



How SBOMs Change Software Supply Chain Management

Dr. Stephen Magill

The Old World



The New World



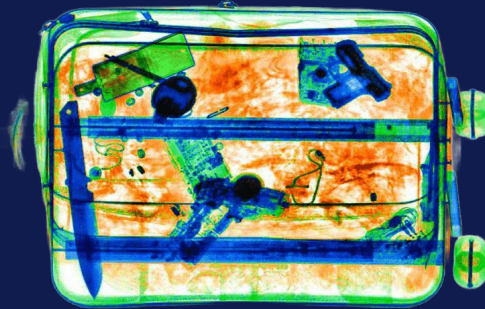
Checking Your Work / Inspecting the Inspectors



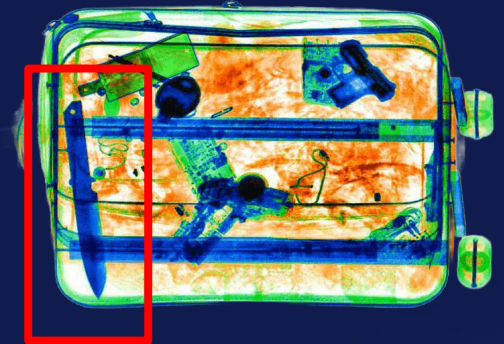
Software Composition Analysis



Identify
Contents



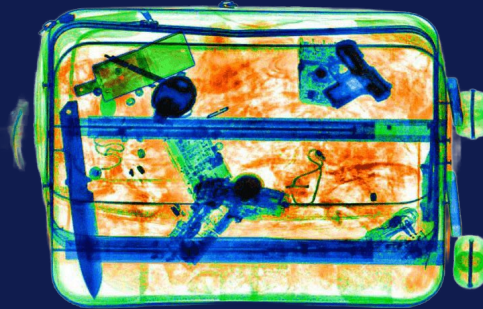
Identify
Threats



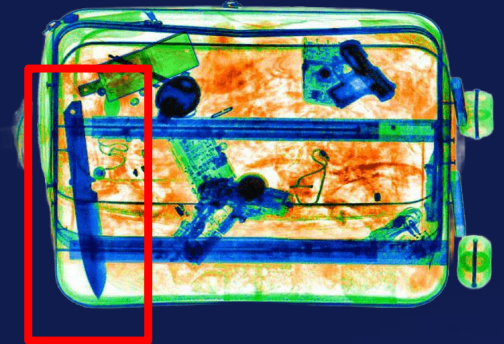
Software Composition Analysis



Identify
Contents

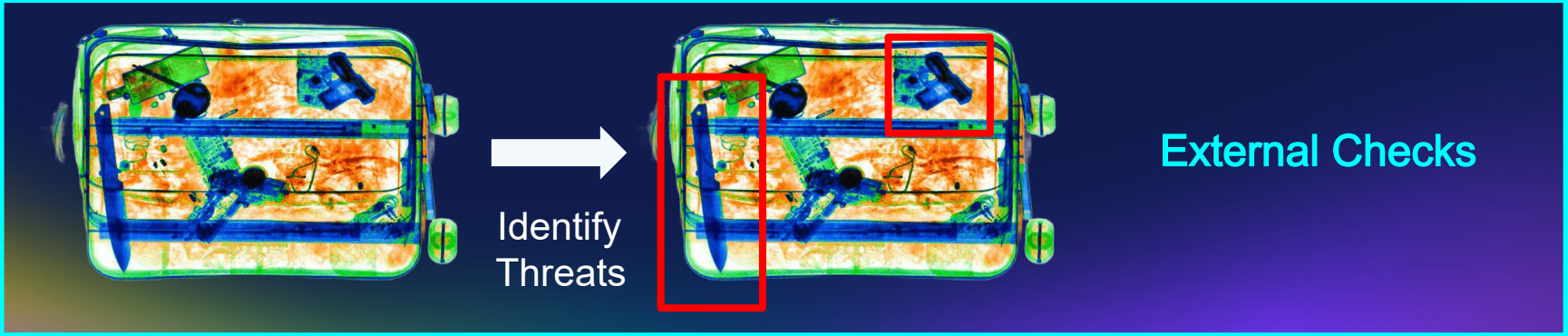
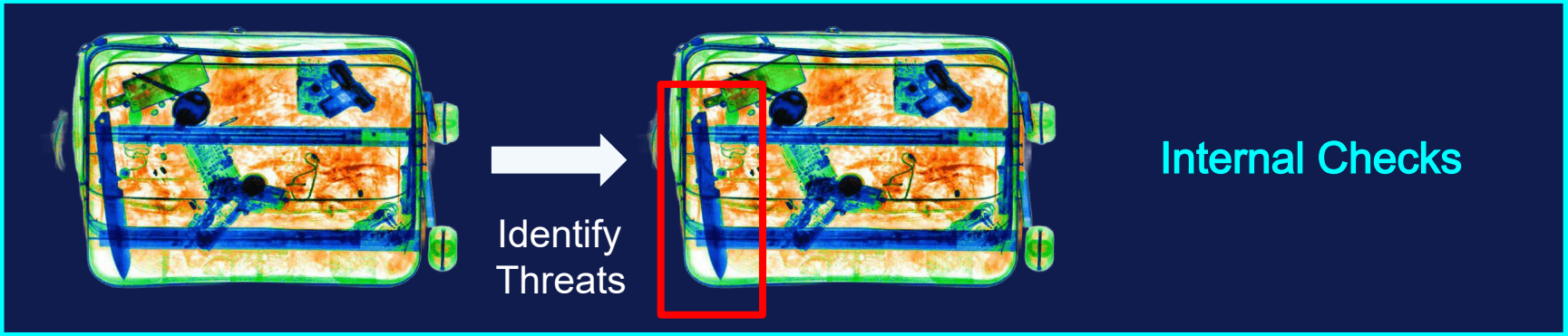


