CYCRAFT
奧義智慧科技

2022/06/24
林高裕 Gary Lin

善用資安情資，強化校園資安防護策略

2022/06/24 林高裕 Gary Lin

Gary Lin

gary.lin@cycarrier.com

奧義智慧科技

經歷：

現任於奧義智慧 專案管理辦公室 主任

臺灣科技大學 資訊工程所 博士班

台灣網際空間與安全策略發展協會 理事

曾任職 財團法人電信技術中心 資通安全組 主任

曾擔任 國家級資安聯防計畫 負責人

5G資通安全維護計畫 負責人

專長：

資安聯防策略

資安情資及資通訊應用

誘捕欺敵戰術

Subjects

01 什麼是情資

02 情資的策略

03 應用分享

Subjects

01 什麼是情資

02 情資的策略

03 應用分享

什麼是情資

X = Intelligence
Y = Information
Z = Critical Assets, Business Flow, Supply Chain

① $X \equiv Y$　② $X \cong Y$　③ $X \neq Y$　?

$$X = Y \forall Z$$

情資，其實比你我想像的更有價值

什麼是情資

新聞

> 首

鴻

漏

據Secu
擊，這

文/ 林

F5
許
並

內容

研究

過iC

360 萬台以上 MySQL 伺服器，曝露於 Internet 上

發布日期：2022-06-02

字型大小： 小 中 大

發布單位:TWCERT/CC　　更新日期:2022-06-02　　點閱次數:199

資安研究團體 The Shadowserver Foundation 日前發表研究報告，指出全世界有 360 萬台以上的 MySQL 伺服器，未經適當防護而在 Internet 上曝露，且可接受各種指令進行操作，因而成為駭侵者的最佳攻擊目標。

調查顯示全球網路約有 360 萬台 MySQL server 於 Internet 上曝露，且使用 MySQL 預設的通訊埠 TCP 3306。這些為數眾多的 MySQL 伺服器，有約 230 萬台使用 IPV4，其餘 130 萬台使用 IPV6 連線。

報告也指出，若以曝露數量來排序，美國境內曝露於 Internet 上的 MySQL server 數量最多，有超過 120 萬台以上，其餘國家則包括中國、德國、新加坡、荷蘭、波蘭等。

報告也指出，除了這些確定曝露在 Internet 上，可能遭到攻擊的 MySQL server 外，也有一些具備部分防護，不會對掃瞄用的 TLS / 非 TLS 於 port 3306 上的連線要求提供回應的 MySQL server；但在所有偵測到的 MySQL server 中，高達 67% 都可以直接透過 Internet 存取；這是十分危險的，因為駭侵者將能輕鬆駭入這些幾乎不設防的 MySQL server 中，進行資料竊取或其他進階攻擊。

定義情資 – 情資的類型

- 戰略型情資 (Strategic Intelligence)
  - 是一種High-Level的情資，用來識別情資對組織或對產業所造成的衝擊及影響。通常是一種分析報告、白皮書，且能針對領域及威脅趨勢提出見解。
- 維運型情資 (Operational Intelligence)
  - 持續蒐集，用以進行短中期的趨勢、風險量化、相關績效等分析，提供資安維運檢討之參考。
- 戰術與技術型情資 (Tactical or Technical Intelligence)
  - 其目的用來參與保護數據資源，這類情資它提供了有關如何根據所使用的方法以及防禦或緩解攻擊的最佳實踐，進而掌握攻擊組織的詳細信息。其中技術型情資主要是用來在防禦面發揮起功效。

Ref: I. Alsmadi, “Cyber intelligence,” in The NICE Cyber Security Framework: Cyber Security Intelligence and Analytics, Springer, Berlin, Germay, 2019.

定義情資 - 情資涵蓋的範圍與面向

企業資產的情資角度
Attack Surface

員工身份識別
Attack Surface

攻擊者的
情資角度
Attack Surface

供應商的情資角度
Attack Surface

不同類型的情資需要被關注與管理

CyCraft Proprietary and Confidential Information

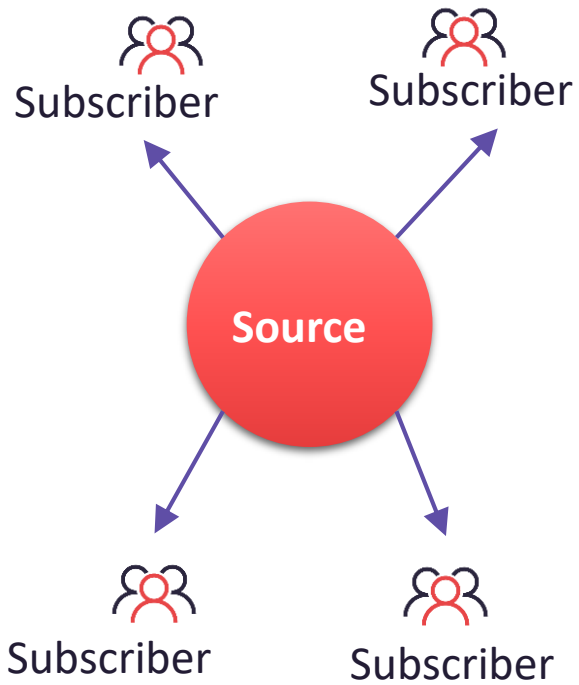
自動化情資交換

- 目的：標準的建立有助於機器/系統讀取和自動化分享
- Managed Incident Lightweight Exchange (MILE)
  - Incident Object Description and Exchange Format (IODEF ）
    早期N-ISAC主要情資交換格式
  - Real-time Inter-network Defense (RID)
- United States Department of Homeland Security (DHS) 支持MITRE
  - **STIX**：情資的描述、**TAXII**：情資的傳輸 (HTTPS)、**CybOX**：詞彙的規範
    - ✓ STIX 1.X，採用XML的資料格式、STIX 2.X，載用JSON的資料格式
    - ✓ TAXII, **T**rusted **A**utomated e**X**change of **I**ndicator **I**nformation
  - N-ISAC 以版本2.1的格式納入聯防情資交換標準

