2025 臺灣資安大會
CYBERSEC 2025
Brand Day 701A

DevSecOps 中
您可能沒想到的軟體供應鏈安全
從案例中學習

達友科技 Docutek Solutions, Inc,
林皇興 Lambert Lin /CISSP

2025-04-15

SYSTEX A I 生 成 。 無 限 可 能

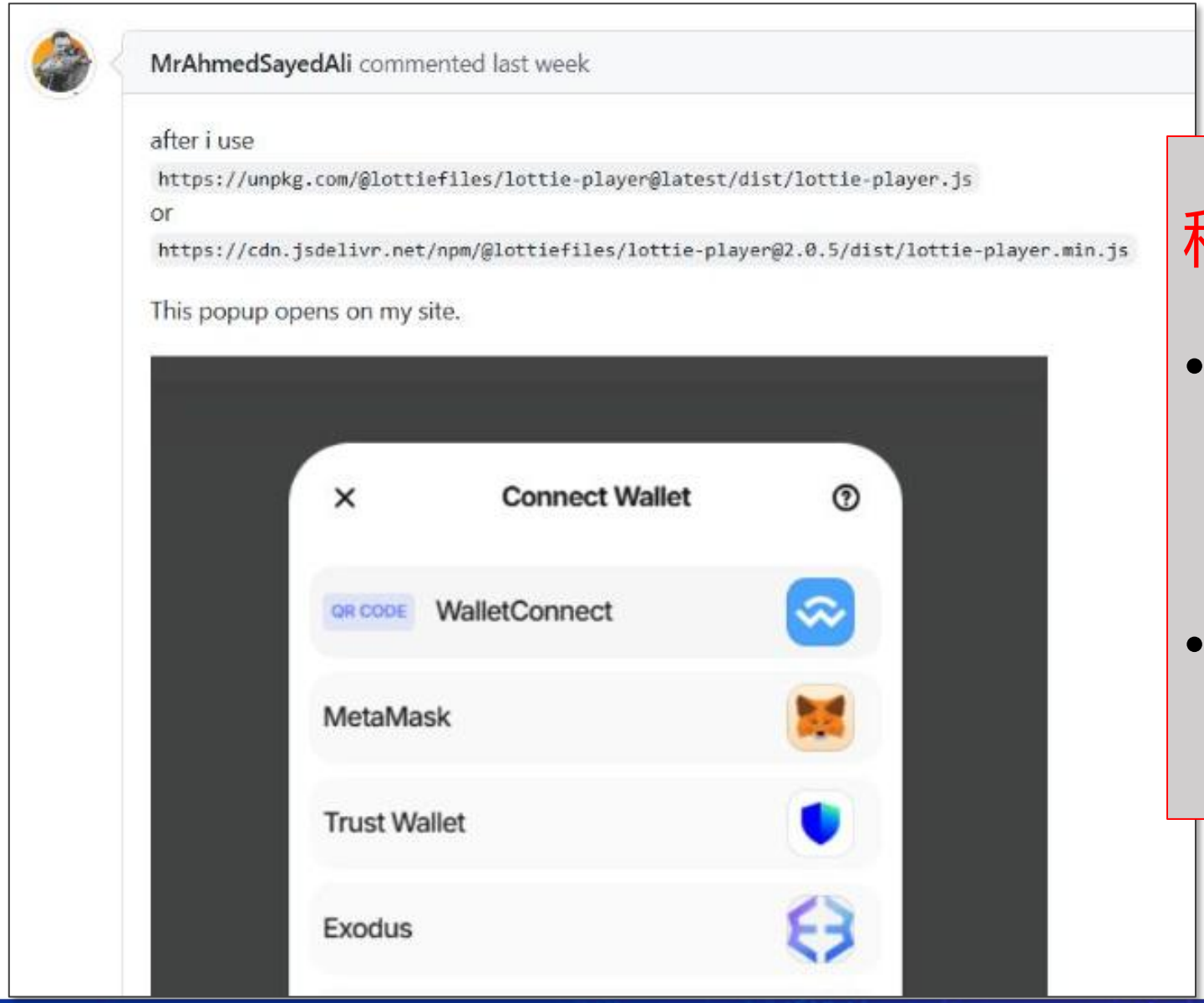
1.供應鏈攻擊手法，於 Lottie Player NPM 套件植入惡意程式

- **Lottie Player** 是一個開源的 JavaScript 第三方元件，用來於端點顯示動畫，被廣泛使用
- 當時每週都有8.4萬筆下載使用紀錄
- 2024-10-30 被發現三個版本的套件，被駭客植入惡意程式，會小額偷取終端瀏覽者的數位加密錢包

- 2.0.5 – pushed to npm at 8:12 PM GMT, 30 Oct 2024
- 2.0.6 – pushed to npm at 8:35 PM GMT, 30 Oct 2024
- 2.0.7 – pushed to npm at 9:57 PM GMT, 30 Oct 2024