Identify
Threats



SBOMs make this
shareable

Checking Your Work





Who is asking?



You Need SBOMs If...

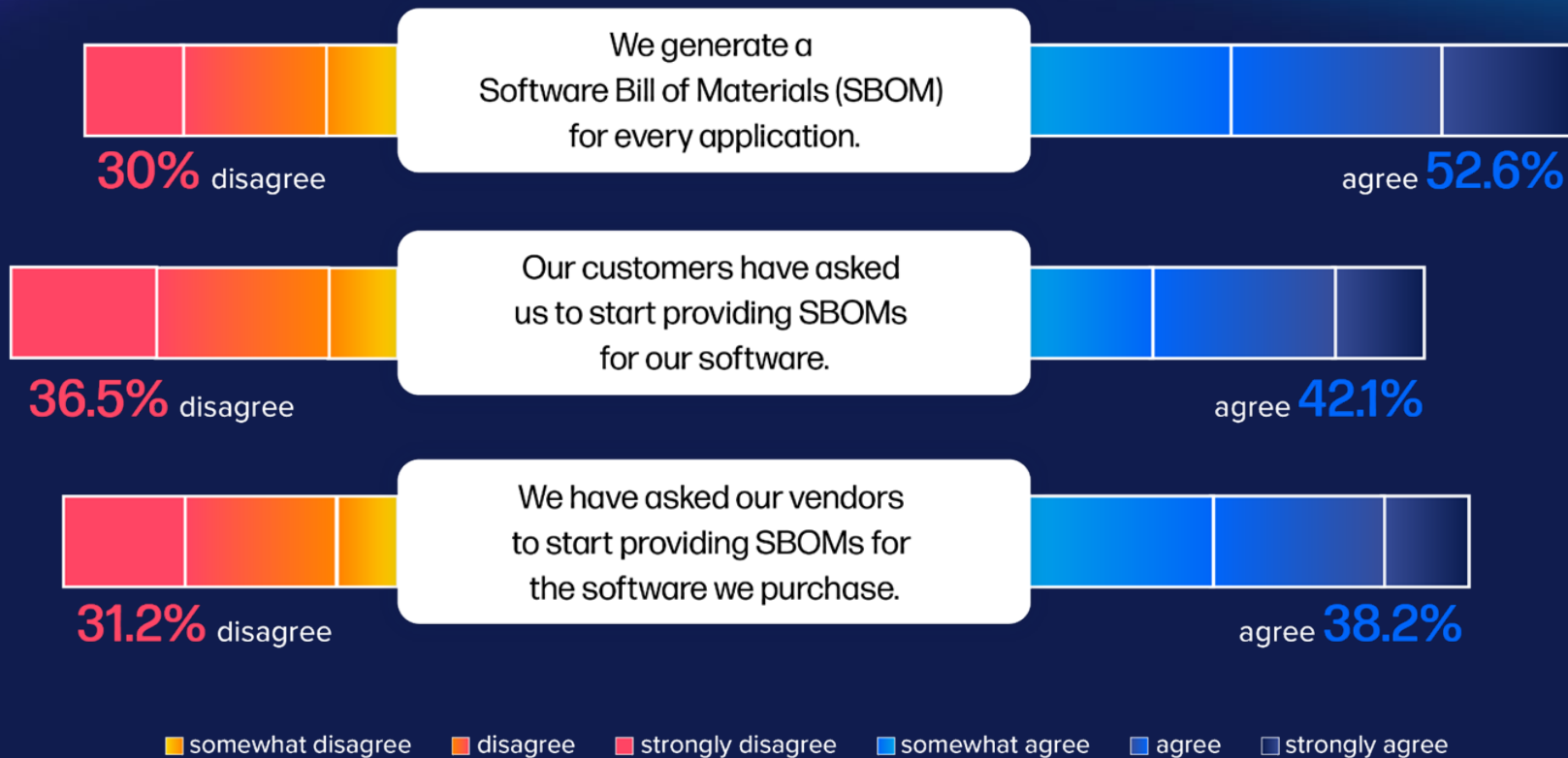
1. You store, process or transmit payment cardholder data. (PCI 4.0)
2. You sell physical products containing software in the EU (CRA)
3. You operate a digital service or serve a critical industry in the EU (NIS2)
4. You're a financial entity or serve financial entities (DORA)
5. You sell medical devices (FD&C Act / FDA)
6. You sell software to the US Federal Government (CISA Attestation Form)
7. You develop software under contract for the US Federal Government (FAR)