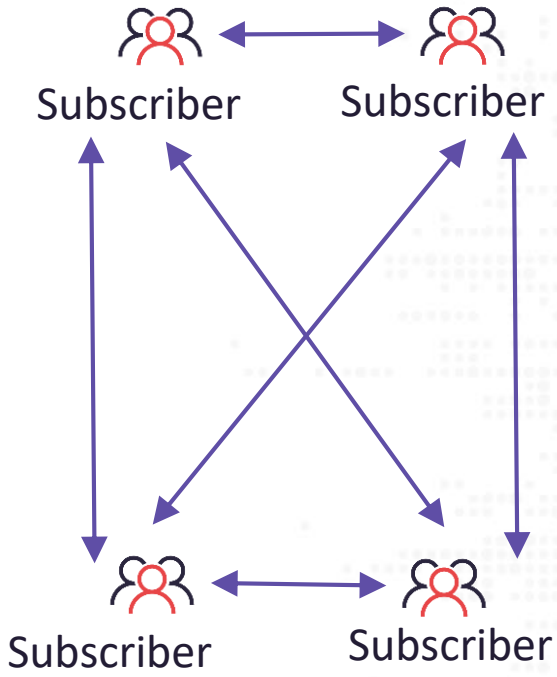
自動化情資交換

- 情資交換模型：　（N-ISAC採用哪種架構？）

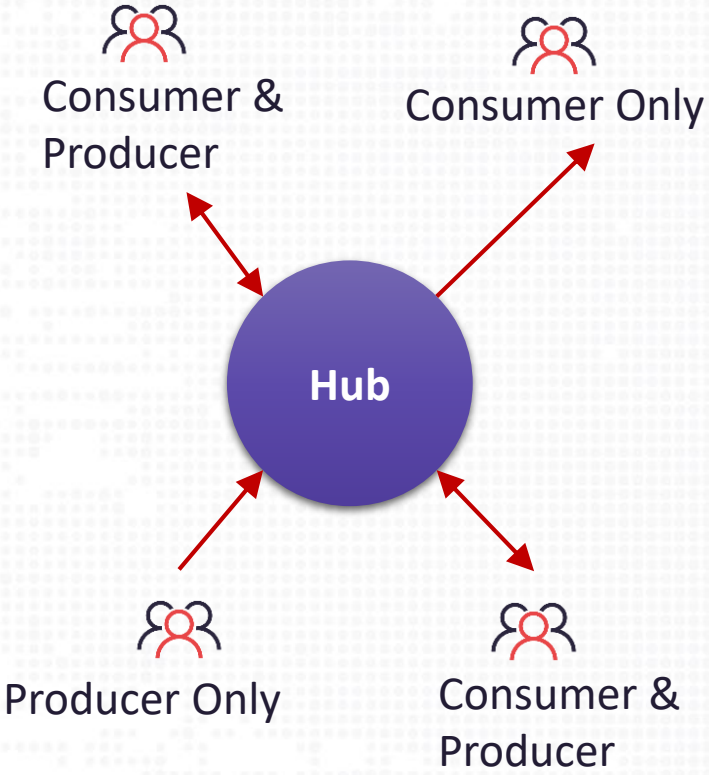
Source and Subscriber



Peer to Peer



Hub and Spoke



Subjects

01

什麼是情資

02

情資的策略

03

應用分享

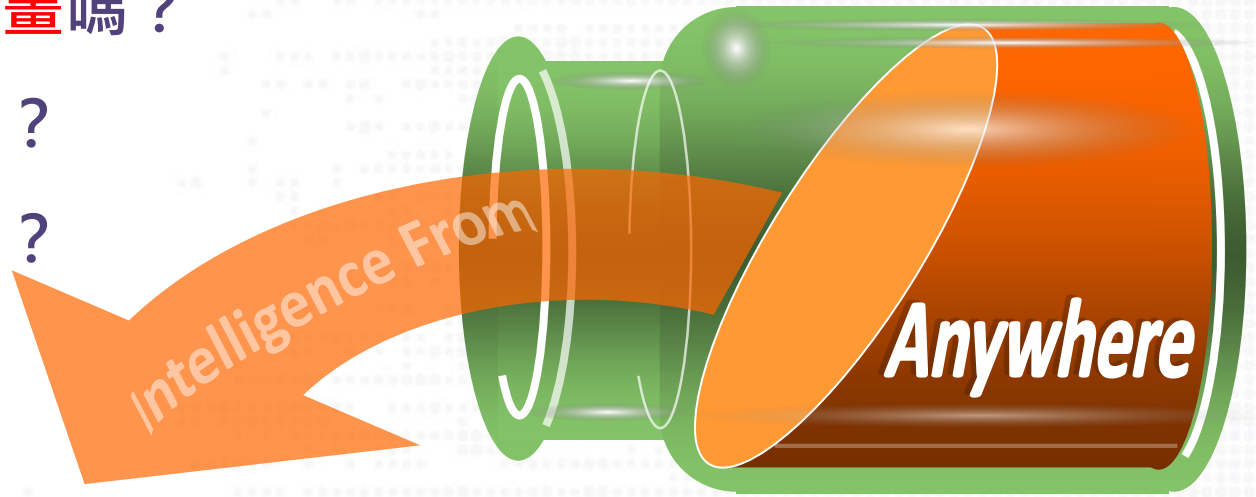
取得情資前，請先自我檢視

你知道你會拿到的是蛋白？還是蛋黃？

你有制訂情資相關策略與制訂計畫嗎？

你知道情資有效期限需要被管理？

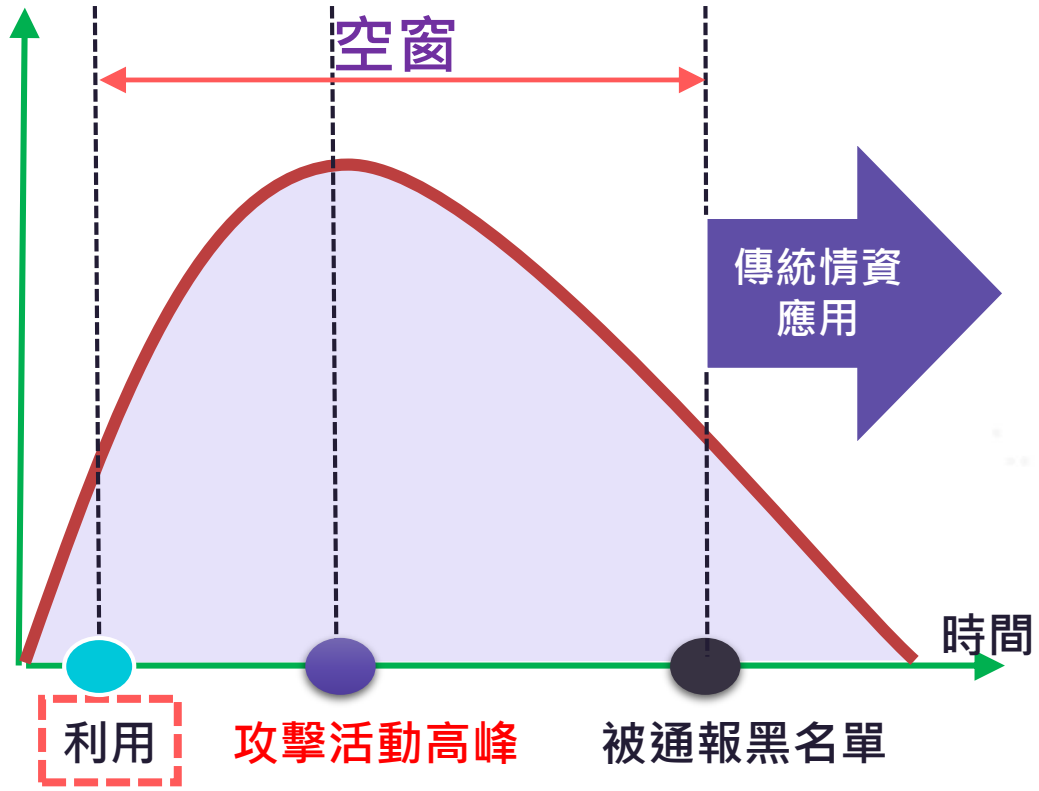
你真的知道你拿到情資的用途嗎？



取得情資時，先確認有效性

43%新註冊域名具有惡意意圖

奧義智慧獨家技術及時掌握全球域名動態



> 仰賴黑名單的侷限性

- → 缺乏攻擊地區的針對性
- → 依賴黑名單將會低估資安風險

黑名單，即將過期？特定區域有效？

> 當威脅情資遇到網路詐騙

- → 惡意域名 具備仿真 跟 自動化建立
- → 根據CYREN，惡意網址**列入黑名單後**

20% 3hr 消失、50% 24hr 消失

- → 快速域名替換，可以繞過黑名單

天下武功 唯快不破 ~ 金庸

