webcomm 偉康科技

軟體產品開發視角下的供應鏈安全實務分享

From SBOM to Zero CVE

偉康科技
資深研發經理 Fiona Cheng

About Me

Fiona Cheng

目前任職於偉康科技
負責 OEth 系列
FIDO/ZTA等相關的產品

Agenda

1. 關於SBOM的國際趨勢
2. 實務分享
3. 未來展望

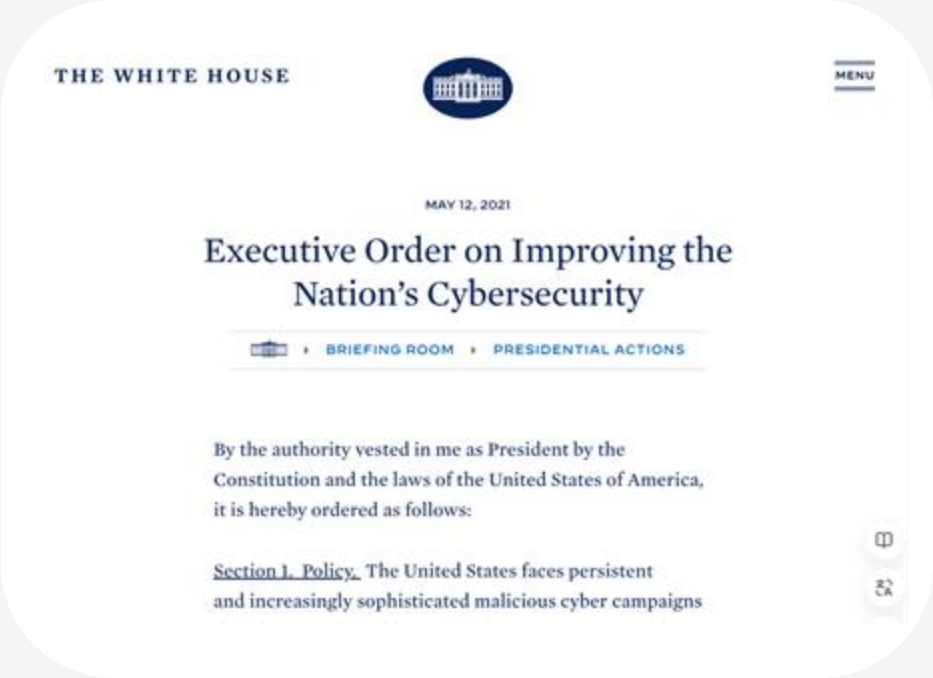
01

提供 SBOM 成為國際趨勢

US, EU, South Korea, Singapore, India

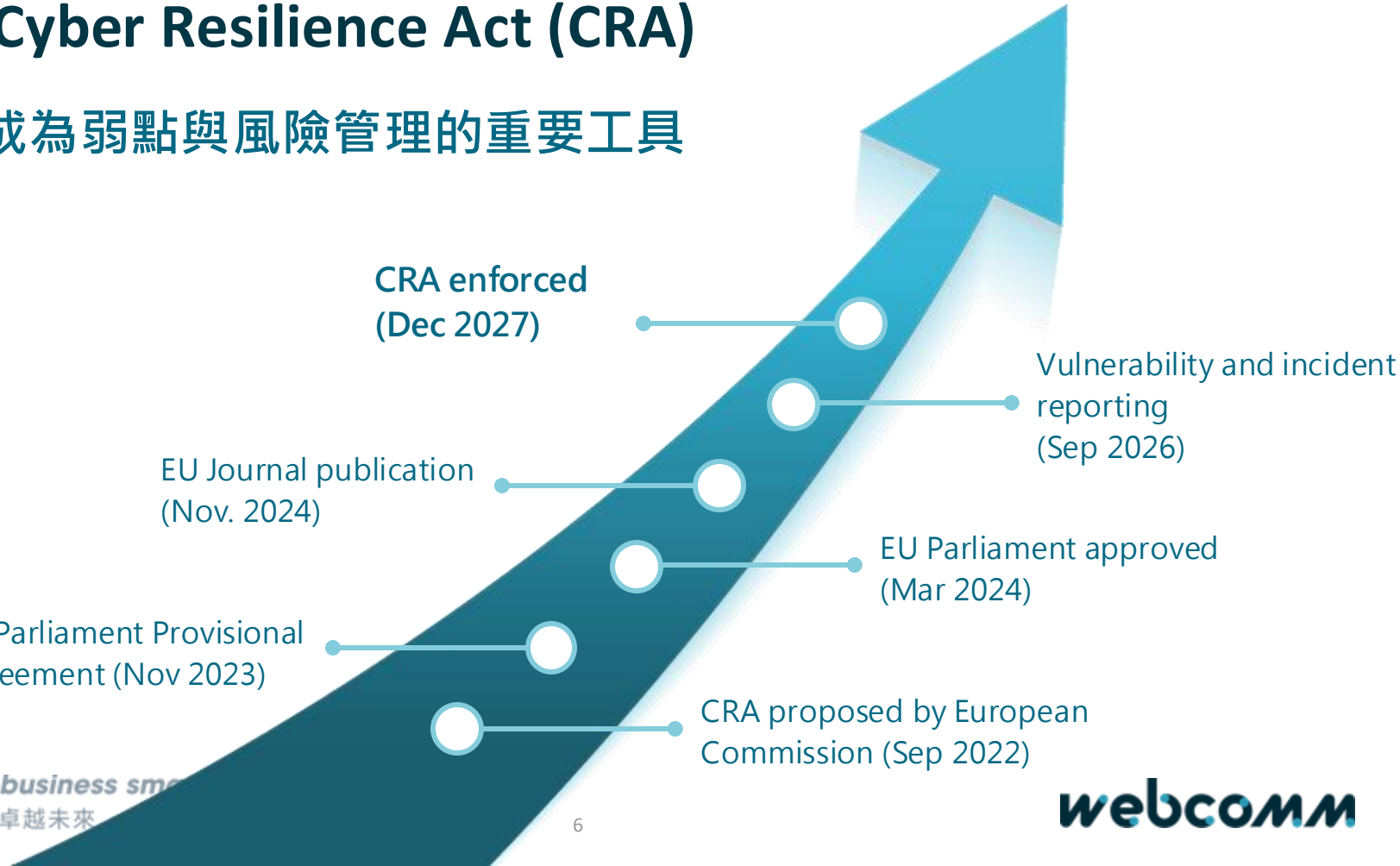
美國 - EO 14028

(vii) providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website;