You Need SBOMs If...

1. You store, process or transmit payment cardholder data (PCI DSS)
2. You sell physical products containing software (EU Cyber Resilience Act)
3. You operate a digital service or system in the EU (NIS2)
4. You're a financial entity or financial entities (DORA)
5. You sell medical devices (EU MDR / FDA)
6. You sell software to the US Federal Government (CISA Attestation Form)
7. You develop software under contract for the US Federal Government (FAR)

Or you deliver software to anyone in these categories

Requirements Are Spreading



■ somewhat disagree ■ disagree ■ strongly disagree ■ somewhat agree ■ agree ■ strongly agree

FDA

FEDERAL FOOD, DRUG, AND COSMETIC ACT

[As Amended Through P.L. 118–15, Enacted September 30, 2023]

SEC. 524B. [21 U.S.C. 360f~~2~~] ENSURING CYBERSECURITY OF DEVICES.

(b) CYBERSECURITY REQUIREMENTS. The sponsor of an application or submission described in subsection (a) shall—

(3) provide to the Secretary a **software bill of materials** , including commercial, open-source, and off-the-shelf software components

FDA

(2) design, develop, and **maintain processes and procedures** to provide a reasonable assurance that the device and related systems are cybersecure, and **make available postmarket updates** and patches to the device and related systems to address—

(A) on a reasonably justified regular cycle, known unacceptable vulnerabilities; and

(B) as soon as possible out of cycle, critical vulnerabilities that could cause uncontrolled risks;

Monitor & Remediate

CRA (Cyber Resilience Act)



Adds requirements for this

CRA (Cyber Resilience Act)

CRA Annex 1

1 (2): Products with digital elements shall be delivered **without any known exploitable vulnerabilities** ;

2 (1) identify and document vulnerabilities and components contained in the product, including by drawing up a **software bill of materials** ...;

2 (2) ...address and **remediate vulnerabilities without delay** , including by providing security updates;

FAR

“This rule proposes a new requirement for contractors to develop and maintain a software bill of materials **(SBOM) for any software used in the performance of the contract** regardless of whether there is any security incident.”

CISA Attestation

“The software producer has made a good-faith effort to **maintain trusted source code supply chains** by employing automated tools or comparable processes to address the security of internal code and third-party components and manage related vulnerabilities”

PW.4.1: Acquire and maintain well-secured software components (e.g., software libraries, modules, middleware, frameworks) from commercial, open-source, and other third-party developers for use by the organization’s software.

Example 3: Obtain provenance information (e.g., SBOM, source composition analysis, binary software composition analysis) for each software component, and analyze that information to better assess the risk that the component may introduce.