Ref: https://www.cyren.com/campaigns/phishing-emea

情資蒐集三層次

Ref: SANS FOR508

1. 在整個組織範圍內的規模進行蒐集與分析。明確定義欲分析的資料蒐集範圍。
2. 具目標且針對性的數據蒐集，進一步驗證及發現，並開採出對應威脅情資
3. 對影響的系統以及惡意程式進行深入分析，進一步識別關聯性並構建IoC

情資策略三構面

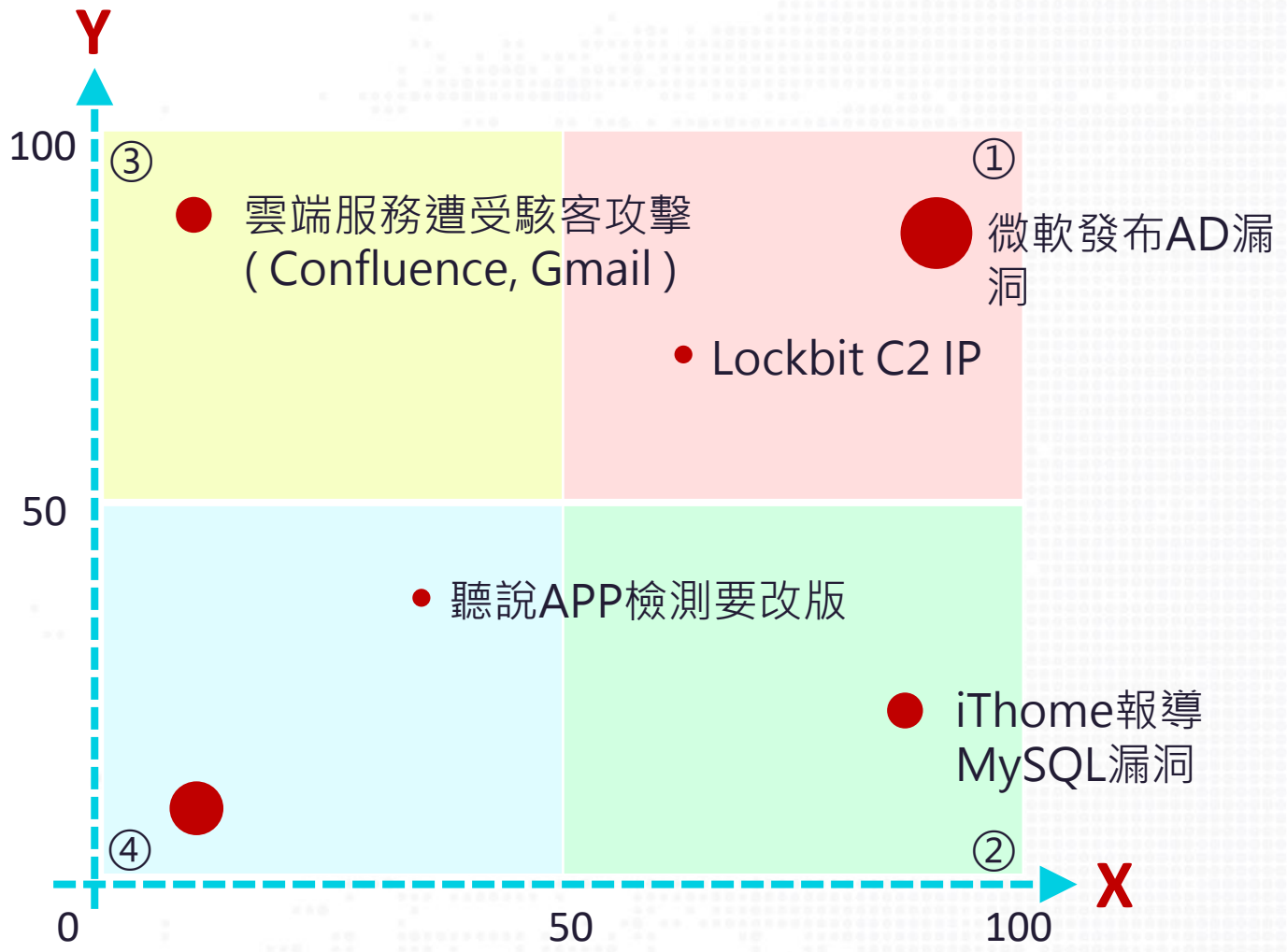
- 訂定情資相關計畫
  - 蒐集來源及方式
  - 情資取得頻率
  - 衝擊應變評估
- 明訂核心業務流程
- 規劃情資部署步驟
- 制訂關鍵資訊資產盤點計畫

- 資訊資產盤點
- 影響風險評估
- 衝擊因應及應變
- 採購預算編列
  - CTI情資平台
  - 商用黑名單
  - 專家分析報告
- 更新部署Checklist
- 授權分工R&R
- 驗證情資生命週期

- 情資更新自動化
- 情資平台IoC調查
- 暗網情資調查分析
- 其他因應計畫實施所需的CTI工具、裝置

情資框架四象限

- 參數
  - 資產重要性：**X**
  - 業務/流程影響：**Y**
  - 取得來源可靠度：●
- 處置方式(供參考)
  - ① 積極處理
  - ② 備案規劃（備份計畫）
  - ③ 謹慎實施（測試計畫）
  - ④ 瞭解與評估（研究分析）