參考文章: 1, 2, 3

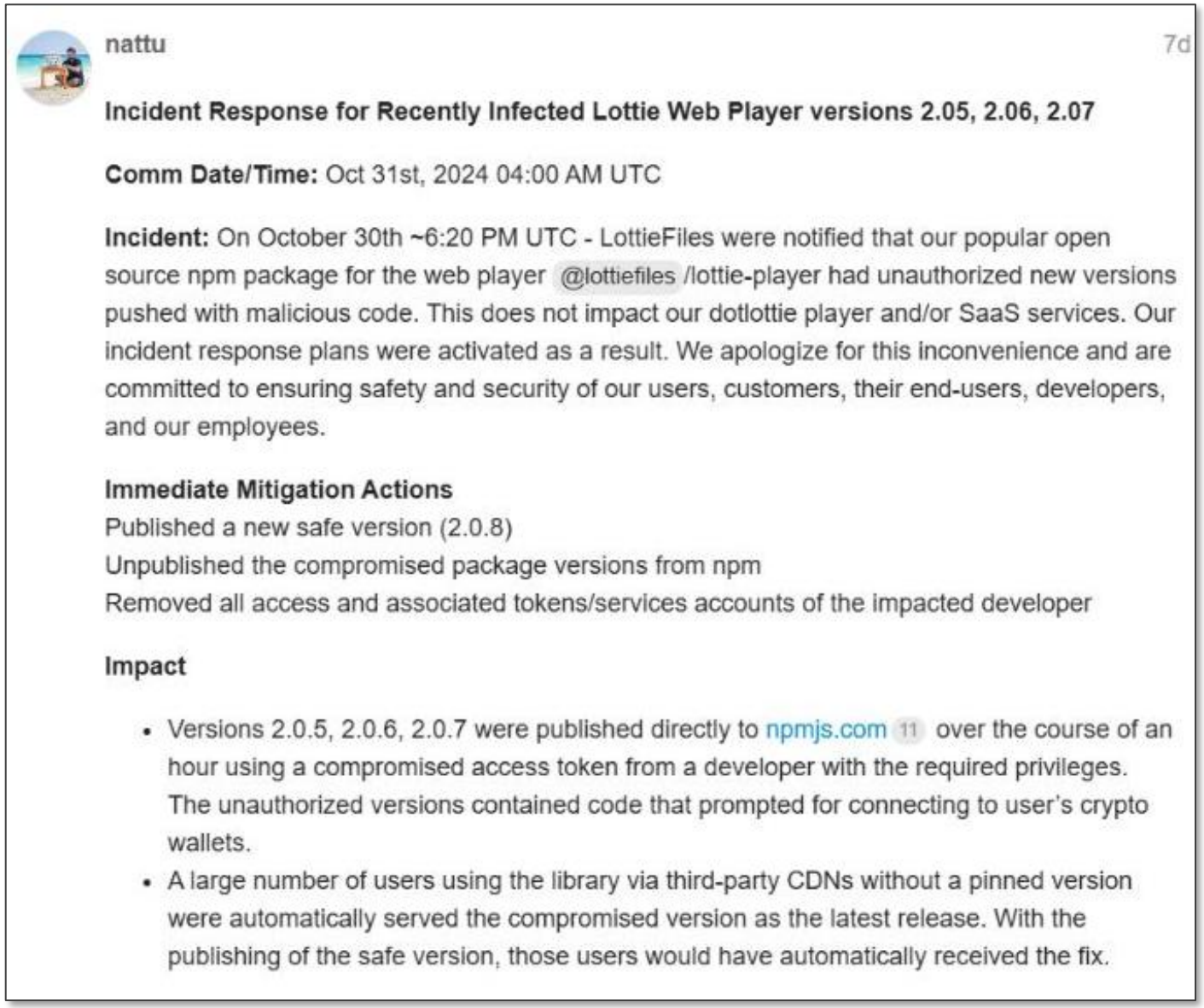
攻擊事件是如何被發現的?



程式行為的改變

- 有使用者瀏覽利用該套件的網站時，會彈出 web3 數位錢包的選擇畫面
- 紛紛貼到論壇與 GitHub 上詢問，才開始調查

Lottie Player 事件，官方之後發布調查結果



nattu 7d

Incident Response for Recently Infected Lottie Web Player versions 2.05, 2.06, 2.07

Comm Date/Time: Oct 31st, 2024 04:00 AM UTC

Incident: On October 30th ~6:20 PM UTC - LottieFiles were notified that our popular open source npm package for the web player @lottiefiles /lottie-player had unauthorized new versions pushed with malicious code. This does not impact our dotlottie player and/or SaaS services. Our incident response plans were activated as a result. We apologize for this inconvenience and are committed to ensuring safety and security of our users, customers, their end-users, developers, and our employees.

Immediate Mitigation Actions
Published a new safe version (2.0.8)
Unpublished the compromised package versions from npm
Removed all access and associated tokens/services accounts of the impacted developer

Impact

- Versions 2.0.5, 2.0.6, 2.0.7 were published directly to npmjs.com 11 over the course of an hour using a compromised access token from a developer with the required privileges. The unauthorized versions contained code that prompted for connecting to user's crypto wallets.
- A large number of users using the library via third-party CDNs without a pinned version were automatically served the compromised version as the latest release. With the publishing of the safe version, those users would have automatically received the fix.

