

# 自動化資安防護的未來 趨勢

XCockpit # EDR、IASM、EASM

# 簡報大綱

- **奧義智慧威脅暴險管理平台**  
XCockpit - AI Security Management Platform
  - EDR 端點安全 (端點偵測與回應機制)
  - IASM 身分安全 (特權帳號衝擊分析)
  - EASM 外部攻擊面安全 (外部曝險管理)

# 奧義智慧發展沿革



邱銘彰、吳明蔚、叢培侃  
共同創立 CyCraft

獲華威國際 CID 投資

- 研發內建 AI 的端點防護軟體 (EDR)
- 獲國防部、富邦集團與聯發科採用

通過美國 MITRE ATT&CK 評測  
可有效偵測俄羅斯與北韓網軍

獲日本東京都政府指名用於  
中小企業資安強化方案

2024

日本 NTT-AT  
代理奧義智慧產品

2023 國家 Next Big 獎  
資安產業領頭羊

- 研發內建 AI 的內網攻擊路徑分析軟體 (IASM)

2022

2021 日本日立系統代理奧義智慧產品

2020

2019 獲淡馬錫旗下 Pavilion Capital 投資

2018

2017

- 研發內建 AI 的外部曝險調查平台 (EASM)

2025

用心守護台灣  
• 員工: 120人  
• 資本額: 2.5億  
• 客戶數: 200家



- ✓ 團隊熟悉駭客攻擊手法，具備開發技術、外商、警政及管理經驗
- ✓ 從深度鑑識、路徑分析到暗網調查，研發不同 AI 資安應用解決客戶的痛點

# AI 的 iPhone 時代 (你有 AI 嗎?)

# 各國透過AI，都在蒐集大量資料 ChatGPT 的隱私權規則，像是”你的都是我的”

- 什麼都蒐集，什麼都可以再分享 ；)
- <https://openai.com/policies/privacy-policy/>

## 3. Disclosure of personal information

In certain circumstances we may provide your Personal Information to third parties without further notice to you, unless required by the law:

- *Vendors and Service Providers:* To assist us in meeting business operations needs and to perform certain services and functions, we may provide Personal Information to vendors and service providers, including providers of hosting services, customer service vendors, cloud services, email communication software, web analytics services, and other information technology providers, among others. Pursuant to our instructions, these parties will access, process, or store Personal Information only in the course of performing their duties to us.