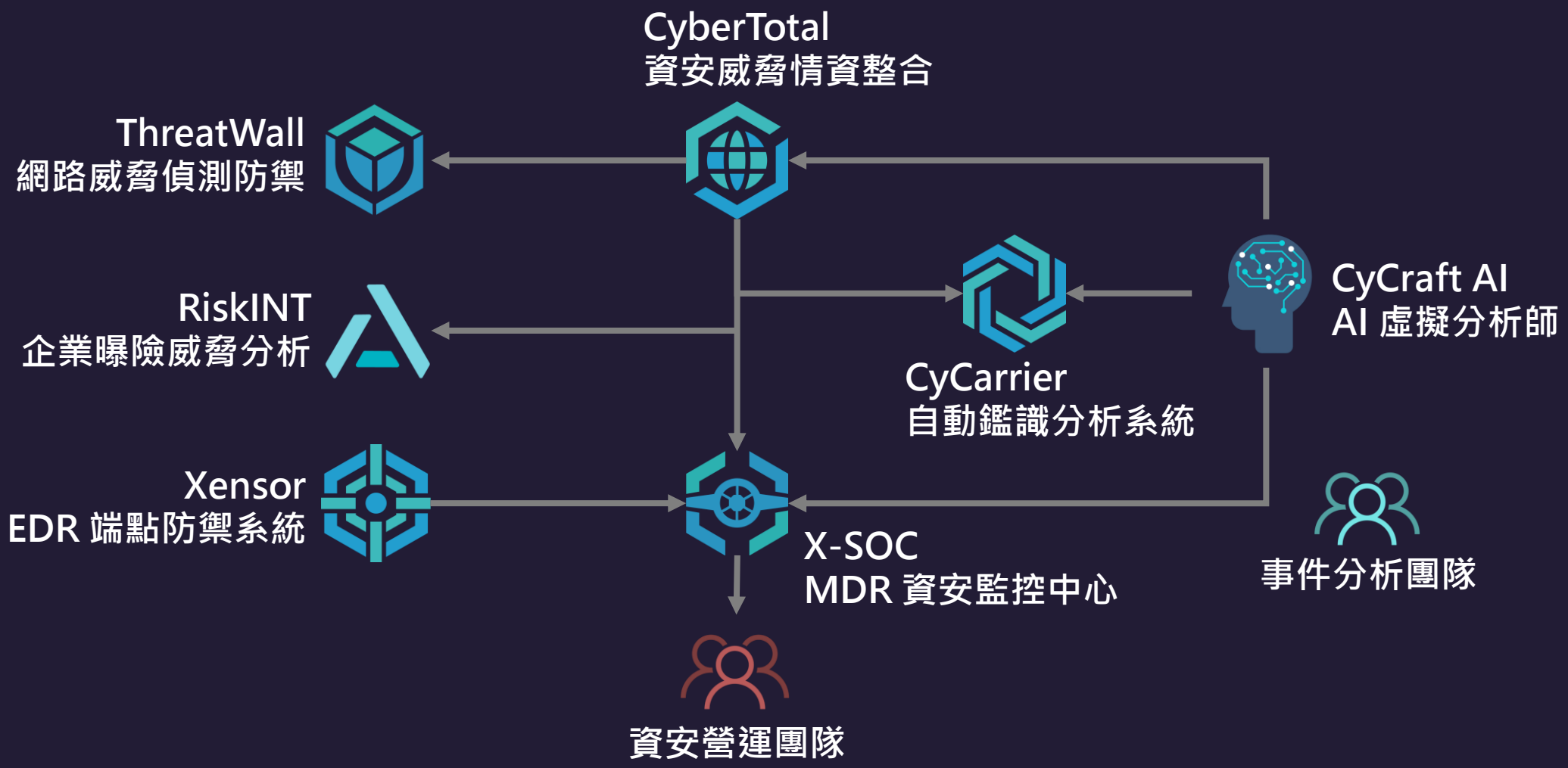
Subjects

01 什麼是情資

02 情資的策略

03 應用分享

奧義智慧 提供全面 AI 資安防護 –
EDR 端點防護、MDR 勢態感知、TIG 閘道防護、TIP 全球威脅情資



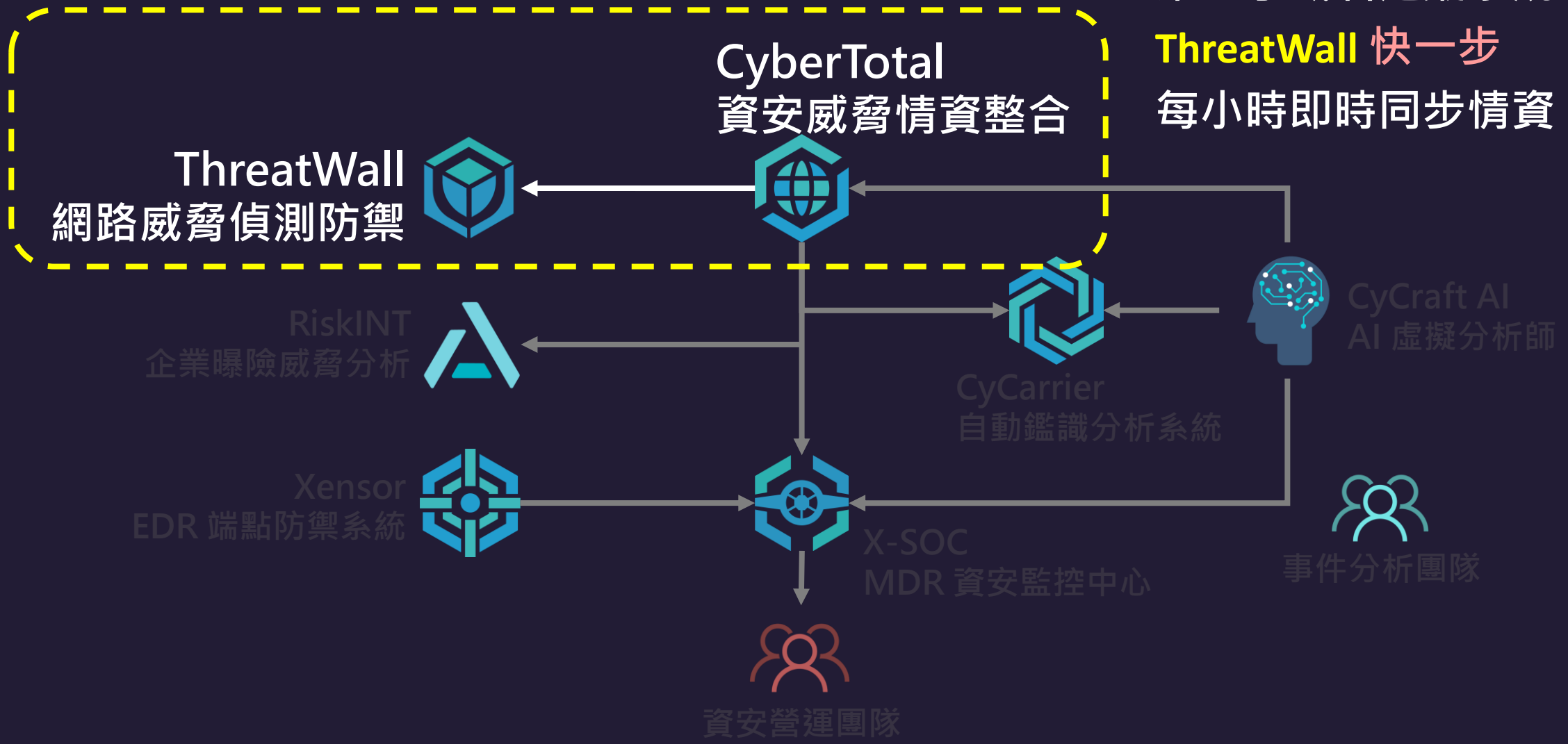
CyCraft Proprietary and Confidential Information