歐盟 - Cyber Resilience Act (CRA)

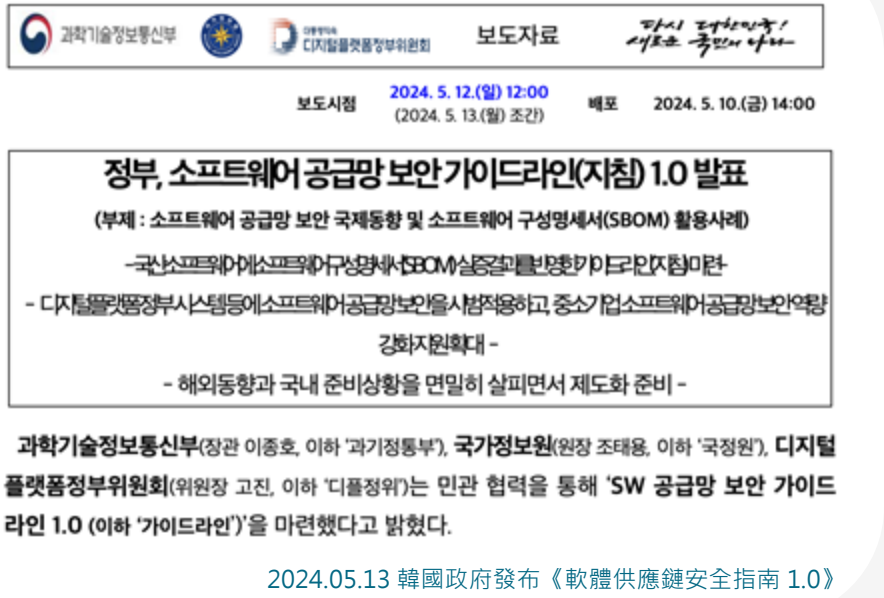
SBOM 成為弱點與風險管理的重要工具



南韓 - 政府軟體供應鏈安全指南 1.0

- **應對美國與歐洲國家政策**
  當提供SBOM成為必要時，政府、公共機構、企業應具備軟體供應鏈安全管理能力。

- **為國產軟體制定標準**
  針對大中小型企業，提供支持，建立制度。



과학기술정보통신부 | 디지털플랫폼정부위원회 | 보도자료

보도시점 2024. 5. 12.(일) 12:00 (2024. 5. 13.(월) 조간) | 배포 2024. 5. 10.(금) 14:00

정부, 소프트웨어 공급망 보안 가이드라인(지침) 1.0 발표

(부제 : 소프트웨어 공급망 보안 국제동향 및 소프트웨어 구성명세서(SBOM) 활용사례)