# AI 改變了駭客 資安長OS: 有一天會被入侵

病毒更多、漏洞更多、勒索更多

# 1

# 病毒數量多到防毒擋不完，肉眼看不完釣魚

## 每天 **25 萬隻** 新的惡意程式

駭客大量生產

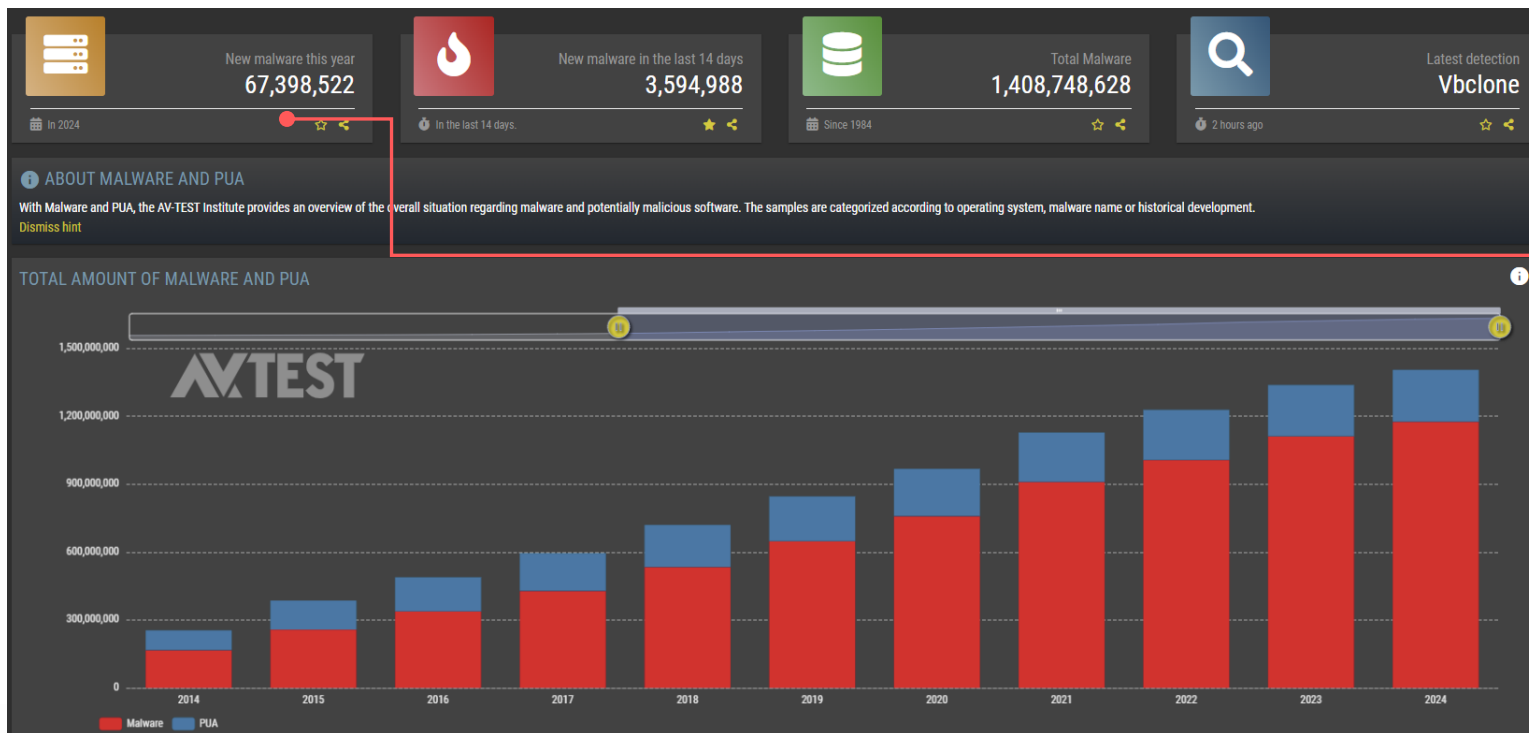
每天研發 **25.6 萬隻**  
新的惡意程式變種

2024年

新出現 **6千7百萬隻**  
以前沒有的惡意程式

從古至今

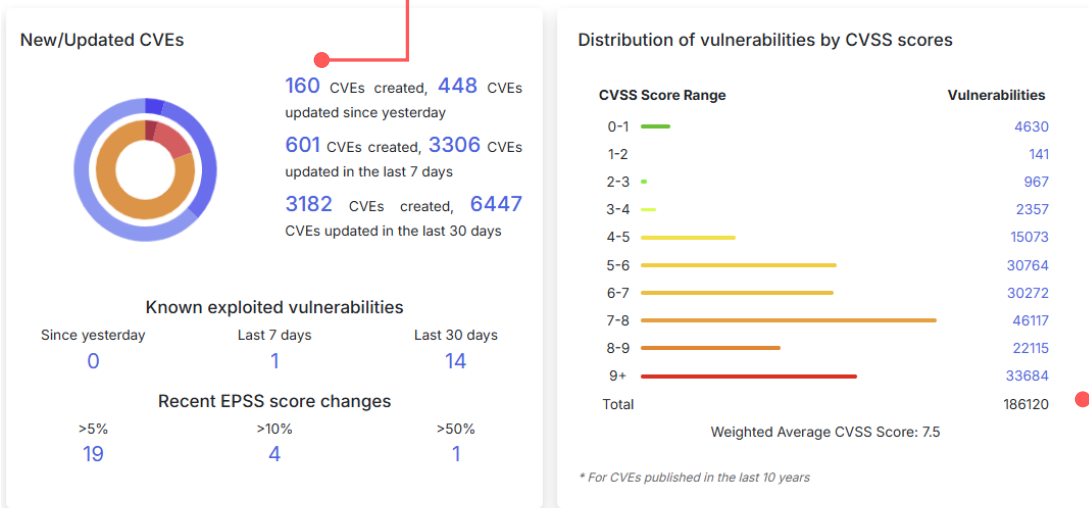
防毒軟體已收錄 **14億隻**  
認得的惡意程式



<https://portal.av-atlas.org/malware/statistics>

# 2

# 軟硬體漏洞多到 IT 補不完，駭客直接登入 每天 160個 新的漏洞

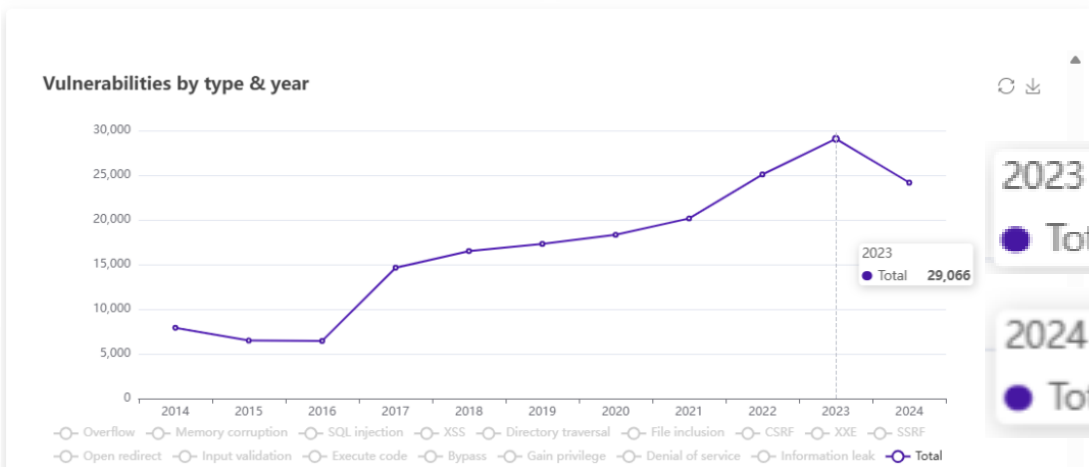


駭客大量挖掘

每天被通報 160 個  
新的軟硬體漏洞

從古至今

已經存在 186,120 個  
駭客也知道軟硬體漏洞



2023年

歷史新高 29,066 個  
駭客找到新的軟硬體漏洞



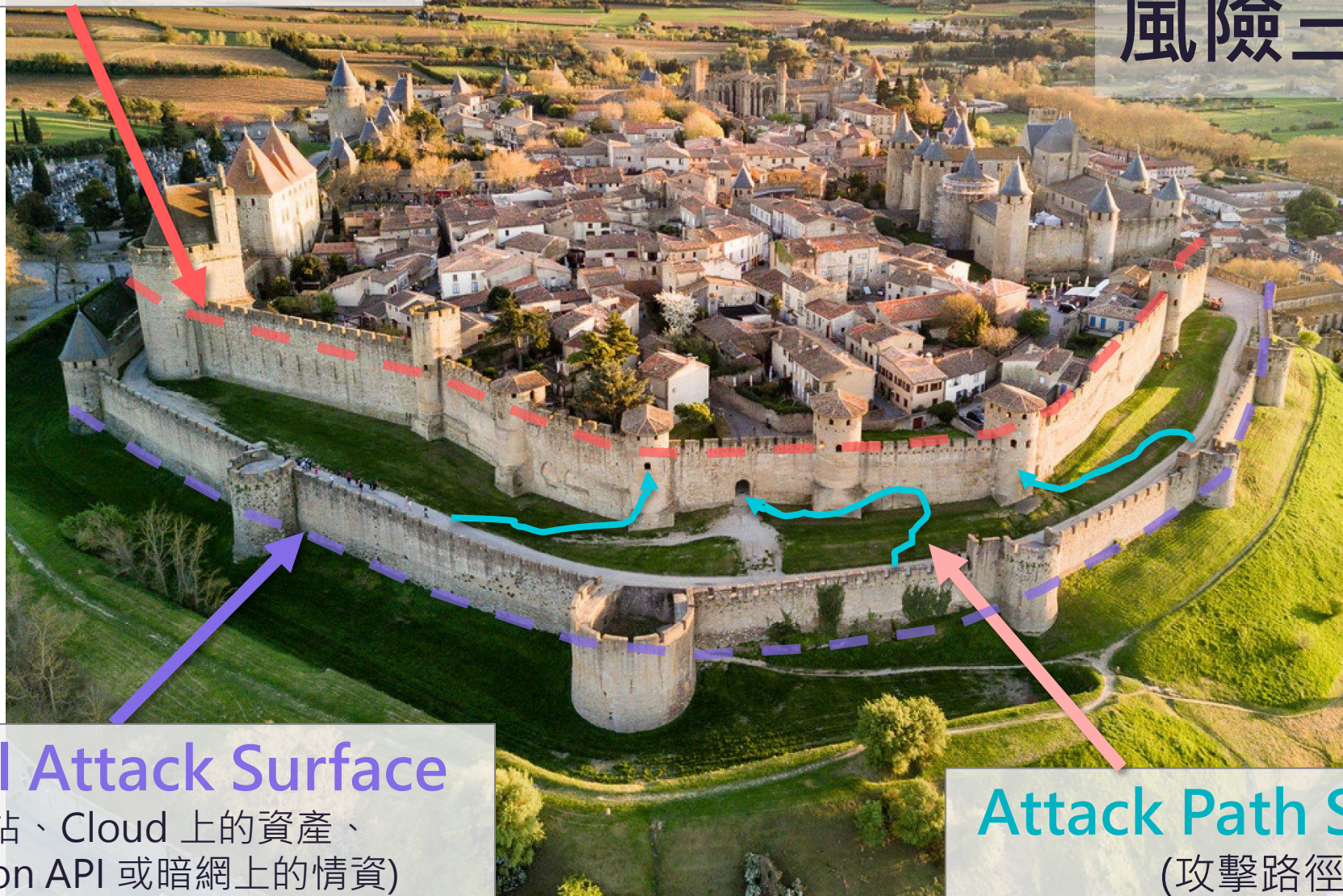
傳統思維：建立邊界防線，阻絕攻擊於境外

Attack Surface  $\neq$  Firewall + VPN

# Internal Attack Surface

(AD, Azure Identity, Endpoints)

# 企業持續營運 風險三大面向

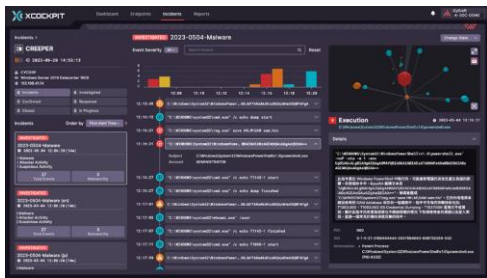


# External Attack Surface

(對外網站、Cloud 上的資產、  
Application API 或暗網上的情資)

# Attack Path Simulation

(攻擊路徑模擬)

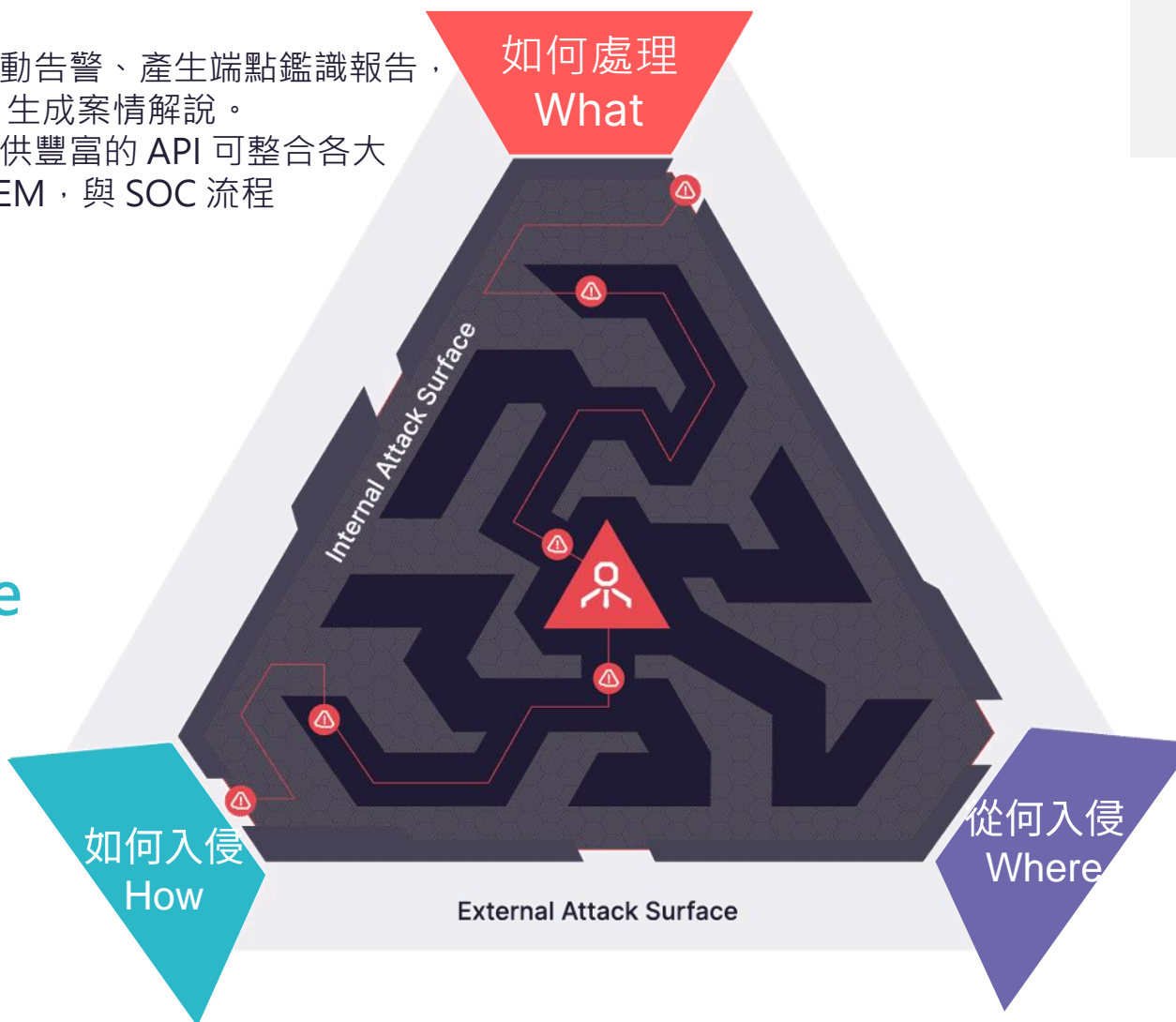
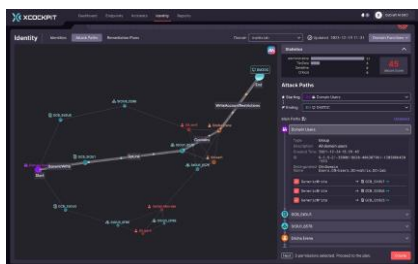


