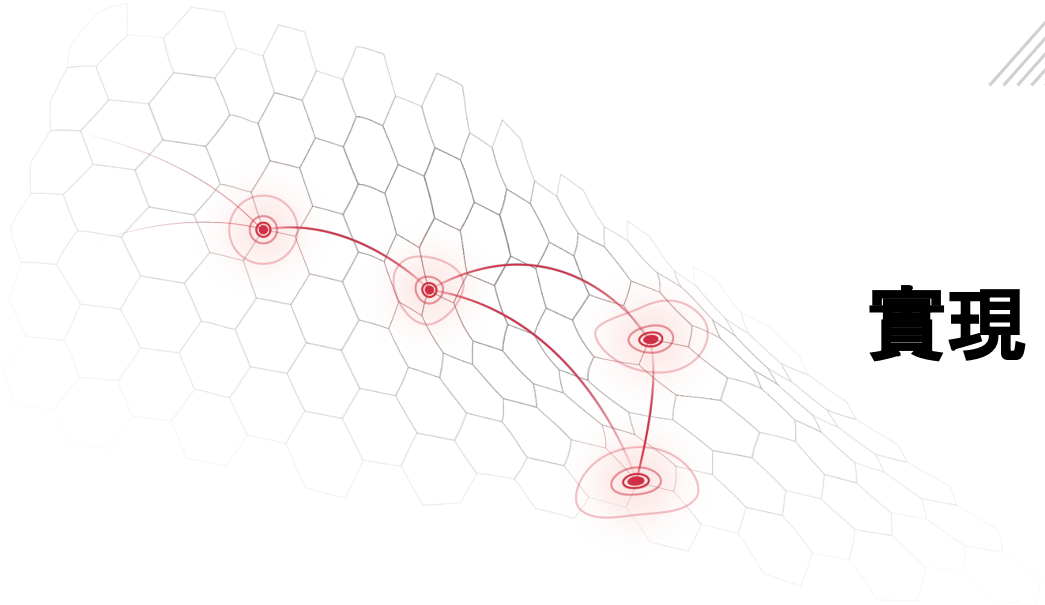
整合式威脅情報平台與攻擊面可視化



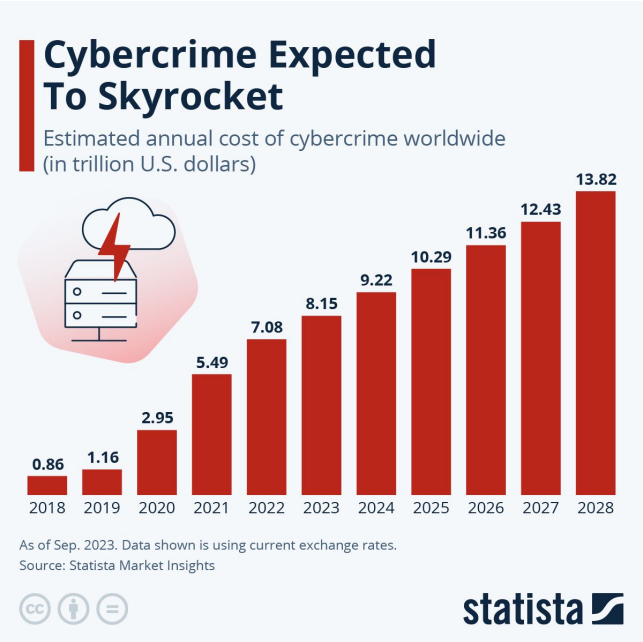
實現 BAS 自動化劇本推薦喵

產學合作組 PR2-01

Members：何宗諺 /鄭宇兩

傳統挑戰

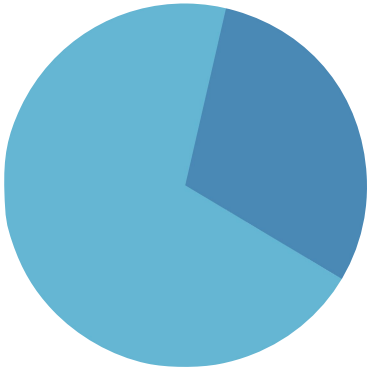
Pain Points



多數企業對自身外部暴露資 產(domains、IP、服務)沒有清楚掌握

約70%攻擊事件是因管理不當的對外風險資 產而發生

- The State of Attack Surface Management 2022



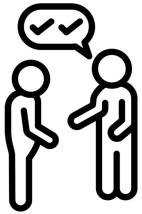
- **全球資安威脅事件不斷上升，帶來巨大損失**

BAS 劇本挑選上的痛點 ...

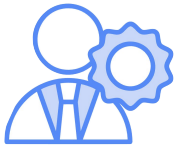
BAS(Breach and Attack Simulation)