-국산소프트웨어에소프트웨어구성명세서SBOM실증결과를반영한가이드라인지침마련-

- 디지털플랫폼정부시스템등에소프트웨어공급망보안을시범적용하고, 중소기업소프트웨어공급망보안역량 강화지원확대 -

- 해외동향과 국내 준비상황을 면밀히 살피면서 제도화 준비 -

과학기술정보통신부(장관 이종호, 이하 '과기정통부'), **국가정보원**(원장 조태용, 이하 '국정원'), **디지털 플랫폼정부위원회**(위원장 고진, 이하 '디플정위')는 민관 협력을 통해 **'SW 공급망 보안 가이드라인 1.0 (이하 '가이드라인')'**을 마련했다고 밝혔다.

2024.05.13 韓國政府發布《軟體供應鏈安全指南 1.0》

新加坡 - CSA 針對開源與第三方軟體的安全建議

通過自動化工具生成SBOM，能夠在軟體開發過程中實現即時監控，並提高漏洞修復的效率。

2025.02.20 新加坡網路安全局(CSA) 發布

印度 - CERT-in 釋出SBOM技術指南

建議將提供 SBOM 作為標準實踐，
以增強安全性並降低風險。

特別是公部門、關鍵設施、軟體
出口與軟體服務業。

02

軟體開發生命週期中加入產製與管理SBOM

Progress since 2024

開始前確定目標

主要目標

- 產出產品的 SBOM
- 提升修正 CVE 的效率和主動性

次要目標

- OSS License 管理
- 根據本次產出的資料規劃未來如何納入產品管理

首先決定要產生哪一類SBOM

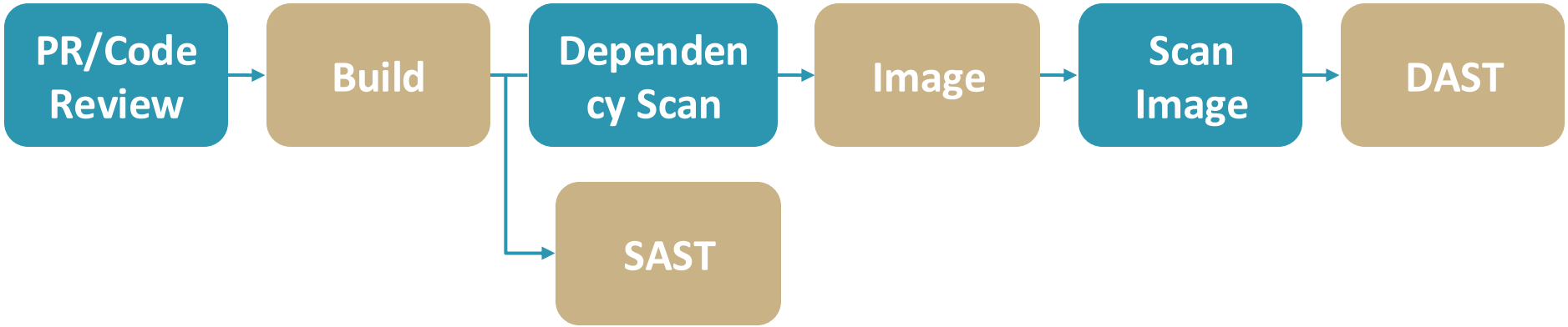
- **Source/Build SBOM**
- **Analyzed SBOM**

  - **Design** : Created on early dev stages from design documents
  - **Source** : Created from the source code
  - **Build** : Created during CI/CD process for separate releasable artifacts
  - **Analyzed**: Created from a set of bin/executable files or from installation files or virtual machine images through analysis of artifacts
  - **Deployed**: A set of images/install files which represent the system as a whole
  - **Runtime**: SBOM extracted from working system

