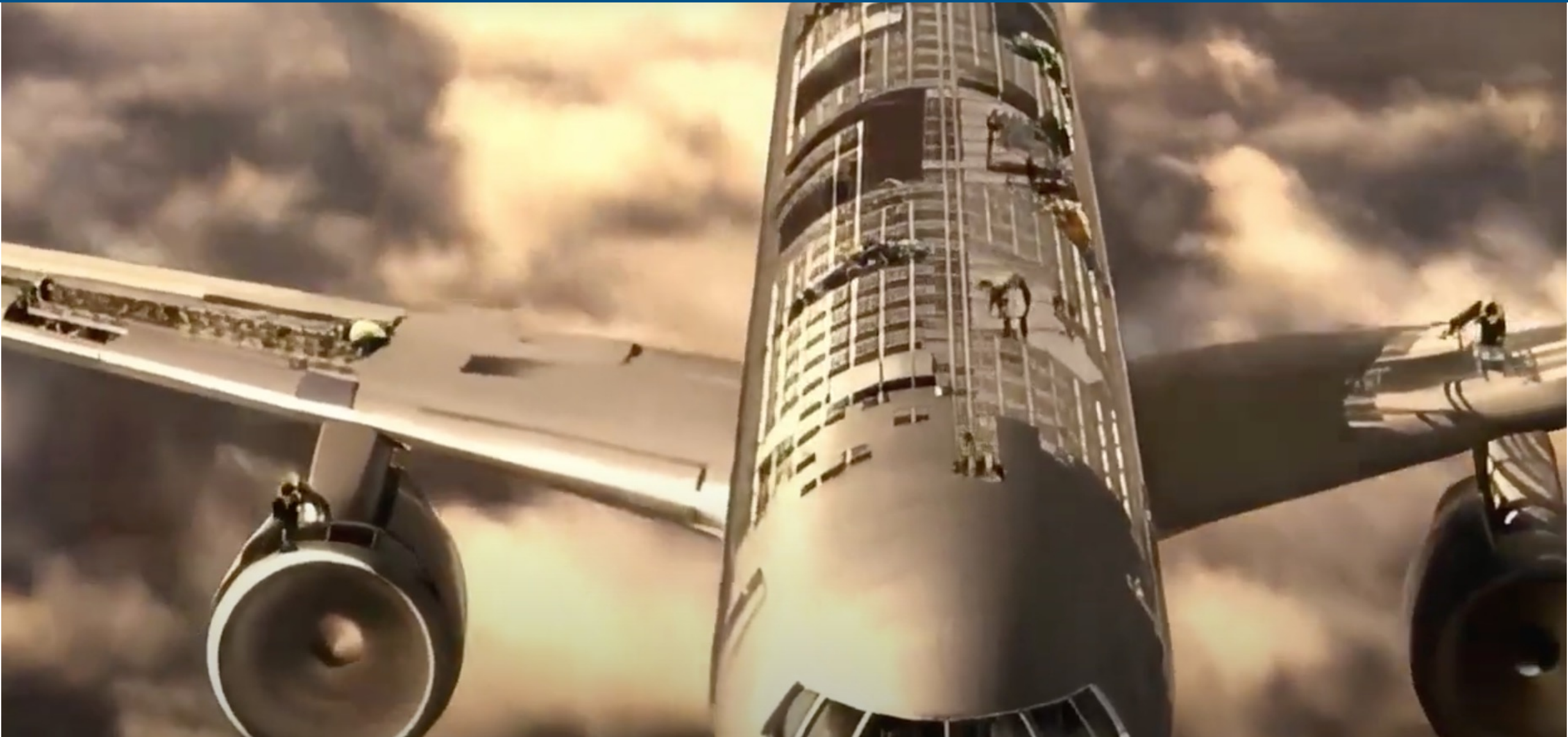


SBOM AND SECURITY TRANSPARENCY HOW IT ALL FITS TOGETHER

Allan Friedman, PhD
“The SBOM Guy”



“Building the Plane While Flying It”



Overview (Why should I watch a video?)

- **SBOM – remind me what this is again?**
- **Is this really happening?**
- **How easy is it?**
- **What else?**
 - **What's bad? Improving CVD**
 - **What's this? Software Identity**
 - **Should I care? VEX**
- **What's the big picture?**