- 透過挑選 **攻擊劇本** 來進行資安演練
- 挑選合適的攻擊劇本是成功演練的 **關鍵因素**

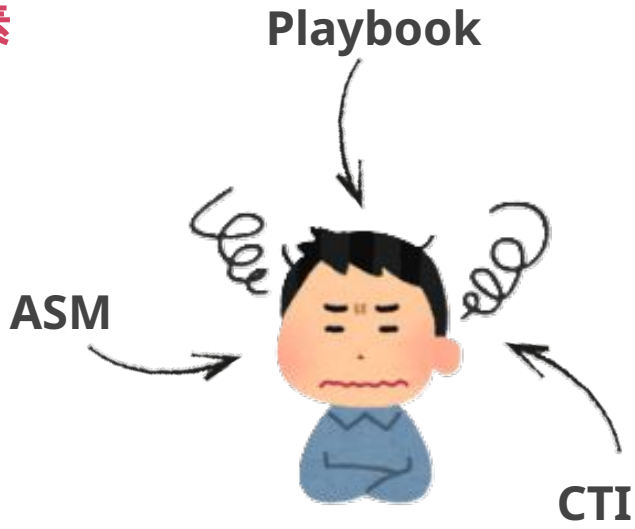
數據過於分散且無系統化的整合



缺乏一套標準化的推薦依據與流程



漫長而瑣碎的準備時間



我們的目標

「看不見、看不懂風險」 - - -► 『了解、預測並防禦風險』

- Asset Inventory
- ASM
- CTI

帶來的價值

智慧化的 BAS 劇本推薦
外暴資產了解與預防

攻擊鏈可視化

風險資產判讀、識別

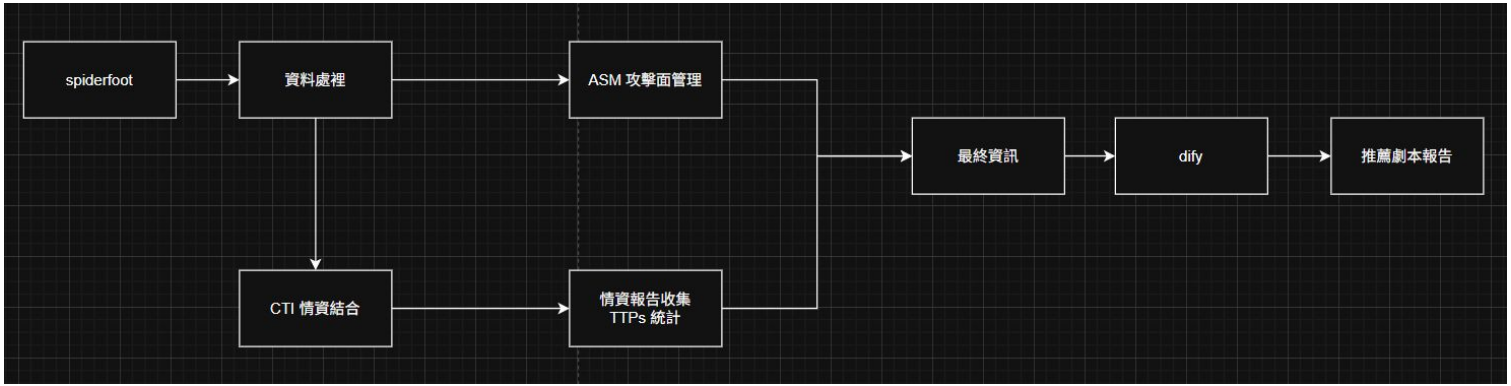
威脅情資整合

實作

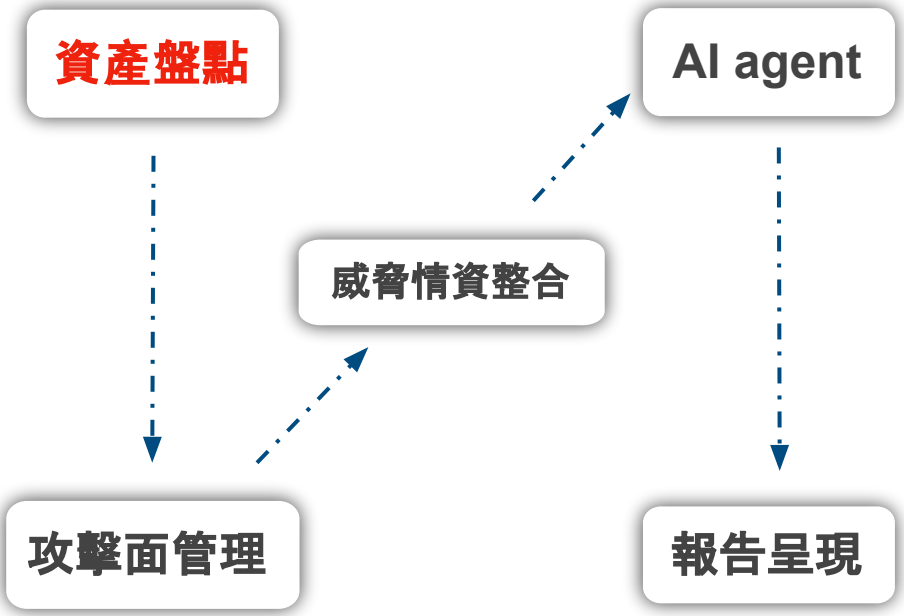
預期實作流程

- 整合多個開源平台與工具
- 模組化管理

資產盤點 → 攻擊面管理(ASM) → 威脅情資整合 → 劇本推薦



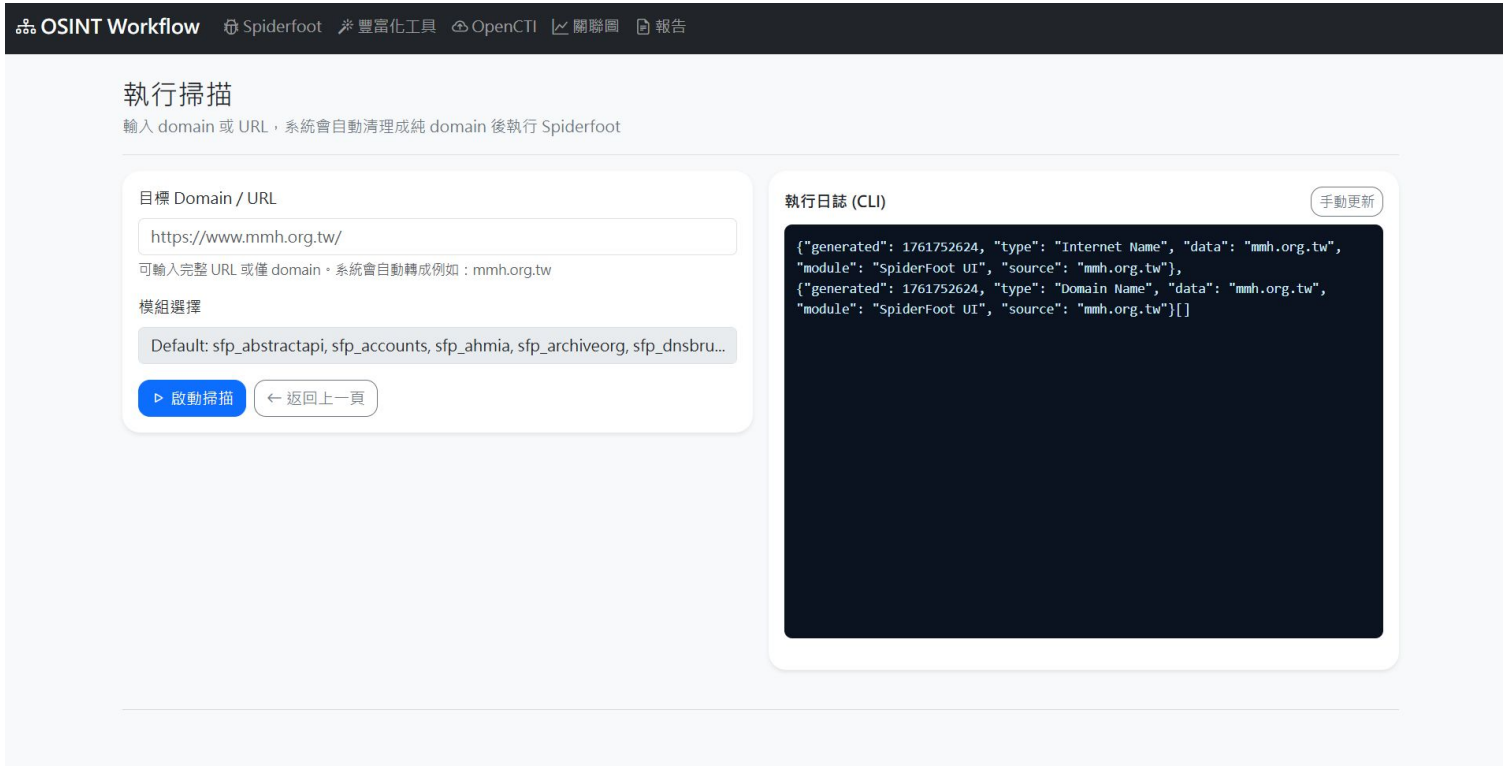
具體工作流程



- **資產盤點 / 攻擊面管理**
  - 進行大規模資 產掃描
  - 過濾、移除雜訊，並豐富化資 產資訊
- **威脅情資整合：**
  - 整合先前結果進 OpenCTI
  - 蒐集相關威脅情資報告
- **AI agent：**
  - 透過 Dify 串接多個 LLM，以進行資料消化與分析，進而去推薦劇本與生成報告
- **報告呈現：**
  - 可視、網頁化所有資訊，方便 閱讀