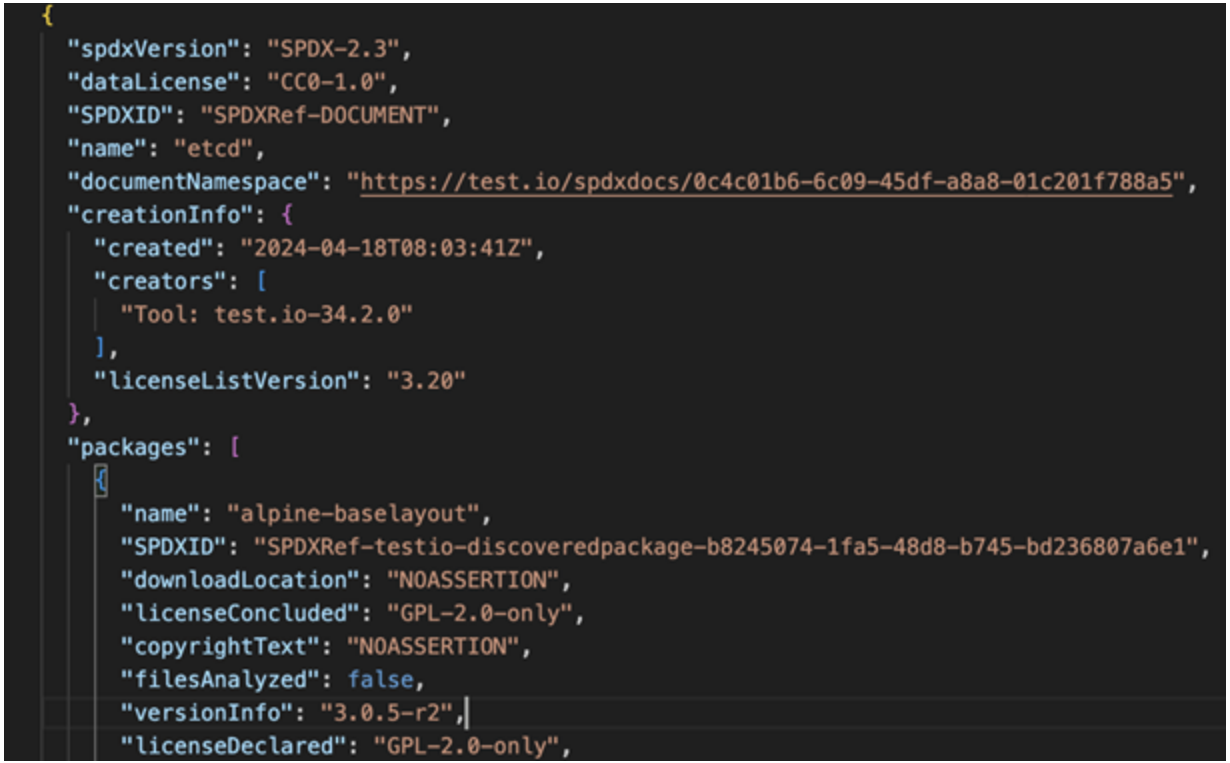
Ref: https://www.cisa.gov/resources-tools/resources/types-software-bill-materials-sbom

其實我們好像都已經有做了？

只是替換報告產生的格式？



檔案長出來之後故事才開始...



第一個困難：SBOM 不是給人讀的

- 資料品質很難驗證
- OSS 是良心事業

那我們先看 CVE 好了


```
{
  "spdxVersion": "SPDX-2.3",
  "dataLicense": "CC0-1.0",
  "SPDXID": "SPDXRef-DOCUMENT",
  "name": "etcd",
  "documentNamespace": "https://test.io/spdxdocs/0c4c01b6-6c09-45df-a8a8-01c201f788a5",
  "creationInfo": {
    "created": "2024-04-18T08:03:41Z",
    "creators": [
      "Tool: test.io-34.2.0"
    ],
    "licenseListVersion": "3.20"
  },
  "packages": [
    {
      "name": "alpine-baselayout",
      "SPDXID": "SPDXRef-testio-discoveredpackage-b8245074-1fa5-48d8-b745-bd236807a6e1",
      "downloadLocation": "NOASSERTION",
      "licenseConcluded": "GPL-2.0-only",
      "copyrightText": "NOASSERTION",
      "filesAnalyzed": false,
      "versionInfo": "3.0.5-r2",
      "licenseDeclared": "GPL-2.0-only",
```

第二個困難：工具產生出來的結果南轅北轍

- 就算只看 CVE，T 牌、C 牌、B 牌、M 牌結果都不一樣
- 工具掃描的邏輯不一樣，理解運作原理之後一個一個判定

第三個困難：修不完的 CVE

- 約有九成的 CVE 數量來自非自行開發的部分
- Linux 更換
  - alpine, centos, debian…
- distroless
- wolfi