CyberTotal 早一步

第一手域名追蹤系統

ThreatWall 快一步

每小時即時同步情資



CyCraft Proprietary and Confidential Information

一直收到「防疫補助」詐騙訊息？王必勝曝「5大釣魚連結」千萬別點

新頭殼newtalk | 張閔雅 綜合報導

發布 2022.08.31 | 15:54

留言

中央流行疫情指揮中心指揮官王必勝。　圖：中央流行疫情指揮中心 / 提供

CyCraft Proprietary and Conf

善用情資，建立主動防禦機制

> 如何透過情資進一步強化資安防禦？

→ 應用情境1：從威脅獵捕到擴大部署

根據情資線頭，如何驗證情資與掌握關聯性，進而擴大部署

→ 應用情境2：掌握已發現的攻擊活動

延續前面的調查，知道誰在試圖攻擊你，持續關注動態

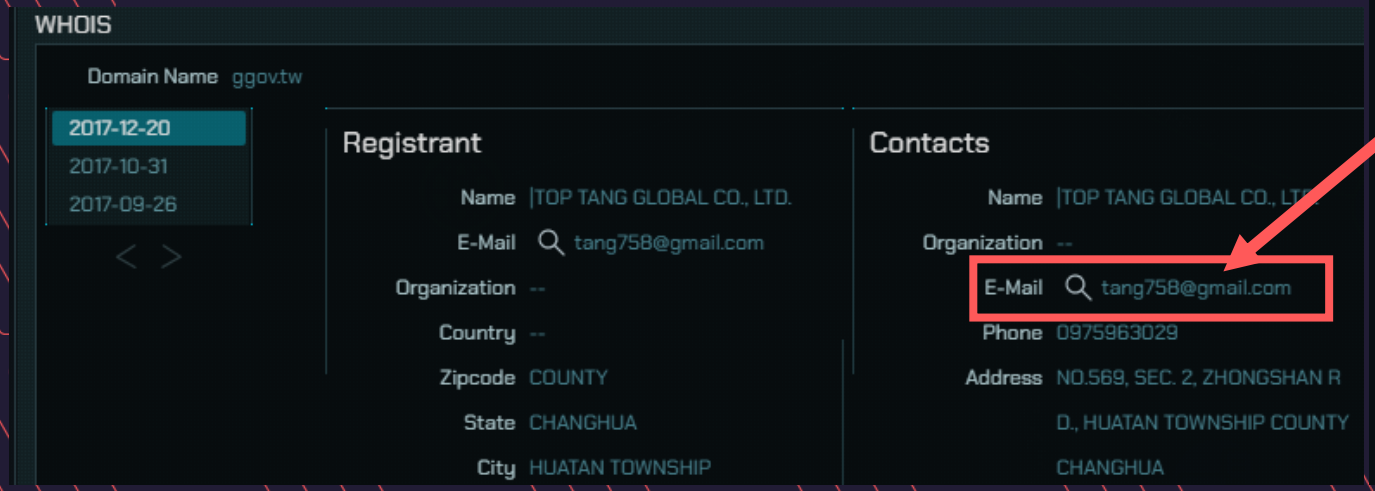
CyCraft Proprietary and Confidential Information

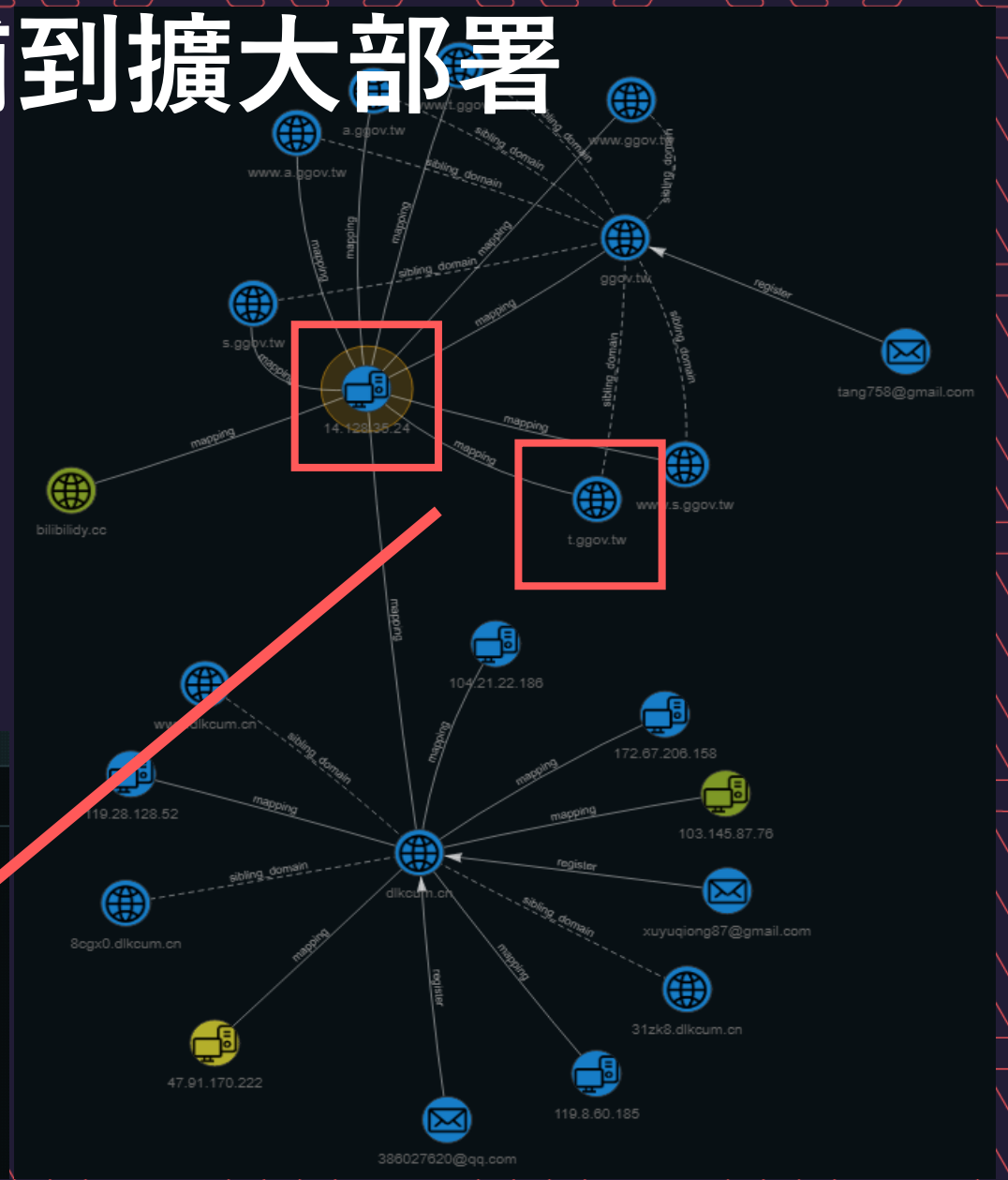
應用情境1 - 從威脅獵捕到擴大部署

CYCRAFT

應用情境1 - 從威脅獵捕到擴大部署

- 針對可疑偽冒網站進行分析其 IP 14.128.35[.]24，找出誰註冊偽冒網站
- 查找任一 Domain 的 whois 資訊，找到註冊的信箱 tang758@gmail.com
  - 該信箱於 2017 年就已註冊該IP對應的 Domain 域名

