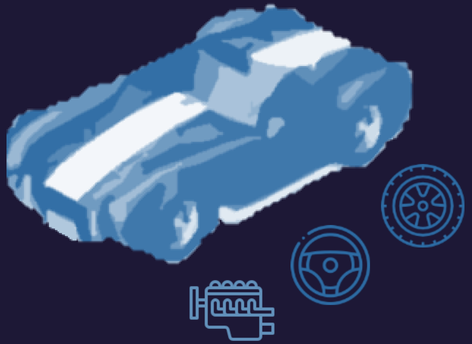
SBOM (軟體物料清單) Ready? How do you turn this on?

關鍵基礎設施產業 SBOM 剖析



Yenting Lee, Sr. Threat Researcher
PSIRT and Threat Research, TXOne Networks Inc.
May 15, 2024 @CYBERSEC 2024

大綱

01 | SBOM 簡介

- 全球關鍵基礎設施產業面臨的資安威脅
- SBOM 為軟體安全關鍵組成

02 | SBOM 運作方式

- SBOM 標準、 類型、組成
- VEX

03 | SBOM 合作與應用

- 關鍵基礎設施產業 SBOM 概念性驗證
- 軟體標示符

04 | SBOM 採用

- 開始使用 SBOM
- 結論與建議

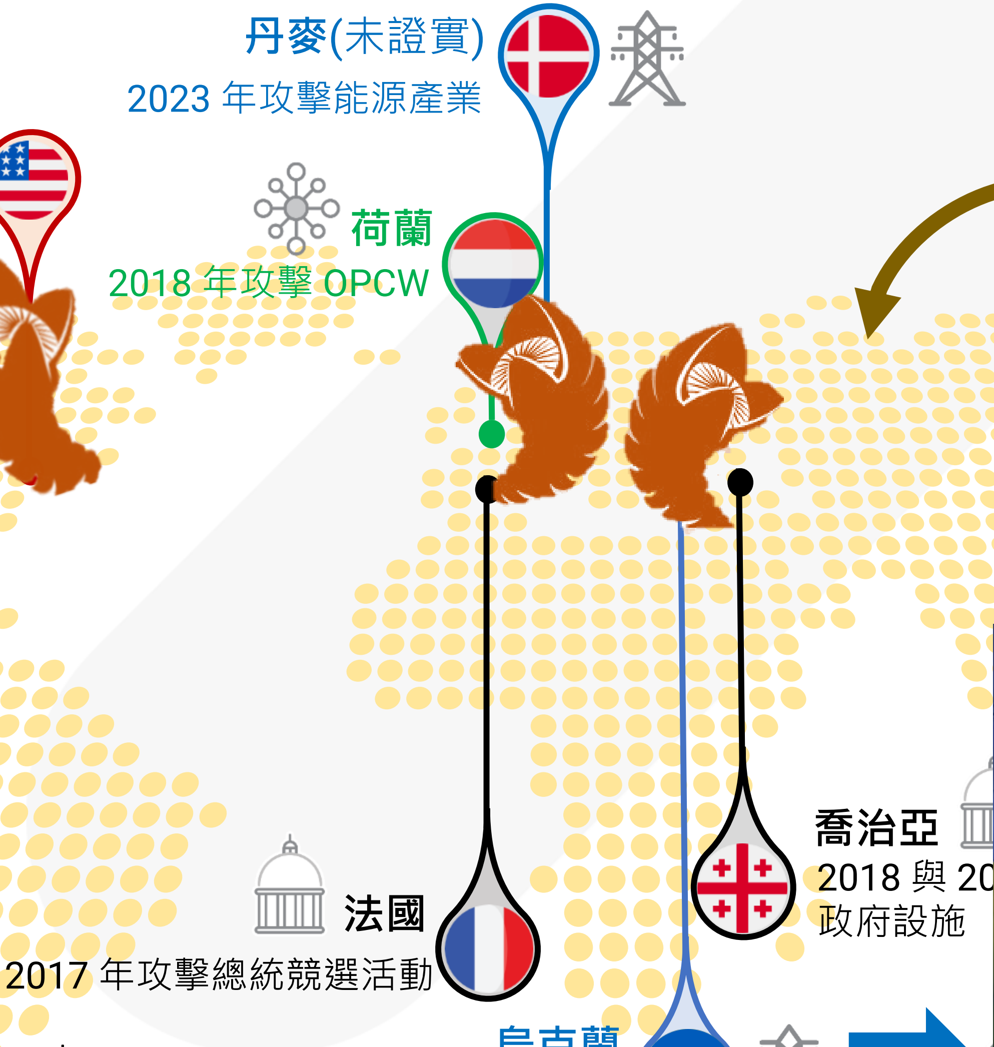
Yenting Lee

Sr. Threat Researcher, PSIRT and Threat Research at TXOne Networks

- ICS/SCADA, IoT, Penetration Testing, Threat Hunting, and Image Processing
- Cyber Offensive and Defensive Exercise
- Spoke at FIRST, ICS Cyber Security Conference USA/APAC, SECCON, CYBERSEC Taiwan, PPAM India, InfoSec Taiwan, C-ISAC Taiwan, etc.
- Lecturer at India government, Taiwan government, and Universities
- Several CVEs and White Papers on the topic of ICS

SBOM 簡介

俄羅斯沙蟲威脅團隊席捲全球



丹麥(未證實)

2023 年攻擊能源產業

美國

- 2017 年攻擊醫療保健與製藥商
- 2024 年鎖定水利設施

荷蘭

2018 年攻擊 OPCW

法國

2017 年攻擊總統競選活動

烏克蘭

2015 與 2016 年攻擊電力公司

喬治亞

2018 與 20

政府設施

沙蟲威脅團隊

NotPetya 毀壞式攻擊造成了 100 億美元的損失，同時損害患者的健康

https://slate.com/technology/2019/11/sandworm-andy-greenberg-excerpt-notpetya-hospitals.html

長達數小時的斷電，影響至 25 萬人

https://www.govinfosecurity.com/ukrainian-power-grid-hacked-a-8779

https://securityaffairs.com/114606/apt/anssi-sandworm-hosting-providers-attacks.html