*A Rose By Any
Other Name...*

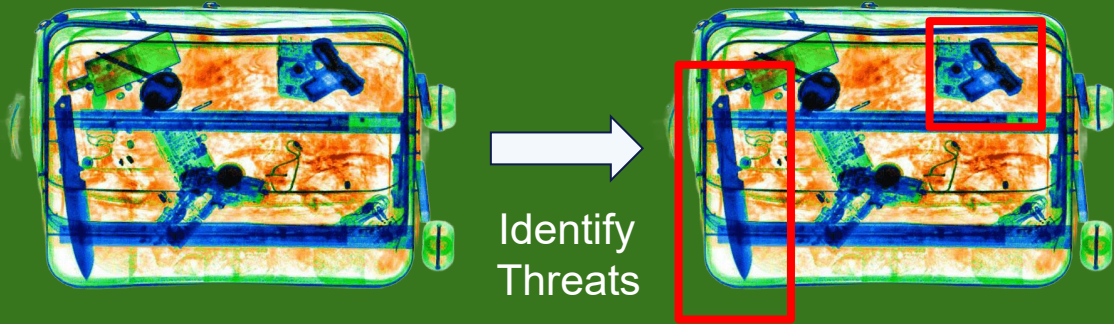
PCI 4.0

“6.3.2. An **inventory** of bespoke and **custom software** , and **third -party software** components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.”

Why is this good?

- Promotes transparency / reduces need to “trust” vendors
- Streamlines communications
- Supports inventory and audit needs
- Pushes back against “check the box” security

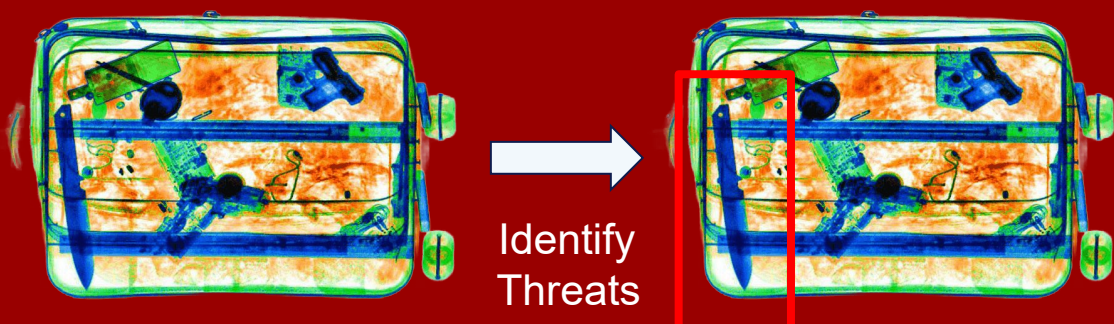
Beyond “check the box”



Identify Threats

You want to be doing this check

This panel illustrates a comprehensive threat identification process. It shows a top-down view of a car interior. A white arrow labeled "Identify Threats" points from the left to the right. On the right, the same car interior is shown with two red rectangular boxes: one around the driver's seat and another around the passenger seat, indicating that both areas are being inspected for threats.