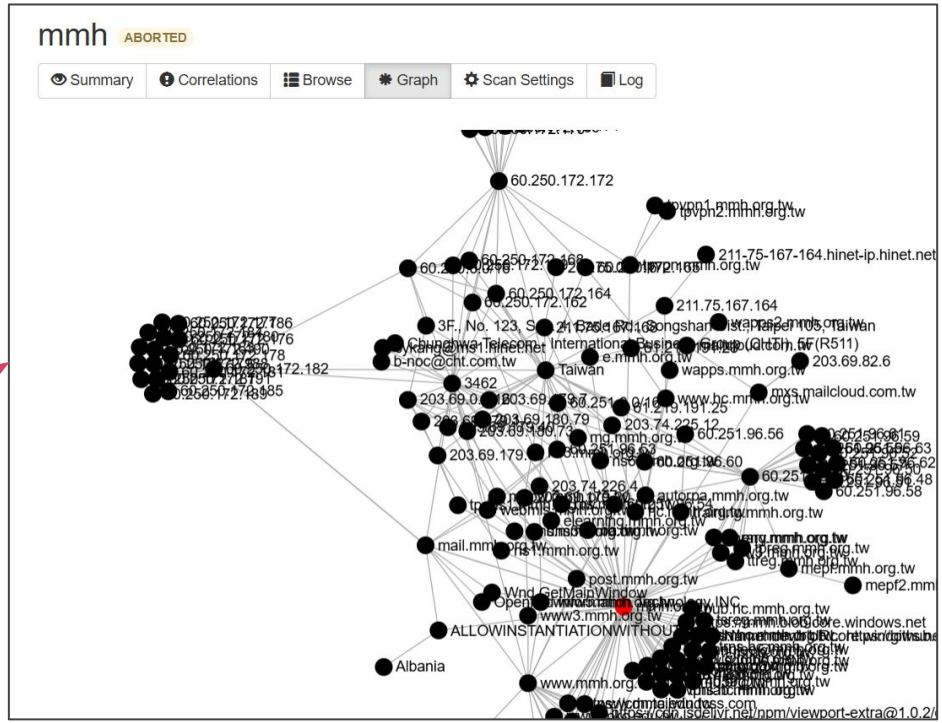
資產盤點 - Spiderfoot

Module Selection



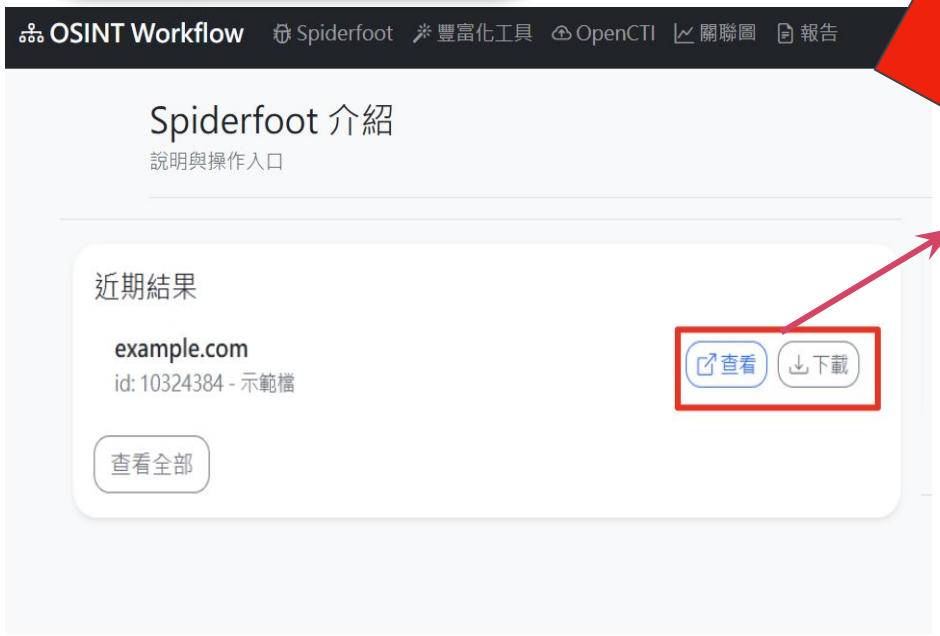
資產盤點 - Spiderfoot

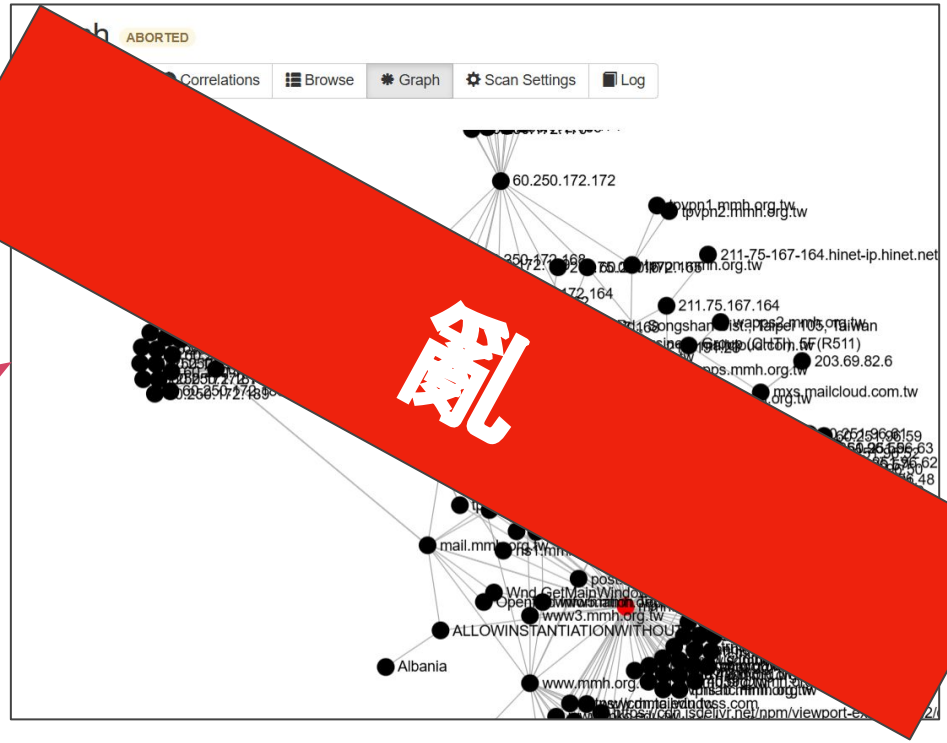
查看掃描結果



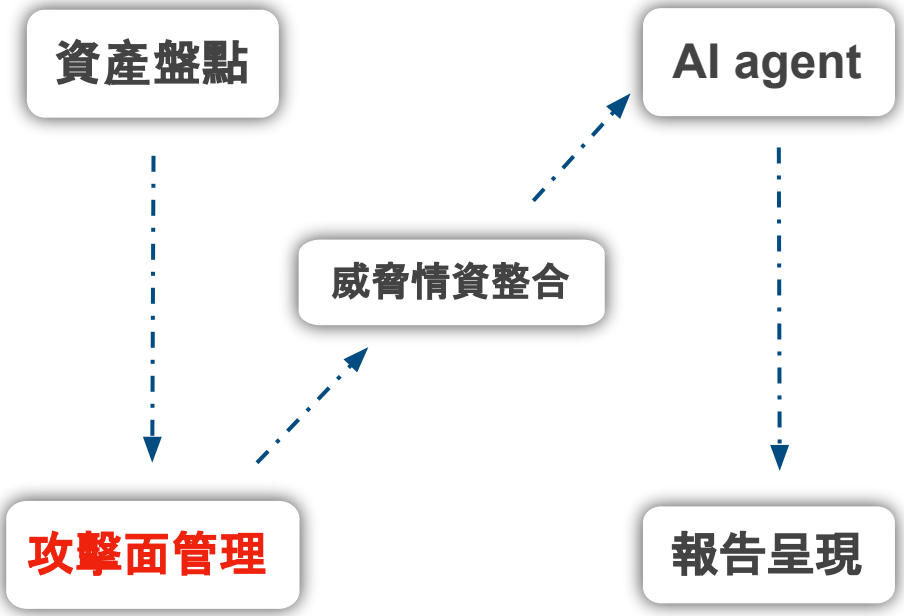
資產盤點 - Spiderfoot

查看掃描結果





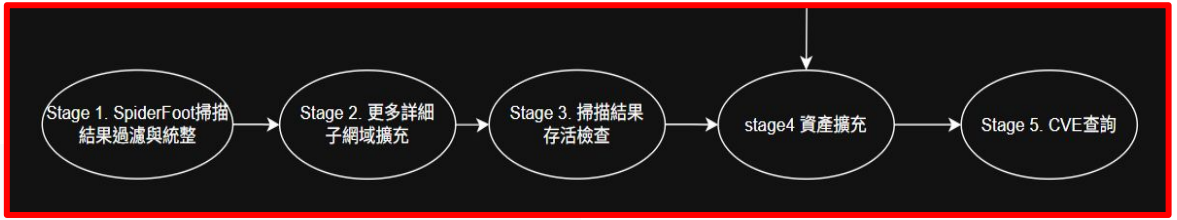
具體工作流程



- **資產盤點 / 攻擊面管理**
  - 進行大規模資 產掃描
  - 過濾、移除雜訊，並豐富化資 產資訊
- **威脅情資整合：**
  - 整合先前結果進 OpenCTI
  - 蒐集相關威脅情資報告
- **AI agent：**
  - 透過 Dify 串接多個 LLM，以進行資料消化與分析，進而去推薦劇本與生成報告
- **報告呈現：**
  - 可視、網頁化所有資訊，方便 閱讀

資產盤點 - 資料過濾與豐富化

Filter & Enrich data



資產豐富化工具鏈

左側選擇階段與 JSON，右側流程圖，底部為執行日誌

選擇要執行的階段

- Stage 1：這是第一階段「資產發現與分類」的腳本，主要任務是從 SpiderFoot 的 JSON 輸出結果 中，自動識別出掃描目標、分類出「內部 / 外部」資產，並整理成一份完整的報告。
- Stage 2：Subfinder Enrich
- Stage 3：Liveness Check
- Stage 4：Enrichment Scan
- Stage 5：CVE Checker

上傳或選擇 data.json

拖曳 JSON 檔案至此或點擊選擇

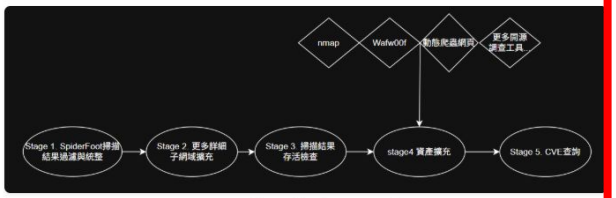
尚未選擇檔案

執行工具鏈　← 返回

流程說明

Stage 1 → Stage 2 → Stage 3 → Stage 4 → Stage 5

Stage 1：這是第一階段「資產發現與分類」的腳本，主要任務是從 SpiderFoot 的 JSON 輸出結果中，自動識別出掃描目標、分類出「內部 / 外部」資產，並整理成一份完整的報告。



圖示：整體資產豐富化流程概覽

資產盤點 - 資料過濾與豐富化

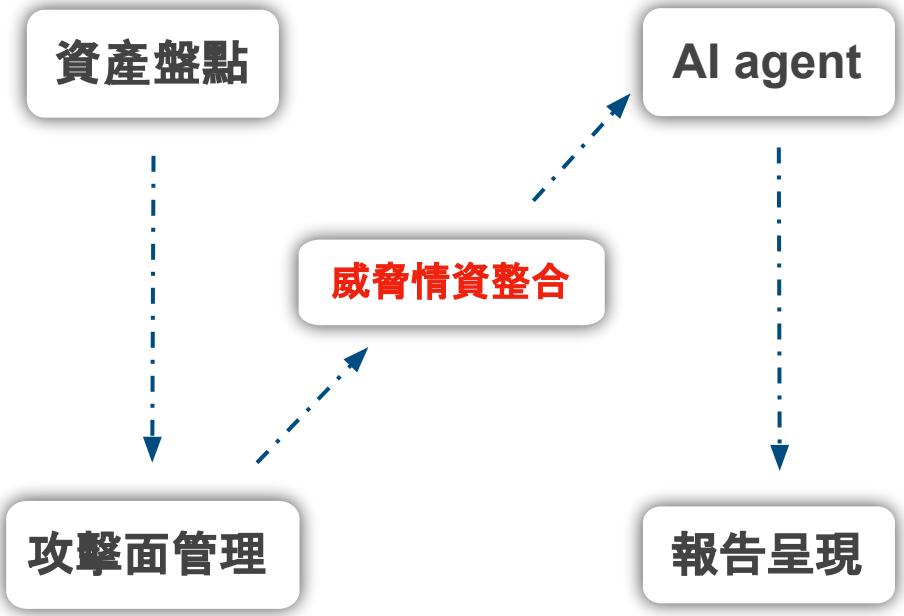
Before:


```
1   [{"data": "\t\n<!DOCTYPE html>\n<html lang=\"zh-tw\">\n<head>\n<meta ch
    content=\"text.php; charset=UTF-8\" />\n<meta http-equiv=\"X-UA-Compati
    content=\"width=device-width\">\n<script src=\"https://cdn.jsdelivr.net
    script>\n<title>\u9996\u9801\uff1a\u53f0\u6771\u99ac\u5055\u7d00\u5ff5\
    content=\"\u672c\u9662\u70ba\u53f0\u6771\u552f\u4e00\u5340\u57df\u7d1a\
    \u7d1a\u6025\u6551\u8cac\u4efb\u91ab\u9662\uff0c\u80a9\u8ca0\u53f0\u677
    6d\u52d9\uff0c\u4e26\u64c1\u6709\u53f0\u6771\u4e03\u6210\u7684\u52a0\u8
    4e00\u7684\u7dca\u6025\u5fc3\u5c0e\u7ba1\u624b\u8853\u3001\u6025\u6027\
    \u89e3\u8853\uff0c\u53ca\u7dca\u6025\u5916\u50b7\u624b\u8853\u300
    c5\u7ae5\u7684\u7167\u9867\u3002\">\n<meta property=\"og:title\"
    content=\"\u9996\u9801\uff1a\u53f0\u6771\u99ac\u5055\u7d00\u5ff5
    content=\"website\">\n<meta property=\"og:url\" content=\"\u9019
    content=\"\u6bcf\u4e00\u9801\u90fd\u9700\u8981\u4e00\u5f35\u5716\u
    \u6293\u4e3b\u5716\">\n<meta property=\"og:description\"
    content=\"\u672c\u9662\u70ba\u53f0\u6771\u552f\u4e00\u5340\u57df\u7d1a\
    \u7d1a\u6025\u6551\u8cac\u4efb\u91ab\u9662\uff0c\u80a9\u8ca0\u53f0\u677
    6d\u52d9\uff0c\u4e26\u64c1\u6709\u53f0\u6771\u4e03\u6210\u7684\u52a0\u8
    4e00\u7684\u7dca\u6025\u5fc3\u5c0e\u7ba1\u624b\u8853\u3001\u6025\u6027\
    \u89e3\u8853\uff0c\u53ca\u7dca\u6025\u5916\u50b7\u624b\u8853\u3001\u9ad
    c5\u7ae5\u7684\u7167\u9867\u3002\">\n<meta property=\"og:site_name\"
    content=\"\u53f0\u6771\u99ac\u5055\u7d00\u5ff5\u91ab\u9662\">\n<meta na
    Phone-->\n<meta name=\"msapplication-navbutton-col", "event_type": "TAR
```


After:

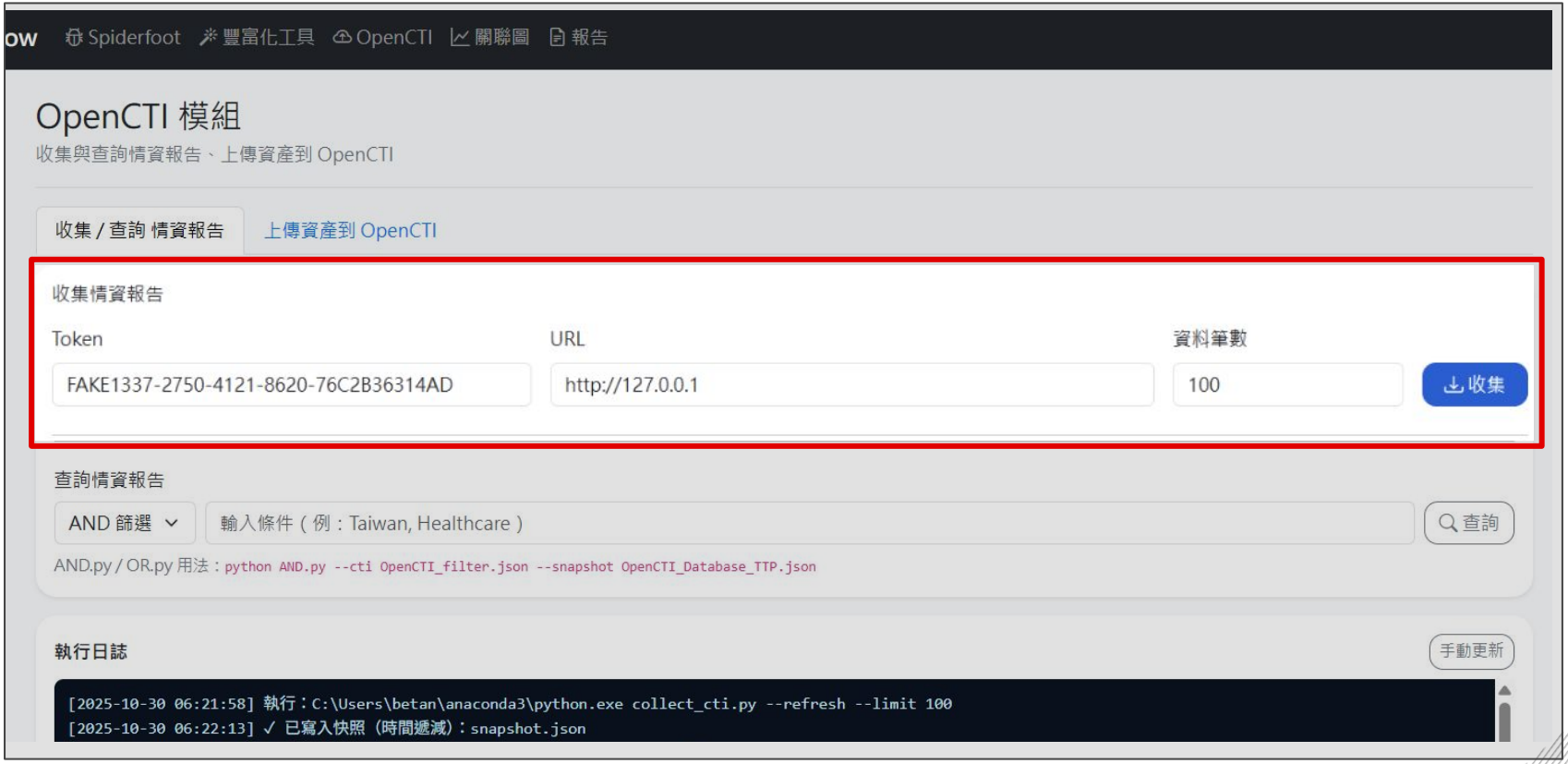

```
{
    "scan_target": "mmh.org.tw",
    "scan_timestamp_utc": "2025-10-29T01:57:31.638296+00:00",
    "assets": {
        "internal": [
            {
                "domain": "1180.ecw.mmh.org.tw",
                "asset_type": "INTERNAL",
                "stage2_results": {
                    "last_scanned_utc": "2025-10-29T02:01:42.967835+00:00",
                    "ips": [
                        "60.250.172.170"
                    ],
                    "ports": {
                        "60.250.172.170": {
                            "80": "open",
                            "113": "closed",
                            "443": "open"
                        }
                    },
                    "technologies": [
                        {
                            "name": "Apache"
```

具體工作流程



- **資產盤點 / 攻擊面管理**
  - 進行大規模資 產掃描
  - 過濾、移除雜訊，並豐富化資 產資訊
- **威脅情資整合：**
  - 整合先前結果進 OpenCTI
  - 蒐集相關威脅情資報告
- **AI agent：**
  - 透過 Dify 串接多個 LLM，以進行資料消化與分析，進而去推薦劇本與生成報告
- **報告呈現：**
  - 可視、網頁化所有資訊，方便 閱讀

威脅情資整合 - 下載資料


ow
Spiderfoot
豐富化工具
OpenCTI
關聯圖
報告
OpenCTI 模組
收集與查詢情資報告、上傳資產到 OpenCTI
收集 / 查詢 情資報告
上傳資產到 OpenCTI
收集情資報告
Token
URL
資料筆數
FAKE1337-2750-4121-8620-76C2B36314AD
http://127.0.0.1
100
收集
查詢情資報告
AND 篩選
輸入條件（例：Taiwan, Healthcare）
查詢
AND.py / OR.py 用法：python AND.py --cti OpenCTI_filter.json --snapshot OpenCTI_Database_TTP.json
執行日誌
手動更新
[2025-10-30 06:21:58] 執行：C:\Users\betan\anaconda3\python.exe collect_cti.py --refresh --limit 100
[2025-10-30 06:22:13] ✓ 已寫入快照（時間遞減）：snapshot.json