2023 年對丹麥能源產業的攻擊鏈

偵查

武裝

遞送

漏洞利用

安裝

命令與控制

行動

知道丹麥能源公
司使用的防火牆

開發可利用 Zyxel
防火牆 1-day 漏洞
的網路攻擊武器

使用攻擊封包對
防火牆 Port 500
服務攻擊

攻擊封包包含 C2
連線與其他指令

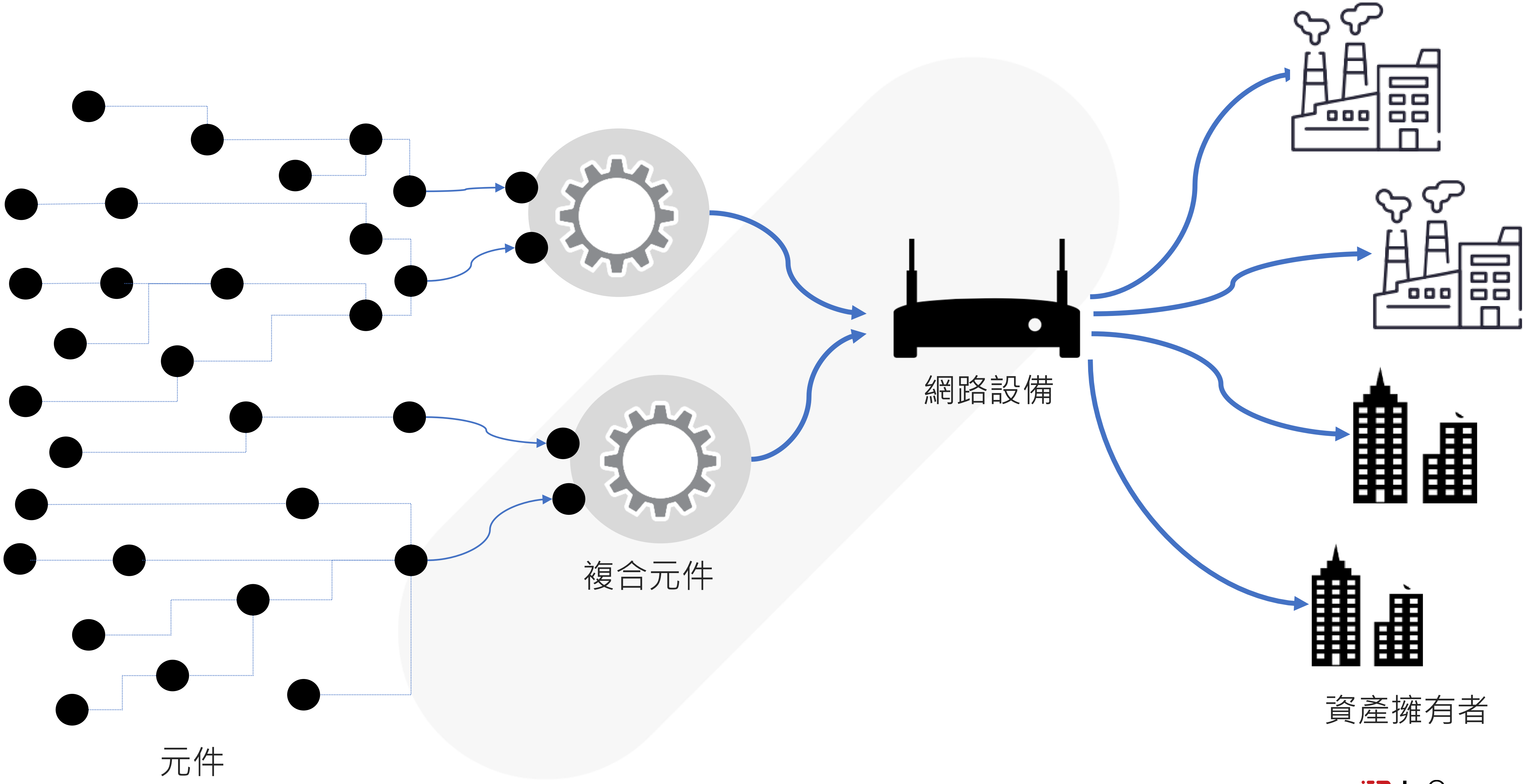
安裝多種 payloads
以確保控制防火牆

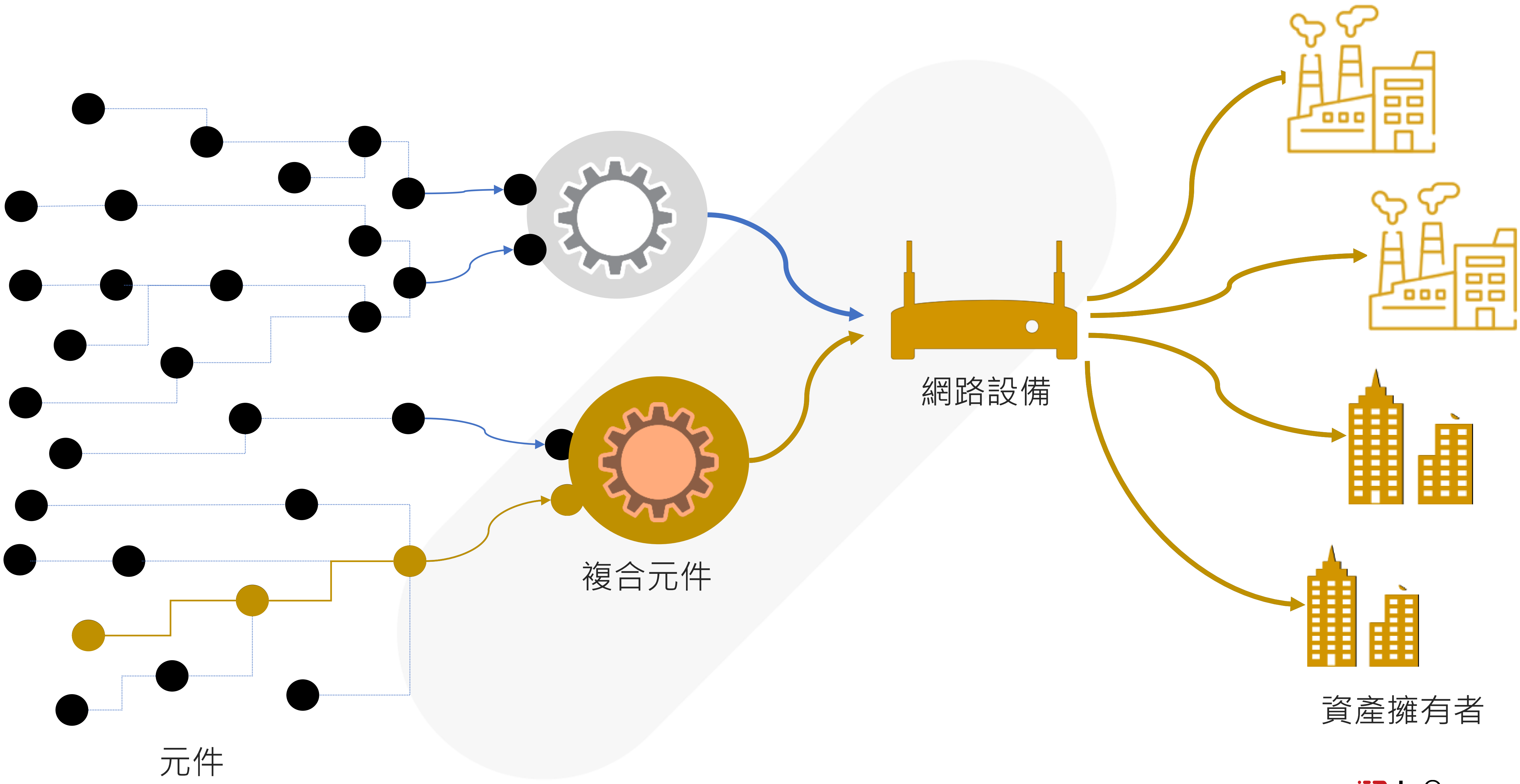
持續與攻擊者
建立連線

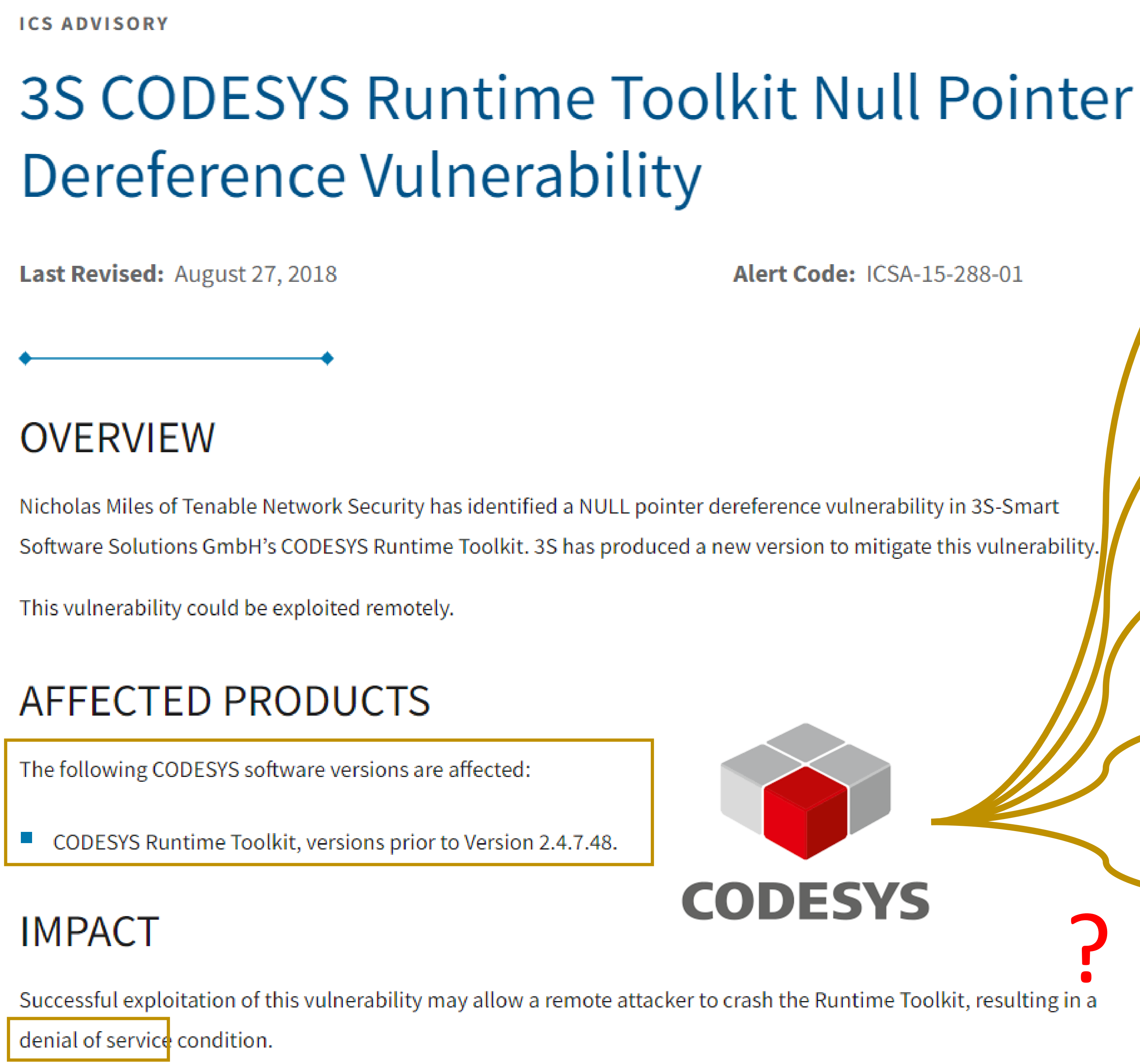
防火牆仍可保持運作，
使攻擊難以偵測

- 在案例中，部分能源廠直接使用該防火牆充當 OT 網路的內部路由器
- 此事件後，丹麥每天遭受約 20 萬次使用此 1-day 漏洞的攻擊

https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf


網路設備
複合元件
資產擁有者
元件


網路設備
複合元件
資產擁有者
元件



ICS ADVISORY

3S CODESYS Runtime Toolkit Null Pointer Dereference Vulnerability

Last Revised: August 27, 2018 **Alert Code:** ICSA-15-288-01

OVERVIEW

Nicholas Miles of Tenable Network Security has identified a NULL pointer dereference vulnerability in 3S-Smart Software Solutions GmbH's CODESYS Runtime Toolkit. 3S has produced a new version to mitigate this vulnerability.

This vulnerability could be exploited remotely.

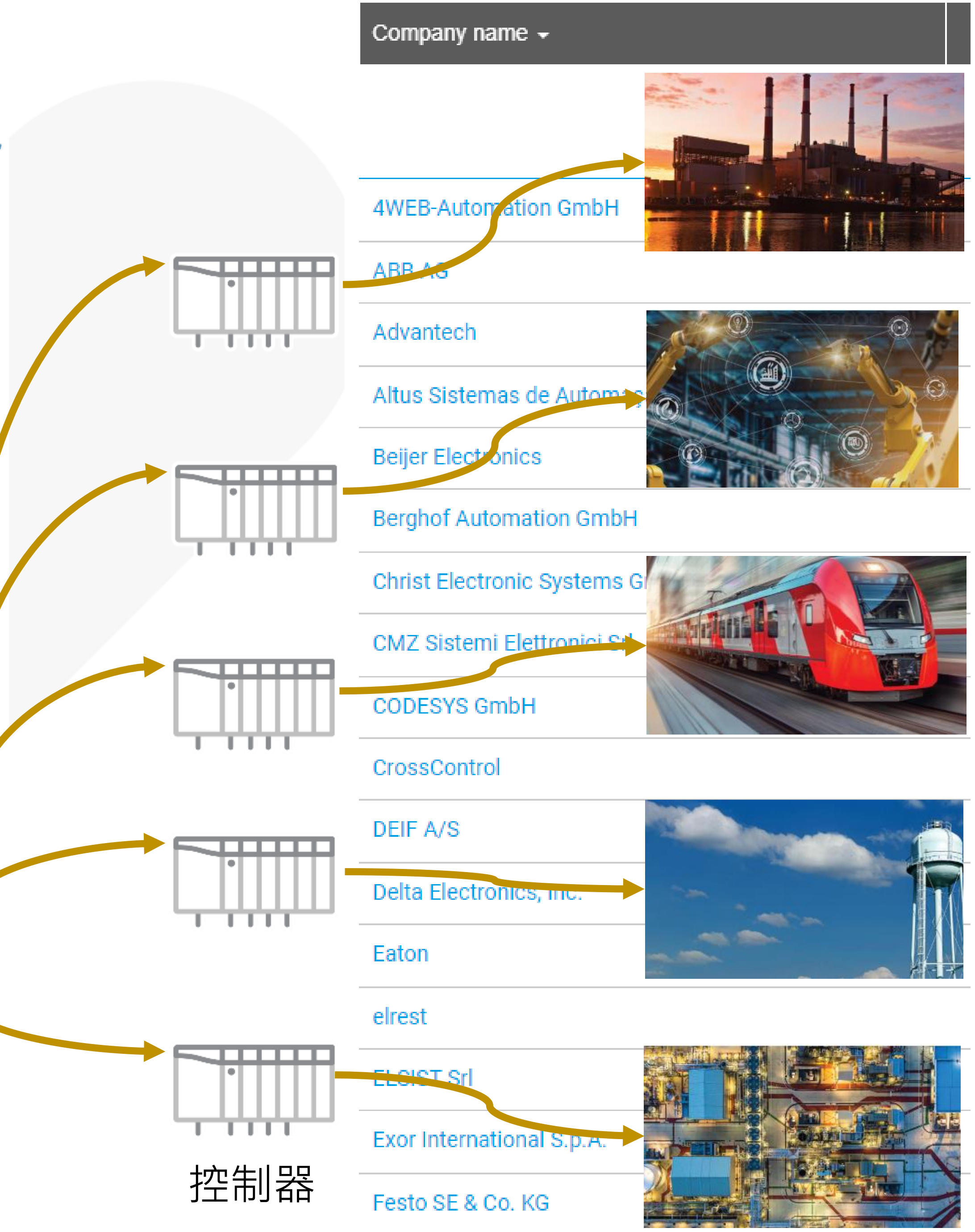
AFFECTED PRODUCTS

The following CODESYS software versions are affected:

- CODESYS Runtime Toolkit, versions prior to Version 2.4.7.48.

IMPACT

Successful exploitation of this vulnerability may allow a remote attacker to crash the Runtime Toolkit, resulting in a denial of service condition.



Company name ▾

- 4WEB-Automation GmbH
- ABB AG
- Advantech
- Altus Sistemas de Autom
- Beijer Electronics
- Berghof Automation GmbH
- Christ Electronic Systems G
- CMZ Sistemi Elettronici S
- CODESYS GmbH
- CrossControl
- DEIF A/S
- Delta Electronics, Inc.
- Eaton
- elrest
- ELSIST Srl
- Exor International S.p.A.
- Festo SE & Co. KG

MITRE ATT&CK for ICS

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	10 techniques	6 techniques	2 techniques	7 techniques	5 techniques	7 techniques	11 techniques	3 techniques	14 techniques	5 techniques	12 techniques
Drive-by Compromise	Autorun Image	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Change Operating Mode	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Command-Line Interface	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Execution through API	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Graphical User Interface	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Hooking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Replication Through Removable Media	Modify Controller Tasking			System Binary Proxy Execution		Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Rogue Master	Native API						Point & Tag Identification		Denial of Service		Loss of Safety
Spearphishing Attachment	Scripting						Program Upload		Device Restart/Shutdown		Loss of View
Supply Chain Compromise	User Execution						Screen Capture		Manipulate I/O Image		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
Wireless Compromise									Rootkit		Theft of Operational Information
									Service Stop		
									System Firm		

CODESYS

SBOM 已成為**軟體安全**與**供應鏈管理**中關鍵組成部分

-- from CISA’s Cyber Threats and Advisories
https://www.cisa.gov/sbom

https://www.youtube.com/watch?v=yTuBf_MFjMc

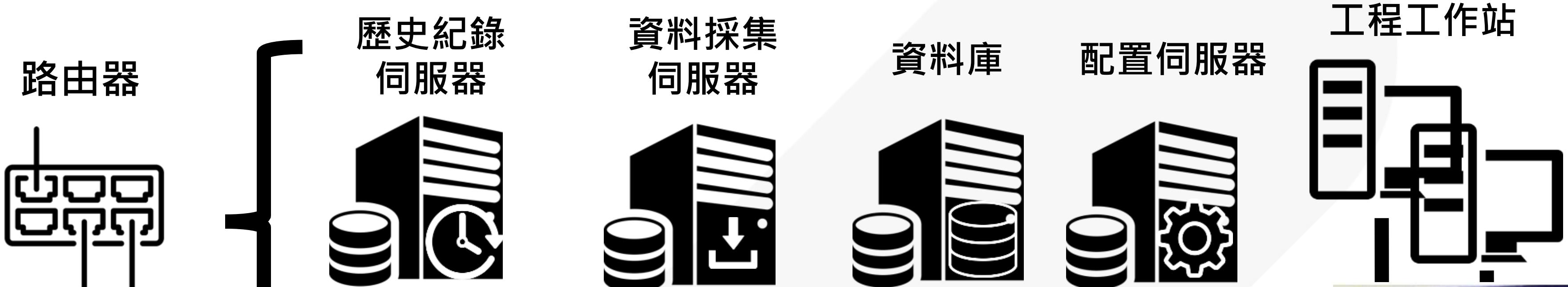
SBOM 的益處

	開發	選擇	操作
花費	減少未預期的工作	更精準的總成本	更有效率的管理
資安管理	避免使用已知漏洞	容易進行安全審查	快速發現已知的漏洞
License 管理	量化與管理 License	容易進行 License 審查	更精準回應 License 聲明
合規管理	在生命週期早期 識別合規要求	在早期發現合規問題	精簡流程
提高保證	對所使用的元件做出保證	對元件做出知情的選擇	在變化環境下驗證聲明

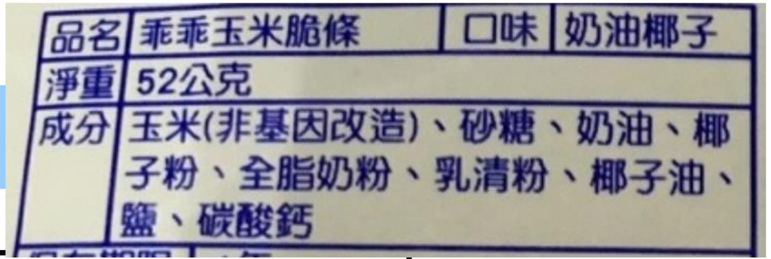
https://www.cisa.gov/sites/default/files/2023-01/Dec15-SBOM-a-rama-slides.pdf