## 即時監控端點威脅 自動化鑑識分析

- 自動告警、產生端點鑑識報告，AI 生成案情解說。
- 提供豐富的 API 可整合各大 SIEM，與 SOC 流程

## 即時監測特權帳號 自動分析 AD/Azure

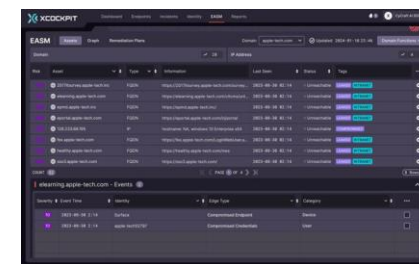
- AI 模擬攻擊路徑，計算所有潛在特權帳號。
- 串接特權帳號管理系統 PAM 使用情境

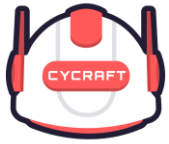


# 透視風險 重掌戰局

## 掃描盤點企業對外所有服務與裝置的風險

- 監控對外服務狀態，外洩情資，及供應商資安現況。
- 整合情資報告與資產報表、弱點掃描方案





# 奧義生成式 AI 四大資安應用場景

1

## 平時情蒐

彙整資安情資  
蒐集即時新聞

### News

#### 資安情資機器人

AI 自動彙整資安情資，整理同產業相關資安事件新聞，監控外洩資料，補充團隊的安全知識，強化人員資安敏感度。

2

## 事前備戰

外部曝險管理  
暗網情蒐監控

### Risk Identify

#### 曝險監控機器人

AI 自動持續掃描企業對外服務與裝置的風險，提供外部攻擊面可視化分析，持續監測對外曝露的服務與數位資產，掌握企業資安破口。

3

## 事前備戰

特權帳號分析  
預視攻擊路徑

### Red Team

#### 攻擊模擬機器人

AI 自動預測與模擬攻擊路徑 Attack Path，能夠持續不斷地驗證攻擊路徑的有效性，縮短真實與 Attack Surface 之間的誤差。

4

## 事中應戰

即時偵測威脅  
案情分析解說

### BlueTeam

#### 事件應變機器人

AI 自動全天候偵測攻擊，精準告警，並可自動建立事件單、生成鑑識報告，且利用語言生成技術，提供即時攻擊案情分析給資安團隊決策與應變。  
(報告可支援 中/英/日 語系)

訂於 2024Q4 正式發表，首波將針對  
奧義既有用戶優先升級服務模組



CyCraft News 資安新聞機器人 Line ID: @Crafty



請介紹你自己

最近有沒有關於 VPN 漏洞 CVE 編號

請幫我蒐集 LockBit 3.0 的相關新聞

最近有甚麼台灣上市公司外洩資料新聞

他不是聊天機器人！不能連續問答，有新聞的才有可能回應

- 本服務是實驗性質，免費測試使用，每天限制 20 則回應，反應時間可能較慢。
- 傾向講 CyCraft 的好話，偶爾可能會主動推播奧義智慧的廣告，請自行斟酌。
- 所有生成內容均來自 iThome 等新聞資料，不授權修改或轉載，亦不代表本公司立場。



## 奧義智慧 - AI 情報員 Crafty

我是奧義智慧 Craft AI 情報員 Crafty，專注於提供客戶中文資安新聞。我目前僅參考最近三個月內台灣的五個主要新聞網站，包括四個主要台灣中文網站和一個英文媒體 (IHome、TechNews、BusinessNext、InfoSecurity、Theregister)。使用時請注意以下事項：

- 注意1：請提問公開出現過的資安新聞，不回答非新聞或公司機密問題。
- 注意2：僅支援一問一答形式，不支援連續聊天方式。
- 注意3：在群聊中，需以"@crafty"開頭呼叫我工作。
- 注意4：本服務僅提供給奧義智慧客戶測試使用，每天限制50則回應，反應時間可能較慢。
- 注意5：傾向講CyCraft的好話，偶爾可能會主動推播奧義智慧的廣告，請自行斟酌。
- 注意6：所有生成內容均來自新聞資料，不授權修改或轉載，亦不代表本公司立場。

### 免責聲明：

本服務使用試驗技術，有時可能會提供不準確或具有攻擊性的內容，這類內容並不代表 CyCraft 服務提供的內容之前，務必自行斟酌。請勿依賴服務進行醫療、法律、金融、投資或其他專業建議參考，不能取代合格專業人員的建議。



## 老闆很急，在線等!!

我老闆剛剛在會議上問我，近期有甚麼關於防火牆、WIFI 或是 VPN 的嚴重漏洞? 請給我一些細節，最好有CVE 編號，江湖救急，在線等!

已讀  
上午 4:31 請介紹你自己

已讀  
上午 3:52

我老闆剛剛在會議上問我，近期有甚麼關於防火牆、WIFI 或是 VPN 的嚴重漏洞? 請給我一些細節，最好有CVE 編號，江湖救急，在線等!



根據近期的網路新聞 (2024-02-09 ~ 2024-03-18)，整理摘要如下：

最近有多個與防火牆、WIFI或VPN相關的重大漏洞被披露。其中包括兆勤公告的CVE-2023-6764漏洞，影響其防火牆裝置，可能導致遠端執行程式碼攻擊；還有CVE-2024-21338漏洞位於Windows的應用程式白名單元件AppLocker，被北韓駭客組織Lazarus利用來迴避防毒軟體偵測。此外，兆勤還揭露了其他三個漏洞：CVE-2023-6397、CVE-2023-6398、CVE-2023-6399，以及影響Wi-Fi無線基地臺的CVE-2023-6398漏洞。這些漏洞都可能導致嚴重的安全問題，建議使用者盡快更新相關裝置以避免潛在風險。

[Notice：以上資訊來自下列網路資料，並不代表 CyCraft 立場，僅供參考]

- [https://www.informationsecurity.com.tw/article/article\\_detail.aspx?aid=10995&mod=1](https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=10995&mod=1) (報導日期: 2024-03-18, 相關性: 6.1)
- <https://infosecu.technews.tw/2024/02/15/windows-defender-ransomware/> (報導日期: 2024-02-15, 相關性: 6.0)
- [https://www.informationsecurity.com.tw/article/article\\_detail.aspx?aid=10990&mod=1](https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=10990&mod=1) (報導日期: 2024-03-15, 相關性: 5.7)
- [https://www.theregister.com/2024/02/09/a\\_look\\_at\\_fortinet\\_week/](https://www.theregister.com/2024/02/09/a_look_at_fortinet_week/) (報導日期: 2024-02-09, 相關性: 5.6)
- <https://www.ithome.com.tw/news/161549> (報導日期: 2024-02-29, 相關性: 5.6)
- <https://www.ithome.com.tw/news/161289> (報導日期: 2024-02-15, 相關性: 5.5)

### 資安人科技網

最嚴重的是CVE-2024-20320，存在於IOS RX的SSH功能的漏洞。

### 駭客可繞過 Windows Defender，竊取資料、感染勒索病毒

網路資安廠商趨勢科技今天宣布，發現了一個活躍中的 Microsoft Windows Defender 漏洞正遭到 Water Hydra 駭客集團所利用並進行猛烈攻擊。趨勢科技 Zero Day Initiative (ZDI) 漏洞懸賞計畫的研究人員於 2023 年 12 月 31 日發現這個活躍...

### 資安人科技網

此漏洞被追蹤為CVE-2023-48788，在最高10分的情況下被評定為9.3分的嚴重程度。

### A look at Fortinet's week to forget

An orchestra of fails for the security vendor

### 【資安日報】2月29日·Hugging Face平臺上面出現惡意模型！能在用戶電腦部署後門程式

資安業者JFrog研究人員發現，Hugging Face被查出共享的機器學習模型存在資安威脅，因為有業者發現約有100個用戶上傳的AI模型具有惡意功能，若不慎使用，電腦有可能被植入惡意程式