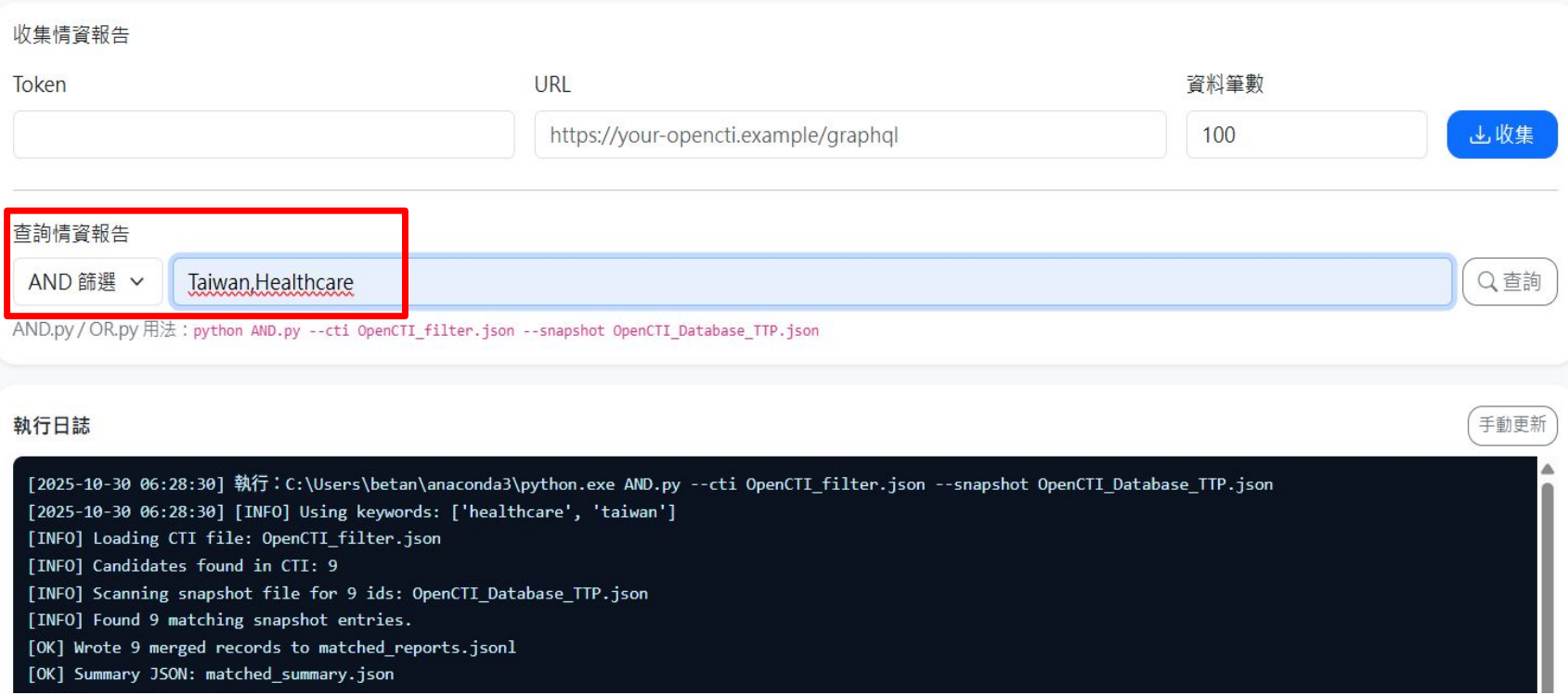
威脅情資整合 - 下載資料

CTI Report


```
1 {"id": "6e58b310-7c5c-4e34-9ae4-2a5875cd6b30", "name": "Deepfake-as-a-Service 2025 – How Voice Cloning and Synthetic Media Fraud Are Changing Enterprise Defenses",
"published": "2025-10-29T01:00:00.000Z", "created": "2025-10-29T01:00:00.000Z", "created_at": "2025-10-29T01:26:09.823Z", "updated_at": "2025-10-29T01:26:09.855Z",
"createdBy": null, "labels": ["deepfake", "deepfake as a service", "hacking news", "voice intelligence"], "countries_from_objects": [], "sectors_from_objects": []}
2 {"id": "0a523a01-f0b0-4c65-ad0b-c74a5143a22d", "name": "New Android Malware Mimics Human Behavior to Evade Detection", "published": "2025-10-28T18:24:45.680Z", "created":
"2025-10-28T18:24:45.680Z", "created_at": "2025-10-28T19:48:42.277Z", "updated_at": "2025-10-28T19:48:42.318Z", "createdBy": "AlienVault", "labels": ["android", "banking
trojan", "behavior mimicry", "brokewell", "credential theft", "device takeover", "herodotus", "hook", "malware-as-a-service", "mqtt", "octo", "remote control"],
"countries_from_objects": ["Poland", "United Kingdom of Great Britain and Northern Ireland", "Brazil", "Italy", "United States of America", "Finance"], "sectors_from_objects":
["Poland", "United Kingdom of Great Britain and Northern Ireland", "Brazil", "Italy", "United States of America", "Finance"]}
3 {"id": "dbaaf1ce-549b-4690-b57c-d4e3c40d6556", "name": "Keeping the Internet fast and secure: introducing Merkle Tree Certificates", "published": "2025-10-28T13:00:00.000Z",
"created": "2025-10-28T13:00:00.000Z", "created_at": "2025-10-28T13:25:23.475Z", "updated_at": "2025-10-28T13:25:23.510Z", "createdBy": null, "labels": ["chrome", "cloudflare
workers", "cryptography", "google", "ietf", "open source", "post-quantum", "research", "rust", "security", "tls", "transparency"], "countries_from_objects": [],
"sectors_from_objects": []}
4 {"id": "96dd7807-6840-400b-a63e-1e8213965dec", "name": "Schneider Electric EcoStruxure", "published": "2025-10-28T12:00:00.000Z", "created": "2025-10-28T12:00:00.000Z",
"created_at": "2025-10-28T17:25:51.647Z", "updated_at": "2025-10-28T17:25:51.681Z", "createdBy": null, "labels": [], "countries_from_objects": [], "sectors_from_objects": []}
5 {"id": "b66d6dfa-7ce0-49fe-b496-9928b9f28fde", "name": "CISA Releases Three Industrial Control Systems Advisories", "published": "2025-10-28T12:00:00.000Z", "created":
"2025-10-28T12:00:00.000Z", "created_at": "2025-10-28T16:16:08.542Z", "updated_at": "2025-10-28T16:16:08.577Z", "createdBy": null, "labels": [], "countries_from_objects": [],
"sectors_from_objects": []}
6 {"id": "902034e9-2185-4eb7-b127-dccaee1572ee", "name": "Crypto wasted: BlueNoroff's ghost mirage of funding and jobs", "published": "2025-10-28T03:41:57.869Z", "created":
"2025-10-28T03:41:57.869Z", "created_at": "2025-10-28T09:50:43.680Z", "updated_at": "2025-10-28T09:50:44.279Z", "createdBy": "AlienVault", "labels": ["cosmicdoor",
"cryptocurrency", "rootroy", "silentsiphon", "sneakmain", "sysphon", "zoomclutch"], "countries_from_objects": [], "sectors_from_objects": []}
7 {"id": "60697e65-2636-4e57-b49a-fd4e080b392c", "name": "Earth Entries alive and kicking", "published": "2025-10-28T03:04:01.487Z", "created": "2025-10-28T03:04:01.487Z",
"created_at": "2025-10-28T09:48:32.650Z", "updated_at": "2025-10-28T09:48:32.762Z", "createdBy": "AlienVault", "labels": ["cve-2025-8088", "shadowpad", "snappybee", "winrar"],
"countries_from_objects": [], "sectors_from_objects": []}
8 {"id": "94e19d20-96f3-4b69-b20e-4082f55ff1b4", "name": "Microsoft WSUS Remote Code Execution (CVE-2025-59287) Actively Exploited in the Wild", "published":
"2025-10-27T20:48:41.917Z", "created": "2025-10-27T20:48:41.917Z", "created_at": "2025-10-27T21:18:05.493Z", "updated_at": "2025-10-27T21:18:05.523Z", "createdBy":
"AlienVault", "labels": ["active exploitation", "cve-2025-59287", "emergency patch", "network reconnaissance", "patch management", "remote code execution", "unauthenticated
rce", "windows server", "wsus"], "countries_from_objects": [], "sectors_from_objects": []}
```

威脅情資整合 - 搜尋並下載

CTI Report Searching (OR & AND filter)



威脅情資整合 - 搜尋並下載

CTI Report Searching

```
[OK] Summary JSON: matched_summary.json
[OK] Summary MD: matched_summary.md
找到報告 1 : Warlock Ransomware: Old Actor, New Tricks?
找到報告 2 : Gunra Ransomware Group Unveils Efficient Linux Variant
找到報告 3 : APT 41: Threat Intelligence Report and Malware Analysis
找到報告 4 : Disruption of Drone Supply Chains Through Coordinated Multi-Wave Attacks in Taiwan
找到報告 5 : CrazyHunter Campaign Targets Taiwanese Critical Sectors
找到報告 6 : CrazyHunter: The Rising Threat of Open-Source Ransomware
找到報告 7 : SmokeLoader picks up ancient MS Office bugs to pack fresh credential stealer
找到報告 8 : Chinese Hackers Toolkit Uncovered And Activity History Uncovered
找到報告 9 : Ransomware Roundup - Underground
[2025-10-30 06:28:30] 結束 (exit=0)
```

威脅情資整合 - 搜尋並下載

CTI report searching:
Get Crazy Hunter Report

```
[OK] Summary JSON: matched_summary.json
[OK] Summary MD: matched_summary.md
找到報告 1 : Warlock Ransomware: Old Actor, New Tricks?
找到報告 2 : Gunra Ransomware Group Unveils Efficient Linux Variant
找到報告 3 : APT 41: Threat Intelligence Report and Malware Analysis
找到報告 4 : Disruption of Drone Supply Chains Through Coordinated Multi-Wave Attacks in Taiwan
找到報告 5 : CrazyHunter Campaign Targets Taiwanese Critical Sectors
找到報告 6 : CrazyHunter: The Rising Threat of Open-Source Ransomware
找到報告 7 : SmokeLoader picks up ancient MS Office bugs to pack fresh credential stealer
找到報告 8 : Chinese Hackers Toolkit Uncovered And Activity History Uncovered
找到報告 9 : Ransomware Roundup - Underground
[2025-10-30 06:28:30] 結束 (exit=0)
```

威脅情資整合 - 上傳

上傳介面

OpenCTI 模組

收集與查詢情資報告、上傳資產到 OpenCTI

收集 / 查詢 情資報告 | 上傳資產到 OpenCTI

上傳資產到 OpenCTI

拖曳 data.json 至此或點擊選擇

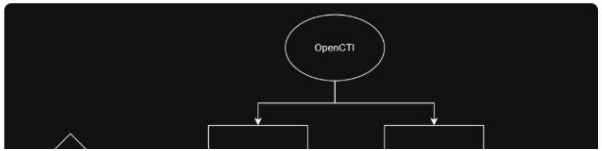
已上傳：mmh-SpiderFoot_output.json (135.5 KB)

Token: FAKE6A8D-2750-4121-8620-76C2B36314AD

URL: http://127.0.0.1

Author Name (org): mmh

上傳到 OpenCTI | 統整為 Bundle | ↑ 推送 Bundle



ervations / Observables

Search these results... | Add filter | Select saved filter | 1 - 25 / 154

thor = mmh

TYPE	REPRESENTATION	AUTHOR	CREATORS	LABELS
DOMAIN N...	msoid.mmh.org.tw	mmh	admin	country-tw port-443 port-8
DOMAIN N...	tpvpn1.mmh.org.tw	mmh	admin	country-tw waf:not applicable
DOMAIN N...	mmh.ecw.mmh.org.tw	mmh	admin	country-tw port-443 port-8
DOMAIN N...	infotech.ecw.mmh.org.tw	mmh	admin	country-tw port-443 port-8
DOMAIN N...	e.mmh.org.tw	mmh	admin	country-tw port-443 servic
DOMAIN N...	mcloud.mmh.org.tw	mmh	admin	country-tw port-443 port-8
DOMAIN N...	mail.mmh.org.tw	mmh	admin	country-tw port-443 port-8
DOMAIN N...	ttreg.mmh.org.tw	mmh	admin	country-tw port-443 port-8

tpworkspace.mmh.org.tw

OVERVIEW | KNOWLEDGE | CONTENT | ANALYSES | SIGHTINGS | DATA | HISTORY

DETAILS

Description
ASM-discovered domain

value
tpworkspace.mmh.org.tw

Indicators composed with this observable +

Malware analyses

No malware analysis on this observable.

BASIC INFORMATION

Marking
TLP:CLEAR

Score
-

Author
MMH

Labels +
country-tw | has:ports | port-443 | port-80 | service-web | tech-jquery | tech:jquery | waf-detected | waf:big-ip appsec...