SBOM 運作方式

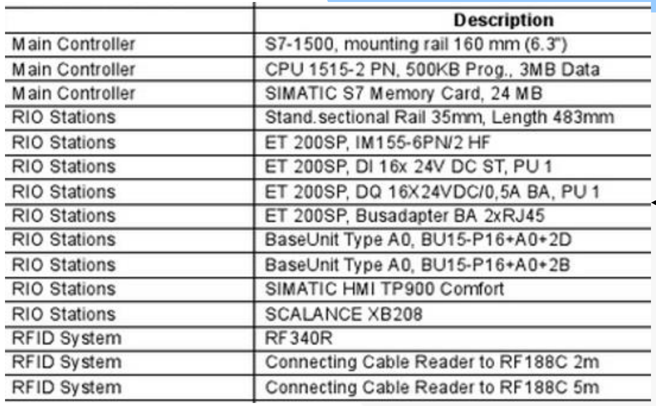
OT 環境架構



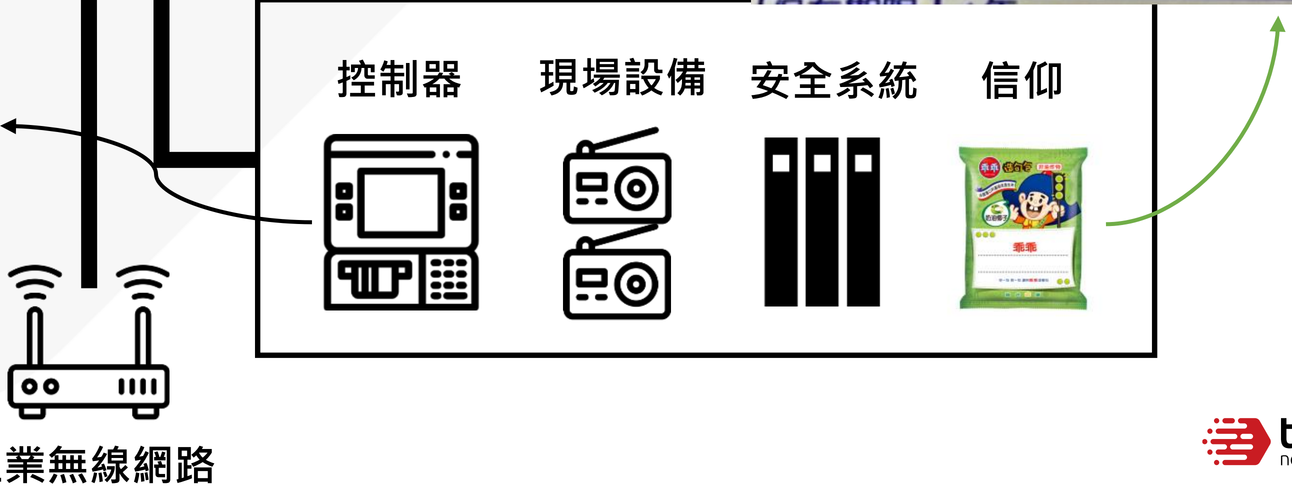
Control System Network



品名	乖乖玉米脆條	口味	奶油椰子
淨重	52公克		
成分	玉米(非基因改造)、砂糖、奶油、椰子粉、全脂奶粉、乳清粉、椰子油、鹽、碳酸鈣		



	Description
Main Controller	S7-1500, mounting rail 160 mm (6.3")
Main Controller	CPU 1515-2 PN, 500KB Prog., 3MB Data
Main Controller	SIMATIC S7 Memory Card, 24 MB
RIO Stations	Stand.sectional Rail 35mm, Length 483mm
RIO Stations	ET 200SP, IM155-6PN/2 HF
RIO Stations	ET 200SP, DI 16x 24V DC ST, PU 1
RIO Stations	ET 200SP, DQ 16X24VDC/0,5A BA, PU 1
RIO Stations	ET 200SP, Busadapter BA 2xRJ45
RIO Stations	BaseUnit Type A0, BU15-P16+A0+2D
RIO Stations	BaseUnit Type A0, BU15-P16+A0+2B
RIO Stations	SIMATIC HMI TP900 Comfort
RIO Stations	SCALANCE XB208
RFID System	RF340R
RFID System	Connecting Cable Reader to RF188C 2m
RFID System	Connecting Cable Reader to RF188C 5m



https://www.scribd.com/document/516884703/PLC-BOM

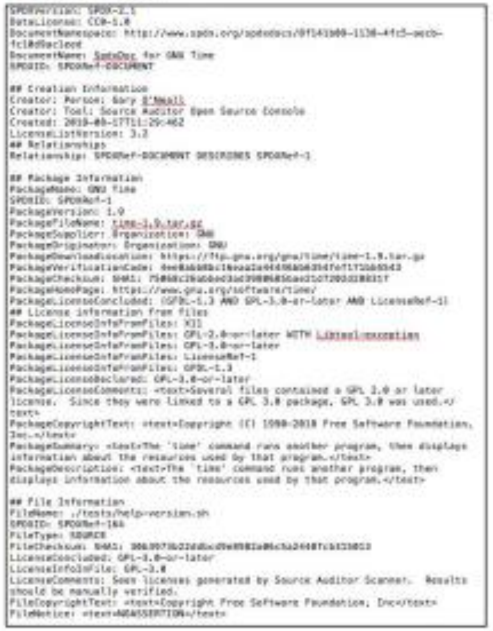
大量的資產需要管理

https://www.chinatimes.com/realtimenews/20201216003832-260405?chdtv

現有的標準

- 美國國家電信暨資訊管理局 (NTIA)
  - 調查了現有的標準、格式，說明 SBOM 最小組成元素

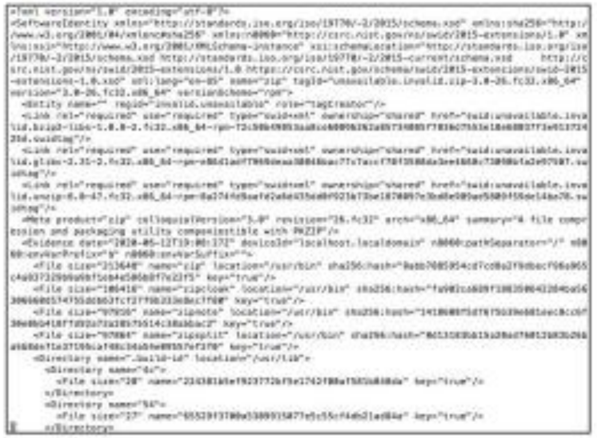
SPDX



```
SPDXVersion: SPDX-2.1
DataLicense: CC0-1.0
DocumentNamespace: http://www.spdx.org/spdxdocs/0f141b00-1130-4fc5-aecb-
fc10d0acled
DocumentName: SpdxDoc for GNU Time
SPDXID: SPDXRef-DOCUMENT

## Creation Information
Creator: Person: Gary O'Neall
Creator: Tool: Source Auditor Open Source Console
Created: 2019-09-17T11:29:46Z
LicenseListVersion: 3.2
## Relationships
Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-1

## Package Information
PackageName: GNU Time
SPDXID: SPDXRef-1
PackageVersion: 1.9
PackageFileName: time-1.9.tar.gz
PackageSupplier: Organization: GNU
PackageOriginator: Organization: GNU
PackageDownloadLocation: https://ftp.gnu.org/gnu/time/time-1.9.tar.gz
PackageVerificationCode: [illegible]
PackageChecksum: SHA1: [illegible]
PackageHomePage: https://www.gnu.org/software/time/
PackageLicenseConcluded: (GFDL-1.3 AND GPL-3.0-or-later AND LicenseRef-1)
## License information from files
PackageLicenseInfoFromFiles: X11
PackageLicenseInfoFromFiles: GPL-2.0-or-later WITH Libtool-exception
PackageLicenseInfoFromFiles: GPL-3.0-or-later
PackageLicenseInfoFromFiles: LicenseRef-1
PackageLicenseInfoFromFiles: GFDL-1.3
PackageLicenseDeclared: GPL-3.0-or-later
PackageLicenseComments: <text>Several files contained a GPL 2.0 or later
license.  Since they were linked to a GPL 3.0 package, GPL 3.0 was used.</
text>
PackageCopyrightText: <text>Copyright (C) 1990-2018 Free Software Foundation,
Inc.</text>
PackageSummary: <text>The 'time' command runs another program, then displays
information about the resources used by that program.</text>
PackageDescription: <text>The 'time' command runs another program, then
displays information about the resources used by that program.</text>

## File Information
FileName: ./tests/help-version.sh
SPDXID: SPDXRef-164
FileType: SOURCE
FileChecksum: SHA1: [illegible]
LicenseConcluded: GPL-3.0-or-later
LicenseInfoInFile: GPL-3.0
LicenseComments: Seen licenses generated by Source Auditor Scanner.  Results
should be manually verified.
FileCopyrightText: <text>Copyright Free Software Foundation, Inc</text>
FileNotice: <text>NOASSERTION</text>
```

File formats: .xls, .spdx, .rdf, .json, .yml, .xml

SWID



```
<?xml version="1.0" encoding="utf-8"?>
<SoftwareIdentity xmlns="http://standards.iso.org/iso/19770/-2/2015/schema.xsd" xmlns:sha256="http:/
/www.w3.org/2001/04/xmlenc#sha256" xmlns:n8060="http://csrc.nist.gov/ns/swid/2015-extensions/1.0" xm
lns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://standards.iso.org/iso
/19770/-2/2015/schema.xsd http://standards.iso.org/iso/19770/-2/2015-current/schema.xsd     http://c
src.nist.gov/ns/swid/2015-extensions/1.0 https://csrc.nist.gov/schema/swid/2015-extensions/swid-2015
-extensions-1.0.xsd" xml:lang="en-US" name="zip" tagId="unavailable.invalid.zip-3.0-26.fc32.x86_64"
version="3.0-26.fc32.x86_64" versionScheme="rpm">
  <Entity name="" regid="invalid.unavailable" role="tagCreator"/>
  <Link rel="required" use="required" type="swid+xml" ownership="shared" href="swid:unavailable.inva
lid.bzip2-libs-1.0.8-2.fc32.x86_64-rpm-[illegible]
[illegible].swidtag"/>
  <Link rel="required" use="required" type="swid+xml" ownership="shared" href="swid:unavailable.inva
lid.glibc-2.31-2.fc32.x86_64-rpm-[illegible].sw
idtag"/>
  <Link rel="required" use="required" type="swid+xml" ownership="shared" href="swid:unavailable.inva
lid.unzip-6.0-47.fc32.x86_64-rpm-[illegible].sw
idtag"/>
  <Meta product="zip" colloquialVersion="3.0" revision="26.fc32" arch="x86_64" summary="A file compr
ession and packaging utility compatible with PKZIP"/>
  <Evidence date="2020-05-12T19:00:17Z" deviceId="localhost.localdomain" n8060:pathSeparator="/" n80
60:envVarPrefix="$" n8060:envVarSuffix="">
    <File size="253640" name="zip" location="/usr/bin" sha256:hash="[illegible]
[illegible]" key="true"/>
    <File size="106416" name="zipcloak" location="/usr/bin" sha256:hash="[illegible]
[illegible]" key="true"/>
    <File size="97936" name="zipnote" location="/usr/bin" sha256:hash="[illegible]
[illegible]" key="true"/>
    <File size="97984" name="zipsplit" location="/usr/bin" sha256:hash="[illegible]
[illegible]" key="true"/>
    <Directory name=".build-id" location="/usr/lib">
      <Directory name="4c">
        <File size="28" name="[illegible]" key="true"/>
      </Directory>
      <Directory name="5d">
        <File size="27" name="[illegible]" key="true"/>
      </Directory>
```