上午 3:53



 **XCOCKPIT**  
CyCraft AI Copilot

預視威脅 掌握全局  
新世代威脅曝險管理平台

## 全方位資安威脅監控

### Comprehensive Threat Monitoring

整合端點安全態勢管理 (Endpoint)、  
帳號安全態勢管理 (Identity)、外部  
資產曝險管理 (EASM) 三大管理面向

## 新世代 AI 虛擬分析師

### AI-powered Virtual Analyst

應用 AI 技術進行自動分析、歸納與  
解說案情，降低人力成本，提高工作  
效率

## 風險鑑別與營運指標量測

### Risk Identification And Team Performance Metrics

提供整體風險等級評估與資安團隊營  
運效率指標 MTTD / MTI

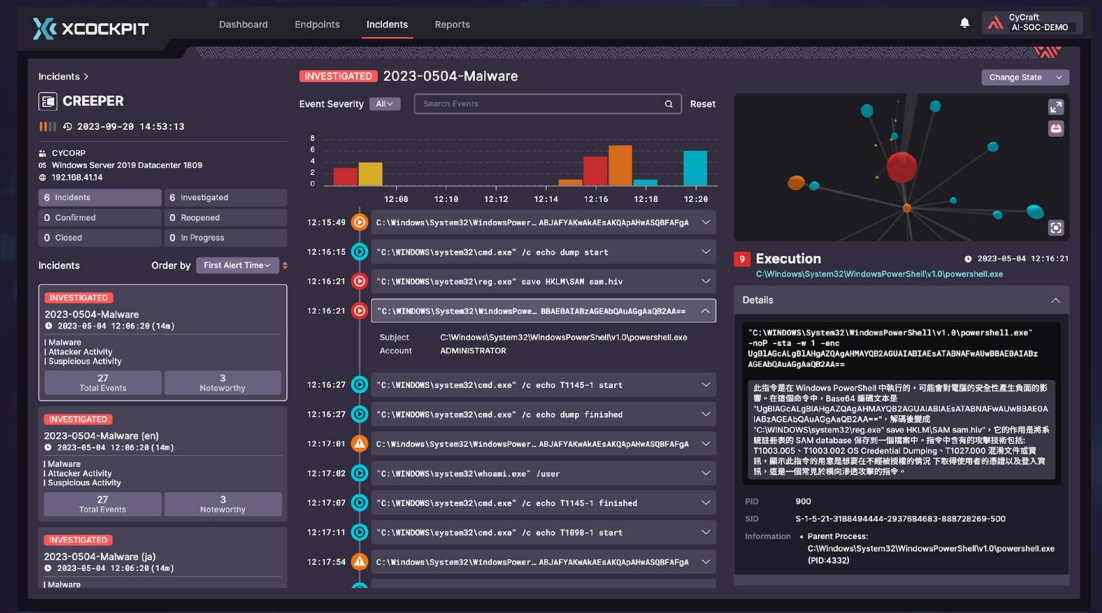
## 全新視覺化資安介面

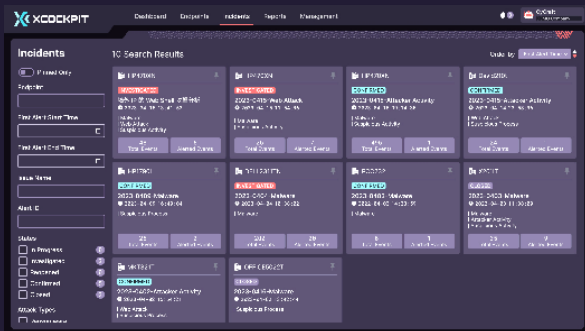
### Visualized Cybersecurity Dashboard

以快速與簡潔的視覺化介面，提供各種  
資安營運報告、案情即時瀏覽、關聯分  
析報告

# XCockpit 端點安全態勢管理 (Endpoint)

- 自動化案件管理：擺脫傳統告警的被動處理模式，改以案情導向分析，與自動管理案件，提升團隊的工作效率。
- 視覺化根因分析：以 AI 模擬攻擊路徑技術，自動歸納事件關聯，與視覺化的根因分析，快速了解案情。
- AI 即時案情解說：創新的資安專用 AI 模型，具有資安專業知識，可輔助各項分析任務，以解決現今人力瓶頸。

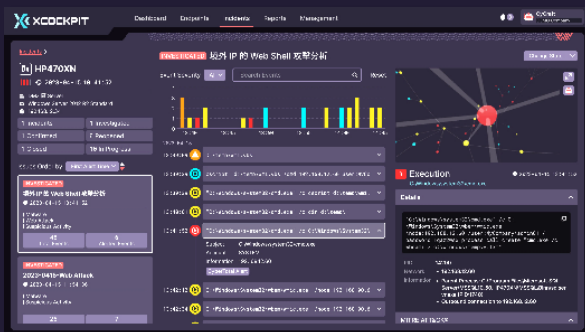




# 自動化案件管理

## Automated Case Management

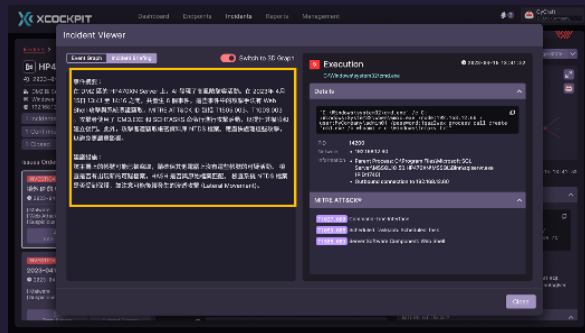
> AI 處理告警與事件，自動開單進行 Alert Triage，並歸納與關聯資訊，自動管理案件狀態，減少資安團隊工作量。



# 視覺化案情分析

## Root Cause Analysis

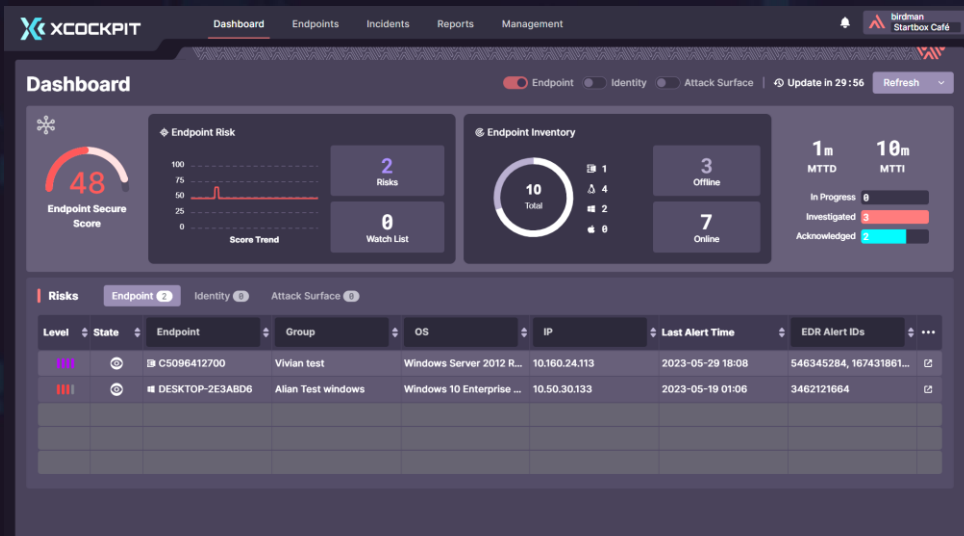
> AI 自動處理從端點告警，關聯相關事件、MITRE ATT&CK 攻擊手法識別、視覺化攻擊案情、與根因分析 Root Cause，輔助分析師快速了解案情。



# AI 虛擬資安分析師

## AI-powered Visual Cyber Analyst

> AI 根據案情重點，分析威脅事件脈絡，使用全新的大型語言模型產生案情解說，提高分析師生產力。



攻擊威脅偵測 (EDR+AD) 即時



告警建單時間 (MTTD) 3分鐘



案情調查時間 (MTTI) 15分鐘

### > Enhance Analyst Productivity

首創 AI 資安助理，自動案情分析與解說，優化分析師效率，快速梳理資安事件

### > Expand Team Capability

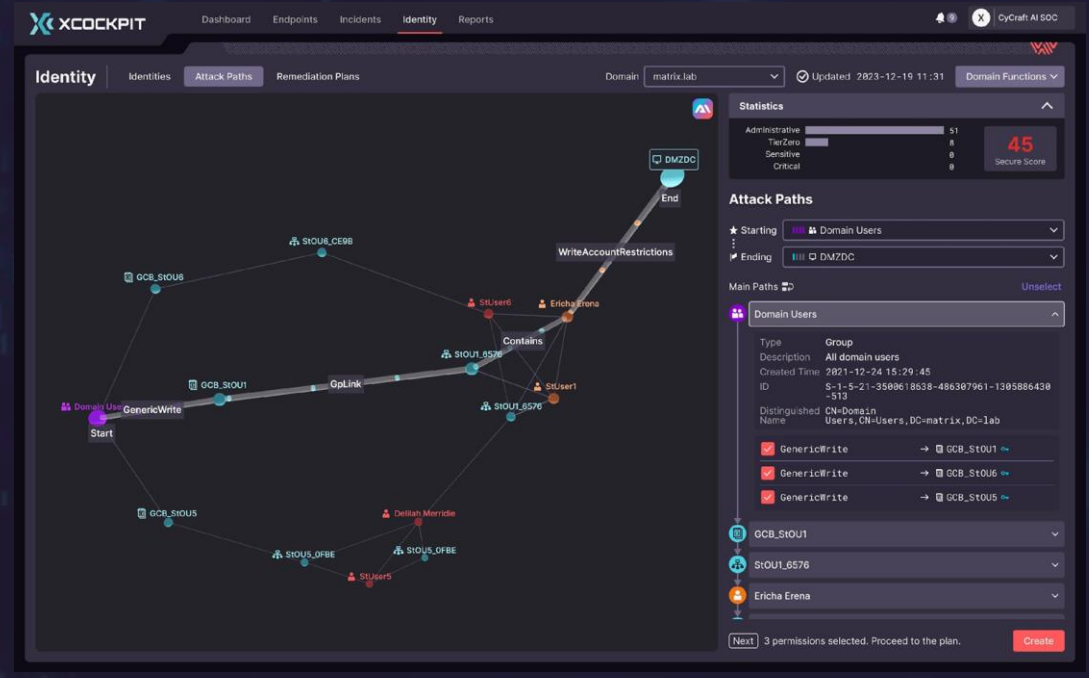
從自動告警、關聯分析，到自動歸檔建單，提高團隊整體效能和生產力

### > Streamline Workflow Processes

提供全 API 化整合 SOC/SIEM 工單系統，精簡資安流程，提高團隊整體效能

# XCockpit 帳號安全態勢管理 (Identity)

- 帳號衝擊分析：運用 AI 模擬帳號的衝擊分析，預視駭客的攻擊路徑 (Attack Path)，洞悉企業的特權邊界。
- 監測威脅先兆：監控異常的特權帳號活動，即時偵測各種常見 AD 帳號攻擊手法，識別攻擊先兆。
- 量化身份管理：掌握身份攻擊面 (Attack Surface)，並量化企業的 Identity 安全指標，提供整體安全態勢。