Library	Vulnerability	Severity	Status	Installed Version	Fixed Version
busybox	CVE-2023-42363	MEDIUM	fixed	1.36.1-r15	1.36.1-r17
	CVE-2023-42364				1.36.1-r19
	CVE-2023-42365				
	CVE-2023-42366				1.36.1-r16
busybox-binsh	CVE-2023-42363				1.36.1-r17
	CVE-2023-42364				1.36.1-r19
	CVE-2023-42365				
	CVE-2023-42366				1.36.1-r16

第三個困難：修不完的 CVE part2

- 剩下一成的 CVE 還是修不完
- Why？

客戶說：我們要 0 CVE

安全性基準 = 0 CVE？

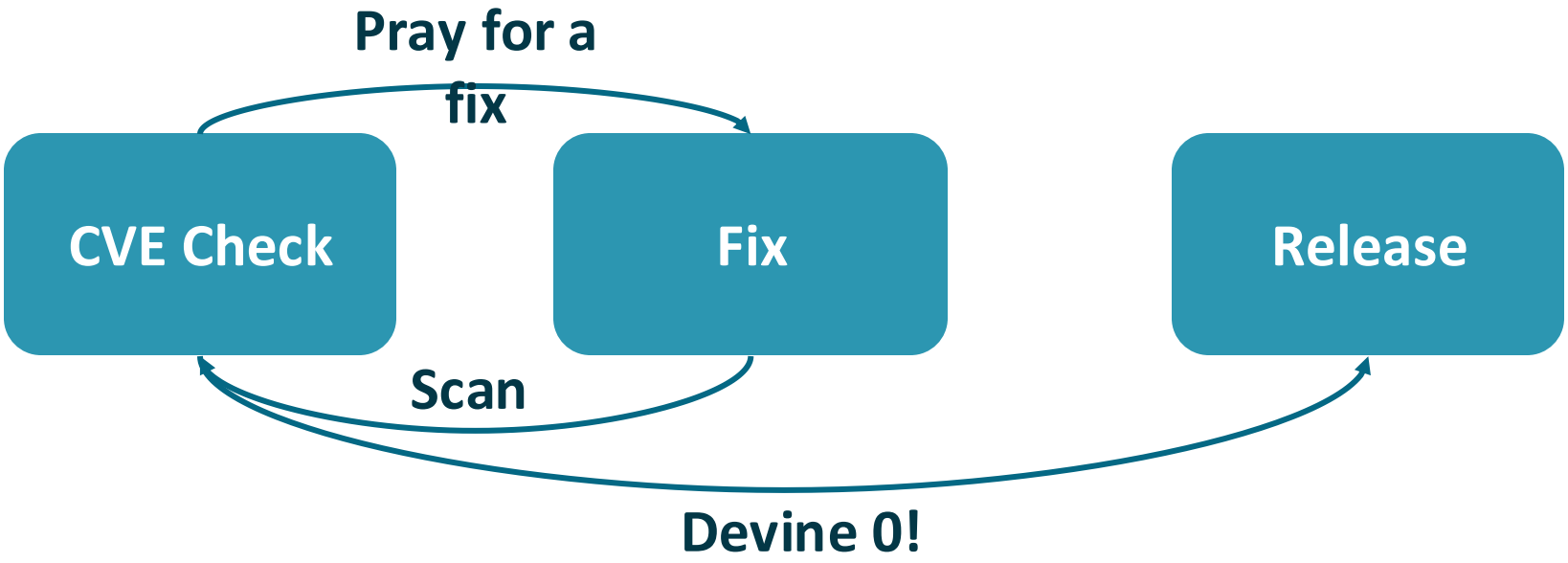
YES

一個標準應該是，簡單，容易有共識，而且可執行的。

NO

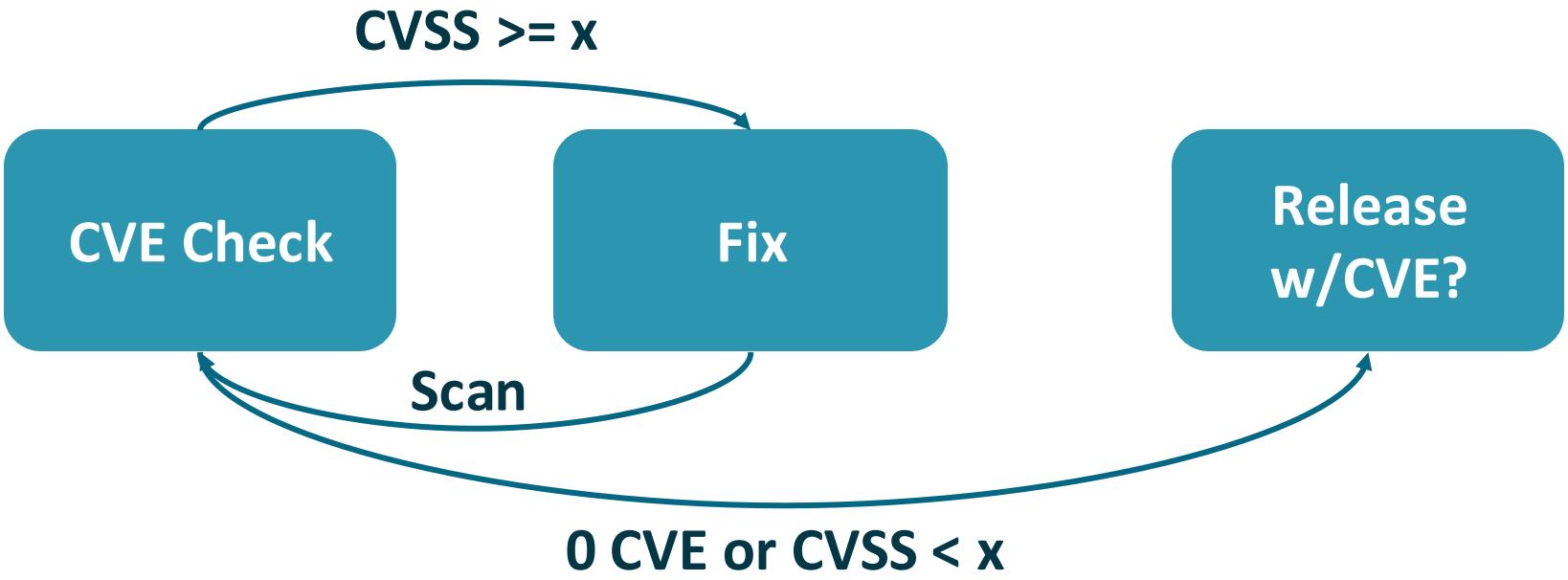
- 還不夠，因為可能還會有 CVE Not
- 不可行，因為無法持續。漏洞可能隨時產生，0 是哪一個時間點的 0？
- 不可能，實務上存在無法修復的情形，無人維護 or 作者不認為該修

追求 0 的話，產品更新得燒香...