- 入侵成功原因，是某個開發者的 token 被竊，因此不須經過 2FA 程序即可發布惡意的新版修改

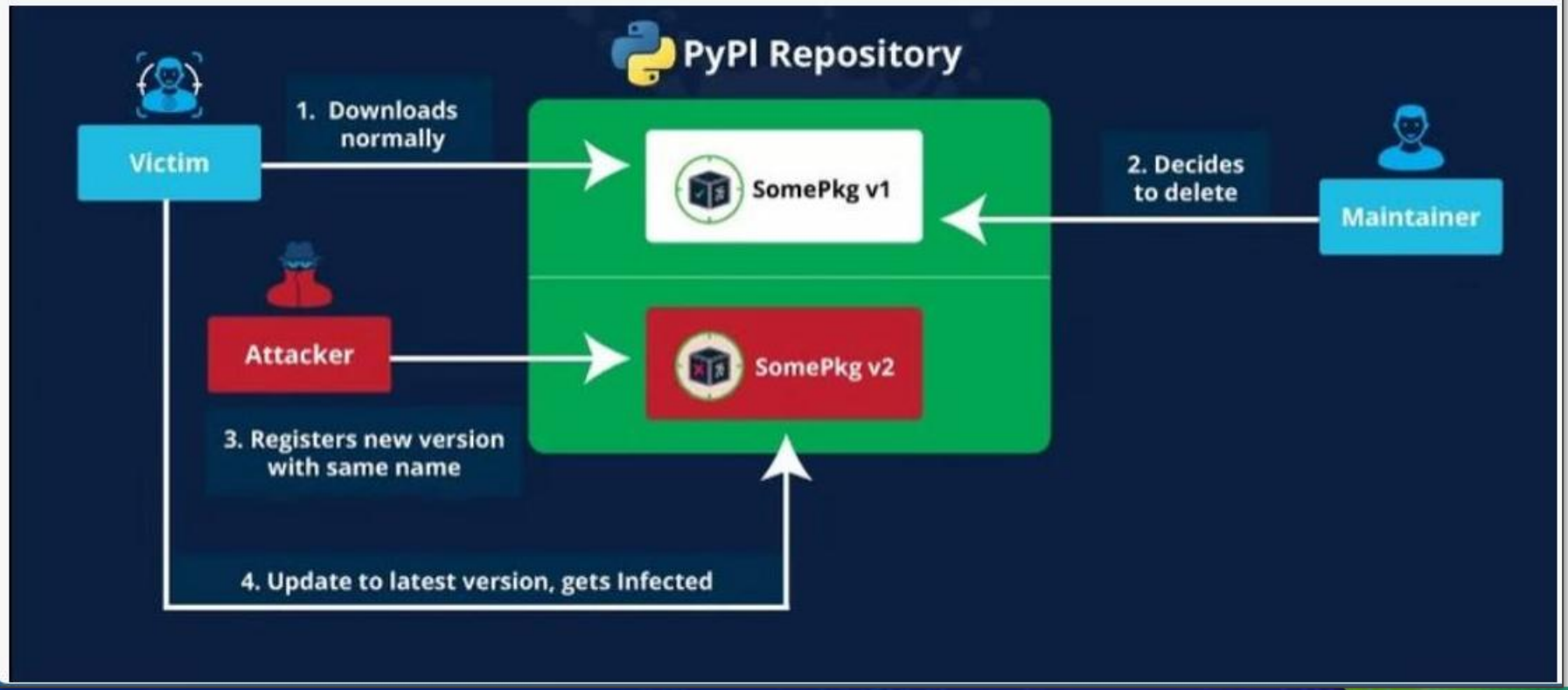
iThome

惡意PyPI套件使用新的挾持手法，假冒正牌套件引誘受害者上當

已下架的套件名稱可被用於攻擊行動！研究人員揭露新型態的攻擊手法Revival Hijack，攻擊者找到已棄用的套件名稱並加以濫用，上架惡意套件來從事攻擊行動

文/ 周峻佑 | 2024-09-05 發表

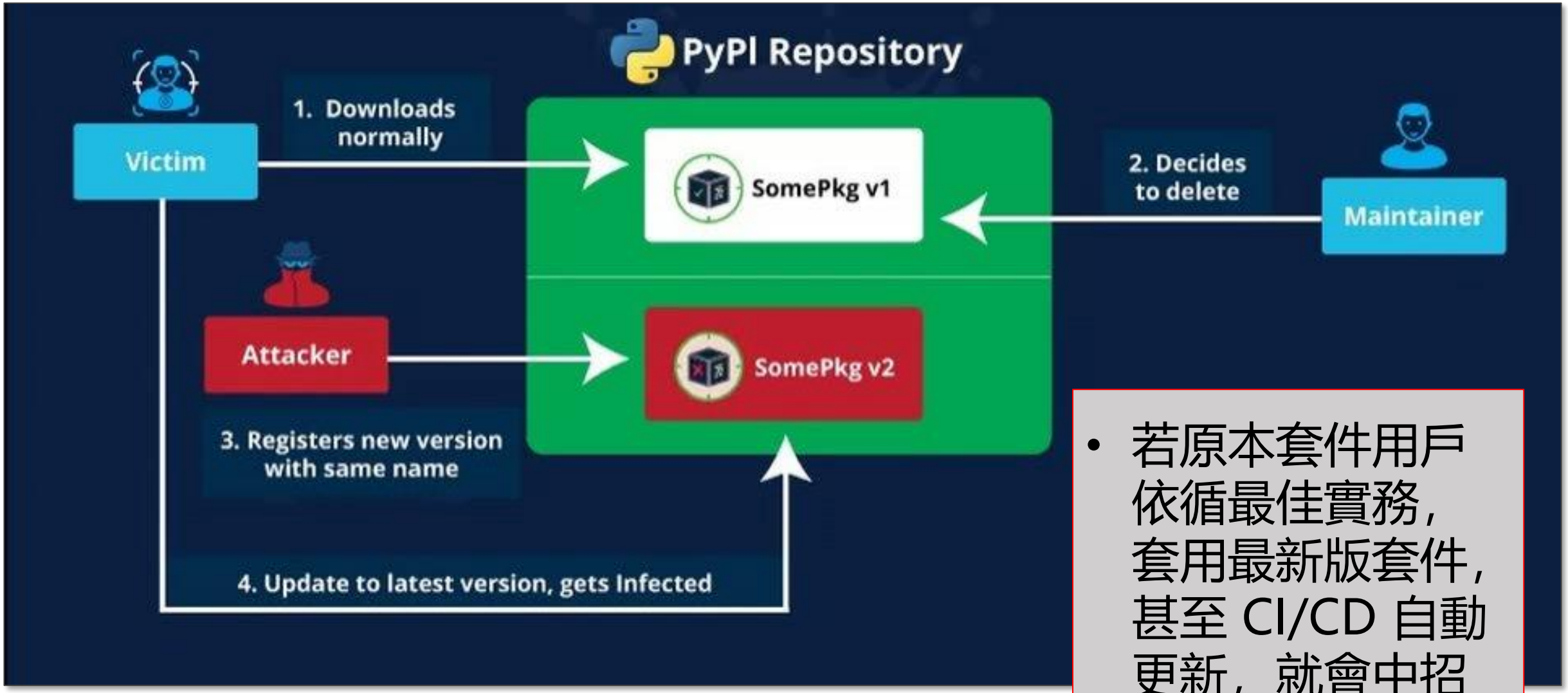
讚 14 分享



攻擊者不斷發揮創意，這次利用 PyPI 套件庫

2024/09
新聞來源:
iThome

2. Revival Hijack攻擊手法, 利用已棄用的 PyPI 套件名稱



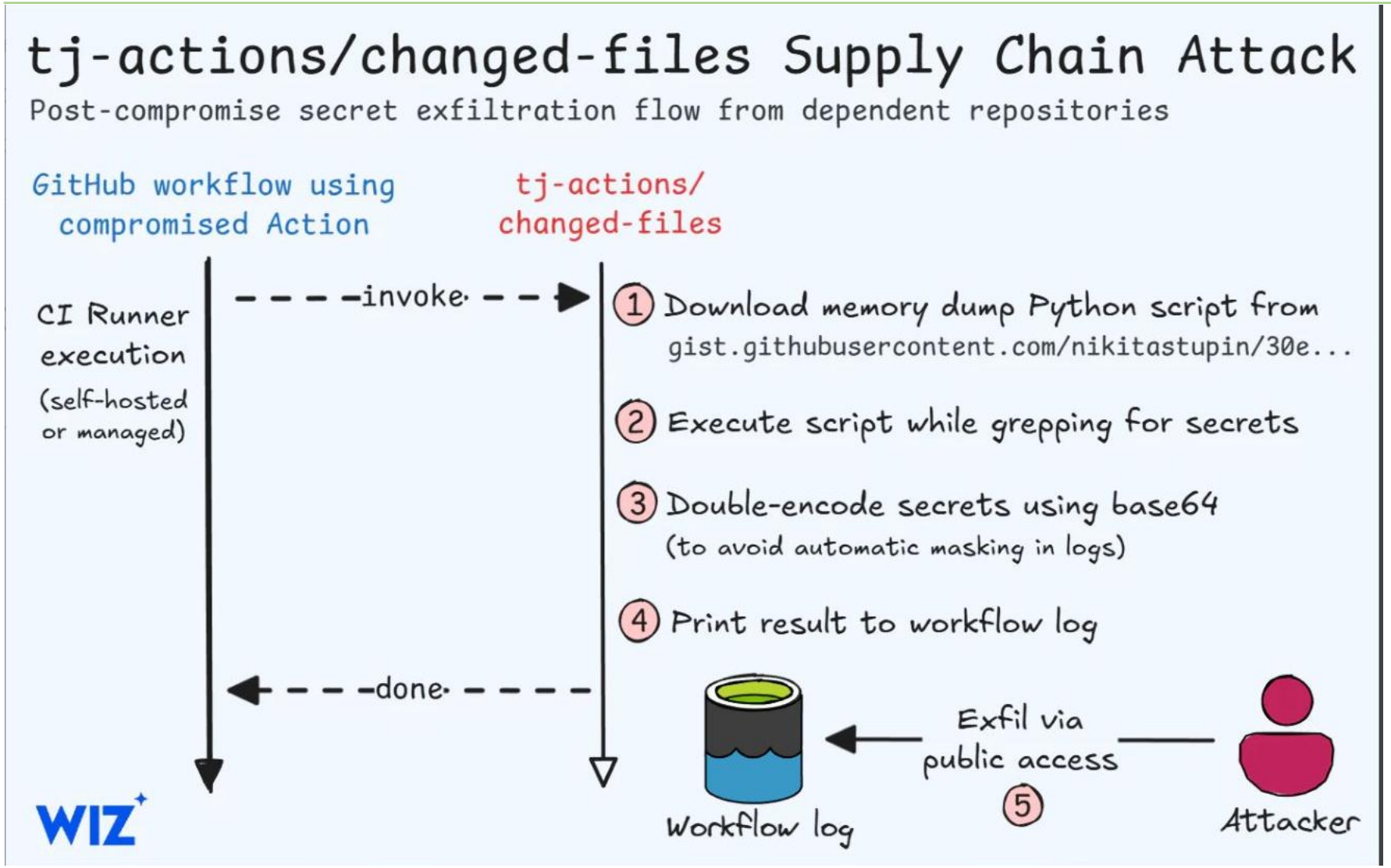