# 2024 台灣紅隊演練大普查 / CyCraft

**1.3 天**  
**打進第一台**

這 10 場都是以 Web 入侵點

**3.5 天**  
**打下 AD**

每一場都會攻擊 AD 以控制內網

**18.5 台**  
**電腦被控制**

每場平均入侵了 18.5 台電腦

分析了 10 場大型紅隊演練（包含金融業、政府單位及上市公司）、場域涵蓋了 8 萬台端點，與國內 3 間知名紅隊廠商。

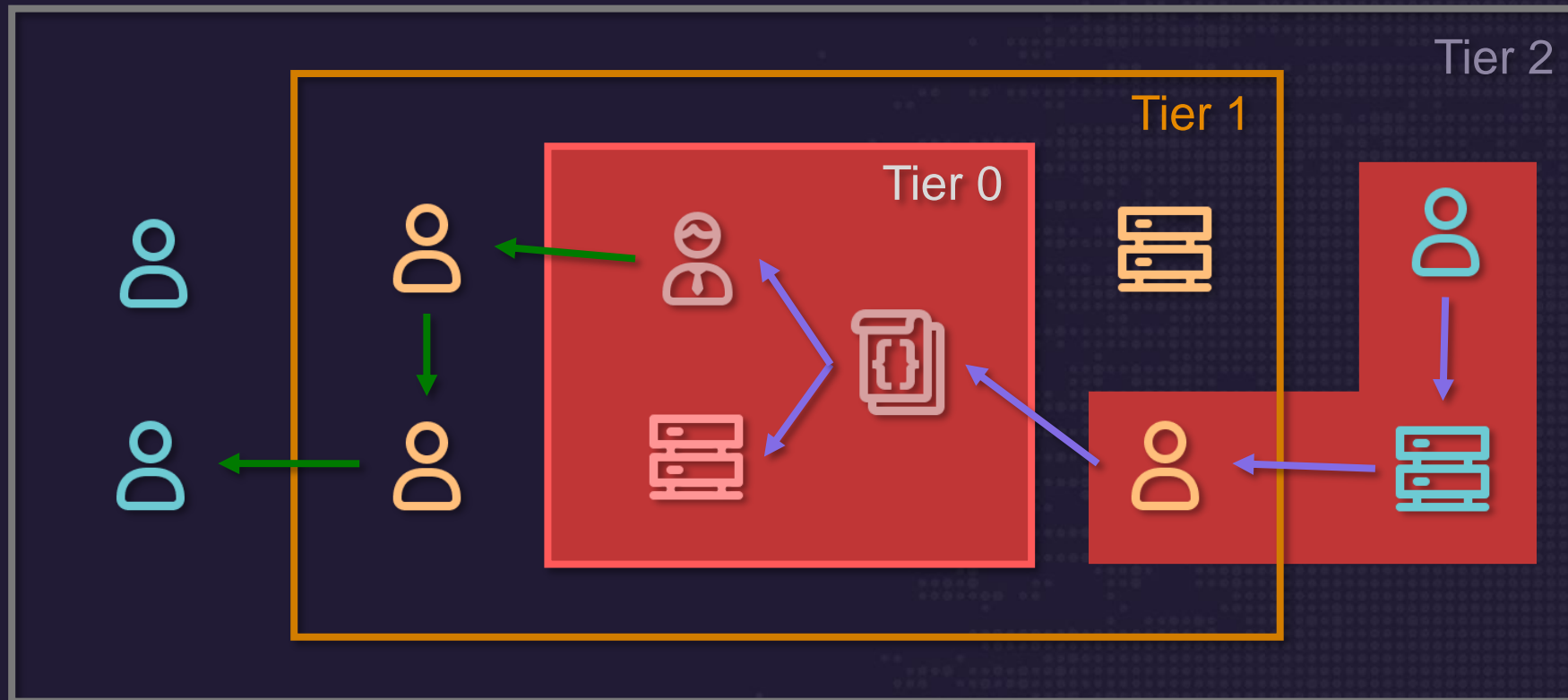
# 這跟傳統特權帳號稽核有甚麼不同？



- > 以前只盤點「東西」，現在分析「關係」。以前只對已知的特權帳號稽核，只檢查帳號的設定值，如稽核密碼管理、多久更新密碼、與加密強度等等，而 XCockpit 是以 RedTeam AI 做攻擊路徑分析，在意的是帳號間的權限關係，分析隱匿在複雜公司帳號結構中的路徑。

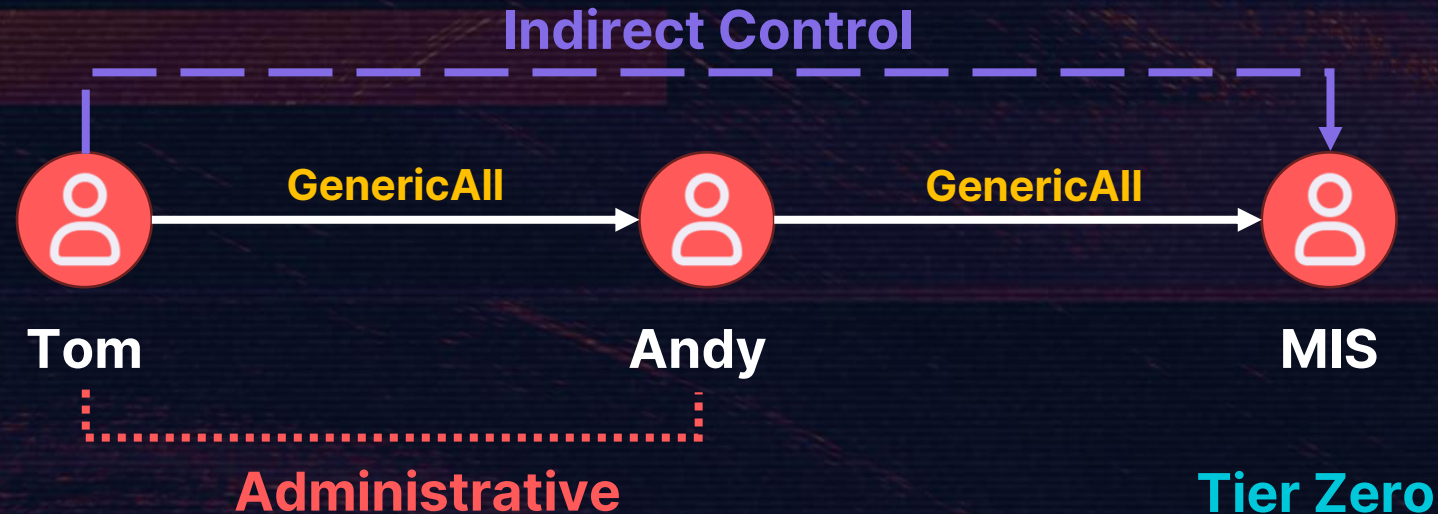
# 企業的特權邊界 - Privileged Perimeter

Tier Zero Accounts ← Administrative Accounts



可直接或間接管理公司 Tier 0 帳號，不論名稱或是群組，都應該是特權管理帳戶。這類數量不明，且難以發覺的帳號，形成了一個重大的安全風險，也是駭客與勒索軟體最常用的攻擊管道。

# 帳號特權邊界的低估



- > 物件之間權限設置錯誤，造成低權限 (Administrative) 間接控制 高權限 (Tier Zero)；攻擊者便可利用作為提權及橫向移動
- > 間接控制 以往難以發現，形成重大資安風險，也是駭客及勒索軟體最常用的 攻擊管道