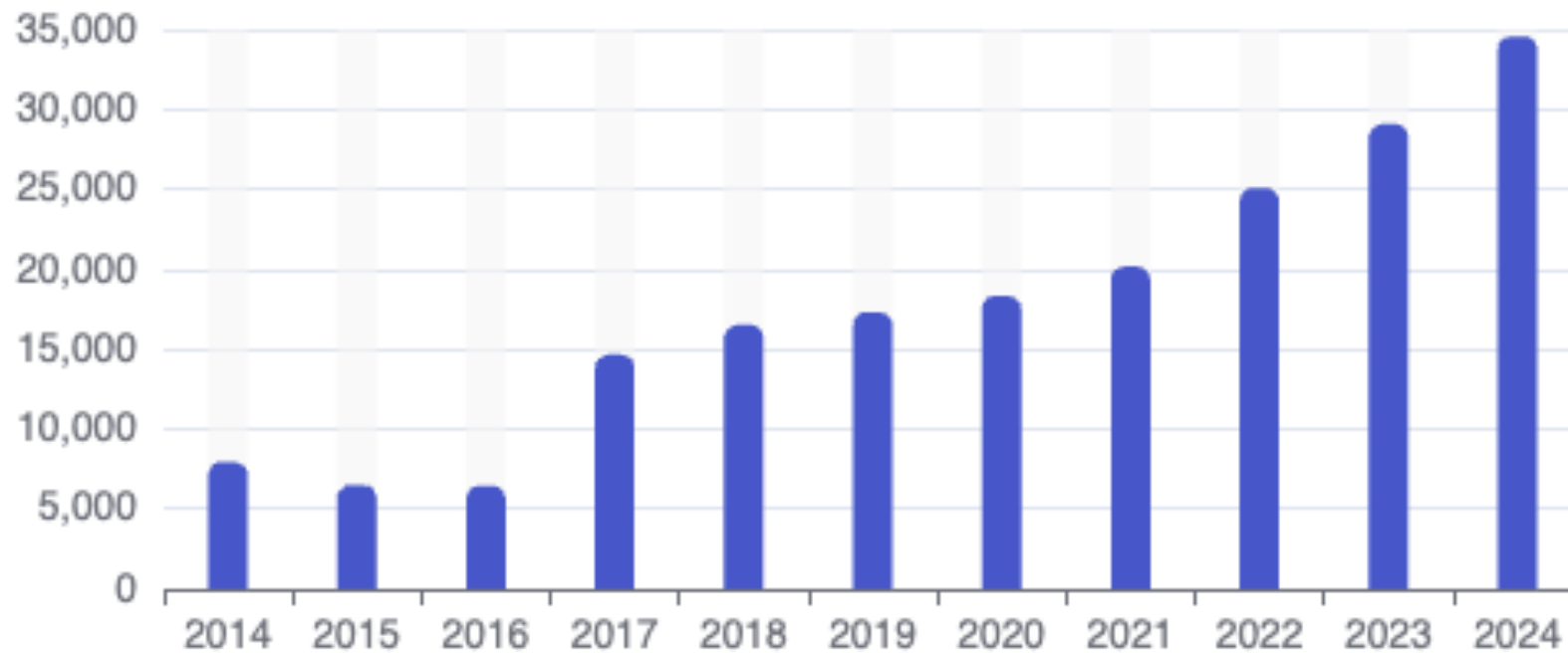
CISA

SBOM

CISA.GOV/SBOM

The “new normal” of risk

- Picture c **Number of CVEs by year**

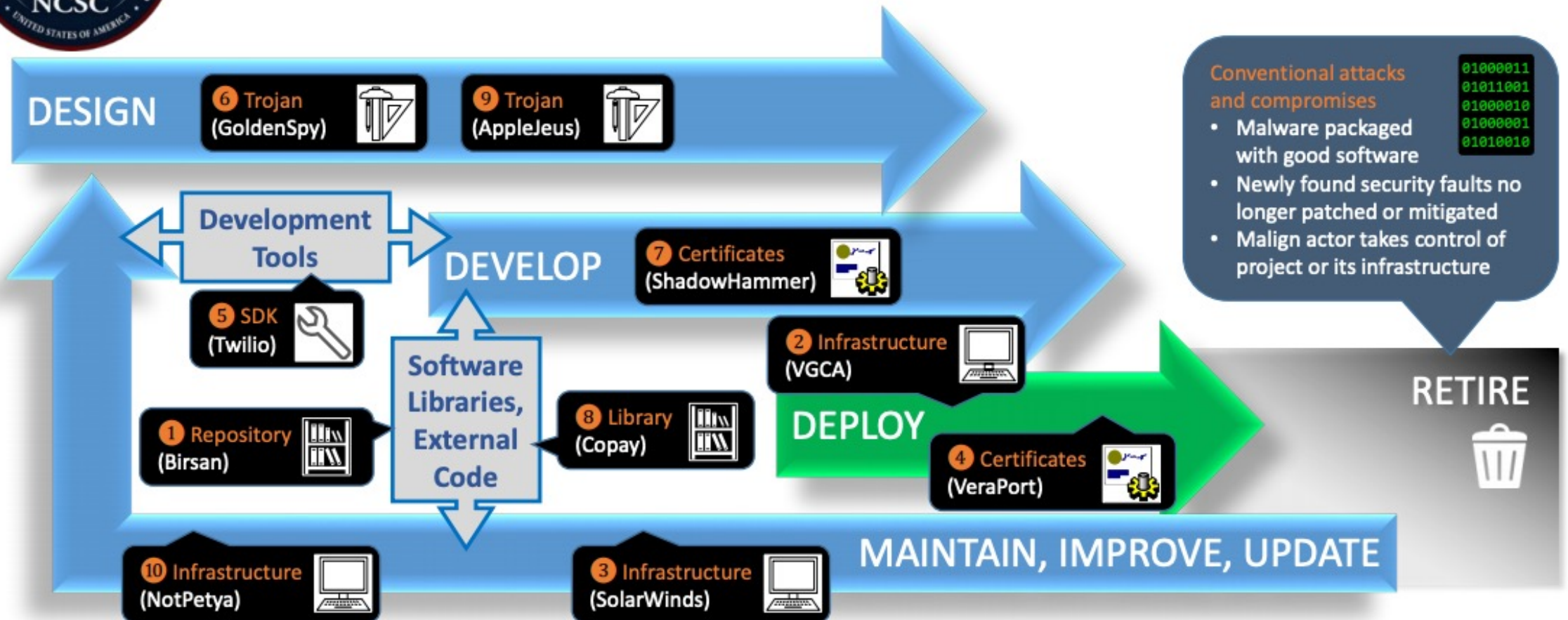


The “new normal” of risk



Software Supply Chain Attacks

Definition: Compromising software through cyber attacks, insider threats, or other malign activities at any stage throughout its entire lifecycle.



Supply chain attacks as the “belly” of security

- Traditionally not as well defended
- Usually an internal issue
- We forget that it is exposed



Types of supply chain risks

- Vulnerabilities
- Intentional malicious insertions upstream
- End-of-life and end-of support code
- Cloned or backdoored versions
- Modified source code
- Risk from open source maintainers
- Midstream compromise – bad updates
- Internal code reuse



Solution: transparency



Transparency can help markets thrive