- 若原本套件用戶依循最佳實務，套用最新版套件，甚至 CI/CD 自動更新，就會中招

針對 PyPI 下架套件的 Revival Hijack 挾持攻擊手法

- 利用已經移除、下架的 PyPI 套件名稱，註冊新套件，聲稱是接手進行後續維護
- 由於每個月都有數百上千個專案下架，估計有2.2萬個專案可能會遭此手法攻擊
- PyPI 套件平台團隊: 目前針對該攻擊手法尚無因應方法

圖片來源: JFrog

3. GitHub Actions 的供應鏈攻擊利用 (2025/03)



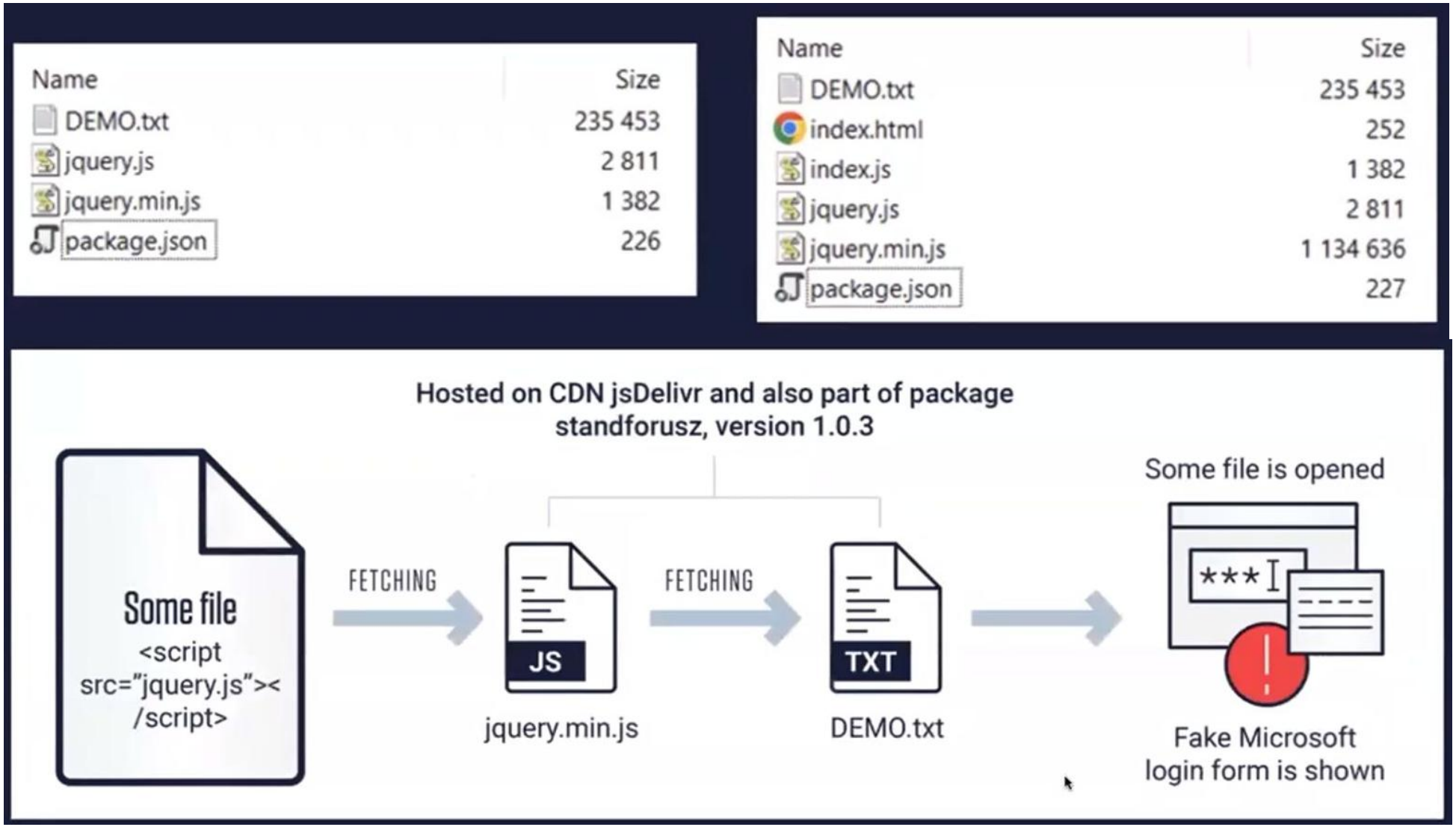
- 藉由入侵知名的 GitHub Actions 名為 tj-actions /changed-files
- 植入惡意的 script 可以用來抓取意用程式的存取憑證、API Key 等機密，並記錄於 workflow log 中