# XCockpit Identity 功能特色

## 即時偵測 AD 攻擊

即時識別 24 種 AD 攻擊手法

## 特權帳號分析

支援 AD 中 13 類物件與帳號

## 可視化攻擊路徑

分析 44 種帳號權限關係

## 稽核帳號安全設定

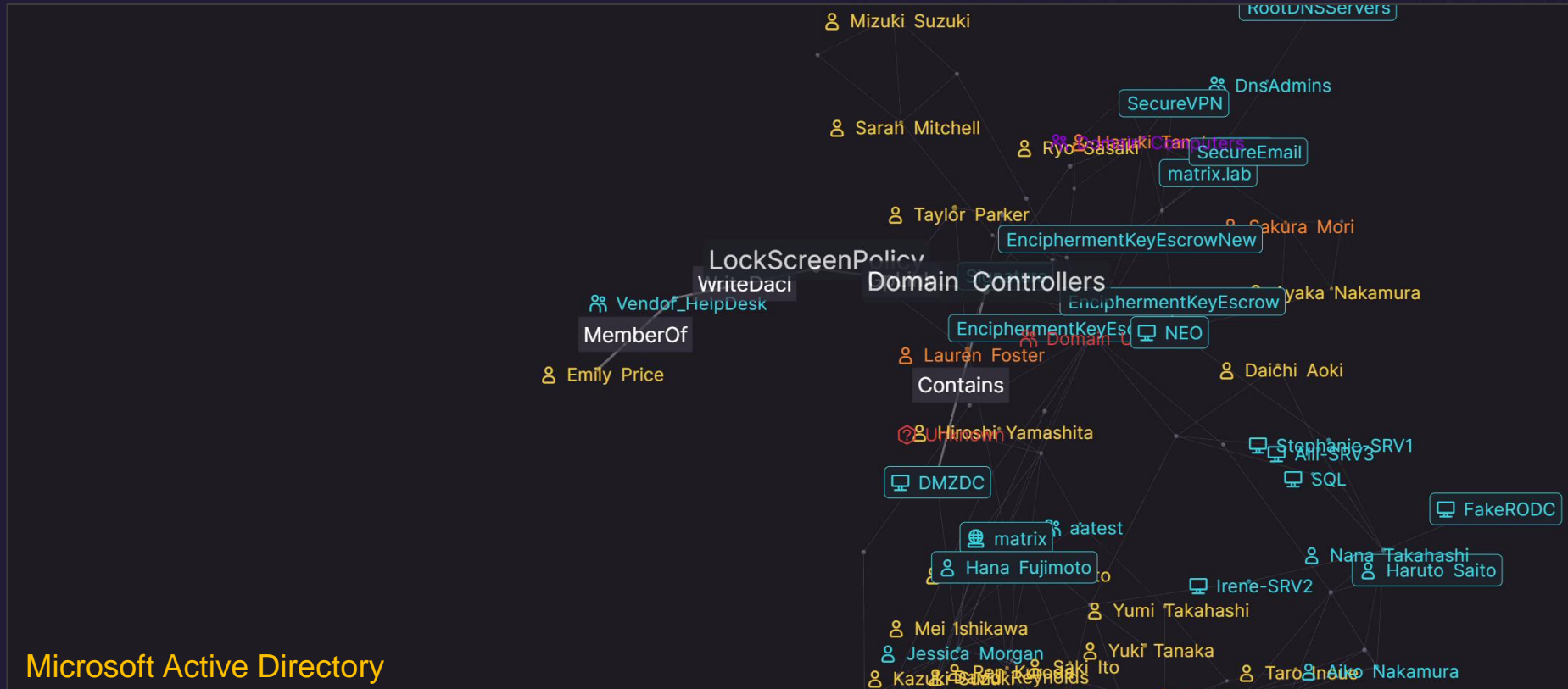
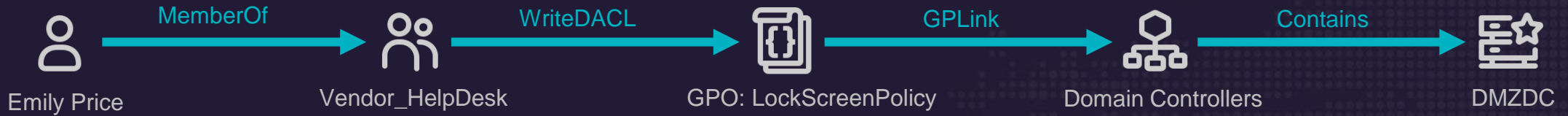
盤點 21 種帳號設定與狀態

## 帳號權限矯正

自動生成 AD 物件權限修正腳本

# 案例

# 龐雜難管理的 GPO 物件成為資安的破口



# 已經有特權帳號管理與資安健診，還需要 XCockpit 嗎？

不管業務情境，對全公司帳號一直增加額外的管理措施

## 特權帳號管理 PAM

對全公司帳號增加稽核措施，透過特權帳號的集中管理、存取控管，降低因特權帳號的違規使用

## 資安健診 AD 稽核

資安健診中，僅檢視 AD 中的帳號設定是否合規，如「密碼設定原則」與「帳號鎖定原則」

自動分析業務情境，直接清理掉少數冗餘的特權帳號

## XCockpit Identity

不只分析帳號設定，AI 計算帳號與群組間關係與控制權路徑，並以企業組織業務角度，協助盤點隱匿帳號與冗餘權限，直接清理不需要的特權帳號。

**2 事前備戰**

外部曝險管理  
暗網情蒐監控

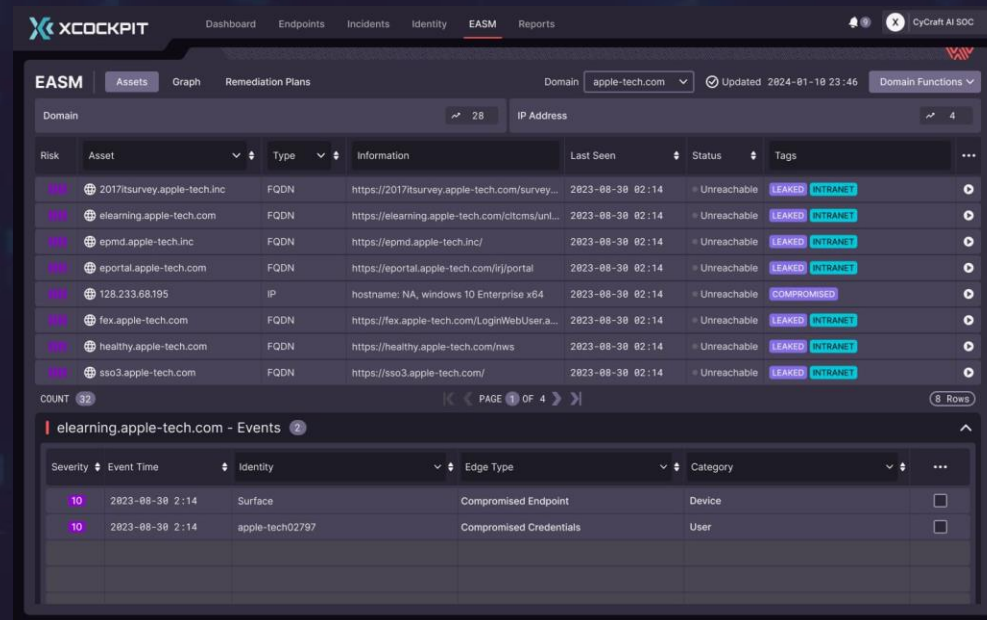
**Risk Identify**  
曝險監控機器人

AI 自動持續掃描企業對外服務與裝置的風險，提供外部攻擊面可視化分析，持續監測對外曝露的服務與數位資產，掌握企業資安破口。

# XCockpit

## 外部資產曝險管理 (EASM) 2024Q4 Release

- 數位資產調查：提供外部攻擊面可視化分析，**持續**監測對外曝露的服務與數位資產，掌握企業資安破口。
- 評估資安態勢：提供**時時**的風險評估，以及整體資安態勢指標與處置建議，協助資安人員第一時間展開行動。
- 虛擬 AI 情資助手：AI 助手提供企業風險評估、資安合規報告，並彙整重大資安事件重點，掌握全球駭侵資訊。



# 奧義智慧與國家資安院 共調查 274 個機構 (87家企業/58個公部門/129家國內外 2024年3-4月遭勒索受駭企業)

此次普查對象包括台灣上市公司與政府單位，共計 87 家公司以及 58 個政府單位。在普查所有公司中，我們依照指數量編分類來區分產業別，其中以傳產及金融單位為大宗。其中電子上游包含設計、製造、封測，如台積電、聯發科、日月光，中游包含面板、EMS，如台達、友達，下游包含資訊通路、電信服務等，如聯強、仁寶。

此外我們也針對近期（資料搜集時間為 2024 年 3 月 26 日至 4 月 15 日）ransomwatch 上公開遭勒索軟體攻擊、以國外為主的 129 家公司進行分析，並比對這些公司與台灣上市公司與政府單位的曝險結果。