Observable type
DOMAIN NAME

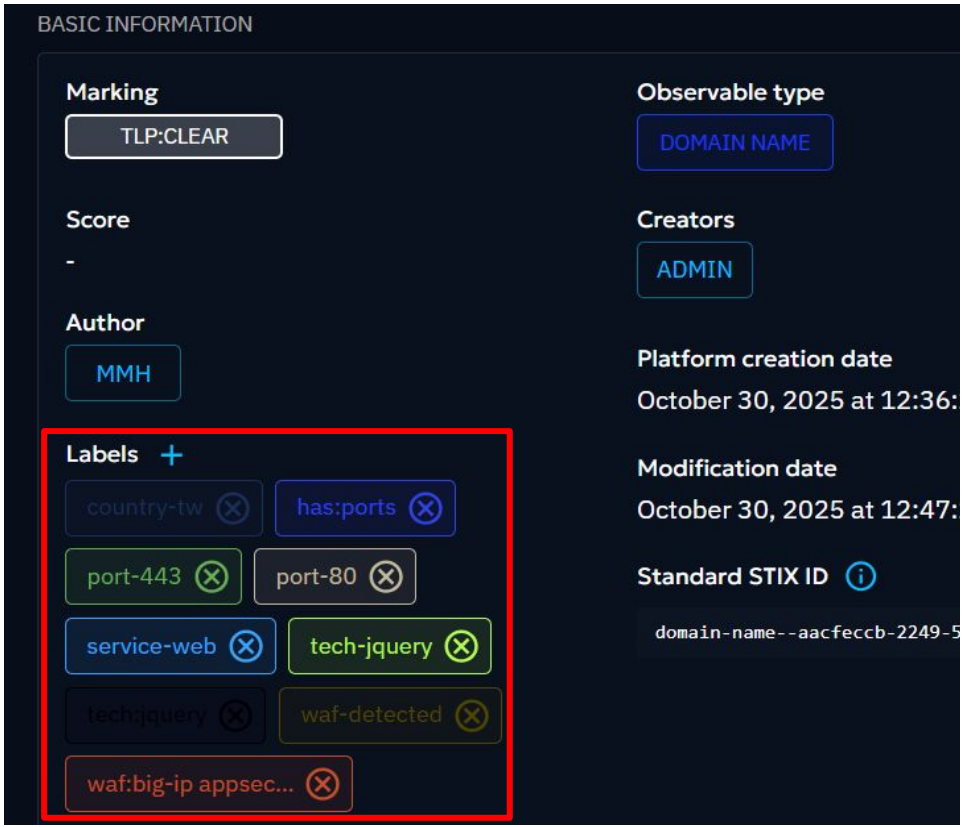
Creators
ADMIN

Platform creation date
October 30, 2025 at 12:36:20 AM

Modification date
October 30, 2025 at 12:47:28 AM

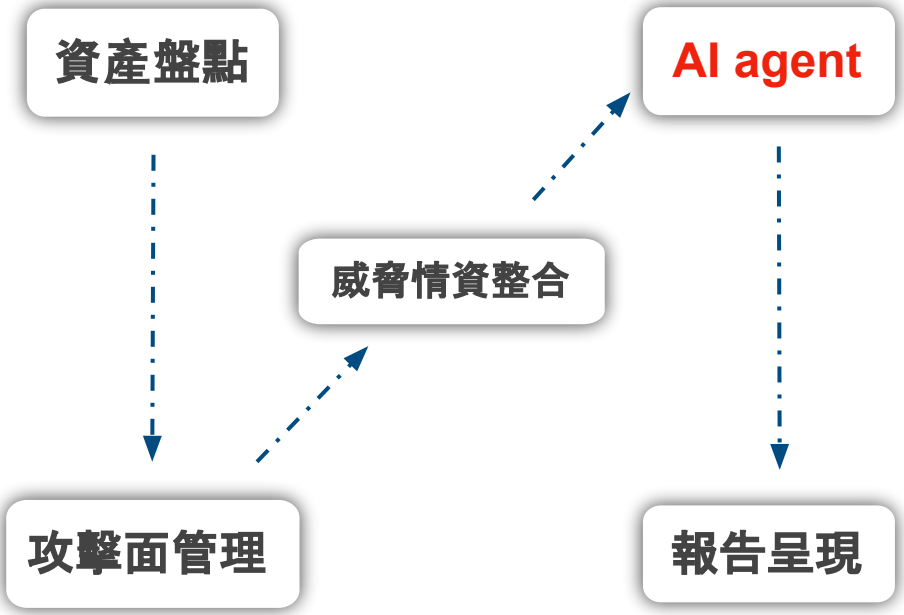
Standard STIX ID
domain-name--aacfeccb-2249-56d4-96

威脅情資整合 - 上傳



- 資料成功上傳
- **先前掃描資訊新增為標籤**
- 更方便追蹤
- 彈性延伸
- 企業自行額外擴充

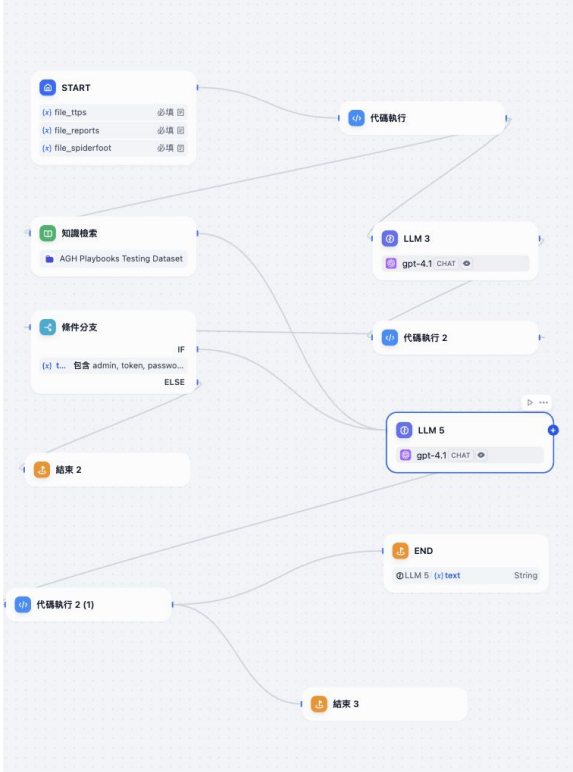
具體工作流程



- **資產盤點 / 攻擊面管理**
  - 進行大規模資 產掃描
  - 過濾、移除雜訊，並豐富化資 產資訊
- **威脅情資整合：**
  - 整合先前結果進 OpenCTI
  - 蒐集相關威脅情資報告
- **AI agent：**
  - 透過 Dify 串接多個 LLM，以進行資料消化與分析，進而去推薦劇本與生成報告
- **報告呈現：**
  - 可視、網頁化所有資訊，方便 閱讀

AI agent

Dify Workflow Chart



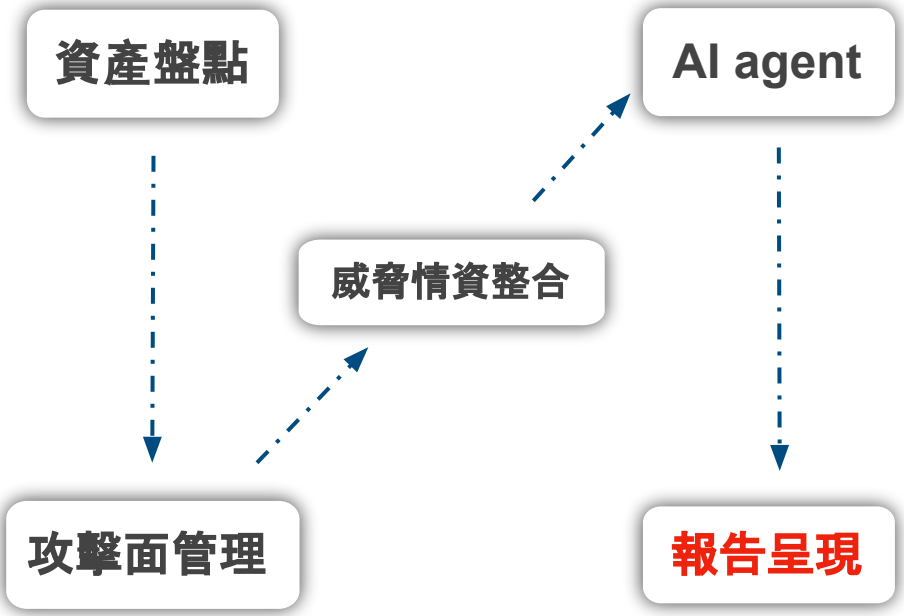
🎯 **推薦演練劇本**

推薦劇本 1

劇本編號： [Playbook] 63003
劇本名稱： Data Leak Prevention and Ransomware contains CVE

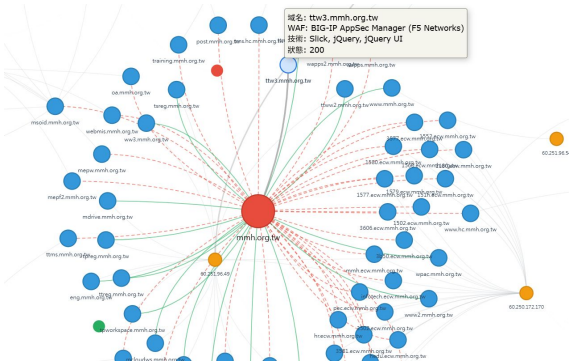
- **演練類型**：Endpoint / DataLeak / Internet
- **推薦理由**：
  - 直接模擬勒索軟體（T1486）與資料外洩複合攻擊，對應本次情資高危勒索威脅
  - 涵蓋 T1486、T1078、T1105、T1567.002 等多個高頻 TTP，驗證端點偵測（EDR）、資料外洩防護（DLP）與權限控管
  - 完全適用於 Windows 作業系統，與組織現有資產環境高度吻合
  - 可驗證備份恢復、權限異常、資料加密行為等多重防護機制
- **涵蓋攻擊技術（MITRE ATT&CK）**：
  - T1486 - Data Encrypted for Impact：模擬資料加密勒索核心流程
  - T1078 - Valid Accounts：利用合法帳號進行權限存取與持續控制
  - T1105 - Ingress Tool Transfer：攻擊工具下載投遞驗證雲端存取防禦
  - T1567.002 - Exfiltration to Cloud Storage：資料外洩至雲端服務
  - T1068 - Exploitation for Privilege Escalation：模擬權限提升場景
  - 其他：T1548.002、T1112、T1027 等防禦規避技術
- **演練環境需求**：
  - 目標作業系統：Windows 10
  - Agent 需求：需要
  - 建議環境：windows/amd64

具體工作流程



- **資產盤點 / 攻擊面管理**
  - 進行大規模資 產掃描
  - 過濾、移除雜訊，並豐富化資 產資訊
- **威脅情資整合：**
  - 整合先前結果進 OpenCTI
  - 蒐集相關威脅情資報告
- **AI agent：**
  - 透過 Dify 串接多個 LLM，以進行資料消化與分析，進而去推薦劇本與生成報告
- **報告呈現：**
  - 可視、網頁化所有資訊，方便 閱讀