File formats: .xml

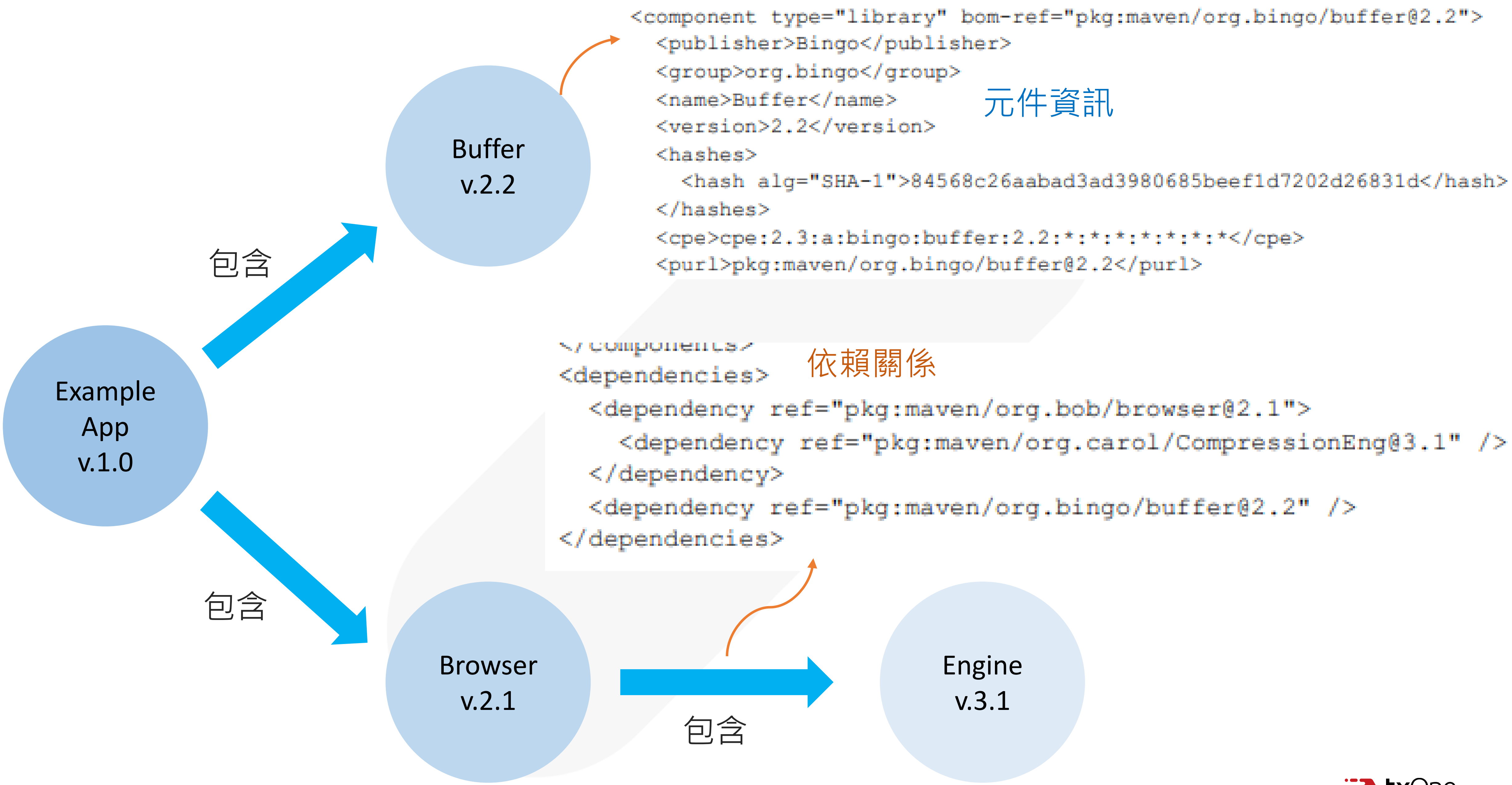
CycloneDX

[illegible]

File formats: .json, .xml

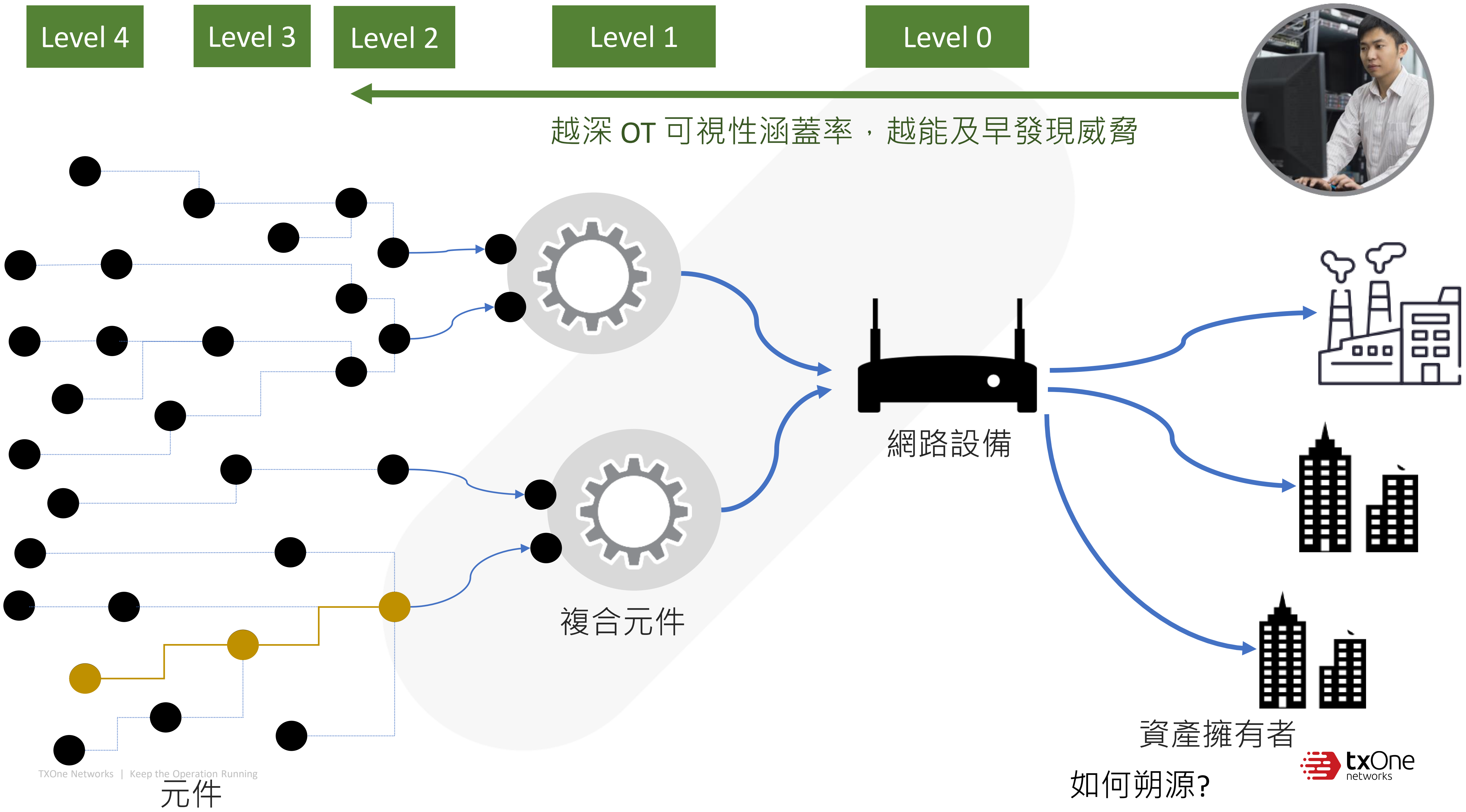
SBOM 最小組成元素

	參數	SPDX	CycloneDX	SWID
文件資訊	作者名稱	Creator	metadata/authors/author	<Entity> tagCreator, @name
	時戳	Created	metadata/timestamp	<Meta>
元件資訊	供應商名稱	PackageSupplier	Supplier	<Entity> softwareCreator, @name
	元件名稱	PackageName	name	<softwareIdnentity> @name
	元件版本	PackageVersion	version	<softwareIdnentity> @version
	Hash	PackageChecksum	hash	<Payload> @hash
	標識符	SPDXID	bom-ref	<softwareIdnentity> @tagID
依賴關係	依賴關係	Relationship	dependency	<Link>



```
<component type="library" bom-ref="pkg:maven/org.bingo/buffer@2.2">
  <publisher>Bingo</publisher>
  <group>org.bingo</group>
  <name>Buffer</name>
  <version>2.2</version>
  <hashes>
    <hash alg="SHA-1">84568c26aabad3ad3980685beef1d7202d26831d</hash>
  </hashes>
  <cpe>cpe:2.3:a:bingo:buffer:2.2:*:*:*:*:*:*:*</cpe>
  <purl>pkg:maven/org.bingo/buffer@2.2</purl>
```

```
</components>
<dependencies>
  <dependency ref="pkg:maven/org.bob/browser@2.1">
    <dependency ref="pkg:maven/org.carol/CompressionEng@3.1" />
  </dependency>
  <dependency ref="pkg:maven/org.bingo/buffer@2.2" />
</dependencies>
```



Level 4

Level 3

Level 2

Level 1

Level 0

越深 OT 可視性涵蓋率，越能及早發現威脅

複合元件

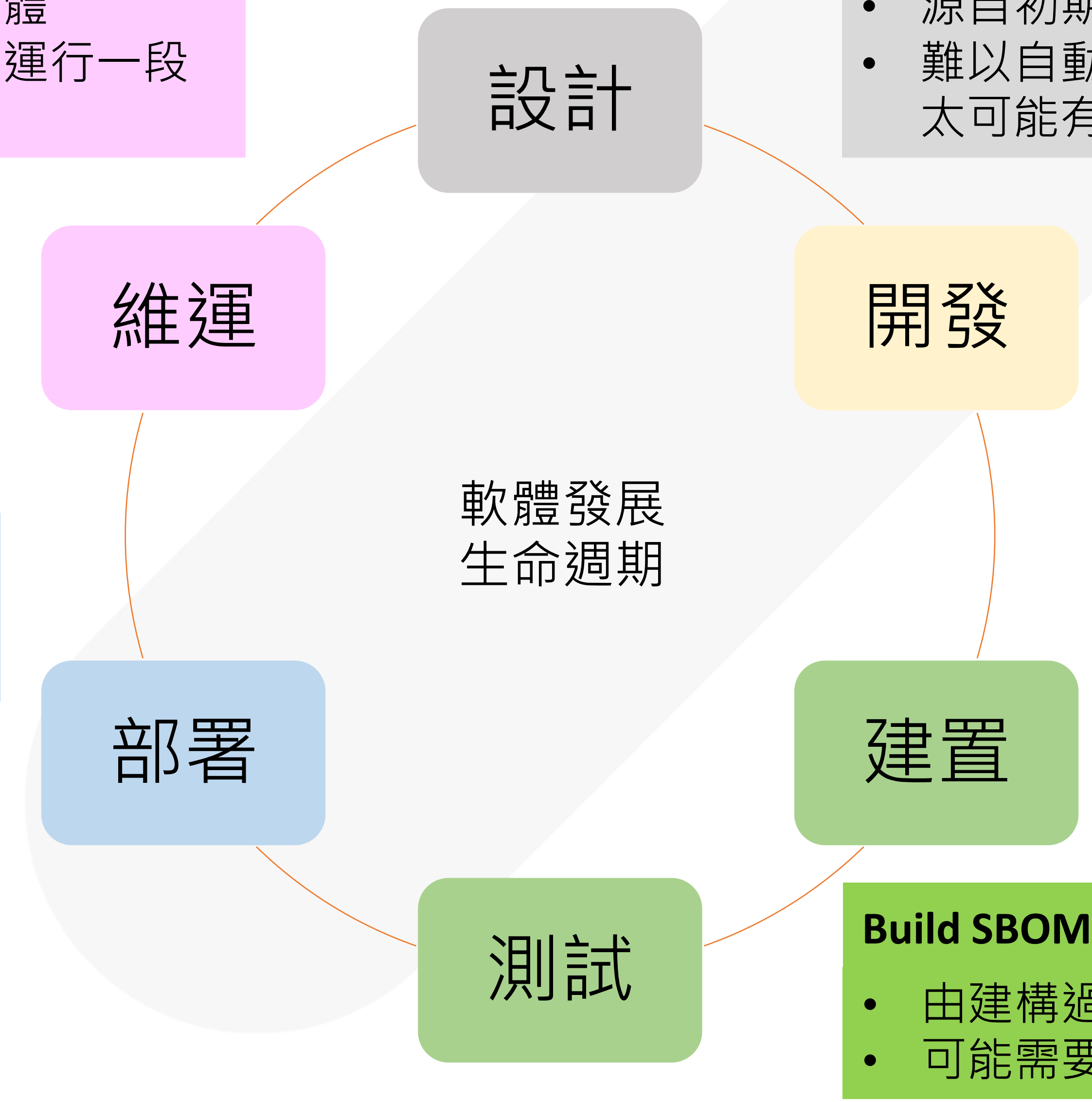
網路設備

資產擁有者

如何朔源?