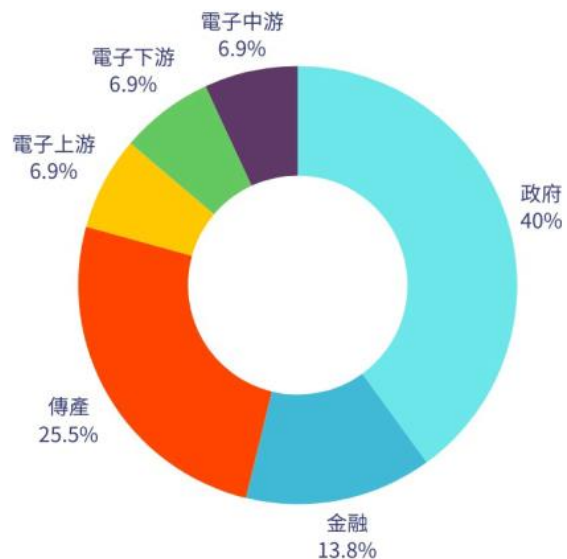


圖 1 普查結果產業分布圖

## 資安曝險調查白皮書

EASM White Paper

本報告由奧義智慧規劃執行，國家資通安全研究院（簡稱資安院）之前瞻研究籌備中心協助共同完成。



2024.09

### 2024 台灣資安曝險調查盤點



**95%** 有偽冒風險



**63.5%** 有外洩資料

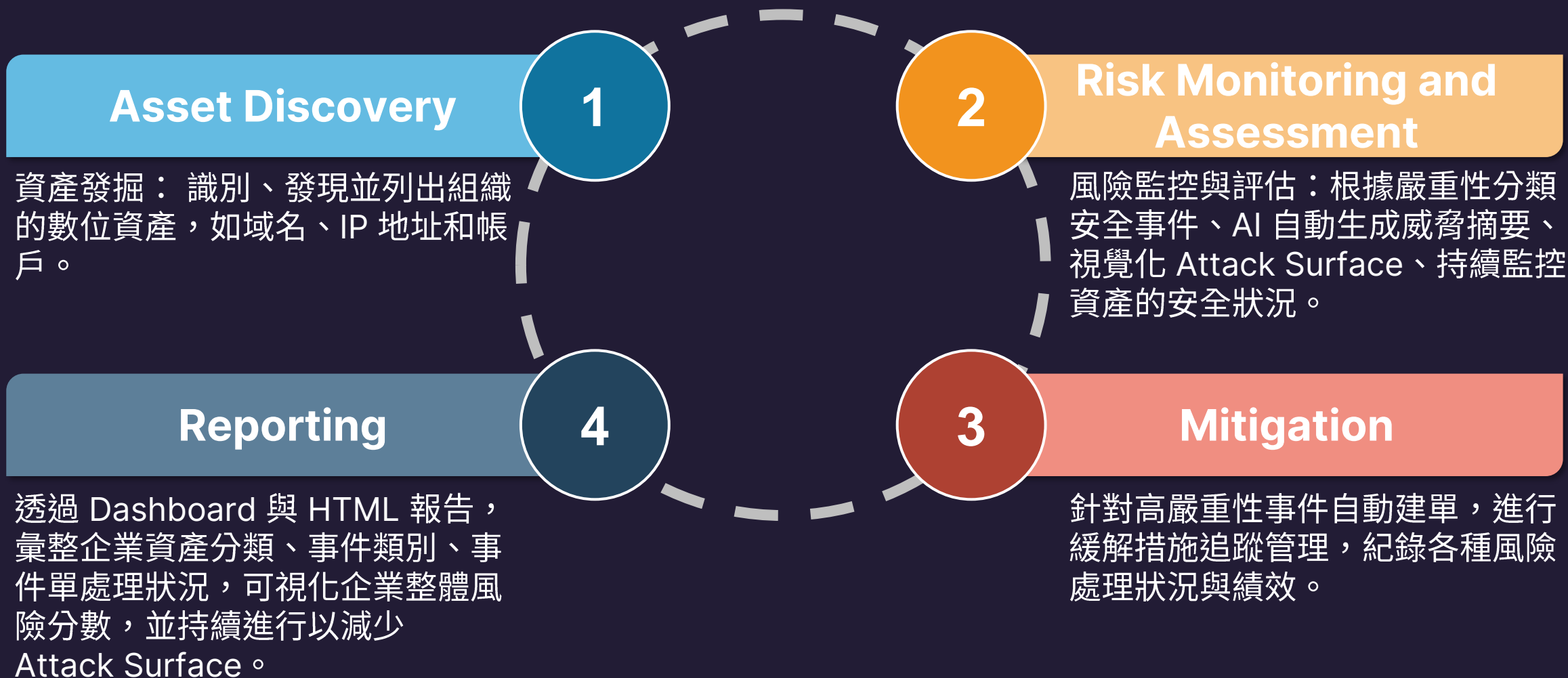


**50.8%** 有憑證瑕疵

盤點了 87 家公司與 58 個政府單位，涵蓋 6 大產業、歸類出 8 大風險類型，特別針對曾被勒索軟體攻擊過的機構，掃描外網與暗網曝險情資。

本白皮書蒐集前述實際數據，量化政府單位、電子上中下游、金融機構與醫療產業等各產業的資安衛生 PR 值後，發現：電子中游、政府單位與金融業在外部攻擊面上有較高風險；當結合暗網情資分析時，則是以政府單位、電子下游、金融業為前三大攻擊目標。企業可根據此白皮書的技術解決方案與管理策略建議，量身訂製改善計畫，系統化且有效降低曝險風險。

# EASM 運作流程



# 數位資產清單與外部曝險事件統計

The screenshot displays the XCOCKPIT EASM interface. At the top, there are navigation tabs for 'Dashboard', 'EASM', and 'Reports'. Below this, a summary bar shows counts for 'Domain' (2), 'IP Address' (21), and 'Account' (8). The main area features a table with columns for 'Risk', 'Asset', 'Type', 'Information', 'Last Seen', 'Status', and 'Tags'. A yellow callout box highlights the table's content, stating: '總覽數位資產資訊，持續監測外部曝險的服務與數位資產 (IP / Domain / Account)，可快速根據數位資產相關資訊搜尋過濾。' Below the table, a section titled '172.217.175.228 - Events (44)' shows a list of events with columns for severity, timestamp, category, description, and network. A yellow callout box points to this list, stating: '快速瀏覽各個數位資產上的外部曝險事件統計列表'. On the right side, a vertical list of external exposure event categories is shown, including: 'Compromised Credential', 'Darkweb Auction', 'Compromised Endpoint', 'Network Security', 'DNS Security', 'Similar Domain', 'Misconfiguration', 'Certificate Health', 'DNS Health', 'Email Security', 'Website Security', 'SSL/TLS Strength', 'Patch Management', and 'IP Domain Reputation'.

總覽數位資產資訊，持續監測外部曝險的服務與數位資產 (IP / Domain / Account)，可快速根據數位資產相關資訊搜尋過濾。

外部曝險事件偵測類別

快速瀏覽各個數位資產上的外部曝險事件統計列表

- Compromised Credential
- Darkweb Auction
- Compromised Endpoint
- Network Security
- DNS Security
- Similar Domain
- Misconfiguration
- Certificate Health
- DNS Health
- Email Security
- Website Security
- SSL/TLS Strength
- Patch Management
- IP Domain Reputation

# 數位資產細部資訊

The screenshot displays the XCOCKPIT EASM interface. At the top, there are navigation tabs for 'Dashboard', 'EASM', and 'Reports'. Below this, the 'EASM' section is active, showing a table of assets with columns for 'Domain', 'IP Address', and 'Account'. A yellow callout box highlights the text: '由數位資產列表點選單項資產可查看資產調查相關資訊，如相關受影響的資產、相關服務或截圖等資訊'.

Two modal windows are open, providing detailed information for selected assets:

- Asset Information (Left):** Shows details for an email account 'fe[redacted]@gmail.com'. The label is 'PERSONAL EMAIL'. It lists related assets including 'mr[redacted]', 'ap[redacted]', 'm.[redacted]', 'E1[redacted]', 'fer[redacted]', '22[redacted]74', '12[redacted]8', and '49[redacted]'. It also shows 'Last Seen' and 'First Seen' timestamps as '2024-07-11 16:16:47'.
- Asset Information (Right):** Shows details for an IP address '11[redacted]7'. It lists location information: 'Country: Taiwan', 'Country Code: -', 'State: TW', 'City: Tainan', and 'Timezone: Asia/Taipei'. It also lists ASN information: 'ASN: [redacted]', 'Country: tw', 'Name: HINFT Data Communication Business Group, TW', 'Domain: [redacted]', 'Route: [redacted]', and 'Company: Chunghwa Telecom Co.,Ltd.'. Additionally, it shows RDAP information: 'Name: HINET Network-Adm', 'Role: administrative, technical', and 'Email: network-adm@hinet.net'. A 'Screenshot' of a web page is also visible. It shows 'Last Seen' and 'First Seen' timestamps as '2024-07-18 18:32:05' and '2024-06-28 14:15:29' respectively.

# 持續監測外部曝險事件

The screenshot displays the XCOCKPIT EASM (External Asset Monitoring) interface. At the top, navigation tabs include Dashboard, EASM, and Reports. The main section is titled 'EASM' and contains sub-tabs for Assets, Graph, and Mitigation Plans. A summary bar shows counts for Domain (2), IP Address (21), and Account (8). Below this is a table with columns for Risk, Asset, Type, Information, Last Seen, Status, and Tags. A yellow callout box highlights the Risk column, stating: '根據相關聯事件嚴重程度分類標示數位資產風險程度，加速資安人員了解資產概況。' (Classify digital asset risk levels based on the severity of related events to accelerate security personnel's understanding of asset status.)

Below the main table, a section titled '172.217.175.228 - Events 44' shows a list of events. A yellow callout box highlights the Severity column, stating: '根據嚴重程度分類外部曝險事件' (Classify external exposure events based on severity). The event list includes details such as time, category (e.g., Certification Health, Website Security), description, and network type.

Risk	Asset	Type	Information	Last Seen	Status	Tags
High	172.217.175.228	IP		2024-07-17 10:48:58	Public	...
High	172.217.175.228	IP		2024-07-17 10:48:57	Public	...
High	172.217.175.228	IP		2024-07-17 10:48:57	Public	...
High	172.217.175.228	IP		2024-07-17 10:48:57	Public	...
High	172.217.175.228	IP		2024-07-17 10:48:58	Public	...
High	172.217.175.228	IP		2024-07-17 10:48:58	Public	...
High	172.217.175.228	IP		2024-07-17 10:48:58	Public	...