The image shows the packaging for Nestlé KitKat Peach. The left side of the box is white with a red circular logo containing the Nestlé and KitKat brand names. Below the logo, the word '白桃' (White Peach) is written in large red characters, followed by 'Peach' in smaller black text. At the bottom left, it says 'mini 3枚入り' (mini 3 pieces). The right side of the box is red with large white Japanese characters '桃' (Peach) and a smaller box containing '日本土産' (Japanese Souvenir). Below this, there is a photograph of a peach and a slice of peach. A white text box is overlaid on the bottom right of the packaging, containing the following information:

●名称: 準チョコレート ●原材料名: 準チョコレート (砂糖、乳糖、植物油脂、全粉乳、ココアバター) (国内製造)、小麦粉、植物油脂、乳糖、砂糖、もも果汁パウダー、ココアパウダー、イースト、カカオマス、全粉乳、ココアバター/乳化剤(大豆由来)、酸味料、香料、着色料(赤ビート、紅麹)、重曹、イーストフード ●内容量: 3枚 ●賞味期限: 枠外底面に記載 ●保存方法: 28℃以下の涼しい場所で、多湿を避けて保存してください。 ●製造者: ネスレ日本株式会社 神戸市中央区御幸通7-1-15

製造所: ネスレ日本株式会社 (霞ヶ浦工場) 茨城県稲敷市神宮寺1751

原材料に含まれるアレルゲン(28品目中) 小麦、乳、大豆、もも

●本品は卵、アーモンド、ごまを含む製品と共通の設備を使用しています。

●本品は高温でやわらかくなった後、冷えて固まると表面が白くなる場合があります。これは油脂分が分離したもので、風味は劣りますが召し上がっても身体にさしさわりはありません。●万一品質に不都合がございましたら、ネスレお客様相談室にご連絡ください。お取り替えいたします。