圖片來源: WIZ.io

原來 CI/CD 滿足了
程式上版流程的自動化需求

但也帶來了意想不到的問題與風險

4. Operation BrainLeeches 供應鏈攻擊 (2023/06)

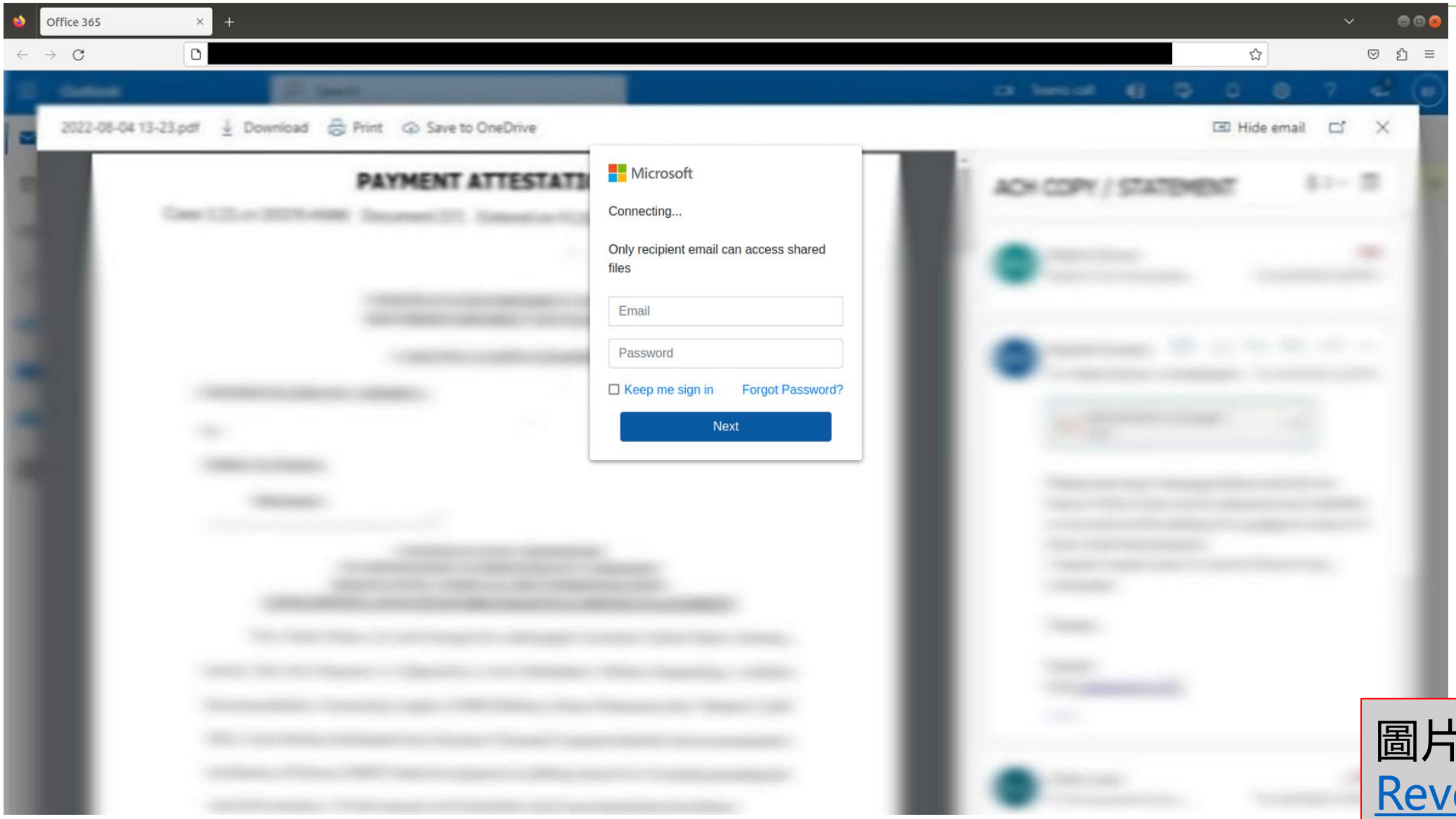


於合法的 jquery 之 npm 套件，植入惡意程式

導致有用到的站點，會彈出微軟 365 的登入認證畫面，以偷取使用者帳密

圖片來源: Reversing Lab

Operation BrainLeeches → 使您的網站變成釣魚網頁



圖片來源:
Reversing Lab

近年一些軟體供應鏈攻擊案例

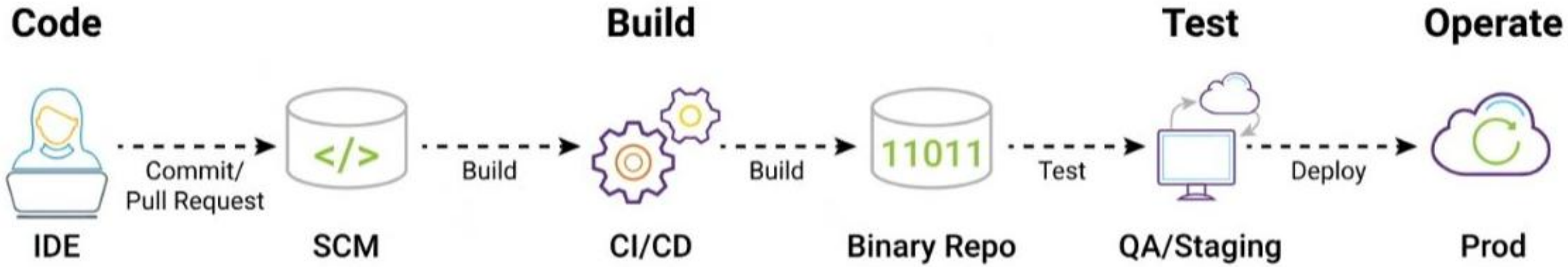
- **3CX 供應鏈攻擊**
  2023/04, VoIP IPBX 軟體開發商 3CX 遭到滲透，將其網站上的3CX Desktop App替換成具有後門程式的惡意版本。影響了 1,200 萬名使用者

- **Okta 客戶支援系統帳密遭駭**
  2023/10,身份存取管理廠商 Okta 被入侵，攻擊者存取了上百位客戶的機敏檔案，導致所有用戶帳密存在外洩風險

- **MOVEit Transfer 遠端任意執行漏洞**
  2023/05, MFT 檔案安全傳輸主要廠商，存在多個高風險提權與 SQL Injection 漏洞，並被駭客利用進行攻擊，影響範圍涵蓋約 32 個國家、超過 2,000 多個組織受害

聽了這些案例
我們學習到了甚麼?