軟體開發現實上，需要一個停止策略

但這樣 Release 可能還是會有 CVE？



VEX登場

- Vulnerability Exploitability eXchange
- 表示軟體產品與已知漏洞之間關聯狀態的機器可讀安全建議格式。
- 標準格式：CycloneDX, CSAF, SPDX 3.0

區塊	說明
VEX 中繼資料 (Metadata)	包含 VEX 格式識別、文件識別碼 (ID)、作者、作者角色及時間戳。這些資訊用於追蹤與管理 VEX 文件的版本，並說明由誰及於何時發布。
產品資訊 (Product Details)	以產品或產品線標識來描述目標軟體，可使用供應商名稱、產品名稱、版本或其他唯一 ID (如 purl、CPE、SWID、SPDXID)。若一次針對多版本、多產品，可在此區塊分別列出。
漏洞資訊 (Vulnerability Details)	以漏洞編號 (如 CVE-2023-XXXX) 與漏洞描述呈現，可視需要補充 CVSS 分數或參考連結，協助讀者快速了解漏洞來源與成因。
產品狀態資訊 (Product Status Details)	針對特定產品版本描述其對應漏洞的可利用狀態，如 NOT_AFFECTED (不受影響)、AFFECTED (受影響)、FIXED (已修復)、UNDER_INVESTIGATION (調查中)。若為 AFFECTED，須提供建議措施；若為 NOT_AFFECTED，須說明為何不受影響。