Transparency can help markets thrive



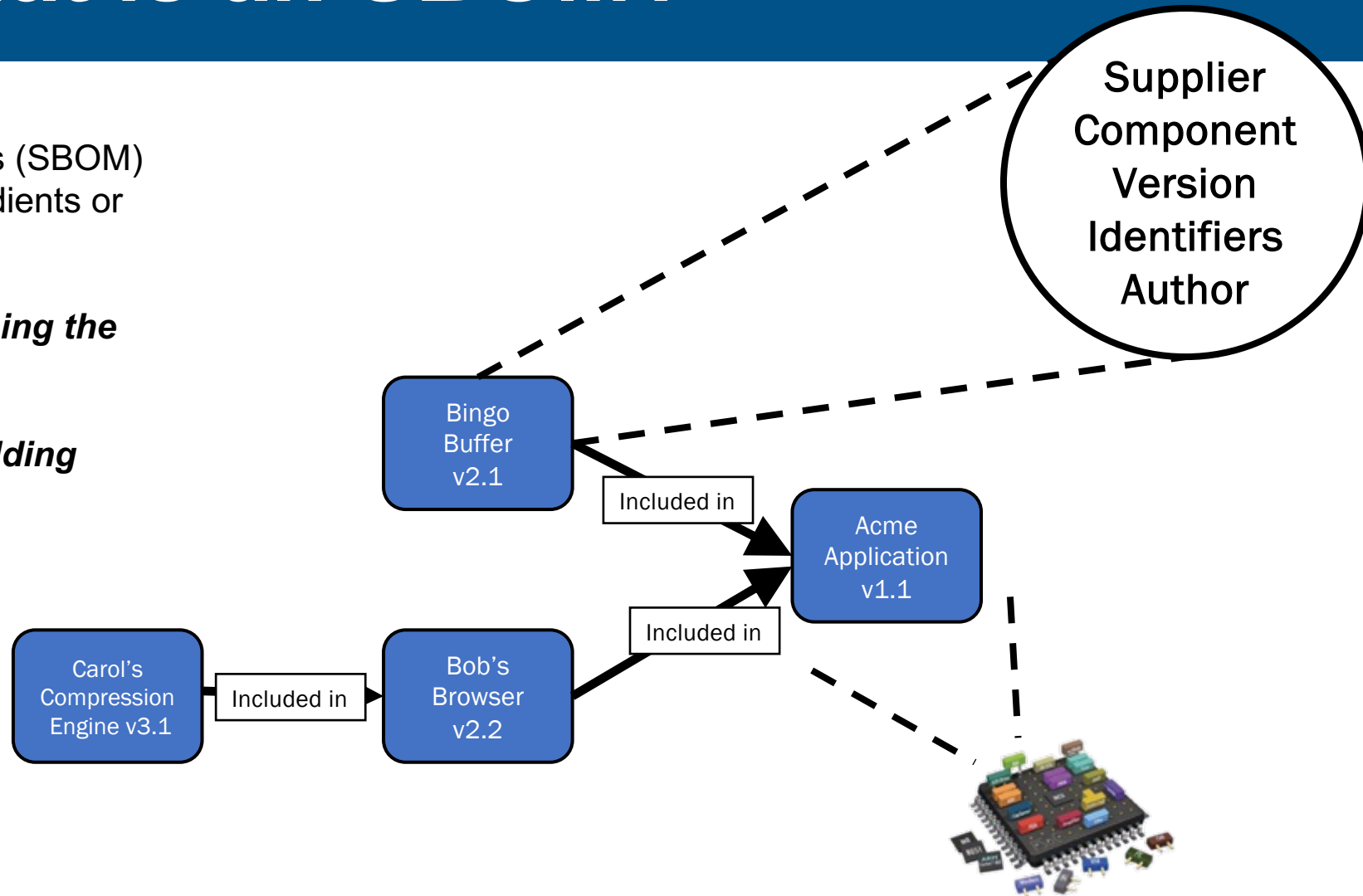
Software Transparency won't solve all our supply chain concerns, but it is necessary component of any scalable solution.



So... what is an SBOM?

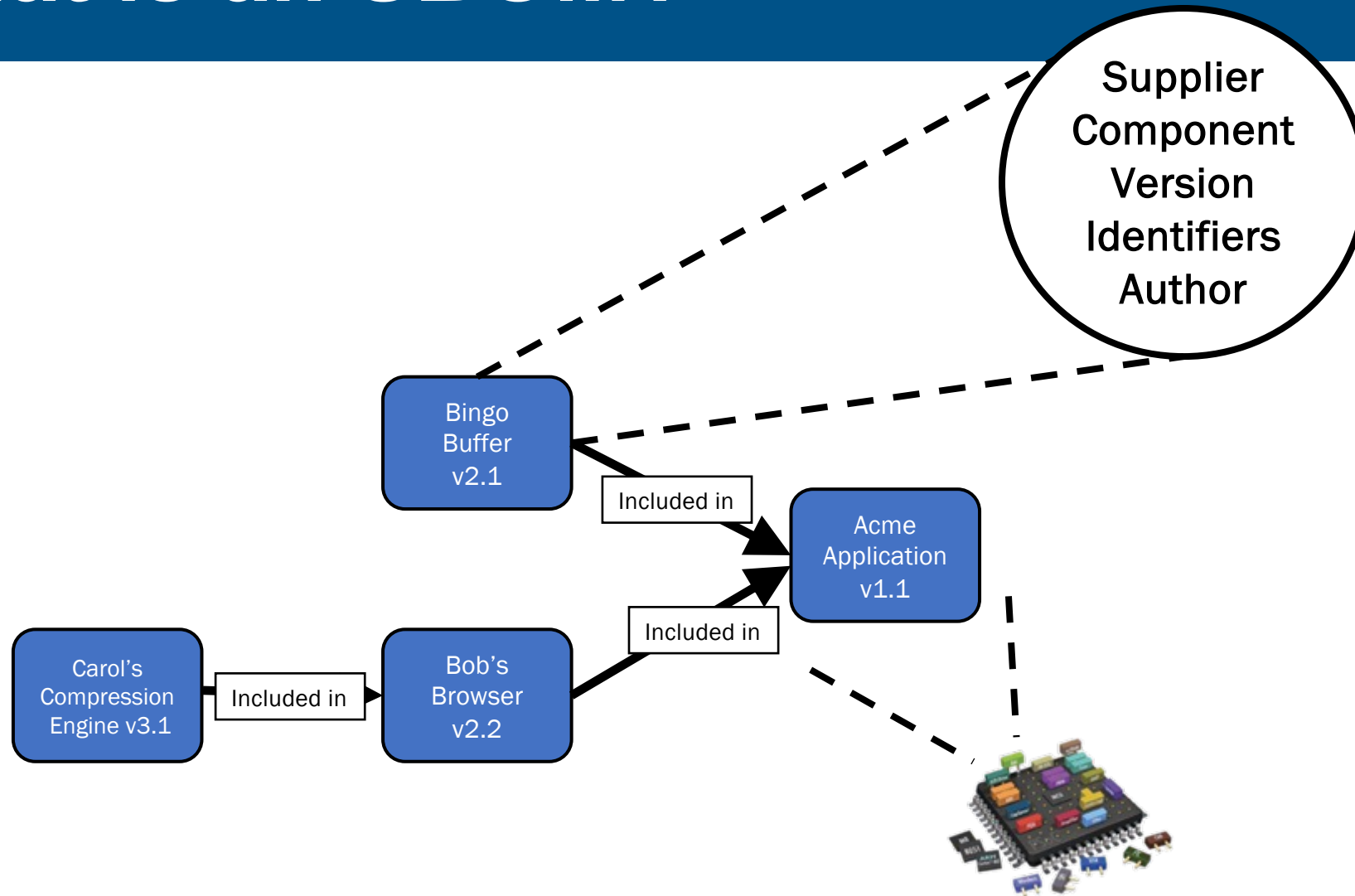
A Software Bill of Materials (SBOM) is effectively a list of ingredients or a nested inventory.