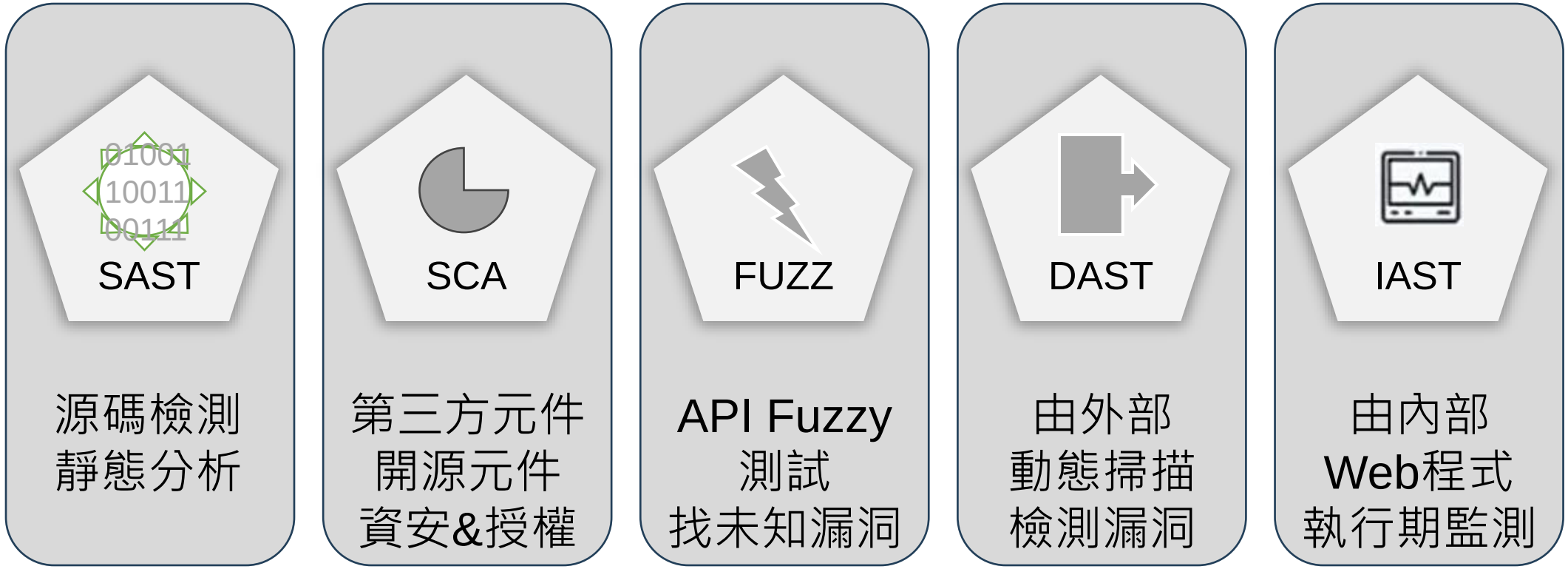
系統開發的常見流程


Code
Build
Test
Operate
Commit/
Pull Request
Build
Build
Test
Deploy
11011
IDE
SCM
CI/CD
Binary Repo
QA/Staging
Prod

? ? ? ? ? ? ?