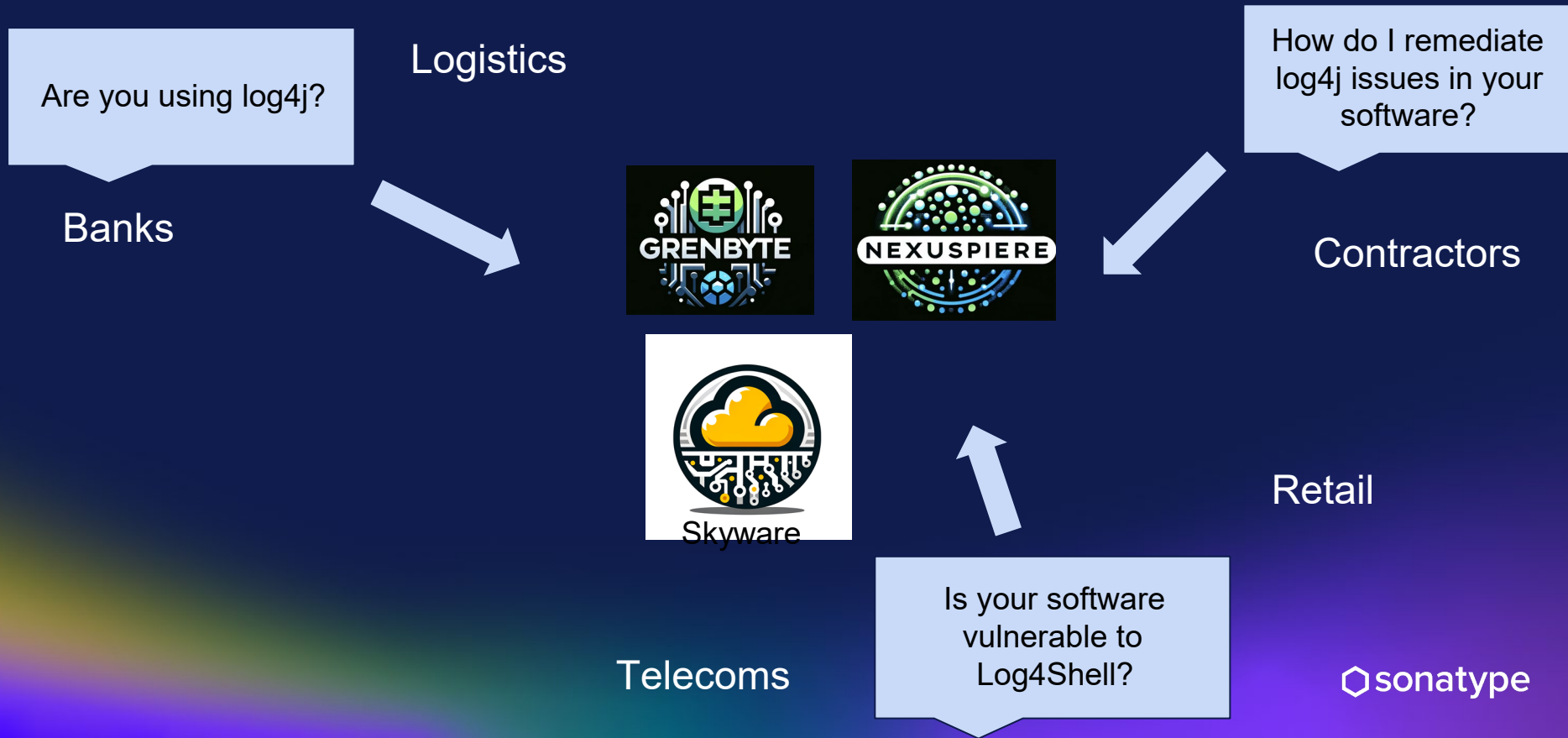


Identify Threats

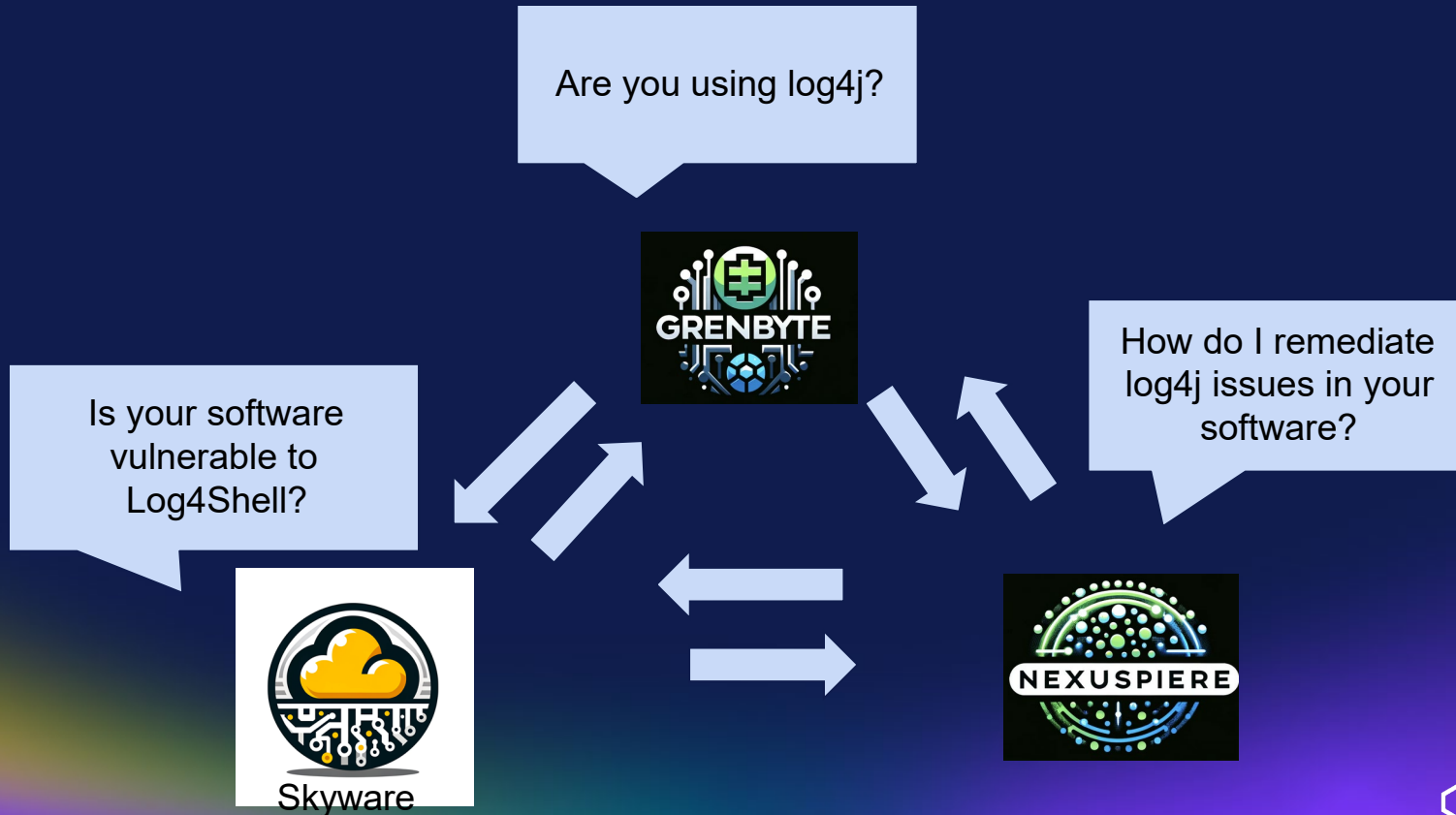
Not this check

This panel illustrates an incomplete threat identification process. It shows a top-down view of a car interior. A white arrow labeled "Identify Threats" points from the left to the right. On the right, the same car interior is shown with a single red rectangular box around the driver's seat, while the passenger seat area is not inspected.