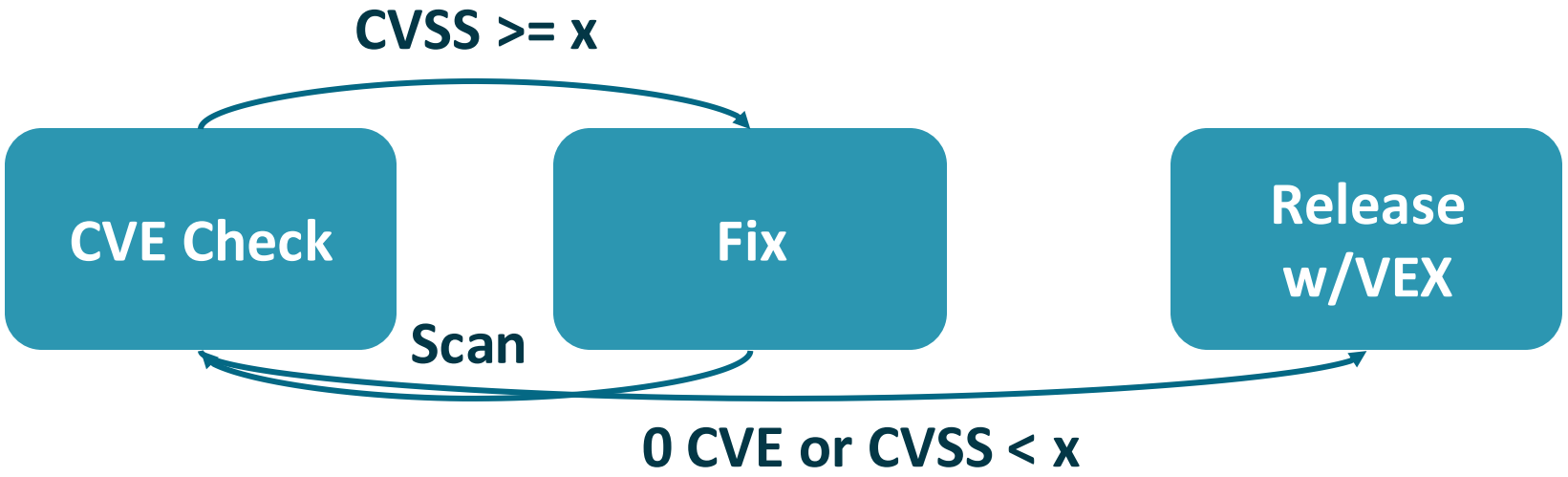
不是所有 CVE 都可被利用

- **Not Affected**
  解釋為何不被影響
- **Affected**
  對策動作，或可能的攻擊手法
- **Fixed**
  更新已經修正
- **Under Investigation**
  如實告知才能聯防

```
"vulnerabilities": [
  {
    "id": "CVE-2023-0001",
    "description": "範例漏洞描述：可能導致服務中斷。",
    "affects": [
      {
        "ref": "pkg:generic/exampleproduct@1.0",
        "versions": [
          {
            "version": "1.0",
            "status": "affected",
            "statusNotes": "建議升級至 1.1"
          }
        ]
```

務實的安全性基準 = 排除可控風險的 0 CVE + 行動

- 重視安全，而不是數字遊戲
- 把資源集中在真的可能造成影響的地方
- 其他原先該有的對策都還是需要做



產品購買方，也可建立一個收斂策略？

- 實際有影響的 CVE 有多少個，多久能有緩解或者對策？
- 測量每個月的 CVSS > 4 的數量並且觀察趨勢

第四個困難：理想很美好，現實...

- 無論是 SBOM 或者 VEX，未能真的傳遞到上下游
- 驗收上仍然以直接掃描工具的 report 為主
- 雖然產品購買方最終也能理解務實的0，但現行溝通成本很高

結論：回顧當初目標

主要目標

- 產出產品的 SBOM 😄
- 提升修正 CVE 的效率和主動性 😄

次要目標

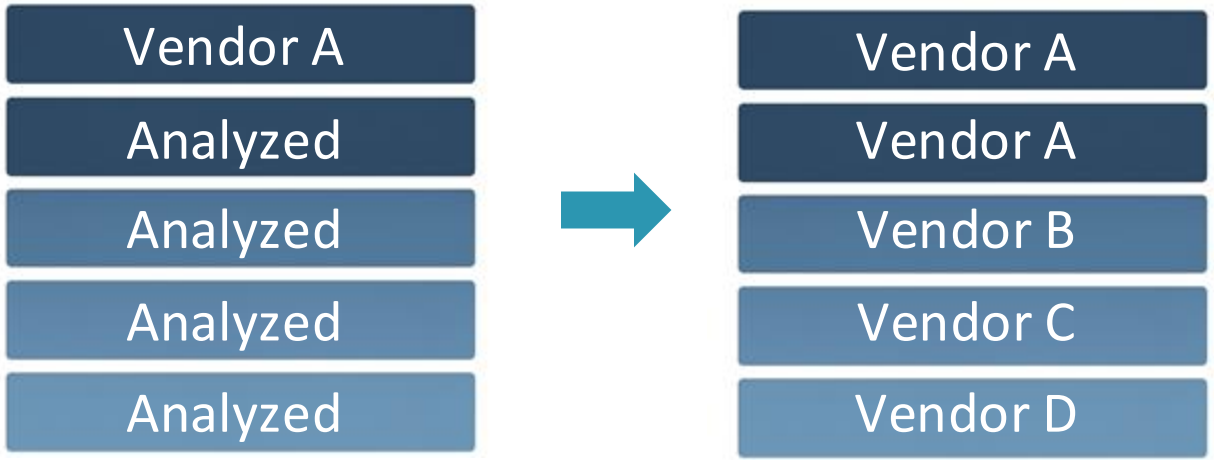
- OSS License 管理 😐
- 根據本次產出的資料規劃未來如何納入產品管理 😐