元件

SBOM 類型



設計

開發

建置

測試

部署

維運

軟體發展
生命週期

Design SBOM

- 源自初期構想、RFP
- 難以自動化生成，也不太可能有夠詳細的資訊

Source SBOM

- 直接於開發環境的原始碼
- 容易產生未實際運行的元件

Build SBOM

- 由建構過程中生成
- 可能需要調整建置流程

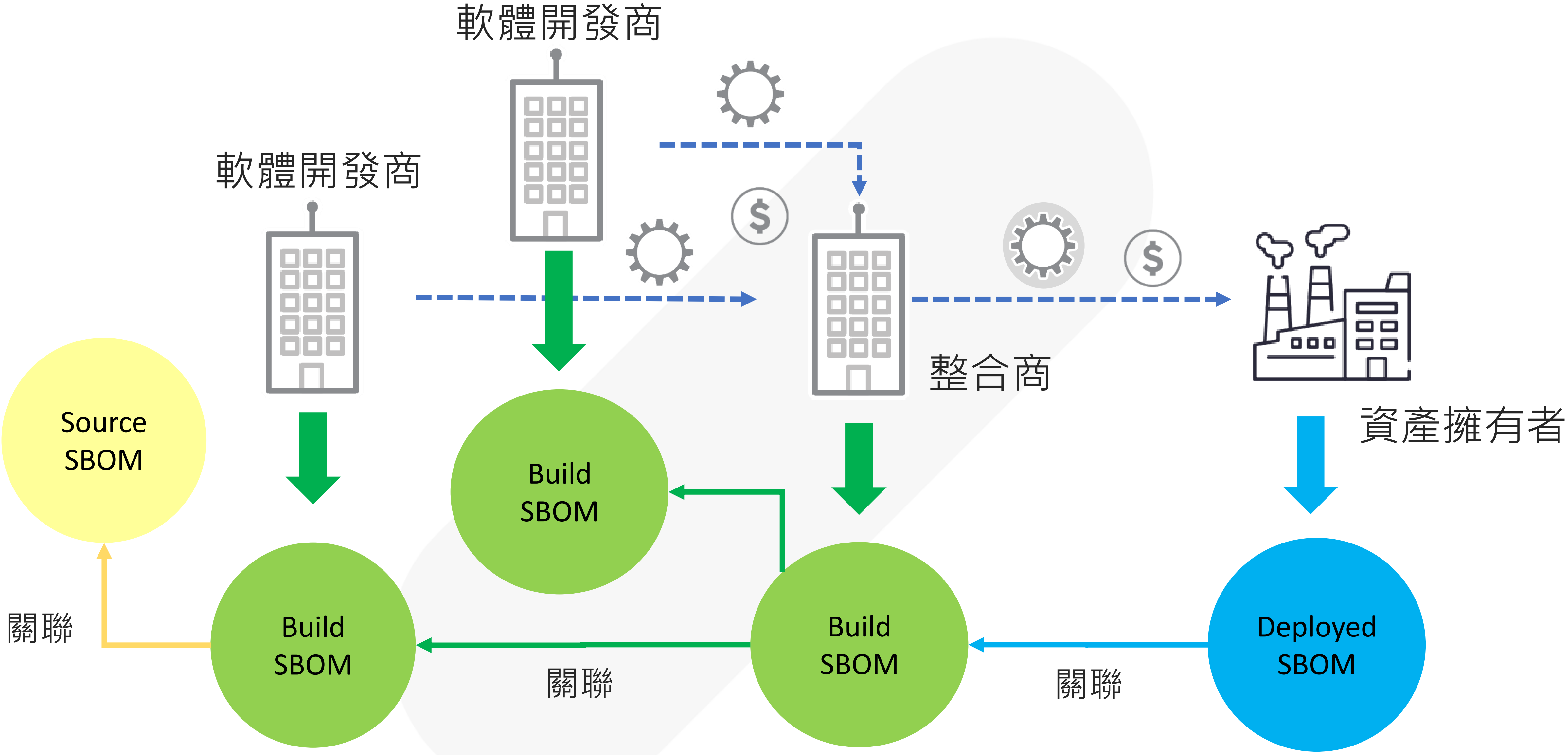
Deployed SBOM

- 系統上存在的軟體清單
- 可能無法準確反映實際運行的環境

Runtime SBOM

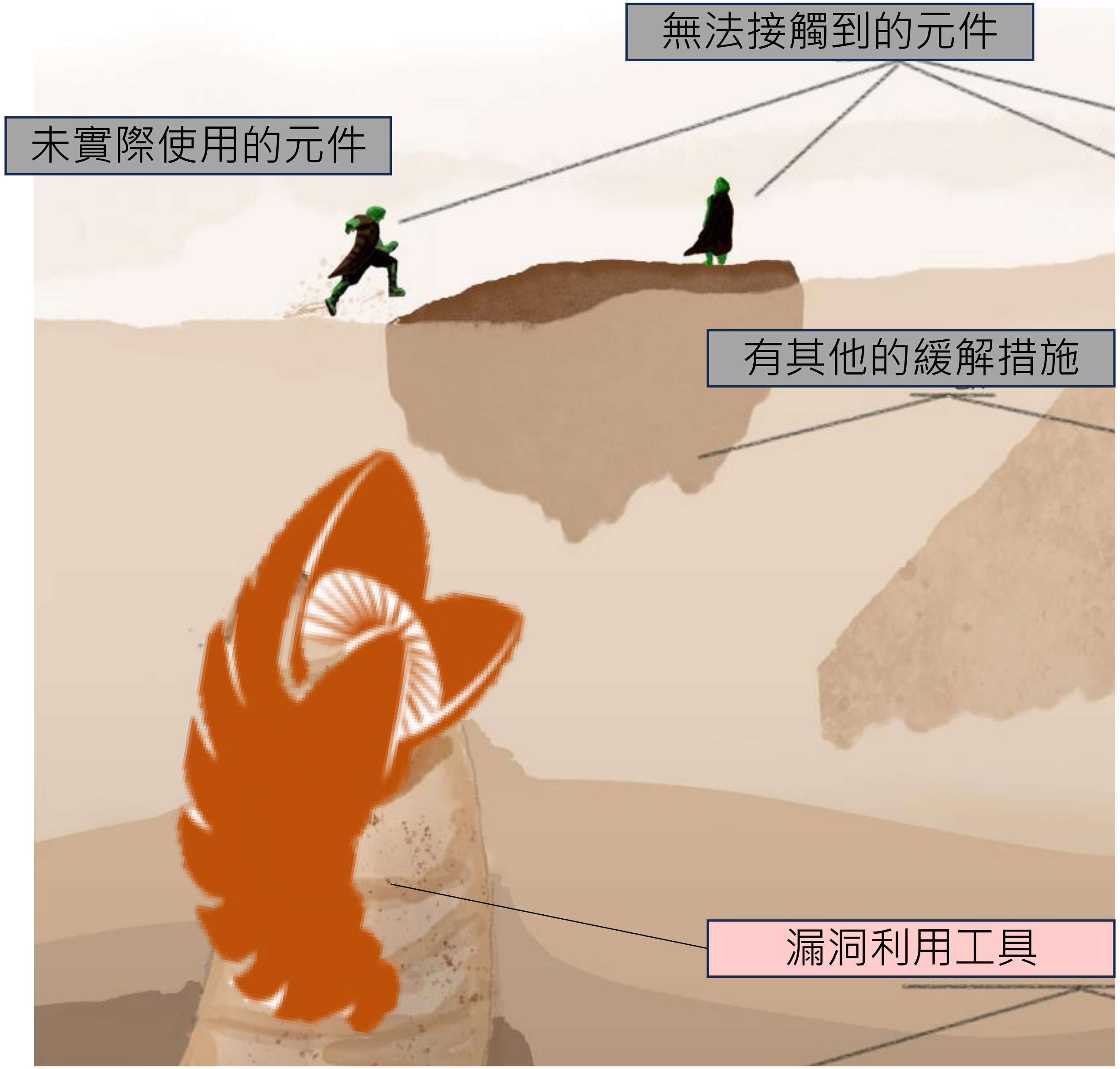
- 系統實際運行的軟體
- 一些功能需要系統運行一段時間才會執行

https://www.cisa.gov/sites/default/files/2023-04/sbom-types-document-508c.pdf

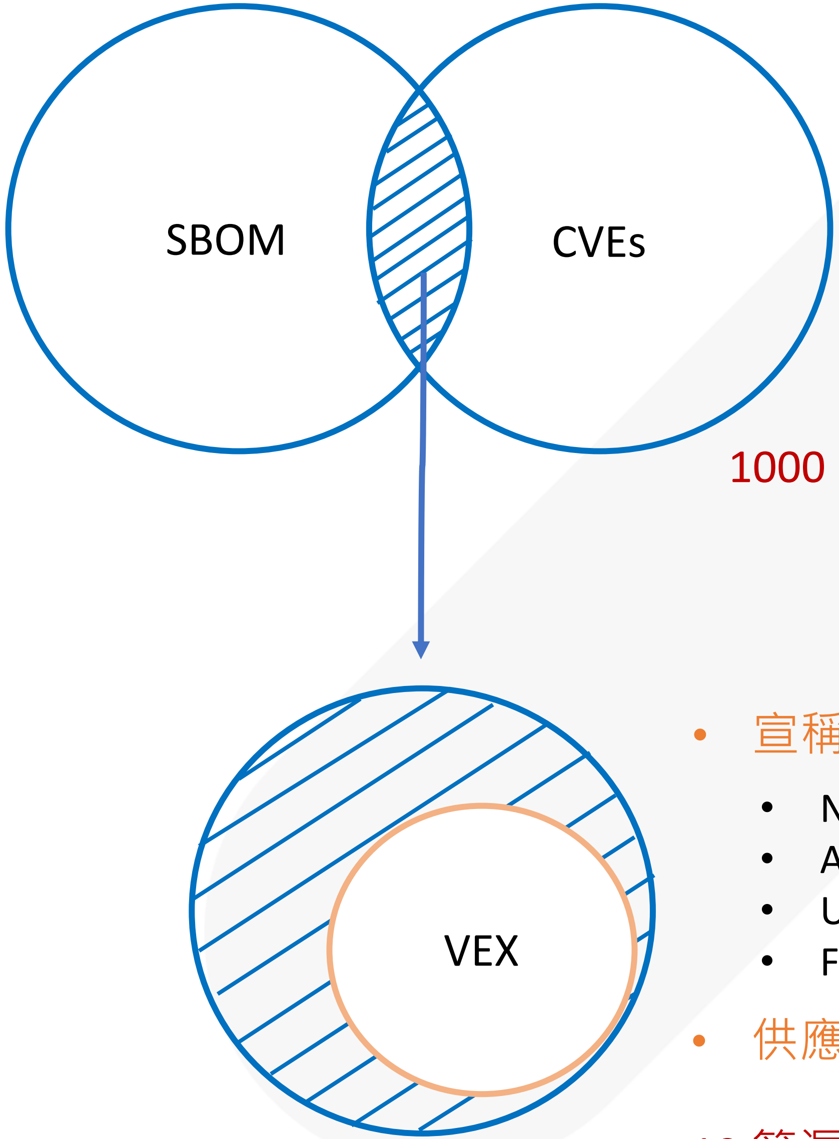

軟體開發商
軟體開發商
整合商
資產擁有者
Source SBOM
Build SBOM
Build SBOM
Build SBOM
Deployed SBOM
關聯
關聯
關聯

SBOM + VEX 分享

並非所有的漏洞都需要修補



https://vrjam.devpost.com/submissions/36635-maker-from-below

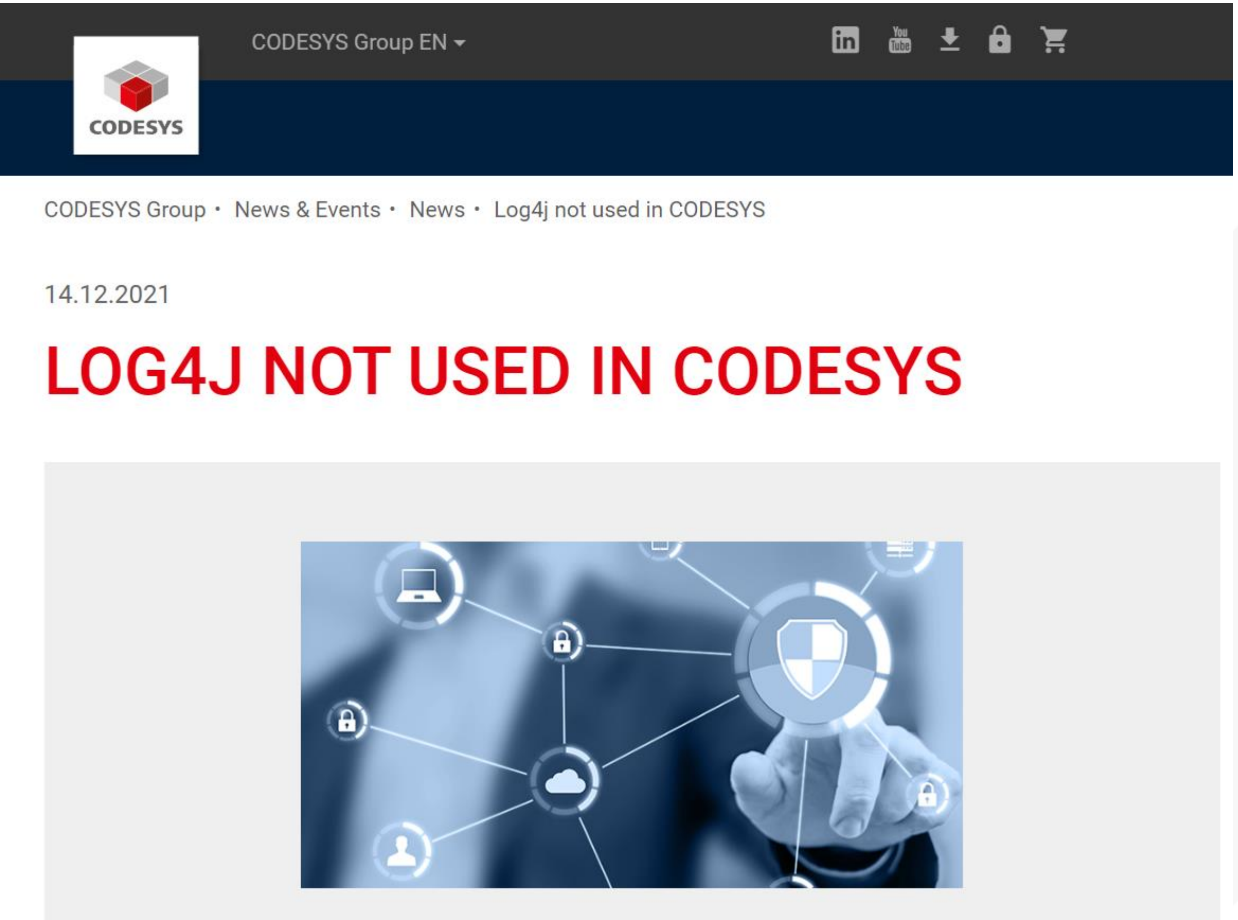


1000 筆漏洞

- 宣稱產品受到漏洞影響狀態
  - NOT AFFECTED: 聲明不受某漏洞影響
  - AFFECTED: 聲明受到影響
  - UNDER INVESTIGATION: 正在調查是否受到漏洞影響
  - FIXED: 說明漏洞已於 X 版本修復
- 供應商、研究人員、漏洞協調者

