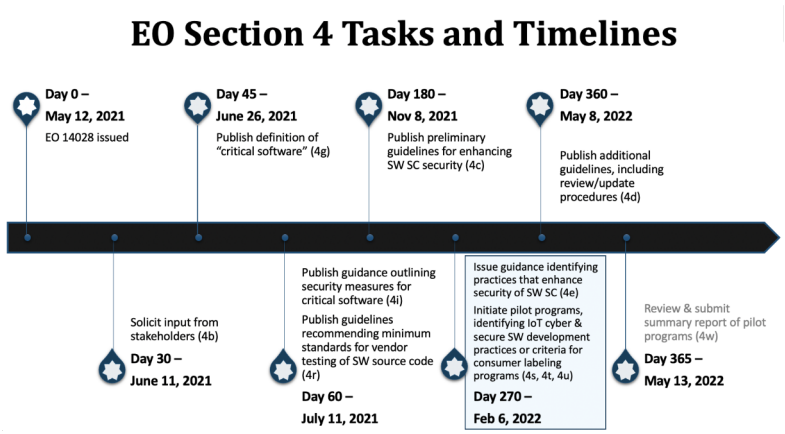
- What libraries (exact version) are used
- In what applications/APIs (all branches)
- Whether they're active
- Whether they're vulnerable
- What servers they are used on
- Continuously up to date

Query: Show apps where I'm using log4j
Query: Show servers where log4j is both active and vulnerable

Software Security Labels Are HERE!!!

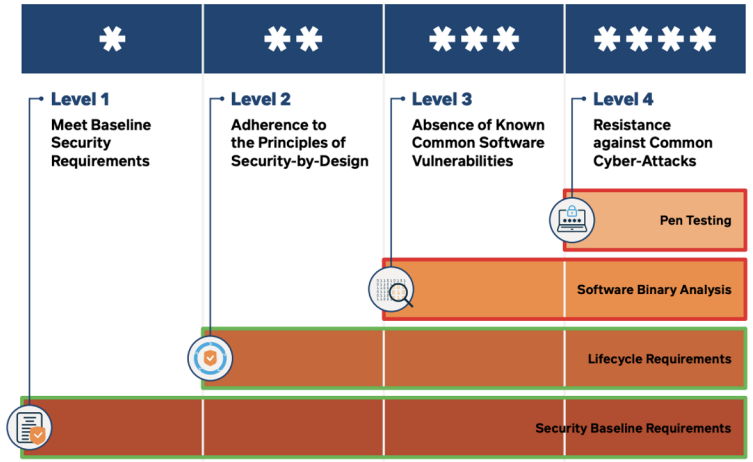
United States

PRESIDENT BIDEN'S EXECUTIVE ORDER ON IMPROVING THE NATION'S CYBERSECURITY



Singapore/Finland

Cybersecurity Labelling Scheme
BY CYBER SECURITY AGENCY OF SINGAPORE



“How to Vulnerability”

https://www.linkedin.com/pulse/how-vulnerability-jeff-williams

“Making Security in a Software Factory”

https://www.linkedin.com/pulse/making-security-software-factory-jeff-williams/

"Ask me ANYTHING!"

Jeff Williams
Cofounder and CTO
Contrast Security

October 2021

Contrast SECURITY