報告呈現



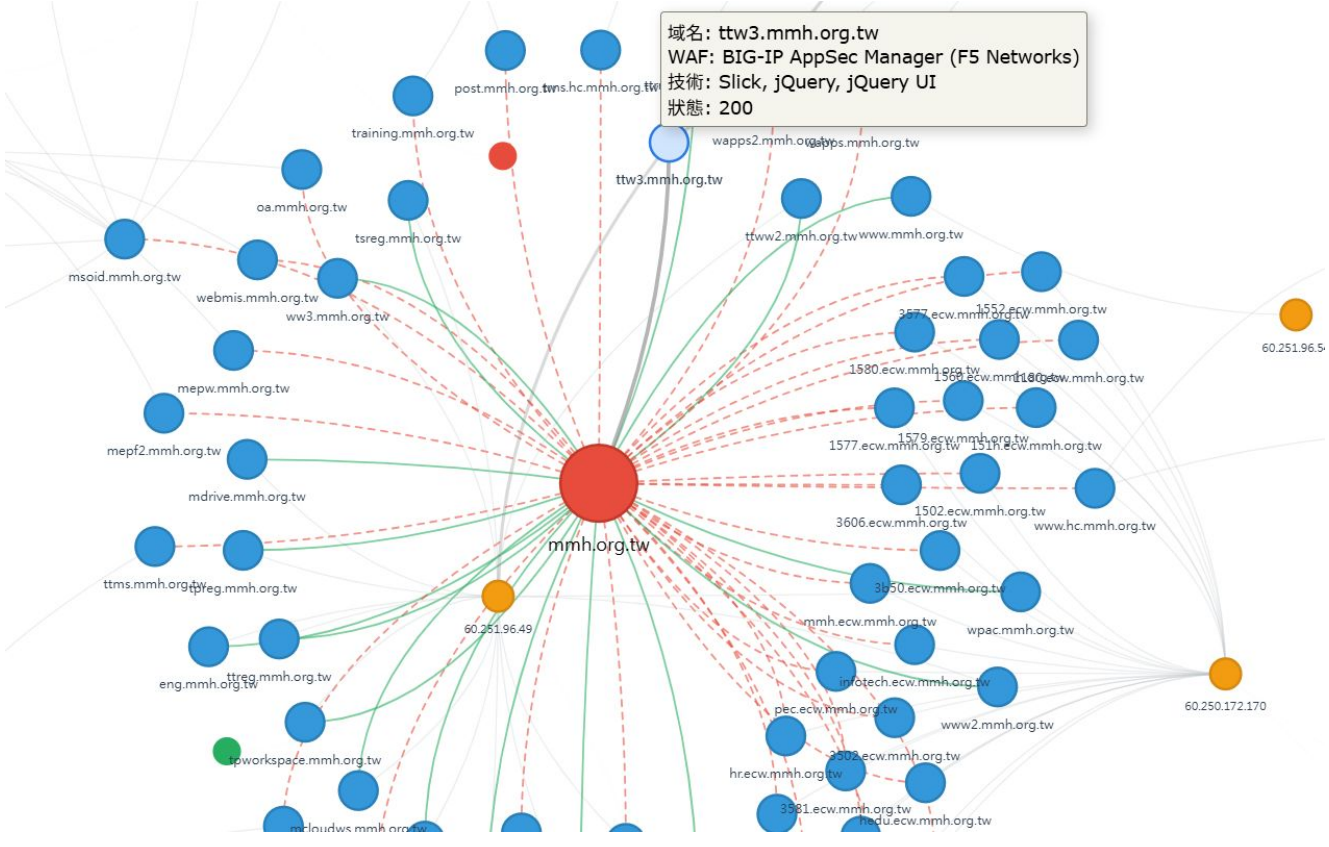
關聯圖

各別網域細節

總覽

報告呈現

關聯圖


域名: ttw3.mmh.org.tw
WAF: BIG-IP AppSec Manager (F5 Networks)
技術: Slick, jQuery, jQuery UI
狀態: 200
mmh.org.tw
ttw3.mmh.org.tw
post.mmh.org.tw
training.mmh.org.tw
oa.mmh.org.tw
tsreg.mmh.org.tw
msoid.mmh.org.tw
webmis.mmh.org.tw
ww3.mmh.org.tw
mepw.mmh.org.tw
mepf2.mmh.org.tw
mdrive.mmh.org.tw
ttms.mmh.org.tw
tpreg.mmh.org.tw
eng.mmh.org.tw
ttreg.mmh.org.tw
tpworkspace.mmh.org.tw
60.251.96.49
wapps2.mmh.org.tw
ttww2.mmh.org.tw
www.mmh.org.tw
1552.ecw.mmh.org.tw
1580.ecw.mmh.org.tw
1577.ecw.mmh.org.tw
1579.ecw.mmh.org.tw
1502.ecw.mmh.org.tw
3606.ecw.mmh.org.tw
www.hc.mmh.org.tw
wpac.mmh.org.tw
mmh.ecw.mmh.org.tw
infotech.ecw.mmh.org.tw
pec.ecw.mmh.org.tw
www2.mmh.org.tw
60.250.172.170
hr.ecw.mmh.org.tw
3581.ecw.mmh.org.tw

報告呈現

各別細節資訊

- 內部資產
  - 1180.ecw.mmh.org.tw
  - 1502.ecw.mmh.org.tw
  - 151h.ecw.mmh.org.tw
  - 1552.ecw.mmh.org.tw
  - 1560.ecw.mmh.org.tw
  - 1577.ecw.mmh.org.tw
  - 1579.ecw.mmh.org.tw
  - 1580.ecw.mmh.org.tw
  - 1581.ecw.mmh.org.tw
  - 1584.ecw.mmh.org.tw

資產詳細資訊: 1180.ecw.mmh.org.tw

技術指紋分析 (Stage 2)

分類	技術名稱	版本
Unknown	Apache	unknown
Unknown	PHP	7.0.33

AI 攻擊面分析報告

預期網站功能

內部醫療機構的會員或員工登入入口，提供身份驗證以存取內部系統

技術棧總結

Apache Web Server 搭配 PHP 7.0.33，無前端 JavaScript，無明顯框架，使用 HTTPS (443) 與 HTTP (80) 端口

攻擊面分析

- **使用過時的 PHP 版本**（嚴重性: High)
  系統使用 PHP 7.0.33，該版本已於 2018 年停止官方支援，存在多個已知漏洞（如遠端代碼執行、資訊洩露等），且無安全更新，增加被攻擊風險。
- **缺少安全相關 HTTP 標頭**（嚴重性: Medium)
  HTTP Headers 未發現安全標頭（如 Content-Security-Policy、X-Frame-Options、X-Content-Type-Options、Strict-Transport-Security），容易受到點擊劫持、MIME 類型混淆及中間人攻擊等威脅。

報告呈現

最終總覽


威脅情資分析與防護演練劇本推薦報告
機密文件 - 僅供內部使用
報告生成日期：2025年10月31日
整體安全態勢：高風險
概況總覽
威脅分析
攻擊面評估
演練劇本
行動建議
執行摘要
本次分析涵蓋 2024 年 8 月至 2025 年 4 月間，彙整自 AlienVault 等情資來源的 12 份威脅情報報告， 聚焦於針對台灣醫療與科技產業的勒索軟體、APT、供應鏈攻擊及網路釣魚等核心威脅。 最緊迫的安全風險來自於公開服務漏洞利用、憑證竊取與資料加密等高頻 TTP，與組織現有攻擊面的多項弱點高度重疊。
分析報告數量
12 份
內部資產
42 個
外部資產
13 個
高優先級威脅
8 項
主要威脅類型
勒索軟體 (Ransomware)
利用外部服務漏洞滲透，迅速加密關鍵
APT 高級持續威脅
針對醫療、科技等高價值產業，採多階
供應鏈攻擊
鎖定第三方軟體/服務，利用更新或授
網路釣魚 (Phishing)
定向郵件夾帶惡意附件，誘導員工執行

情資報告呈現

主要威脅類型

勒索軟體 (Ransomware)

利用外部服務漏洞滲透，迅速加密關鍵資料，造成業務中斷

LockBit　Conti　BlackCat

APT 高級持續威脅

針對醫療、科技等高價值產業，採多階段滲透與長期潛伏

APT41

地緣威脅態勢

TW 台灣威脅態勢

7 份報告中明確提及台灣為攻擊目標

主要威脅：勒索軟體、APT、供應鏈攻擊

產業聚焦：醫療、科技、半導體

特殊情境：攻擊集團偏好利用台灣本地 IT 弱點與人員意識不足作為突破口，並結合社工與漏洞利用進行

MITRE ATT&CK 技術分布

優先級	技術編號	技術名稱	偵測次數	風險等級	攻擊階段
P1	T1486	Data Encrypted for Impact	8	極高	Impact
P2	T1190	Exploit Public-Facing Application	7	極高	Initial Access
P3	T1078	Valid Accounts	6	極高	Persistence
P4	T1083	File and Directory Discovery	6	高	Discovery
P5	T1562.001	Impair Defenses: Disable or Modify Tools	5	高	Defense Evasion
P6	T1059	Command and Scripting Interpreter	5	高	Execution
P7	T1566.001	Phishing: Spearphishing Attachment	4	中	Initial Access
P8	T1210	Exploitation of Remote Services	4	中	Lateral Movement

攻擊鏈分析

1 初始入侵 T1190, T1566.001 → 2 權限提昇 T1078, T1059 → 3 防禦規避 T1562.001 → 4 橫向移動 T1210 → 5 影響破壞 T1486

⚠ 攔截重點：在初始入侵（T1190、T1566.001）和防禦規避（T1562.001）階段即時偵測並阻斷，是防止嚴重資安事件的關鍵。

TTPs 分析 與 攻擊鏈模擬串接

情資報告呈現

主要威脅類型

勒索軟體 (Ransomware)

利用外部服務漏洞滲透，迅速加密關鍵資料，造成業務中斷

LockBit　Conti　BlackCat

APT 高級持續威脅

針對醫療、科技等高價值產業，採多階段滲透與長期潛伏

APT41

地緣威脅態勢

TW 台灣威脅態勢

7 份報告中明確提及台灣為攻擊目標

主要威脅：勒索軟體、APT、供應鏈攻擊

產業聚焦：醫療、科技、半導體

特殊情境：攻擊集團偏好利用台灣本地 IT 弱點與人員意識不足作為突破口，並結合社工與漏洞利用進行

MITRE ATT&CK 技術分布

優先級	技術編號	技術名稱	偵測次數	風險等級	攻擊階段
P1	T1486	Data Encrypted for Impact	8	極高	Impact
P2	T1190	Exploit Public-Facing Application	7	極高	Initial Access
P3	T1078	Valid Accounts	6	極高	Persistence
P4	T1083	File and Directory Discovery	6	高	Discovery
P5	T1562.001	Impair Defenses: Disable or Modify Tools	5	高	Defense Evasion
P6	T1059	Command and Scripting Interpreter	5	高	Execution
P7	T1566.001	Phishing: Spearphishing Attachment	4	中	Initial Access
P8	T1210	Exploitation of Remote Services	4	中	Lateral Movement

攻擊鏈分析

1 初始入侵 T1190, T1566.001 → 2 權限提昇 T1078, T1059 → 3 防禦規避 T1562.001 → 4 橫向移動 T1210 → 5 影響破壞 T1486

⚠ 攔截重點：在初始入侵（T1190、T1566.001）和防禦規避（T1562.001）階段即時偵測並阻斷，是防止嚴重資安事件的關鍵。

TTPs 分析 與 攻擊鏈模擬串接

情資報告呈現

資產盤點
攻擊面管理

報告呈現

防禦改善建議

風險緩解建議

立即行動項（1-2 週內）

- 優先關閉不必要的外部端口（如3389、8080），並部署WAF於關鍵Web服務
- 立即修補所有已知漏洞的Web框架和中介軟體
- 強制啟用雙因素認證於所有管理與關鍵帳號
- 使用EDR/防毒軟體即時監控端點異常行為，強化RDP連線警示

短期強化（1-2 個月）

- 定期執行資產與漏洞全盤掃描，建立自動化修補流程
- 強化雲端與地端混合架構的存取控制與異常行為偵測
- 推動資安團隊演練（如勒索軟體、供應鏈攻擊全鏈路模擬）

BAS 劇本推薦

演練劇本推薦與原因

推薦方法論

本次劇本推薦以情資中高頻發生的TTP（如T1486、T1190、T1078等）為核心，結合組織目前外部攻擊面（RDP/Web端口、老舊系統、帳號管理）及產業特性，優先挑選可直接驗證關鍵防禦能力、對應活躍攻擊組織（LockBit、FIN7、Conti、APT41）的劇本，協助組織建立端到端、可量化的攻擊防禦驗證鏈路。