10 筆漏洞

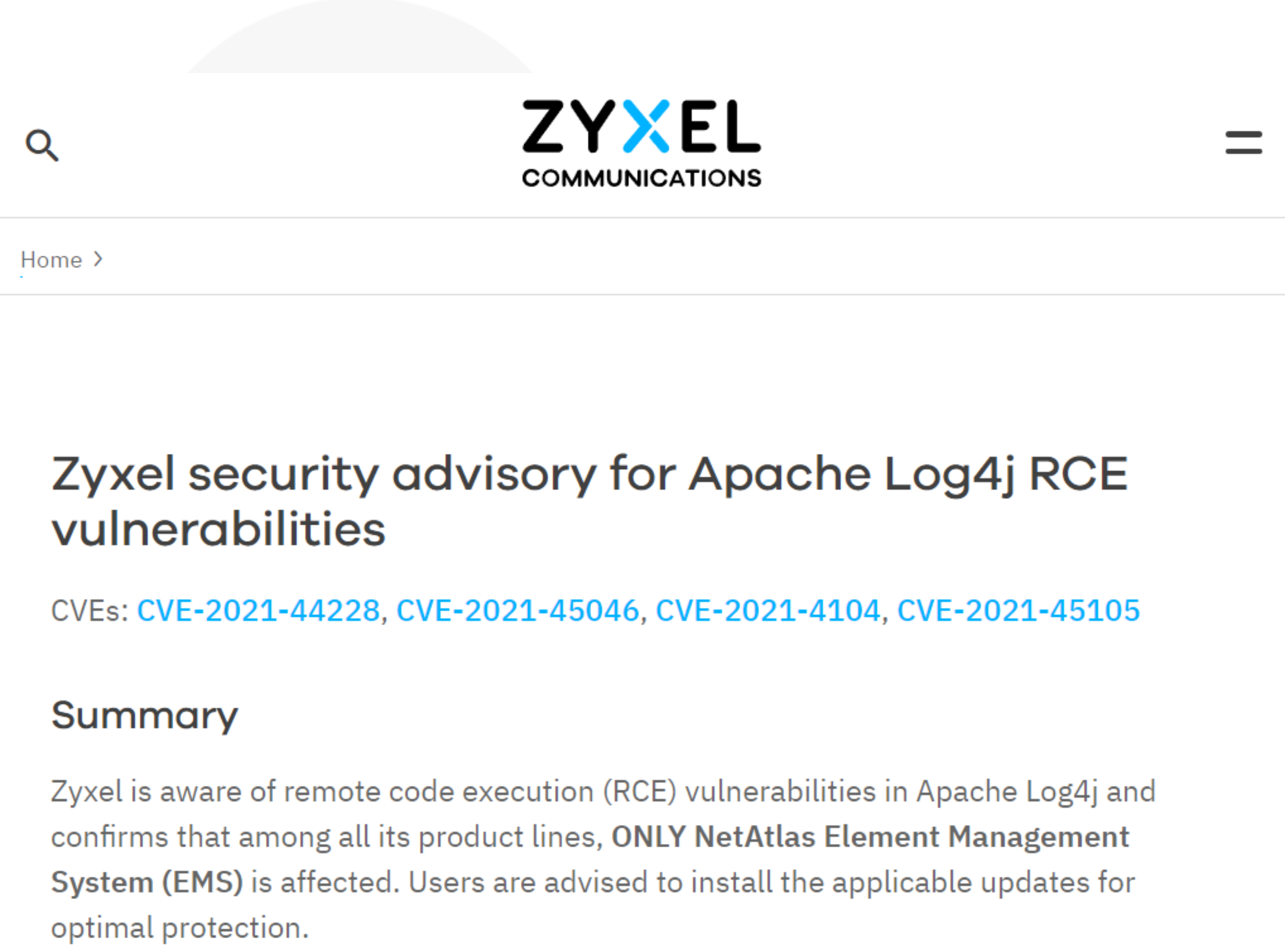
https://www.ntia.doc.gov/files/ntia/publications/framing_2021-04-29_002.pdf



CODESYS Group • News & Events • News • Log4j not used in CODESYS

14.12.2021

LOG4J NOT USED IN CODESYS



Zyxel security advisory for Apache Log4j RCE vulnerabilities

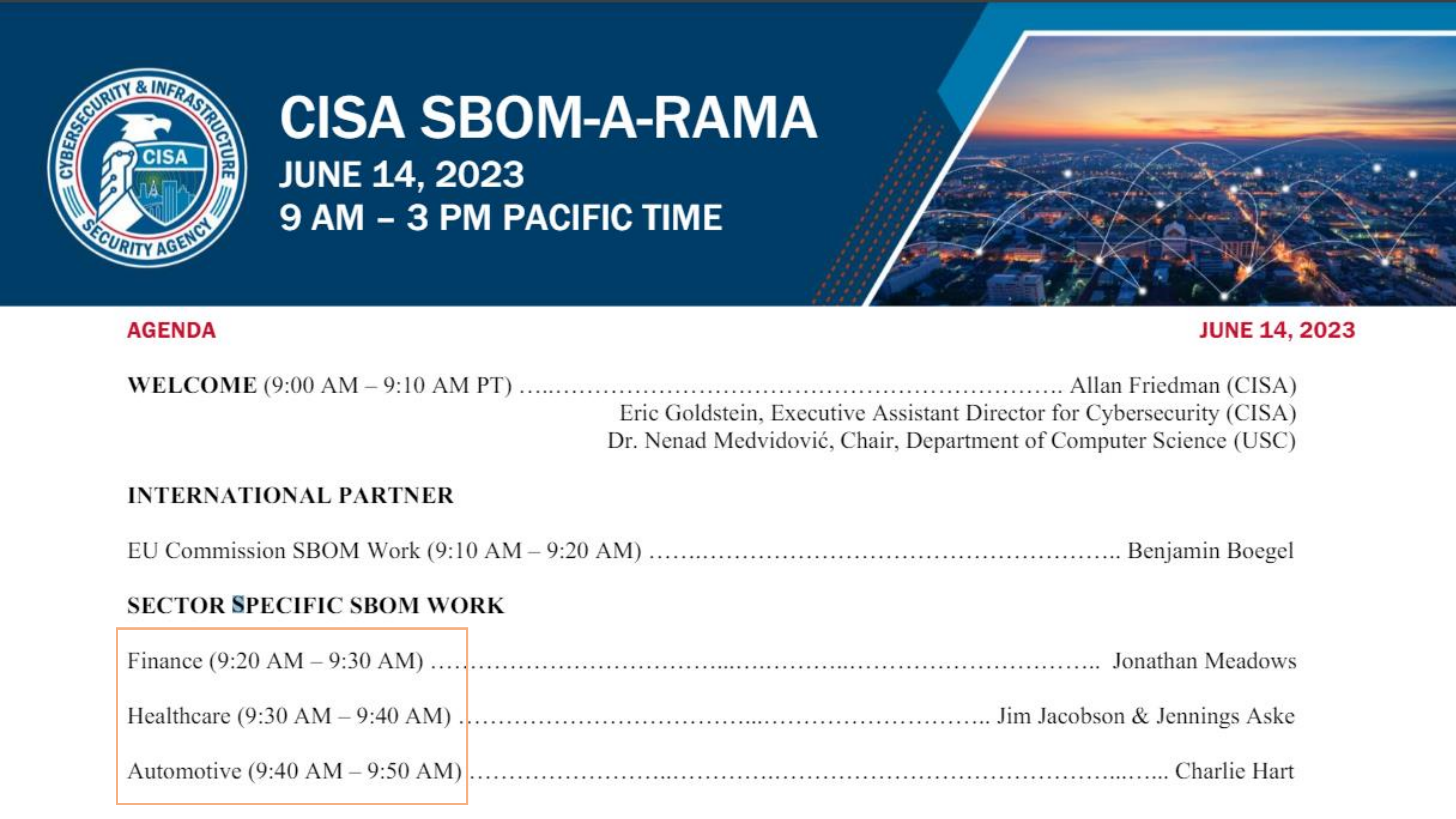
CVEs: CVE-2021-44228, CVE-2021-45046, CVE-2021-4104, CVE-2021-45105

Summary

Zyxel is aware of remote code execution (RCE) vulnerabilities in Apache Log4j and confirms that among all its product lines, **ONLY NetAtlas Element Management System (EMS)** is affected. Users are advised to install the applicable updates for optimal protection.

https://www.codesys.com/news-events/news/article/log4j-not-used-in-codesys.html
https://www.zyxel.com/service-provider/na/en/zyxel-security-advisory-apache-log4j-rce-vulnerabilities

SBOM 合作與應用



CISA SBOM-A-RAMA

JUNE 14, 2023

9 AM – 3 PM PACIFIC TIME

AGENDA **JUNE 14, 2023**

WELCOME (9:00 AM – 9:10 AM PT) …………………………………………… Allan Friedman (CISA)
Eric Goldstein, Executive Assistant Director for Cybersecurity (CISA)
Dr. Nenad Medvidović, Chair, Department of Computer Science (USC)

INTERNATIONAL PARTNER

EU Commission SBOM Work (9:10 AM – 9:20 AM) …………………………………… Benjamin Boegel

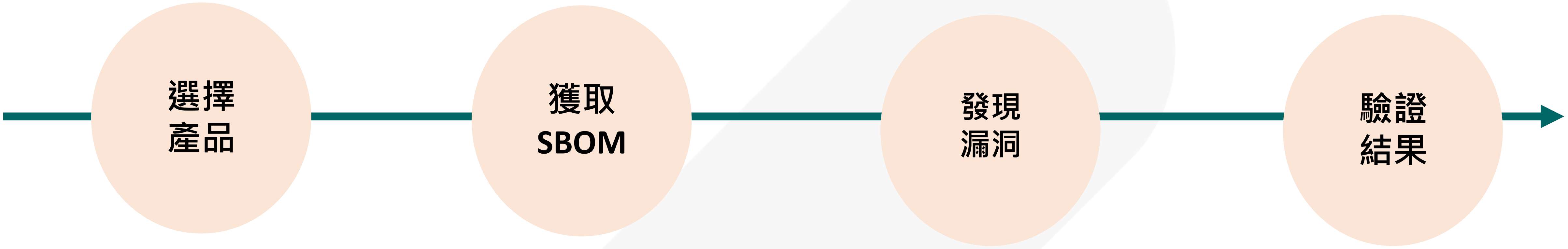
SECTOR SPECIFIC SBOM WORK

Finance (9:20 AM – 9:30 AM) ……………………………………………… Jonathan Meadows

Healthcare (9:30 AM – 9:40 AM) ………………………………………… Jim Jacobson & Jennings Aske

Automotive (9:40 AM – 9:50 AM) ……………………………………………… Charlie Hart

醫療保健產業 SBOM 概念性驗證



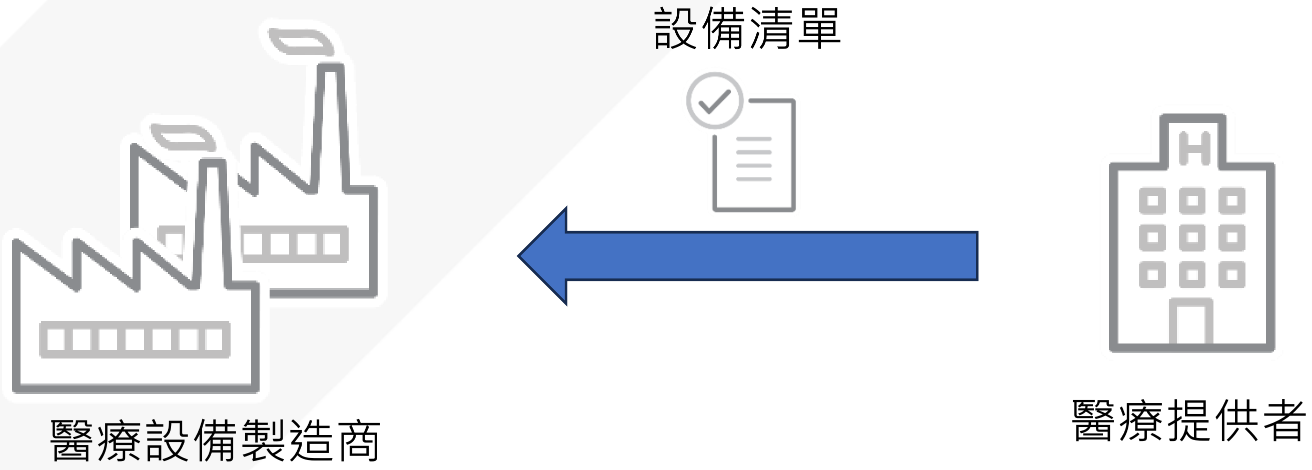
選擇產品

獲取 SBOM

發現漏洞

驗證結果

- 醫療提供者提供參與 PoC 的製造商現有的醫學設備的清單



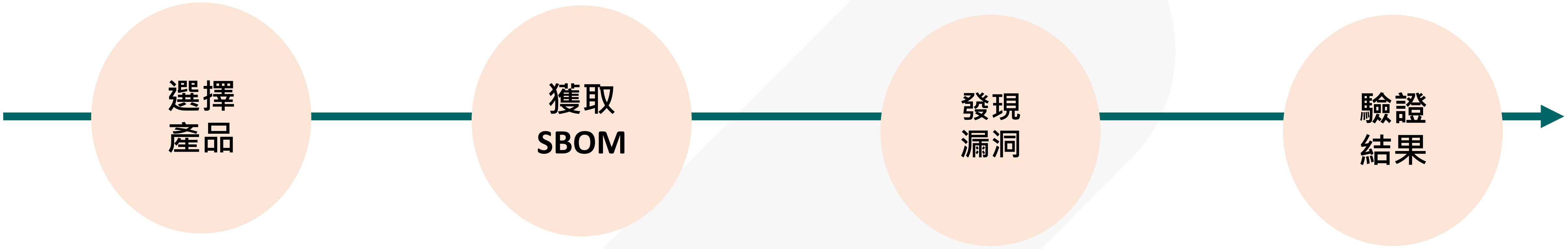
設備清單

醫療設備製造商

醫療提供者

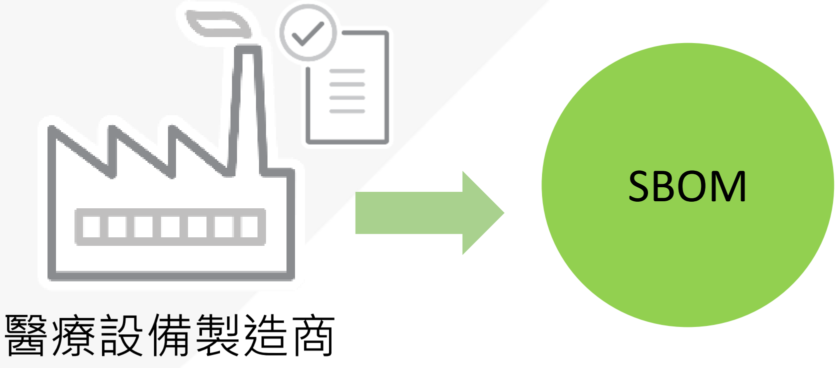
https://www.cisa.gov/sites/default/files/2023-09/Healthcare_508c.pdf