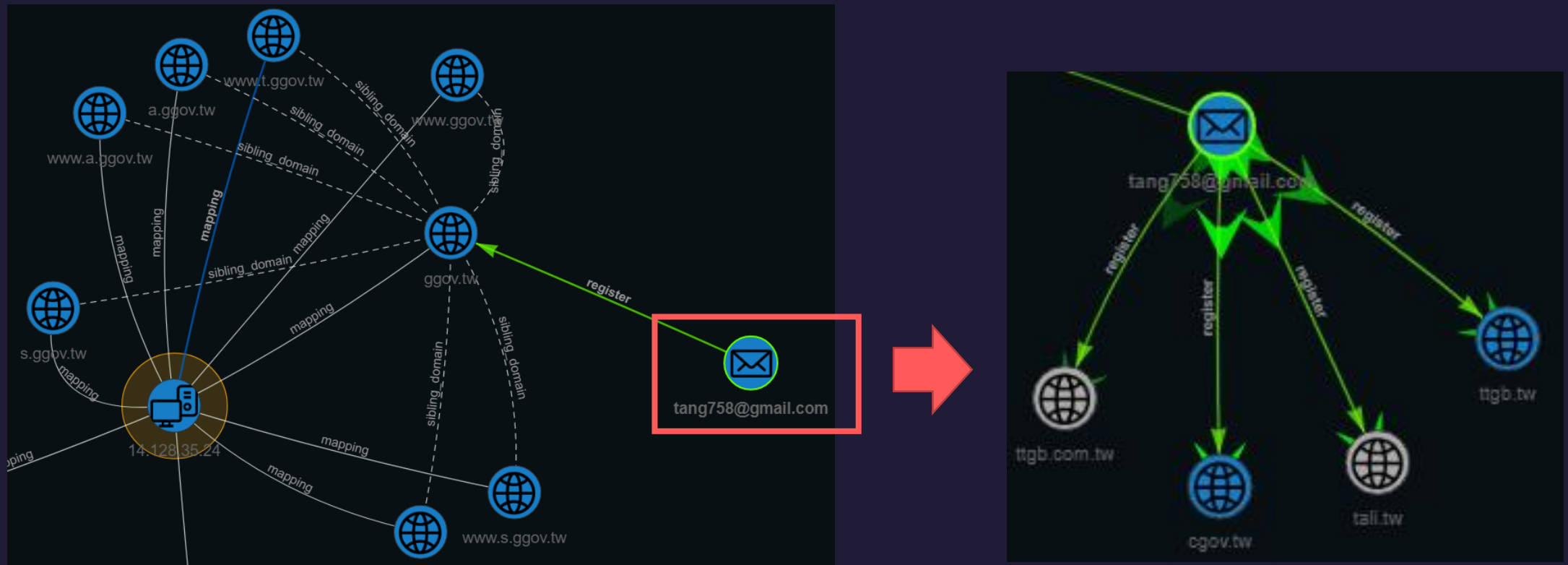




應用情境1 - 從威脅獵捕到擴大部署

CYCRAFT

- 將信箱 tang758@gmail.com 展開調查更多情資，發現駭客使用該信箱註冊了更多偽冒網站。奧義智慧獨家技術 掌握全球域名註冊動態

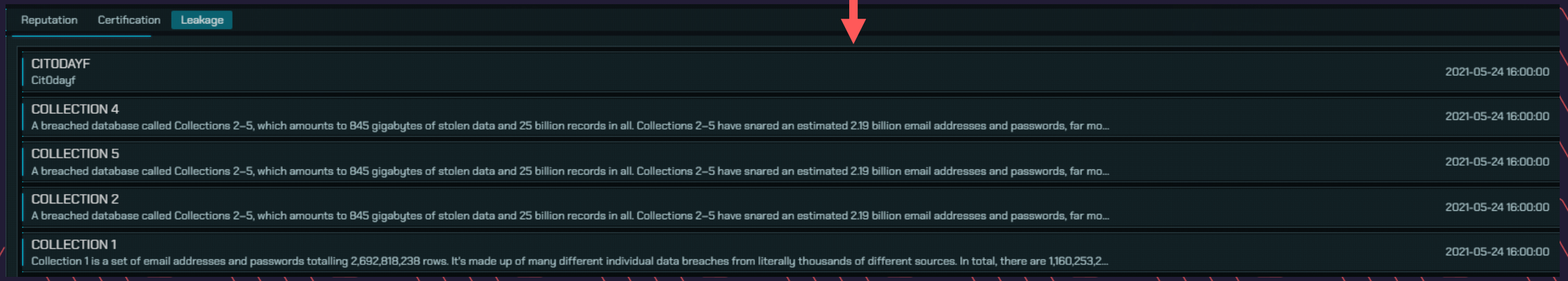


應用情境1 - 從威脅獵捕到擴大部署

CYCRAFT

- 查詢註冊偽冒網站的信箱 tang758@gmail.com 相關情資，發現該信箱曾經有經歷帳密外洩事件。

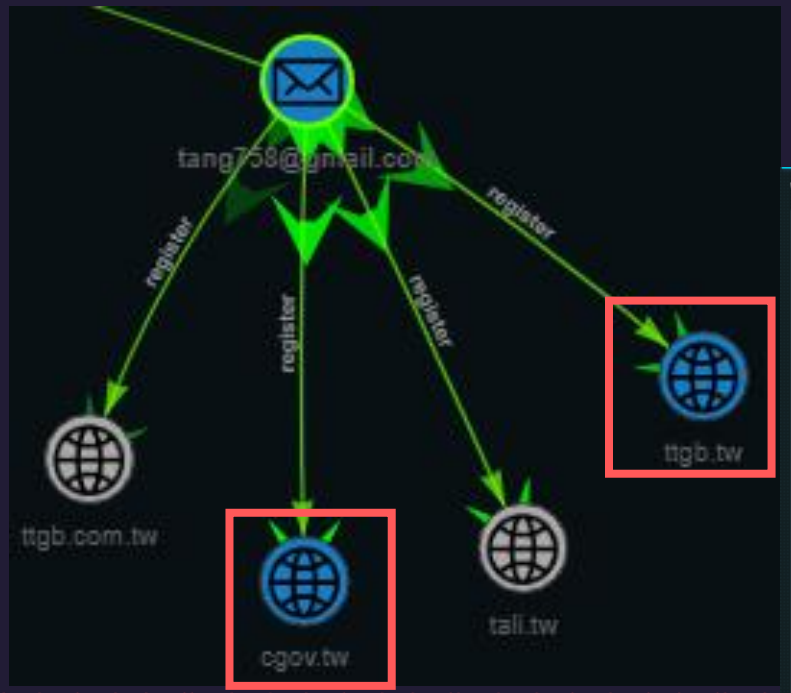
如果是單純透過 Whois 及開源情資獲得的資訊，你只會得到低風險的資訊而忽略其重要性。奧義智慧給你更多