“A formal record containing the details and supply chain relationships of various components used in building software”

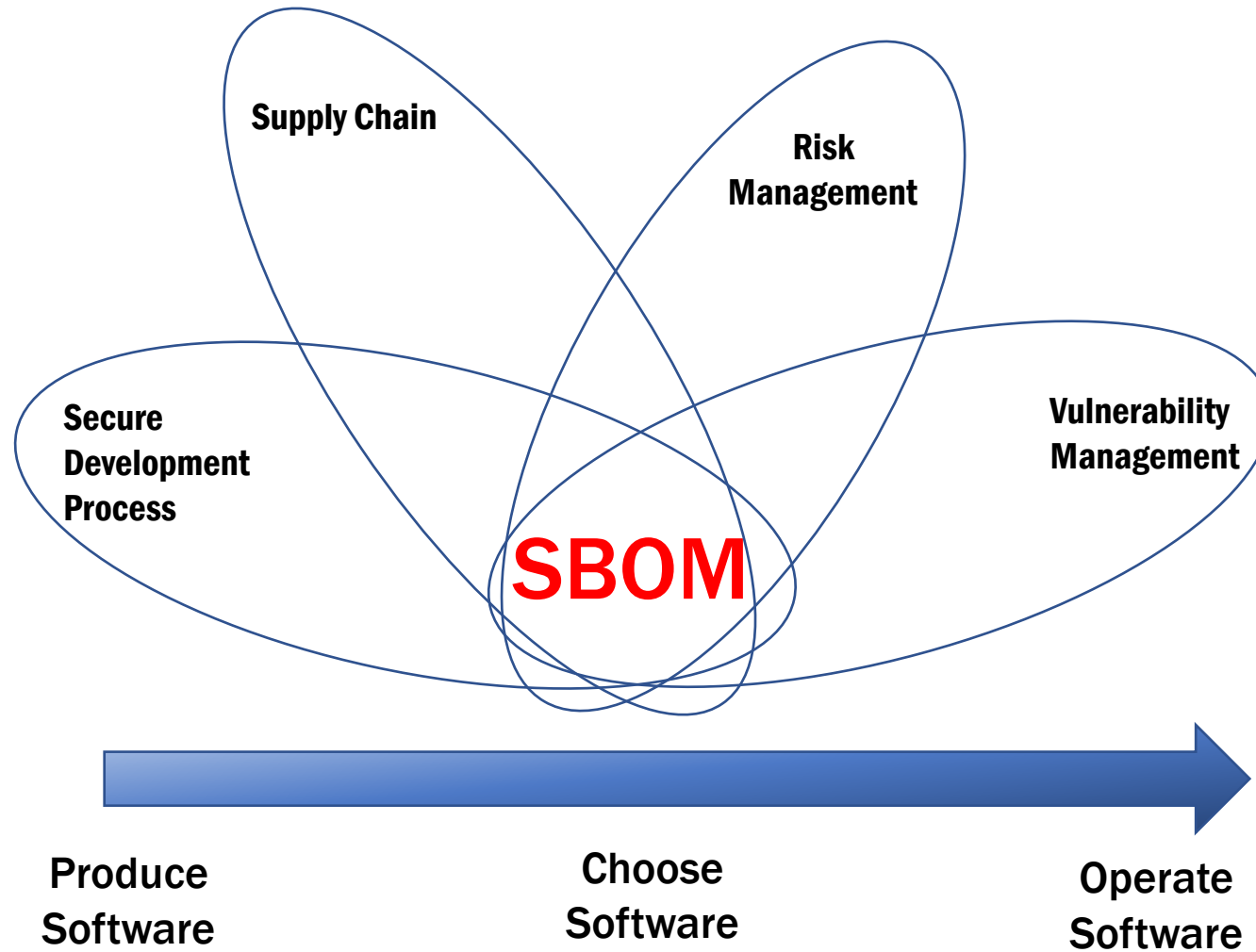


So... what is an SBOM?