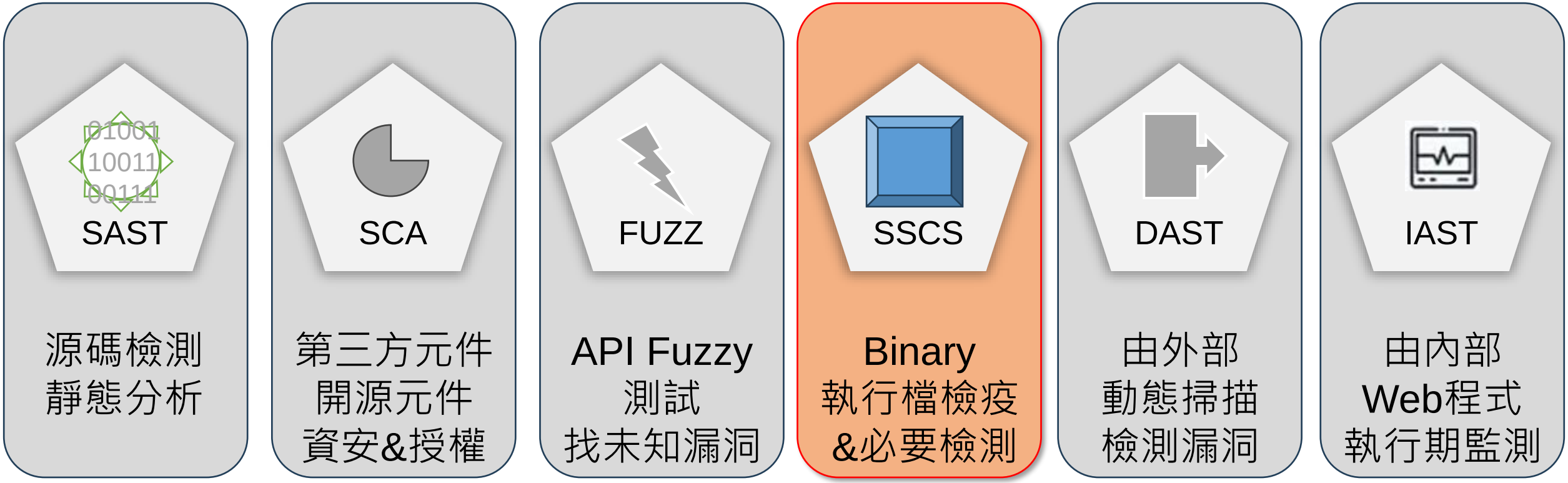

為了安全，會進行需要的檢測，即使代價很高
ADAC
OD4323TNE1
GLOBAL FOR SAFER CARS NCAP
OD4323TNE1

為了應用程式安全，通常會加上多個檢測措施

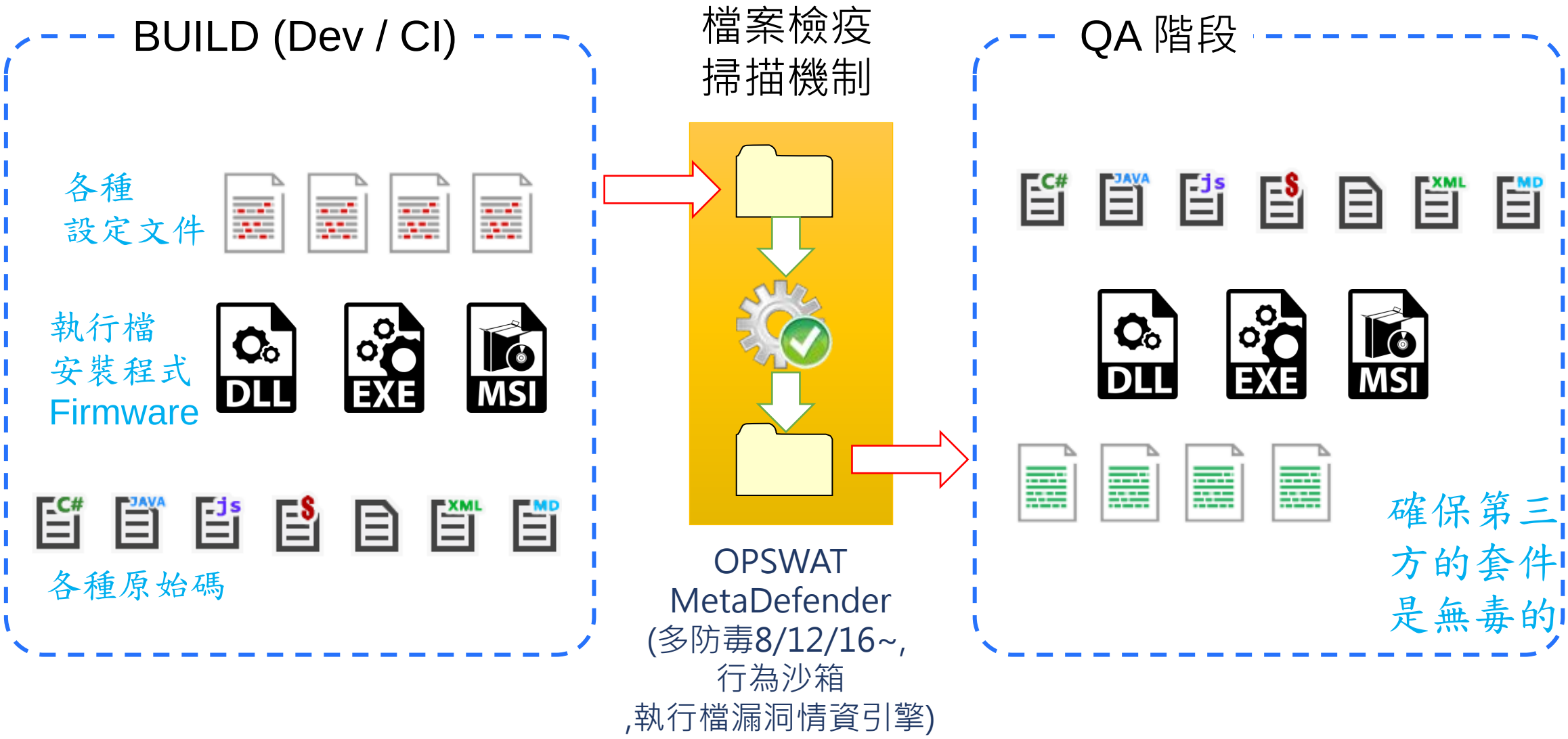


還可能加上滲透測試、紅隊演練....