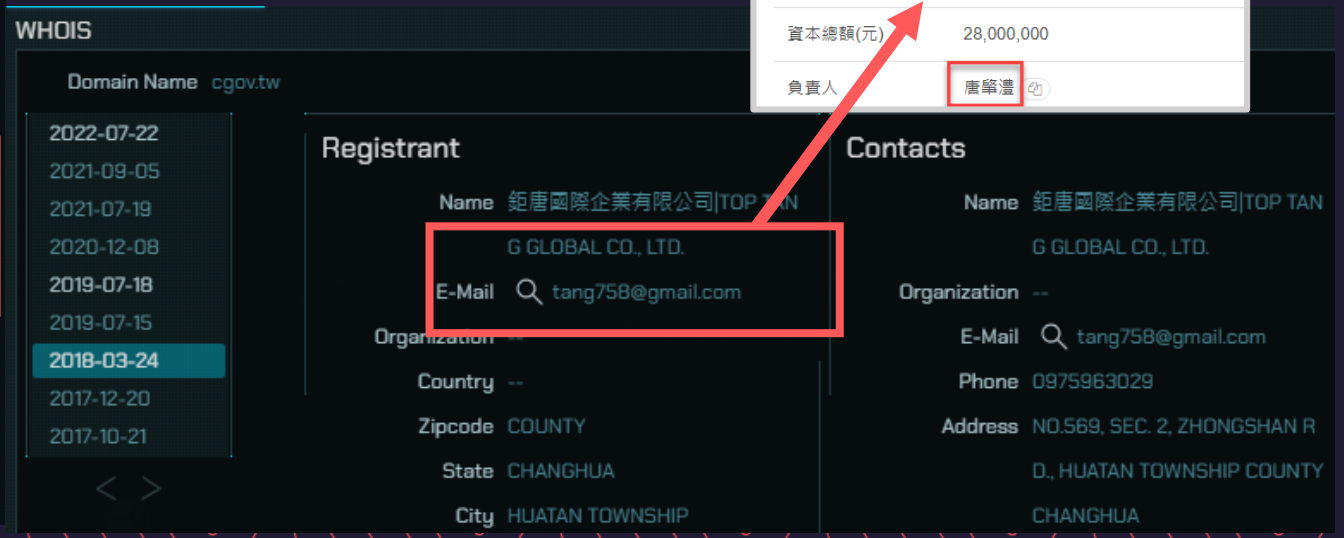


應用情境1 - 從威脅獵捕到擴大部署

CYCRAFT

- 透過調查 tang758@gmail.com 擴展開的情資，包含從釣魚域名 cgov[.]tw 的 whois 資料交叉比對，找到該信箱的聯絡人所屬公司
  - 透過9組 Seed 以及受駭信箱，調查出超過200個有問題的域名
  - 藉由調查結果，擴大部署資安防護措施