- Proprietary Software
- In-house Modules
- Open Source Code
- Contractor Software
- Built Binaries



Value across roles



Regulation and Compliance are coming






SBOM in Regulations and Guidance Around the World

- US Executive Order 14028
- US FDA Medical Device Requirements
- US BIS Connected Vehicles
- US Army
- Indian Securities and Exchange Board
- CERT-In Technical Guidance
- Japan METI Guide
- German BSI TR-03183
- PCI DSS 4.0
- EU DORA
- **EU Cyber Resilience Act**

Data quality



- Risk: poor quality or immature tools providing insufficiently useful metadata
 - Not complete lists of dependencies (depth)
 - Incomplete or incorrect data about dependencies
- Risk: ambiguities or different interpretations in SBOM specs
 - E.g. How to take a hash
 - How to deal with “known unknowns”
- Data from different sources

Quality of Free Tools

On the Accuracy of GitHub's Dependency Graph

Daniele Bifulco
University of Sannio
Benevento, Italy

Massimiliano Di Penta
University of Sannio
Benevento, Italy

Sabato Nocera
University of Salerno
Fisciano, Italy

Rita Francese
University of Salerno
Fisciano, Italy

Simone Romano
University of Salerno
Fisciano, Italy

Giuseppe Scanniello
University of Salerno
Fisciano, Italy



*"No single tool on the market
meets our needs..."*

-Major US medical device manufacturer

Defining SBOM

- How do we determine whether what is generated, maintained, or shared is an SBOM?
- Defining the data fields
- Defining based on Use Cases
 - Identifying vulnerabilities
 - Mapping to other sources
- Need for global harmonization



Software by any other name...



21

**There are only two hard things in
Computer Science: cache
invalidation and naming things.”**

- attributed to Phil Karlton

Software by any other name...

22

The image shows a hand holding a tablet displaying the CISA website. The page title is "Software Identification Ecosystem Option Analysis". The header includes the CISA logo and the text "CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY" and "AMERICA'S CYBER DEFENSE AGENCY". The navigation menu contains "Topics", "Spotlight", "Resources & Tools", "News & Events", "Careers", and "About". The breadcrumb trail is "Home / Resources & Tools / Resources". The publish date is "October 26, 2023". A search bar is visible in the top right corner.

<https://www.cisa.gov/resources-tools/resources/software-identification-ecosystem-option-analysis>

...there are only two hard things in Computer Science: cache invalidation and naming things."

- attributed to Phil Karlton

Finding the “Known Badness”



Finding the “Known Badness”

- Research!
- Reporting
- Acknowledgement
- Assessment and Validation
- Remediation
- Disclosure



How Organizations can make CVD work

- Acknowledge the Issue
- Engage with the researchers constructively
- Provide Timely Updates
- Don't shoot the messenger!