03 未來的發想與課題

Future Plans

未來的課題一：如何提升資料正確性？

- 來源的正確性可以技術解決
- 內容的正確性，需要更多人投入

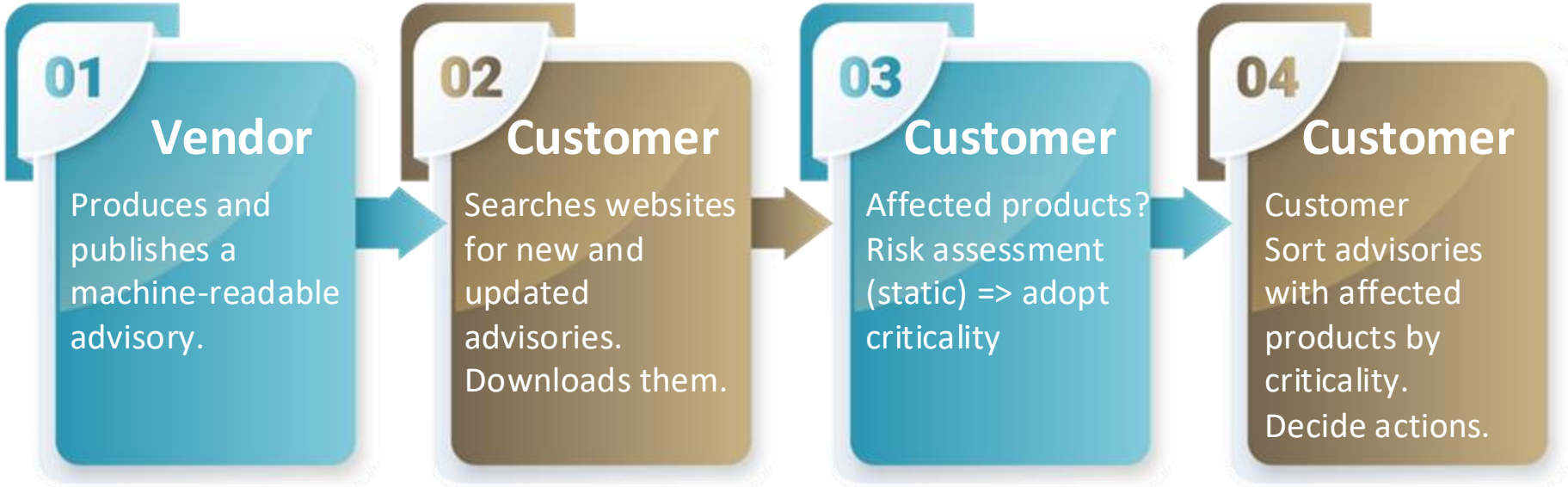


未來課題二：供應鏈間如何有效運用 SBOM/VEX？

- NDA 之後 email
- Vendor Portal
- Distributed Ledger？
- **CSAF (Common Security Advisory Framework)**

Oasis CSAF 2.0

取代 CVRF(Common Vulnerability Reporting Framework)



Ref: https://www.csaf.io

目前試行 CSAF 的政府單位與企業

Ref: https://www.csaf.io

關於產業未來的想像

- 交換控管
  - 產業 ISAC：Health-ISAC 有共同的 SBOM Repo
- 台灣
  - 政策之外，中介的角色也會是產業 ISAC擔任？

國家資通安全研究院
National Institute of Cyber Security

衛生福利部資安資訊分享與分析中心
Hospital Cybersecurity Information Sharing and Analysis Center

金融資安資訊分享與分析中心
Financial Information Sharing and Analysis Center

THANK YOU

We make your business smarter
透過科技創新邁向卓越未來