應用情境1 - 從威脅獵捕到擴大部署

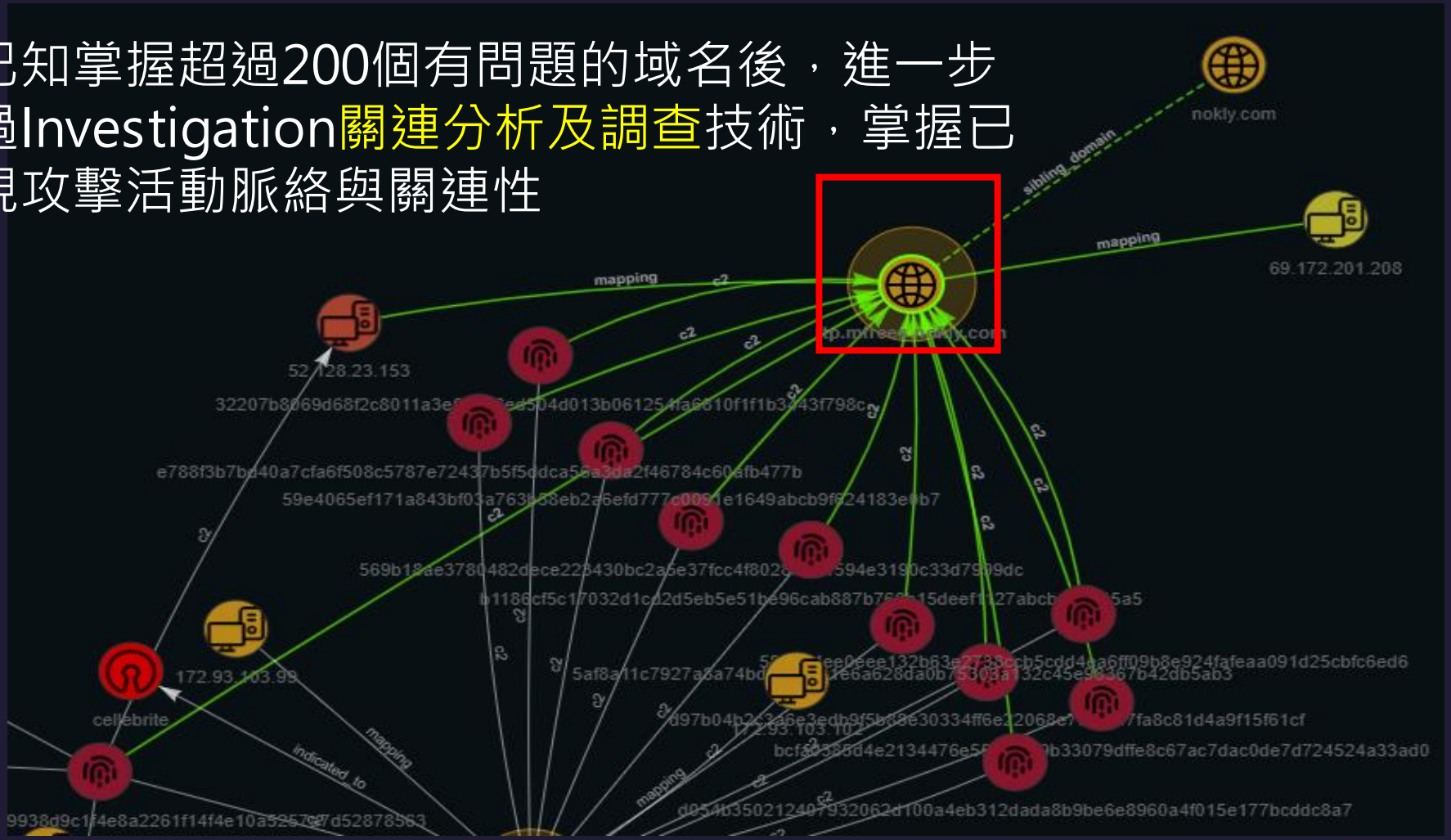
CYCRAFT

你可以透過奧義智慧ThreatWall (TIG) 網路資安防護措施，即時偵測高頻率或高風險的攻擊來源 。

應用情境2 - 掌握已發現的攻擊活動

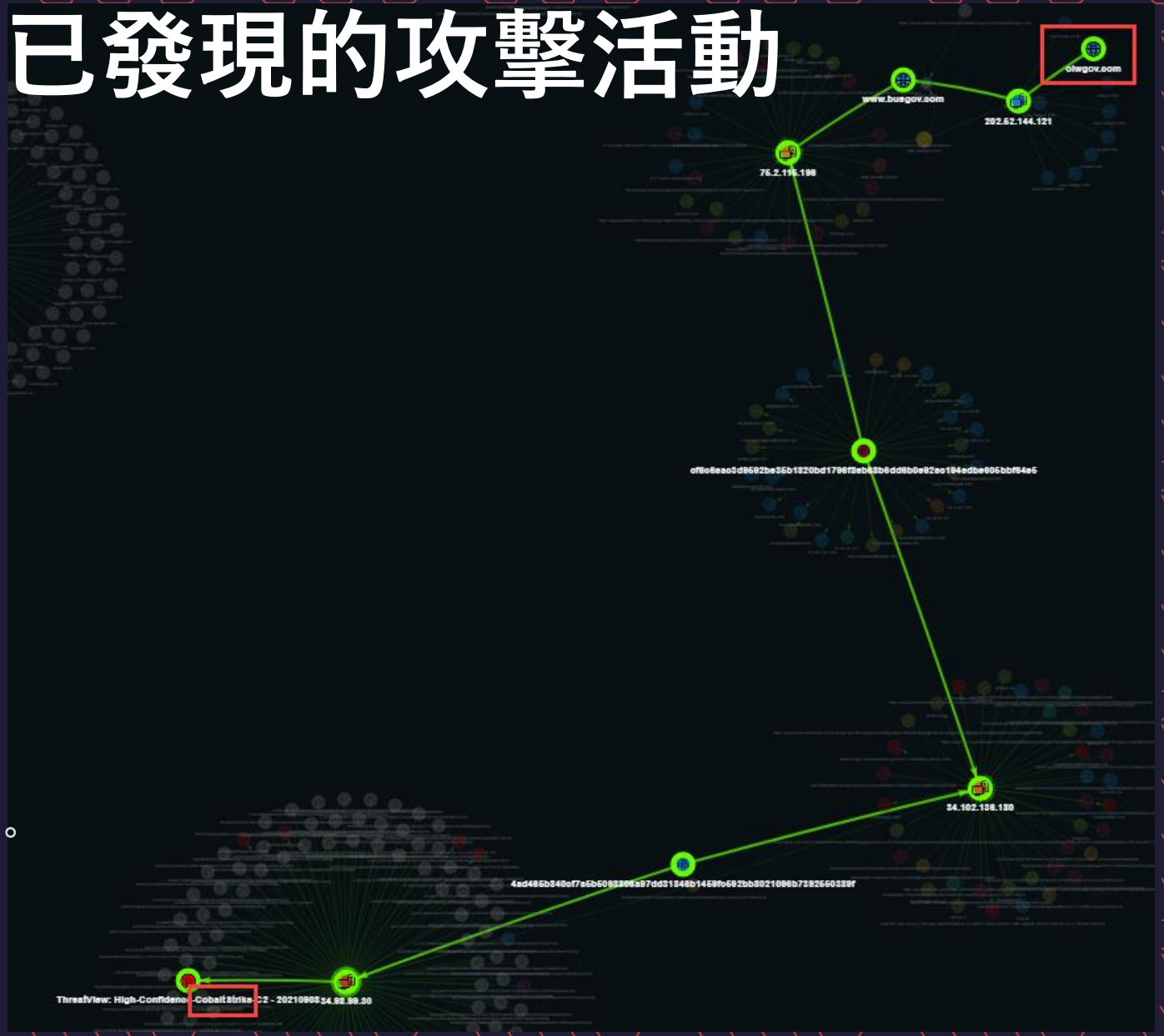
CYCRAFT

- 在已知掌握超過200個有問題的域名後，進一步透過Investigation關連分析及調查技術，掌握已發現攻擊活動脈絡與關連性



應用情境2 - 掌握已發現的攻擊活動

- 透過奧義智慧**獨家 AI 分析技術**，建立攻擊脈絡 。
- 藉由線頭的掌握進而發現 Cobalt Strike 攻擊軌跡。(Winnti)
- 部分Fake Domain 其IP所在位置在香港，且偽冒釣魚網站出現簡體中文字。
- 推斷近期一波**防疫補助釣魚**疑似來自特定地區攻擊事件。



善用資安情資 - 主動防禦零時差攻擊

- 情資排序 分析對企業的影響
- 情資驗證 融入資安意識訓練
- 關連分析 擴大掌握攻擊的來源
- 持續監控 掌握已知的攻擊威脅

CyCraft Proprietary and Confidential Information

情資平台CyberTotal開放學術單位申請

資安卓越中心規劃建置計畫
Cybersecurity Center of Excellence (CCoE)

CYCRAFT
奧義智慧科技

向窗口提出申請

1. 填寫申請表單: https://reurl.cc/EZ0KLg
2. 開放 CyberTotal - 威脅情資查詢申請服務
3. 提出申請後統一由CCOE進行審查

申請檢附相關資訊

1. 單位(如學校+系所)
2. 姓名
3. 職稱(如教授、研究生)
4. 學校的Email帳號
5. 特殊需求說明
6. 檢附保密切結簽署及學生證或在職證明掃描檔

遞交申請靜候通知

1. 完成申請後，CCOE承辦窗口會回覆您收到申請受理的回信。
2. 受理申請後進入審查作業階段。
3. 審核通過後會主動發送通知信。

CyCraft | Website

CyCraft | Medium

CyCraft | Twitter

Appendix - 常見的情資類型與來源

- 媒體社群 – iThome、資安人、The Record、 BLEEPINGComputer、ZDNet Security、Twitter、Medium
- 漏洞資訊 – NCCST、CVE、資安防護廠商網站公告
- 主題性分群 –
  - 以事件及威脅報告為主： TWCERT/CC、US-CERT、JP-CERT、CSIRT
  - 以情資交流及分享為主：8大關鍵基礎設施ISAC、A-ISAC、NationalISACs
  - 以定期或不定期的分析研究：FIRST、Blackhat、HITB、ICS Cybersecurity Conference
- 專家報告 – CyCraft（選擇標的：高嚴重性、易實作重現、影響範圍廣大）
- 專業平台 – CyberTotal、RiskInt（後面進一步介紹）
- 其他 – Gartner Security and Risk Management Summit、Top 30 cybersecurity conferences of 2022