Severity	Time	Category	Description	Network	Time	Source	Tags
9	2024-07-10 11:12:08	Certification Health	Chain of certificate trust failed	Network	2024-07-10 11:12:08	AI-Created_20240710_0312	...
9	2024-07-10 17:55:34	Website Security	HTTP response header is ignored	Network	2024-07-10 17:55:34	AI-Created_20240710_0955	...
9	2024-07-12 11:36:55	Certification Health	Chain of certificate trust failed	Network	2024-07-10 11:12:08	AI-Created_20240710_0312	...
9	2024-07-12 11:36:56	Website Security	HTTP response header is ignored	Network	2024-07-10 17:55:34	AI-Created_20240710_0955	...
9	2024-07-12 11:36:59	Website Security	HTTP response header is ignored	Network	2024-07-10 17:55:34	AI-Created_20240710_0955	...
9	2024-07-12 11:37:01	Website Security	HTTP response header is ignored	Network	2024-07-10 17:55:34	AI-Created_20240710_0955	...
9	2024-07-12 11:37:02	Website Security	HTTP response header is ignored	Network	2024-07-10 17:55:34	AI-Created_20240710_0955	...
9	2024-07-13 13:17:31	Certification Health	Chain of certificate trust failed	Network	2024-07-10 11:12:08	AI-Created_20240710_0312	...
9	2024-07-13 13:17:32	Website Security	HTTP response header is ignored	Network	2024-07-10 17:55:34	AI-Created_20240710_0955	...
9	2024-07-15 17:48:17	Website Security	HTTP response header is ignored	Network	2024-07-10 17:55:34	AI-Created_20240710_0955	...
9	2024-07-16 11:54:54	Website Security	HTTP response header is ignored	Network	2024-07-10 17:55:34	AI-Created_20240710_0955	...
9	2024-07-17 10:40:58	Website Security	HTTP response header is ignored	Network	2024-07-10 17:55:34	AI-Created_20240710_0955	...
5	2024-07-13 13:17:50	SSL / TLS Strength	Obsolete CBC ciphers	Network	-	-	...
5	2024-07-10 11:12:08	Website Security	HTTP response headers vulnerable to fingerprinting	Network	-	-	...
5	2024-07-12 11:36:55	Website Security	HTTP response headers vulnerable to fingerprinting	Network	-	-	...
5	2024-07-12 11:36:59	Website Security	HTTP response headers vulnerable to fingerprinting	Network	-	-	...
5	2024-07-12 11:37:04	Website Security	HTTP response headers vulnerable to fingerprinting	Network	-	-	...

# 盤點外部曝險事件列表

Type	Description	Category
Compromised Credential	偵測從駭客論壇和暗網市場中被偷走的用戶名、密碼和其他敏感數據，這些數據可用於未經授權的存取。	User
Darkweb Auction	識別在暗網上提到的組織訊息，可能揭露洩露的憑證、與網絡攻擊的關聯或涉及非法活動。	User
Compromised Endpoint	偵測來自駭客論壇和暗網市場的惡意軟體感染、被攻擊的端點和其他攻擊跡象。	Device
Network Security	網路通訊問題，例如同伺服器不支援 DNS over TLS/HTTPS。	Network
DNS Security	突顯未受 DNSSEC 保護或已過時的 DNS 記錄（如 SPF 和 DMARC）。	Network
Similar Domain	近似域名偵測	Network
Misconfiguration	識別可通過調整配置修復的問題，例如不安全的預設設定、使用非建議的 bucket policy 或權限設定。	Network
Certificate Health	涵蓋憑證問題，包括弱簽名算法、不當密鑰大小、錯誤使用、缺少 SAN 和過期問題。	Network

# 盤點外部曝險事件列表 (續)

Type	Description	Category
DNS Health	包括錯誤的 CNAME 和 SOA 記錄，以及使用過時的 DNS 記錄類型。	Network
Email Security	電子郵件安全檢查包括配置不符合最佳實踐的問題，例如缺少/無效的 SPF、DMARC 和 MTA-STS 記錄，錯誤的 MTA-STS 設定，SMTP 用戶名枚舉，SMTP 開放中繼，以及多個 SPF、DMARC 或 MTA-STS 記錄。	Network
Website Security	網站安全問題包括目錄列表、缺少安全標頭、易受攻擊的標頭、Cookie 問題，以及各種 Web 應用程式漏洞，如 SSRF、XSS 和 SQL 注入。	Application
SSL/TLS Strength	SSL/TLS 強度包括過時且不安全的密碼套件、缺乏安全重協商以及 TLS 協議漏洞。	Network
Patch Management	網頁應用程式弱點檢查，包括像 OpenSSL 和 Apache Tomcat 等軟體中的漏洞，如不立即修補，可能會導致 RCE、LFI 和 SSRF 攻擊。	Application
IP Domain Reputation	公司數位資產 IP Domain 信譽狀況偵測	Network

# 外部曝險事件細部資訊

The screenshot displays the XCOCKPIT EASM interface with three event detail panels highlighted in yellow:

- Compromised Endpoint (Event #9):** Occurred on 2024-07-11 at 16:17:11. The endpoint was compromised. Details include: Event Time: 2024-06-27 00:00:00; Account: jack; Impacted Domain: supply; Hostname: JA-H; IP: 111; Category: Device; Source: Initial Access Broke's Log; Information: Country: TW, OS: Windows 10 Home, Malware: C:\Windows\SysWOW64\explorer.exe; Related Assets: supply, ja@gmail.com; Description: The credentials in the compromised endpoint can be used to access other assets; References: CWE-200, CWE-522, CWE-1392, CWE-789, CAPEC-580, CAPEC-600, CAPEC-653, CAPEC-655, CAPEC-21; Mitigation: Immediately isolate the compromised endpoint from the network to prevent further unauthorized access. Change all passwords and credentials associated with the compromised endpoint and any other assets that may have been accessed. Conduct a thorough investigation to determine the extent of the compromise and identify any other potential vulnerabilities. Implement multi-factor authentication to add an extra layer of security to prevent unauthorized access even if credentials are compromised. Educate users on best practices for securing credentials and regularly update security protocols to prevent similar incidents in the future.
- SSL / TLS Strength (Event #6):** Occurred on 2024-07-17 at 10:43:48. Category: Network. Description: The use of obsolete CBC (Cipher Block Chaining) ciphers in encryption protocols poses a significant security risk. These ciphers are vulnerable to attacks such as padding oracle attacks and are no longer considered secure for modern cryptographic standards. The continued use of obsolete CBC ciphers can lead to data breaches and unauthorized access to sensitive information. References: https://roberttheon.com/2013/07/29/padding-oracle-attack/, https://www.iacr.org/archive/eurocrypt2002/23320530/cbc02\_e02d.pdf, CWE-327, CWE-328, CAPEC-463, CAPEC-217, CAPEC-97.
- Patch Management (Event #1):** Occurred on 2024-07-13 at 13:17:50. Category: Network. Description: SWEET32 is a vulnerability that affects 64-bit block ciphers, such as Triple-DES and Blowfish. It allows attackers to perform birthday attacks, which can lead to the recovery of plaintext data from encrypted traffic. This vulnerability poses a significant threat to systems that use 64-bit block ciphers for encryption. References: https://nvd.nist.gov/vuln/detail/CVE-2016-2183, https://nvd.nist.gov/vuln/detail/CVE-2016-6329, https://sweet32.info/, CVE-2016-2183, CVE-2016-6329, CWE-327, CWE-328, CAPEC-463, CAPEC-217, CAPEC-97.

點選單一事件可查看外部曝險事件細部資訊，如相關暗網外洩帳號、被攻擊端點資訊、或是建議緩解措施等

# 數位資產調查概況總覽與工作指標



# 報告下載

## Reports

Report Type EASM

Generated Date YYYY-MM-DD

• 報表可自訂時間區間產出並直接下載 EASM 外部資產曝險管理報告

Generate

Completed Only

Status	Generated Time	Report Date	Type	Report Name	Endpoint	Report ID	Creator	Locale	...
✓				global.com_EASM-Report...	-	4515f64ca7464ea0...	john	ZH-TW	📄 ⬇
✓				global.com_EASM-Report...	-	6475d60b1b344386...	puppy	ZH-TW	📄 ⬇
✓				ediatek.com_EASM-Report...	-	082e8d7398e64b15...	eileen	EN	📄 ⬇

**Dem**  
XCockpit EASM 外部資產曝險管理報告

Report ID: 6475D60B1B344386FA6CE382B95F4C8  
2024-07-15 14:20:00

PROPRIETARY AND CONFIDENTIAL INFORMATION

### 域名資訊

報告摘要: demo

域名	demo.com
報告生成時間	2024-07-15 14:20:00 (Asia/Taipei)
資料範圍	2024-07-01 00:00:00 ~ 2024-07-15 14:20:00 (14 天)
外部資產排除安全分數	0 / 100
MTTR	0
資產總數	62
IP 資產 (私有/公開)	0/5
域名資產 (私有/公開)	6/8
帳戶資產	35
有風險的資產	62 / 62
未處理的資產	61
已處理的資產	1

資產風險層級 (62)

Category	Normal	Watched	High	Urgent High
IP	0	0	5	0
Domain	0	0	6	2
Account	0	0	35	0

已處理的資產	1
未處理的資產	61
公開資產數量變動	0
私有資產數量變動	0
企業安全分數	0

### 目錄

1. 域名資訊
2. 資產摘要
3. AI 分析師摘要
4. 風險分層
5. 附錄
  - 未處理風險資產
  - 已處理風險資產

COUNT 3

PAGE 1 OF 1

20 Rows



# Shifting Security with AI

整個世界正在全面加速轉變！  
奧義智慧協資安團隊掌握最新 AI 科技脈動，  
讓工作轉型、團隊升級。