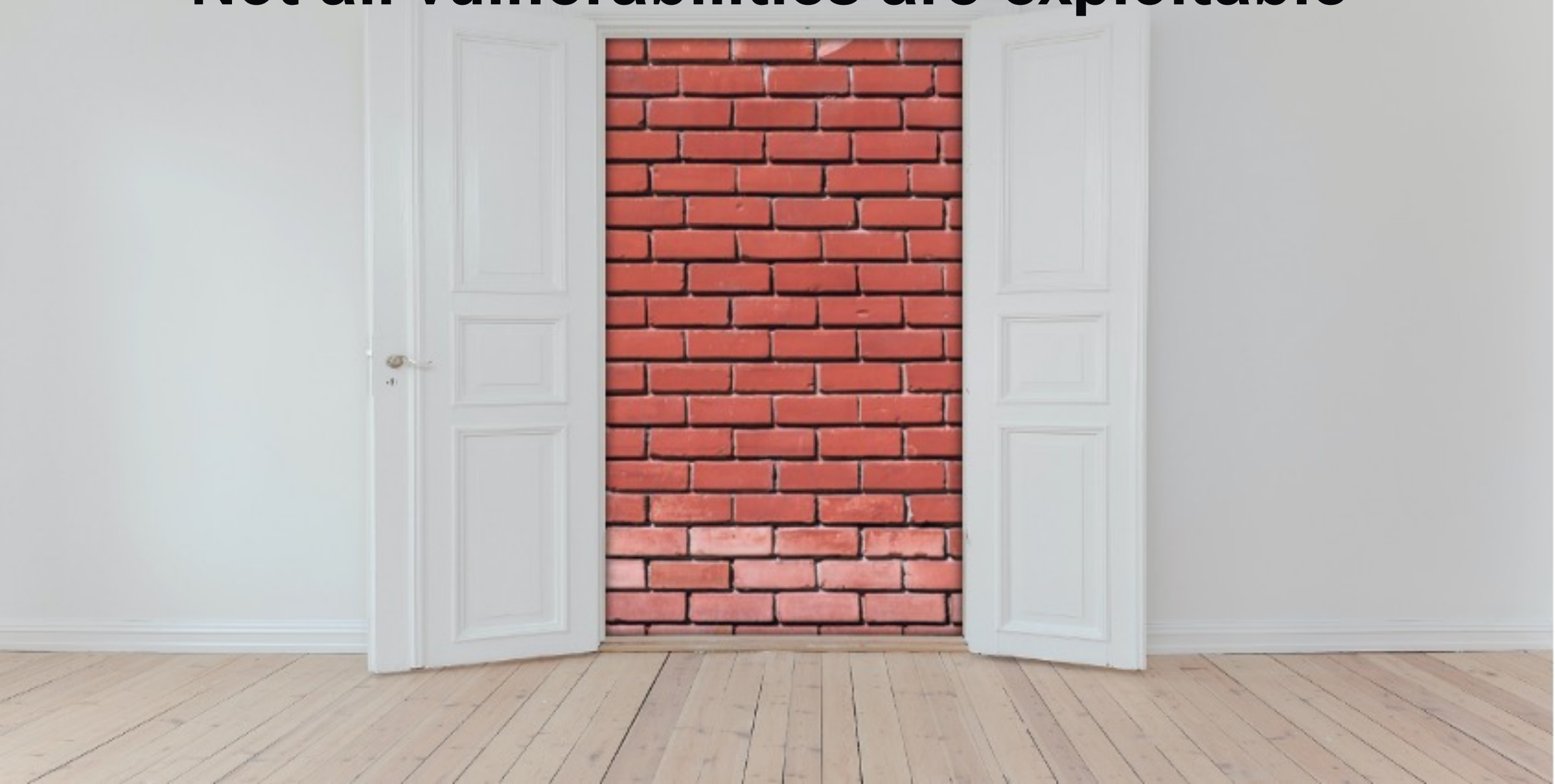


ANNOUNCEMENT

CISA Announces Vulnrichment Repository



Not all vulnerabilities are exploitable



Not all vulnerabilities are exploitable



VEX

Vulnerability Exploitability eXchange

Not all vulnerabilities are exploitable

Component not present

Affected code not loaded

Affected code not in path

Attacker can't touch affected code

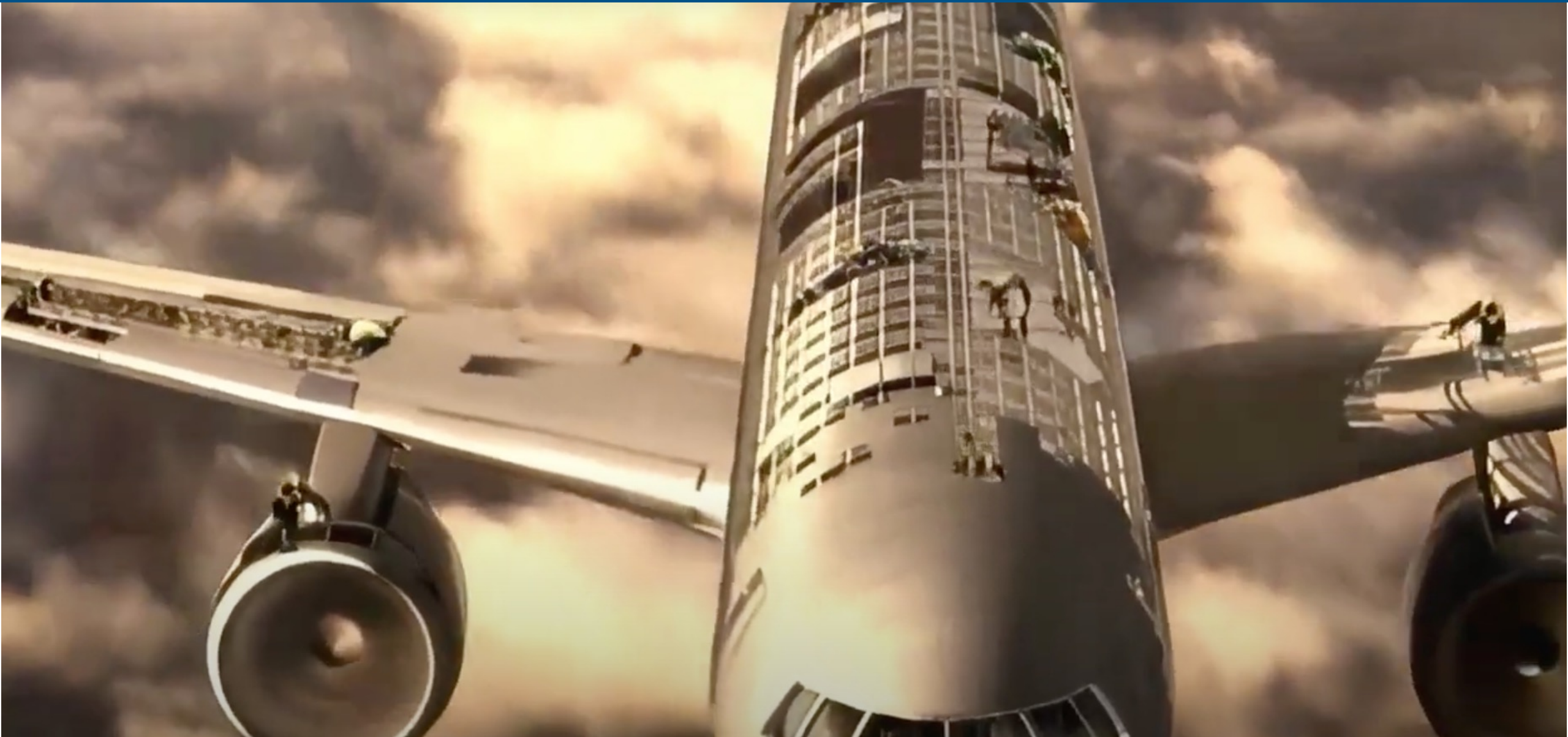
In-line mitigations exist