醫療保健產業 SBOM 概念性驗證



- 醫療提供者提供參與 PoC 的製造商現有的醫學設備的清單

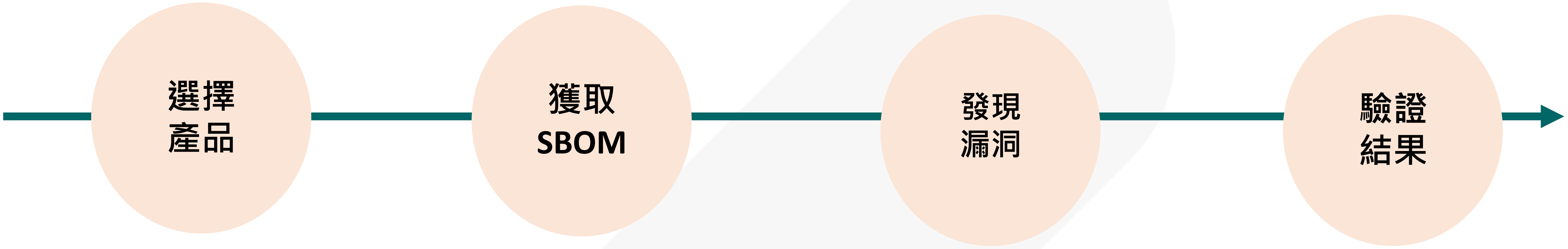
- 製造商選擇清單中的設備
- 嘗試生成 SBOM



- 透過手動與自動方式生成
- 缺乏命名的標準約定，僅能透過常識進行命名
- 提供 SPDX and/or SWID 標準

https://www.cisa.gov/sites/default/files/2023-09/Healthcare_508c.pdf

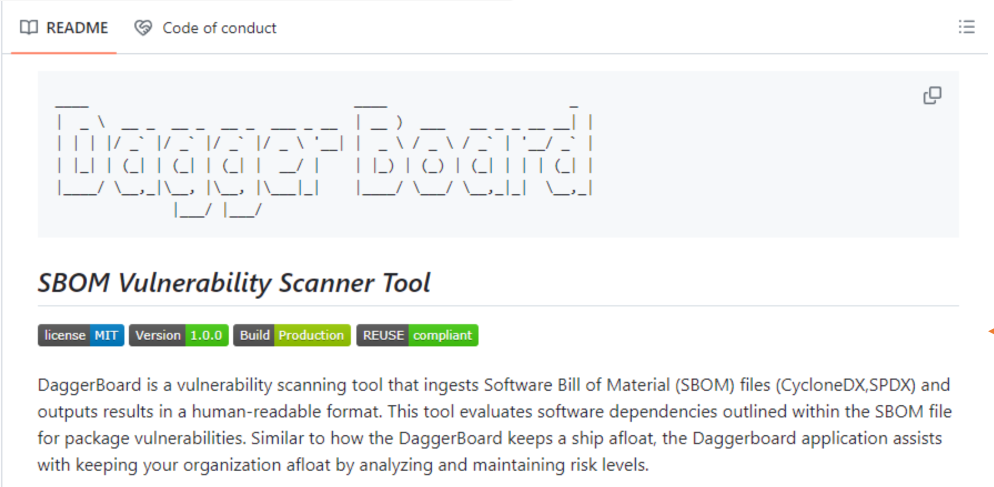
醫療保健產業 SBOM 概念性驗證



- 醫療提供者提供參與 PoC 的製造商現有的醫學設備的清單

- 製造商選擇清單中的設備
- 嘗試生成 SBOM

- DaggerBoard 可以提取 SBOM 檔案 (CycloneDX or SPDX)
- 找出檔案中所概述的軟體漏洞



SBOM Vulnerability Scanner Tool

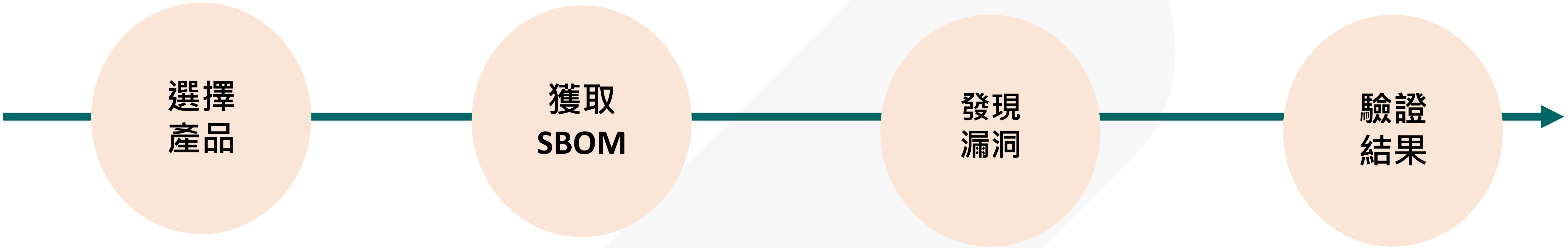
license MIT | Version 1.0.0 | Build Production | REUSE compliant

DaggerBoard is a vulnerability scanning tool that ingests Software Bill of Material (SBOM) files (CycloneDX,SPDX) and outputs results in a human-readable format. This tool evaluates software dependencies outlined within the SBOM file for package vulnerabilities. Similar to how the DaggerBoard keeps a ship afloat, the Daggerboard application assists with keeping your organization afloat by analyzing and maintaining risk levels.

NVD

https://www.cisa.gov/sites/default/files/2023-09/Healthcare_508c.pdf

醫療保健產業 SBOM 概念性驗證



選擇產品

獲取 SBOM

發現漏洞

驗證結果

- 醫療提供者提供參與 PoC 的製造商現有的醫學設備的清單

- 製造商選擇清單中的設備
- 嘗試生成 SBOM

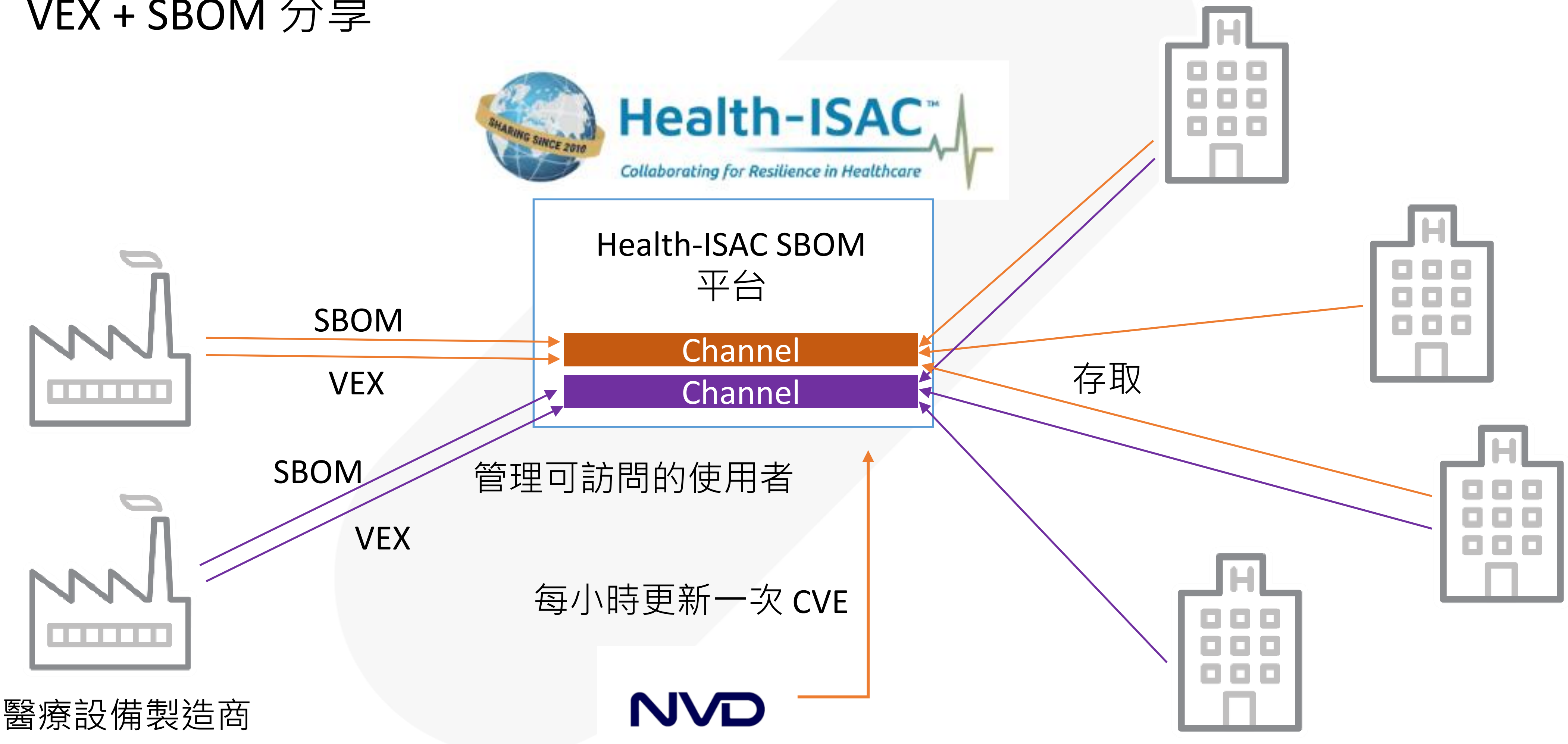
- DaggerBoard 可以提取 SBOM 檔案 (CycloneDX or SPDX)
- 找出檔案中所概述的軟體漏洞

- 醫療行業可以使用通用的 SBOM 格式
- 缺乏命名的標準約定
- 無法驗證 SBOM 的完整性與準確性

https://www.cisa.gov/sites/default/files/2023-09/Healthcare_508c.pdf

醫療保健產業 SBOM 概念性驗證

VEX + SBOM 分享



醫療提供者

https://www.cisa.gov/sites/default/files/2024-03/Healthcare%20Feb%202024%20SBOM-a-Rama%20508c.pdf

SBOM 概念性驗證相似的議題

- 醫療保健產業、 汽車產業、金融產業
  - SBOM 資料品質基準/驗證
  - 命名的標準約定

Ransomware

Clop Cl0p

APT Group (MITRE ID: G0034)