為了因應軟體供應鏈攻擊，開始考慮加上新的檢測措施



CI/CD 加上新的檔案檢疫檢測措施



Black Duck SCA 方案提供三個面向的開源元件風險管理

Security
資安風險

SBOM
掃描完整性

漏洞情資
即時性與價值

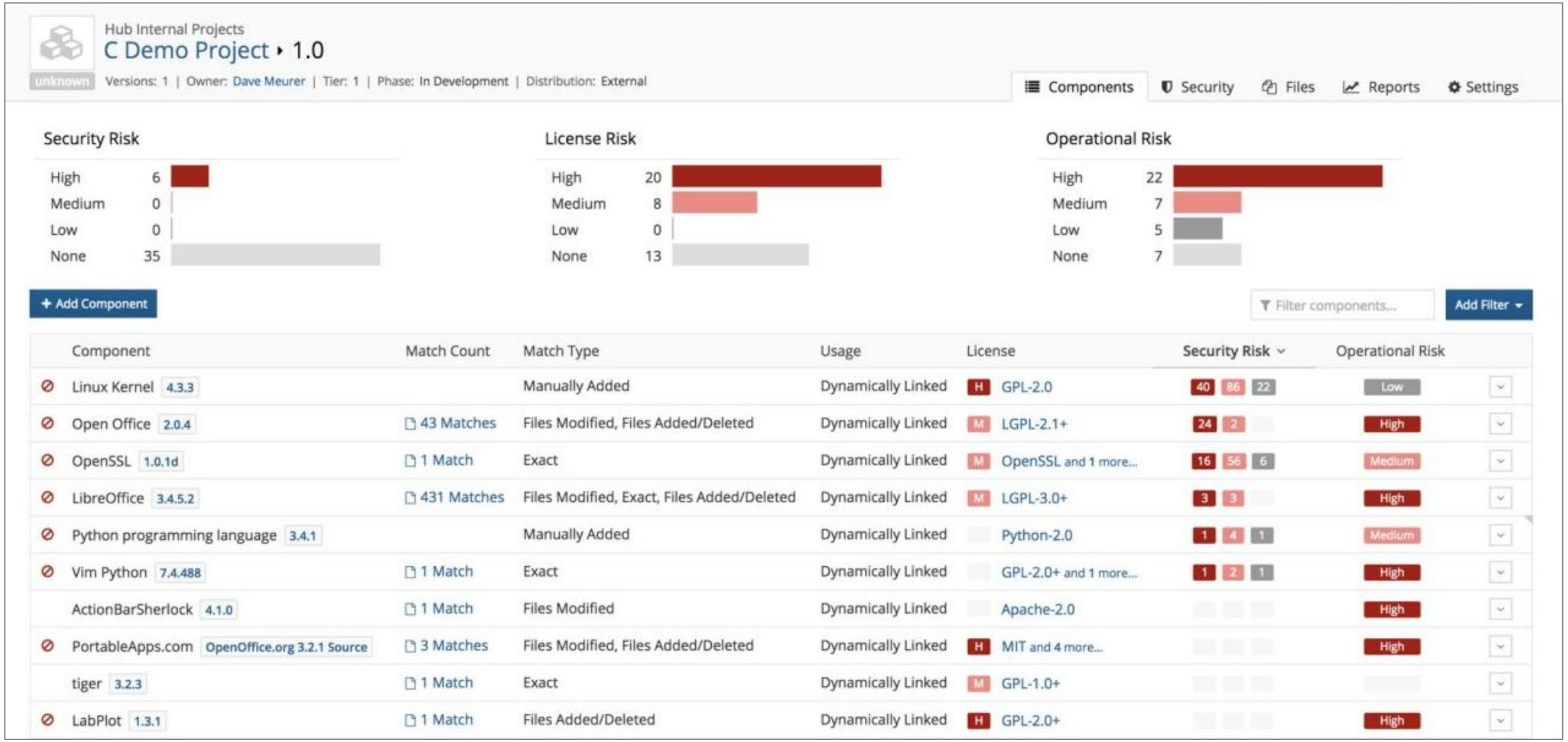
Lisense
開源授權合規

引用 OSS
開源元件
避免授權違規

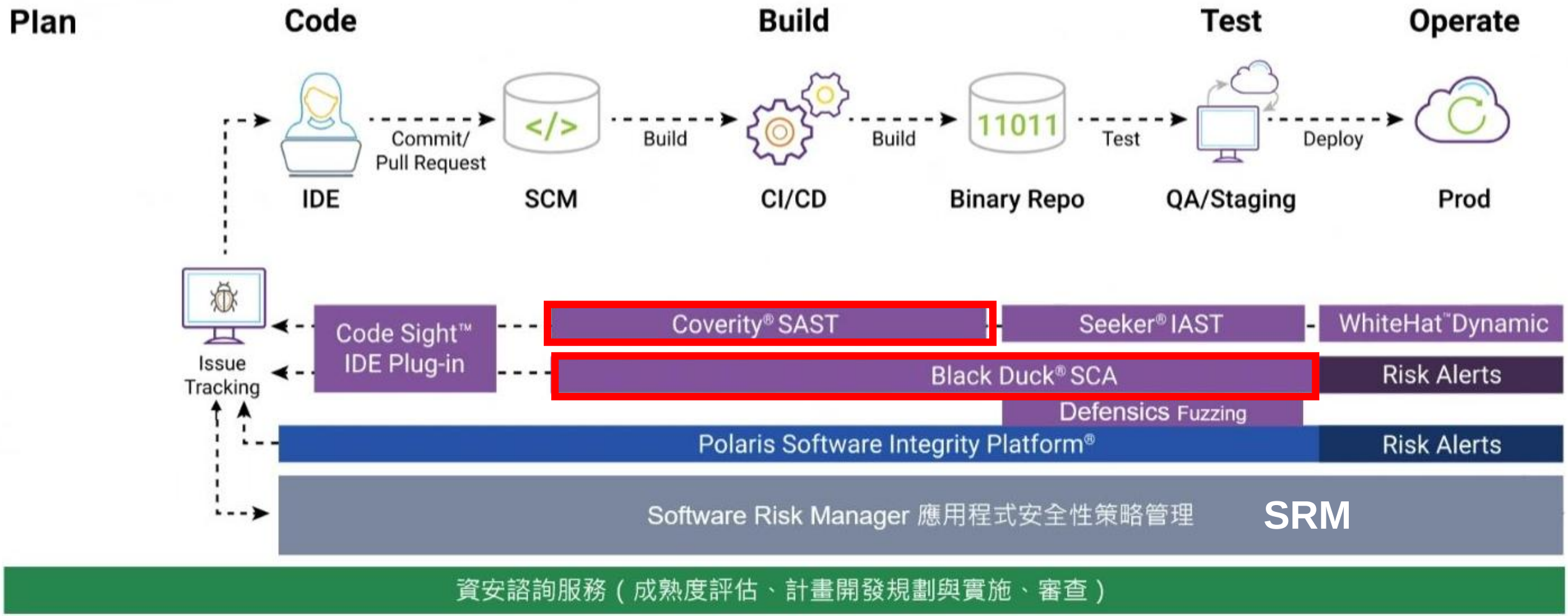
Operation
維運風險

避免用到的OSS
開源元件
已經宣布停止開發
造成維運風險

透過儀錶板，呈現軟體專案的SBOM清單與對應風險狀態



BlackDuck 的應用安全方案，將資安融入 DevOps 中



ISO27001:2022 新版/附錄 A /新增之技術控制措施 5項

編號	項目	控制措施說明
8.11	資料遮蔽	應根據組織關於資訊存取控制與其它相關的特定營運要求，對個資、敏感資訊使用資料遮蔽，並考量合規要求
8.12	預防資料外洩(DLP)	資料外洩預防 DLP 措施，應涵蓋組織中各個可以對外傳送資訊的通道。進行 Content Aware 內容感知偵測，並掌握單位的個資或機敏資料的外送控制
8.16	監視活動	應監視網路、系統和應用程序的異常行為並採取適當的措施來評估潛在的資訊安全事故
8.22	網頁過濾	應加強管控對上網閘道，針對外部網站的存取活動防護，以減少曝露於釣魚/惡意網站，或回報中繼站等活動
8.28	安全程式設計	軟體開發/應用程式安全 (源碼檢測/第三方元件弱點監控)

Overview

OPSWAT Filescan Sandbox

Adaptive Threat Analysis 適應性威脅分析

- 快速且深入的威脅分析服務
- 設計來針對 目標式攻擊分析偵測 以及 IOC 萃取
- 可地端佈署 & 自管的雲端

10x
較傳統沙箱快10倍以上

100x
所需資源少，僅需其他沙箱平台1/100

25k+
一台主機每天可分析 25000 個檔案以上

達友科技所代理的產品線

ISC2 CHAPTER | TAIPEI

【關於我們】

ISC2 Taipei Chapter 是 ISC2 在台灣的分會組織，致力於推廣資安專業知識、交流與社群互助。成員包括經 ISC2 認證的資安專家，及各領域資安專業人士。

【成立宗旨】

提升台灣資安專業社群的能見度與凝聚力。

【使命與活動】

- 推廣資安認證與專業發展
- 舉辦技術講座、各種資安研討活動
- 促進會員交流與跨界合作
- 參與國際資安社群互動

https://www.isc2chapter.tw

contact@isc2chapter.tw

加入 ISC2 Taipei Chapter 讓您的資安之旅，有專家同行！

2025 臺灣資安大會
CYBERSEC 2025
Brand Day 701A

DevSecOps 中
您可能沒想到的軟體供應鏈安全
從案例中學習

達友科技 Docutek Solutions, Inc,
林皇興 Lambert Lin /CISSP
lambert@docutek.com.tw

SYSTEX A I 生 成 。 無 限 可 能

DevSecOps 中，您可能沒想到的軟體供應鏈安全，從案例中學習者安全

填寫問卷送好禮

uniXecure 智慧資安科技

SYSTEX A I 生