Streamline Communications: Log4j Before

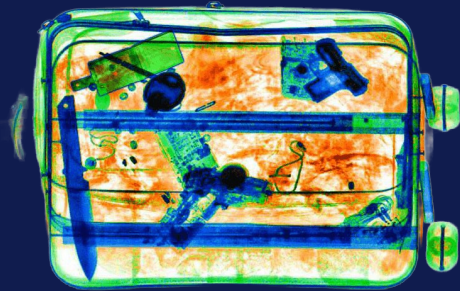


Streamline Communications: Log4j Before

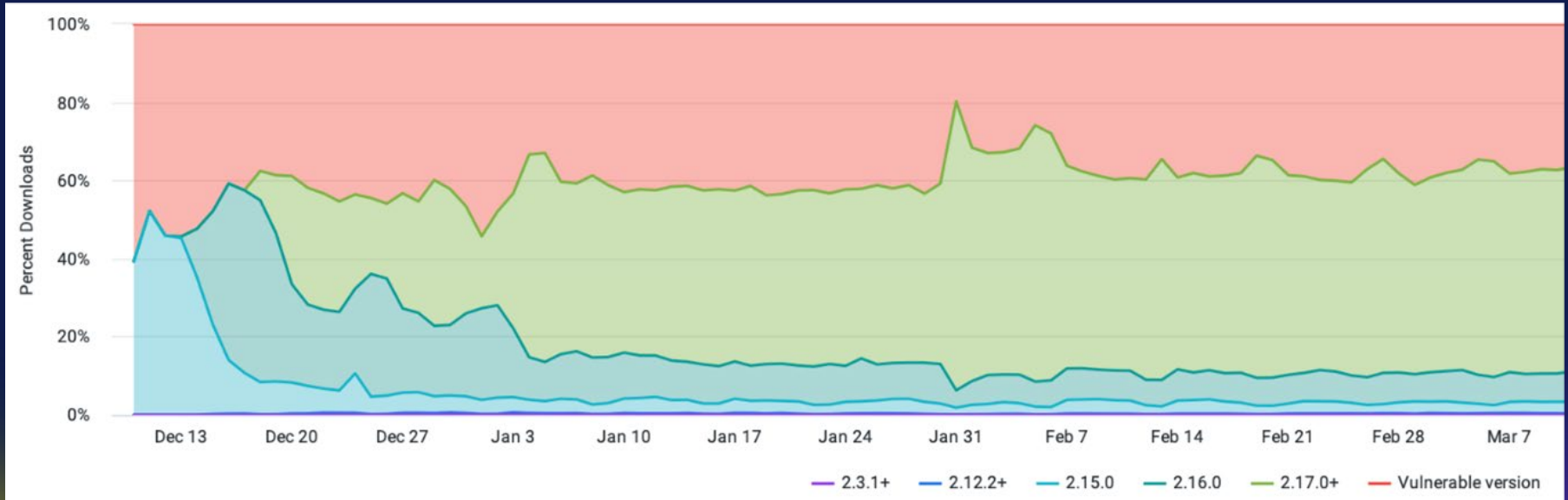


Streamline Communications: Log4j After

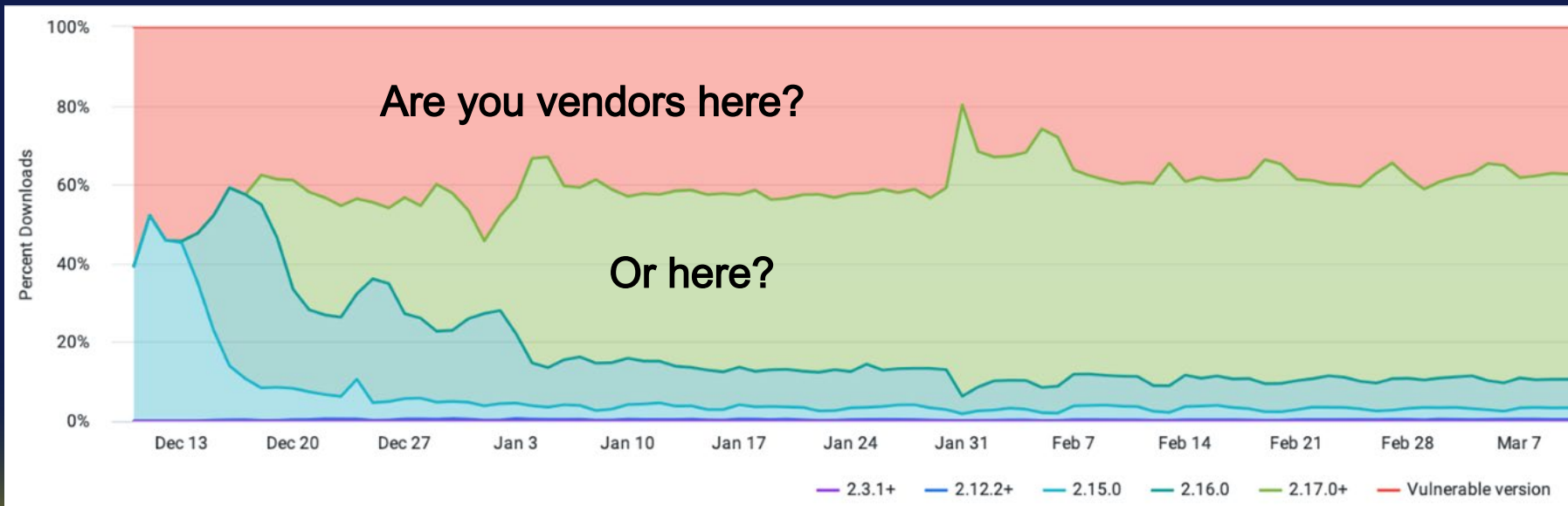
Vendor SBOM



You Can Check Your Vendors



You Can Check Your Vendors



Summary: For Compliance and SBOM Sharing

- **Generate** SBOMs during build, as part of your CI process
- **Collect** SBOMs for third-party software you use
- **Store** SBOMs for each deployed version of the software
- **Retain** these SBOMs as long as that software is in the field
- **Monitor** these SBOMs for vulnerabilities
- Use the most **comprehensive vulnerability database** you can find
- Apply the same security standards to **third-party SBOMs** that you apply to your own