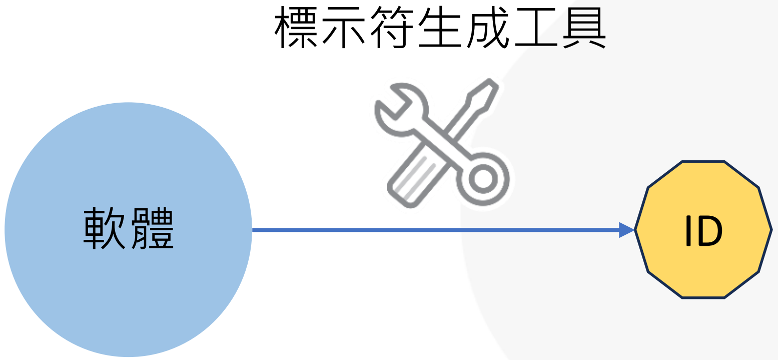
沙蟲

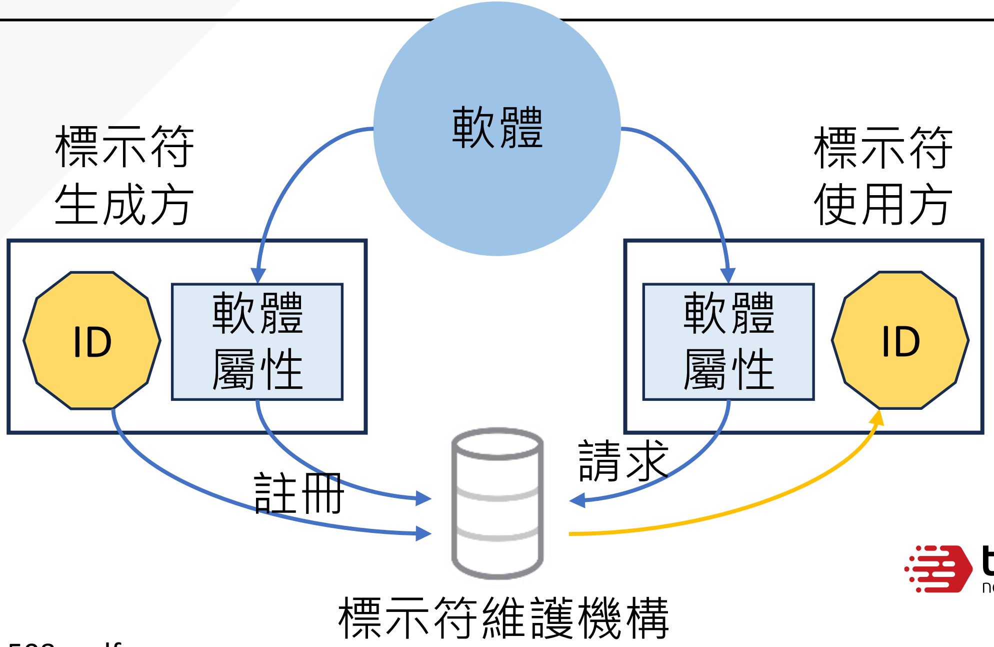
鋼鐵維京人

巫毒熊

軟體標示符

	固定標示符	定義標示符
說明	任何人可由生成工具產生標示符	特定機構定義的標示符
代表	OmniBOR 透過檔案資訊的雜湊值來建立標示符	CPE、purls、 SWID cpe:2.3:o:microsoft:windows_vista:6.0:sp1:-:-:home_premium:-:x64:-
缺點	• 依據生成工具所定義的輸入，不同版本的軟體可能會生成相同的標示符 • 不容易被人類直接理解或使用	• 需有機構承擔維護標示符的功能 • 在該機構定義前，沒有特定軟體的標示符 • 難以涵蓋全球軟體的標示符



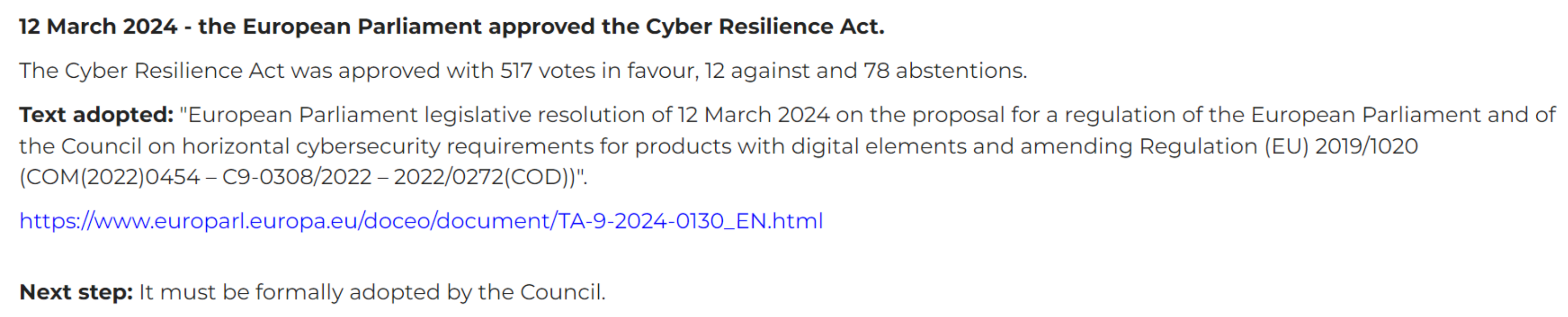


https://www.cisa.gov/sites/default/files/2023-10/Software-Identification-Ecosystem-Option-Analysis-508c.pdf

SBOM 採用

SBOM-a-Rama Winter 2024

- 醫療保健產業、 汽車產業、金融產業已持續進行概念性驗證
- 歐盟資安韌性法 (CRA)
  - 要求製造商在歐盟銷售的產品需提供消費者保障的法案
  - SBOM 要求
    - 必須在內部進行漏洞管理 (不必公開)
    - 必須依照市場監督機構的要求轉交給他們
  - 2024年3月獲得歐盟議會通過
  - 公佈後 36 個月生效



12 March 2024 - the European Parliament approved the Cyber Resilience Act.

The Cyber Resilience Act was approved with 517 votes in favour, 12 against and 78 abstentions.

Text adopted: "European Parliament legislative resolution of 12 March 2024 on the proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (COM(2022)0454 – C9-0308/2022 – 2022/0272(COD))".

https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_EN.html

Next step: It must be formally adopted by the Council.

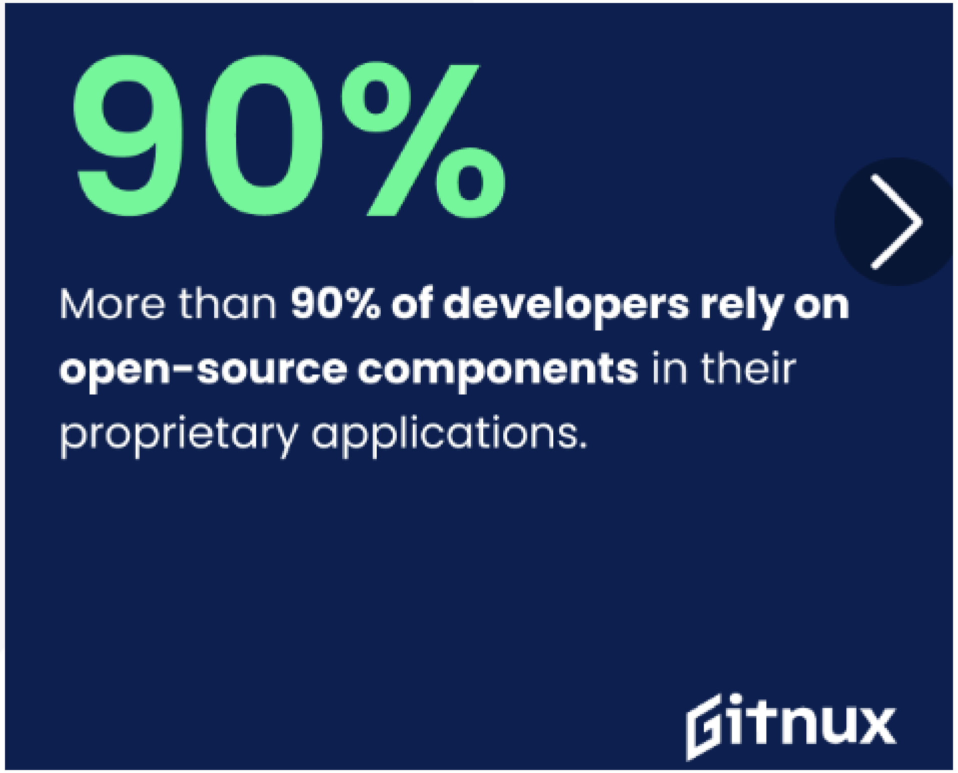
https://www.cisa.gov/sites/default/files/2024-03/BSI%20Feb%202024%20SBOM-a-Rama%20508c.pdf
https://www.european-cyber-resilience-act.com/

SBOM 採用 - 抗拒

- 我們沒有使用開源軟體
- 我們不可能知道軟體中有甚麼
- 沒有工具

SBOM 採用 - 抗拒

- 我們沒有使用開源軟體
- 我們不可能知道軟體中有甚麼
  - SBOM 類型
- 沒有工具
  - SWID: http://tiny.cc/SWID
  - SPDX: http://tiny.cc/SPDX
  - CycloneDX: http://tiny.cc/CycloneDX
  - https://www.nics.nat.gov.tw/core_business/digital_resilience/SBOM_Resources/



90%

More than **90% of developers rely on open-source components** in their proprietary applications.

Gitnux

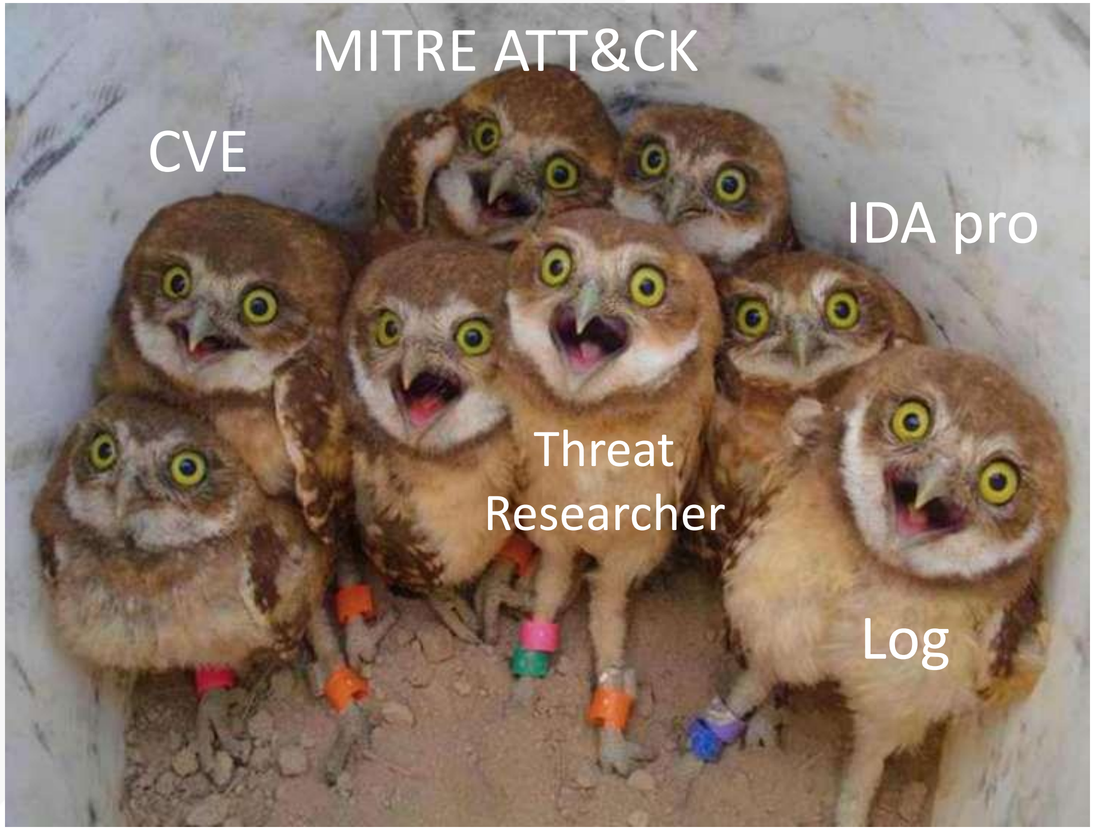
https://www.youtube.com/watch?v=qk2vo7ir1cI

SBOM 採用 - 疑問

- 這是攻擊者的路線圖吧
- 這是我們智慧財產權

SBOM 採用 - 疑問

- 這是攻擊者的路線圖吧
- 這是我們智慧財產權
  - 大多會採用 open source，根據 license 也應聲明使用情形



SBOM 採用 - 完蛋惹

- 我們沒有那個專案的開發人員了，不知道怎麼修復程式碼
- 我們可能需要延遲交付產品
- 我們其實是外包給別人寫，所以我們沒有原始碼，也無法修補

SBOM 採用 - 完蛋惹

- 我們沒有那個專案的開發人員了，不知道怎麼修復程式碼

- 我們可能需要延遲交付產品

- 我們其實是外包給別人寫，所以我們沒有原始碼，也無法修補

DD
高風險的產品
漏洞利用工具
客戶
客戶
客戶
客戶
客戶

SBOM 採用 - 面對

- 醫療設備製造商，透過 SBOM 發現設備有一千多個漏洞，更新了七個軟體包，成功避免了這一千多個洞

- 無法處理的漏洞，傳遞給下游聯防

- Schneider 擁有超過 4000 個工控設備的 SBOMs

-- RSA Conference 2023, The Opposite of Transparency

https://www.rsaconference.com/library/Presentation/USA/2023/The%20Opposite%20of%20Transparency

總結

- 歐盟資安韌性法 (CRA) 已於 2024年3月獲得歐盟議會通過
  - 當公佈後，36 個月生效
- 如何開始
  - 選擇代表的系統，評估應生成哪種類型的 SBOM 與採用的標準
    - SWID: http://tiny.cc/SWID; SPDX: http://tiny.cc/SPDX; CycloneDX: http://tiny.cc/CycloneDX
    - 醫療保健產業 SBOM 概念性驗證採用 SPDX 與 SWID
  - 盡可能連結到 Source SBOM，使用工具找出產品潛在的漏洞
  - 依據已知漏洞與著名的漏洞生成 VEX
  - 制定 SBOM 分享的政策與方式
  - 將 SBOM 納為採購考量

Thank You

Keep the operation running!

txOne networks

感謝您參加講座， 掃描QR Code填寫問券即可到Q106攤位上玩遊戲得好禮