What is the future going to look like?



“Building the Plane While Flying It”



“Building the Plane While Flying It”



Better Data



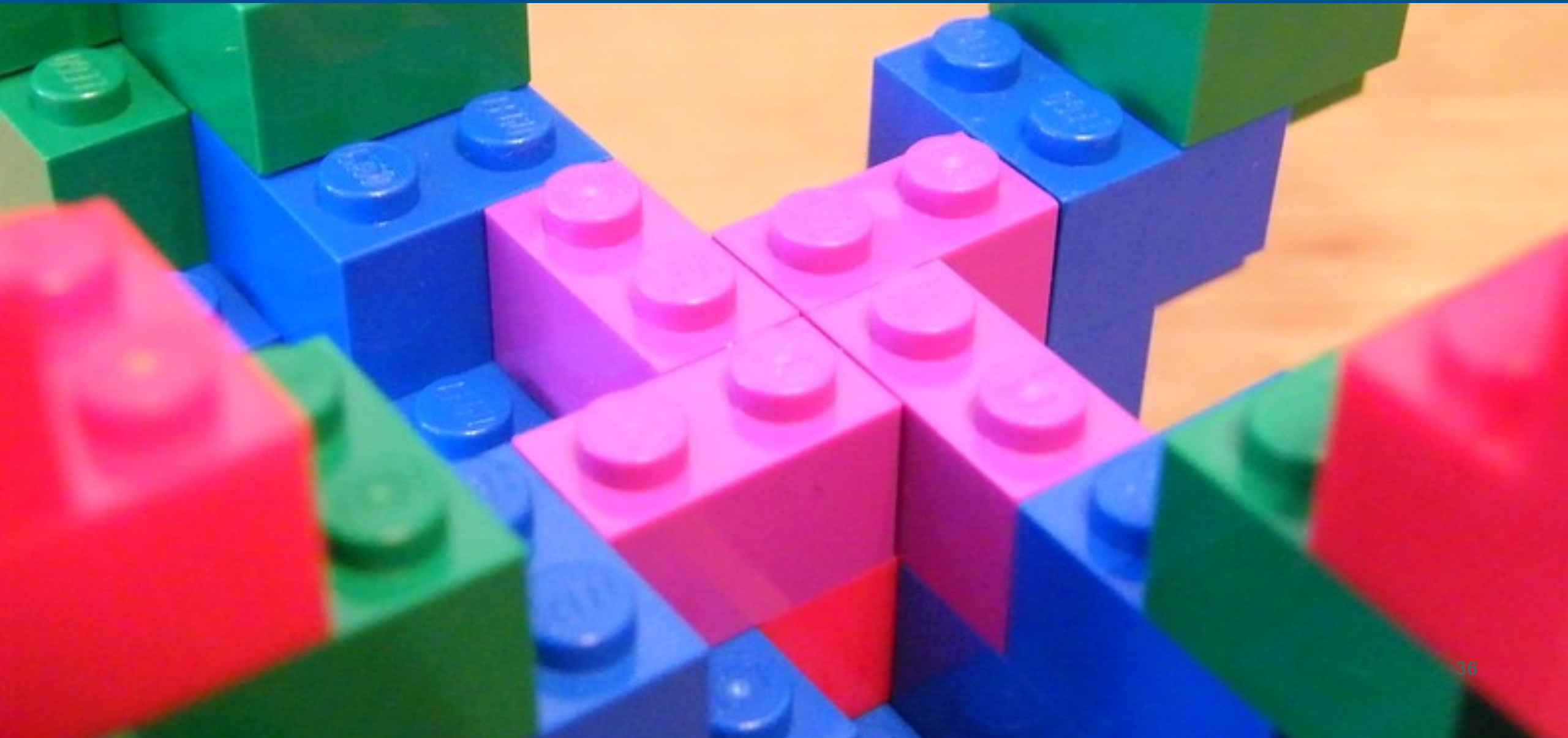
Better Data for Automation



Tooling to Generate and Consume



Build Things... *With Modularity*



Build Things... *With Modularity*

Embrace an evolving world of valuable data





Get involved with any of these projects!

Email:
SBOM@cisa.dhs.gov