推薦劇本 1：[Playbook] 63002 - Data Leak Prevention and Ransomware

Endpoint / DataLeak / Internet

推薦理由：

- 直接對應T1486（Data Encrypted for Impact）與T1078（Valid Accounts），可完整驗證組織對勒索軟體攻擊全流程的檢測與應對能力
- 涵蓋多個高風險TTP（T1486、T1068、T1078、T1562.001），對應LockBit、Conti等活躍團體常用手法
- 適用於Windows環境，與組織現有IT架構及攻擊面發現高度吻合
- 可驗證EDR/NDR對於權限提升、資料外洩、檔案加密及防護工具繞過等行為的偵測反應

涵蓋攻擊技術（MITRE ATT&CK）：

T1486 – Data Encrypted for Impact | T1078 – Valid Accounts | T1562.001 – Impair Defenses | T1068 – Exploitation for Privilege Escalation | T1548.002 / T1112 / T1567.002

預期驗證成果：

- 驗證EDR及SIEM能否準確偵測權限提升、資料外傳與勒索加密行為
- 評估資安團隊對勒索攻擊全流程的回應與復原能力
- 測試備份與還原流程的實用性與緊急應變效能

演練環境需求：

目標作業系統	Agent 需求	建議環境
Windows 10	需要（驗證端點行為）	windows/amd64

FIN7 | LockBit | Conti | Windows | DLP | Ransomware

BAS 劇本推薦

演練劇本推薦與原因

推薦方法論

本次劇本推薦以情資中高頻發生的TTP（如T1486、T1190、T1078等）為核心，結合組織目前外部攻擊面（RDP/Web端口、老舊系統、帳號管理）及產業特性，優先挑選可直接驗證關鍵防禦能力、對應活躍攻擊組織（LockBit、FIN7、Conti、APT41）的劇本，協助組織建立端到端、可量化的攻擊防禦驗證鏈路。

推薦劇本 1：[Playbook] 63002 - Data Leak Prevention and Ransomware

Endpoint / DataLeak / Internet

推薦理由：

- 直接對應T1486（Data Encrypted for Impact）與T1078（Valid Accounts），可完整驗證組織對勒索軟體攻擊全流程的檢測與應對能力
- 涵蓋多個高風險TTP（T1486、T1068、T1078、T1562.001），對應LockBit、Conti等活躍團體常用手法
- 適用於Windows環境，與組織現有IT架構及攻擊面發現高度吻合
- 可驗證EDR/NDR對於權限提升、資料外洩、檔案加密及防護工具繞過等行為的偵測反應

涵蓋攻擊技術（MITRE ATT&CK）：

T1486 – Data Encrypted for Impact | T1078 – Valid Accounts | T1562.001 – Impair Defenses | T1068 – Exploitation for Privilege Escalation | T1548.002 / T1112 / T1567.002

預期驗證成果：

- 驗證EDR及SIEM能否準確偵測權限提升、資料外傳與勒索加密行為
- 評估資安團隊對勒索攻擊全流程的回應與復原能力
- 測試備份與還原流程的實用性與緊急應變效能

演練環境需求：

目標作業系統	Agent 需求	建議環境
Windows 10	需要（驗證端點行為）	windows/amd64

FIN7 | LockBit | Conti | Windows | DLP | Ransomware

BAS 劇本推薦

演練劇本推薦與原因

推薦方法論

本次劇本推薦以情資中高頻發生的TTP（如T1486、T1190、T1078等）為核心，結合組織目前外部攻擊面（RDP/Web端口、老舊系統、帳號管理）及產業特性，優先挑選可直接驗證關鍵防禦能力、對應活躍攻擊組織（LockBit、FIN7、Conti、APT41）的劇本，協助組織建立端到端、可量化的攻擊防禦驗證鏈路。

推薦劇本 1：[Playbook] 63002 - Data Leak Prevention and Ransomware

Endpoint / DataLeak / Internet

推薦理由：

- 直接對應T1486（Data Encrypted for Impact）與T1078（Valid Accounts），可完整驗證組織對勒索軟體攻擊全流程的檢測與應對能力
- 涵蓋多個高風險TTP（T1486、T1068、T1078、T1562.001），對應LockBit、Conti等活躍團體常用手法
- 適用於Windows環境，與組織現有IT架構及攻擊面發現高度吻合
- 可驗證EDR/NDR對於權限提升、資料外洩、檔案加密及防護工具繞過等行為的偵測反應

涵蓋攻擊技術（MITRE ATT&CK）：

T1486 – Data Encrypted for Impact | T1078 – Valid Accounts | T1562.001 – Impair Defenses | T1068 – Exploitation for Privilege Escalation | T1548.002 / T1112 / T1567.002

預期驗證成果：

- 驗證EDR及SIEM能否準確偵測權限提升、資料外傳與勒索加密行為
- 評估資安團隊對勒索攻擊全流程的回應與復原能力
- 測試備份與還原流程的實用性與緊急應變效能

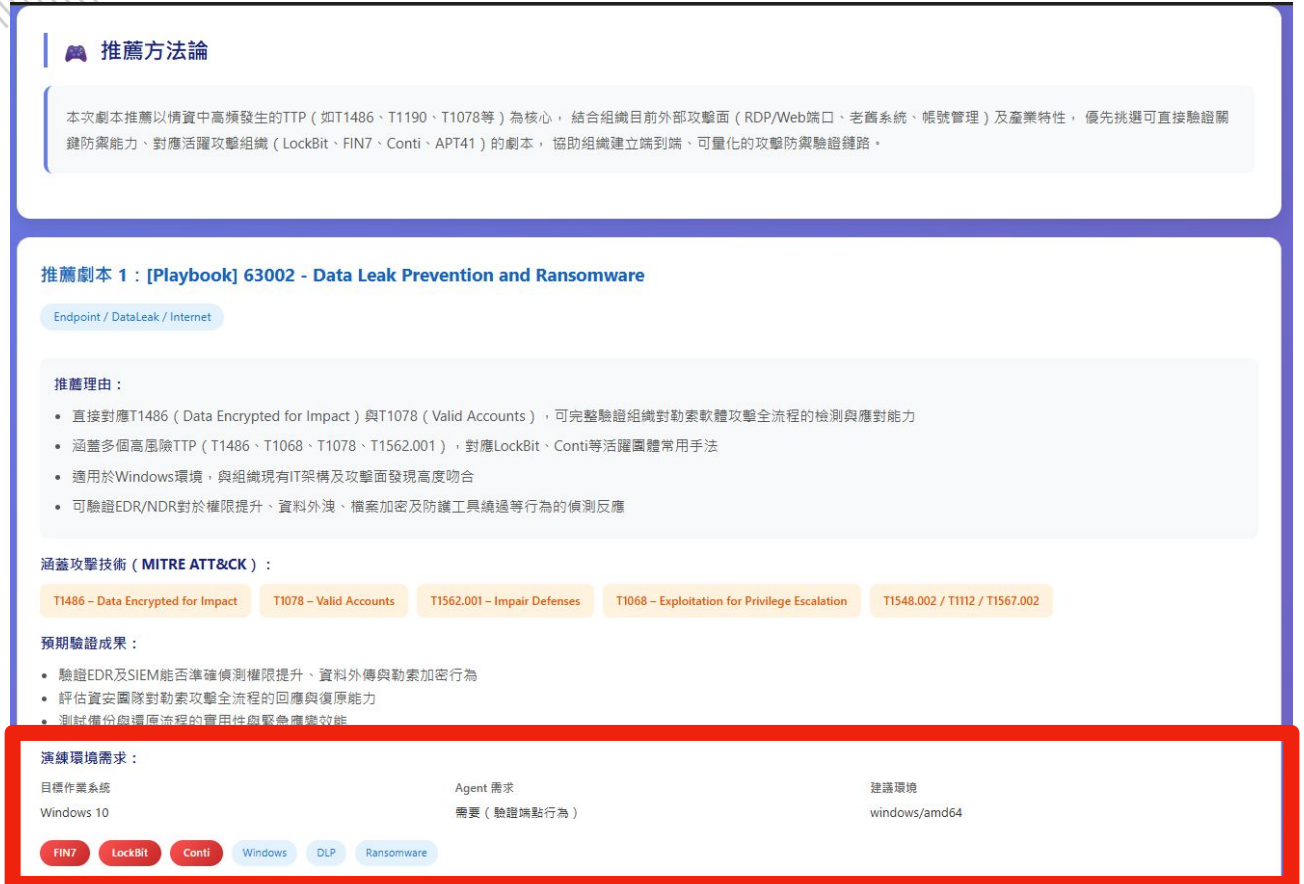
演練環境需求：

目標作業系統	Agent 需求	建議環境
Windows 10	需要（驗證端點行為）	windows/amd64

FIN7 | LockBit | Conti | Windows | DLP | Ransomware

BAS 劇本推薦

演練劇本推薦與原因



推薦方法論

本次劇本推薦以情資中高頻發生的TTP（如T1486、T1190、T1078等）為核心，結合組織目前外部攻擊面（RDP/Web端口、老舊系統、帳號管理）及產業特性，優先挑選可直接驗證關鍵防禦能力、對應活躍攻擊組織（LockBit、FIN7、Conti、APT41）的劇本，協助組織建立端到端、可量化的攻擊防禦驗證鏈路。

推薦劇本 1：[Playbook] 63002 - Data Leak Prevention and Ransomware

Endpoint / DataLeak / Internet

推薦理由：

- 直接對應T1486（Data Encrypted for Impact）與T1078（Valid Accounts），可完整驗證組織對勒索軟體攻擊全流程的檢測與應對能力
- 涵蓋多個高風險TTP（T1486、T1068、T1078、T1562.001），對應LockBit、Conti等活躍團體常用手法
- 適用於Windows環境，與組織現有IT架構及攻擊面發現高度吻合
- 可驗證EDR/NDR對於權限提升、資料外洩、檔案加密及防護工具繞過等行為的偵測反應

涵蓋攻擊技術（MITRE ATT&CK）：

T1486 – Data Encrypted for Impact | T1078 – Valid Accounts | T1562.001 – Impair Defenses | T1068 – Exploitation for Privilege Escalation | T1548.002 / T1112 / T1567.002

預期驗證成果：

- 驗證EDR及SIEM能否準確偵測權限提升、資料外傳與勒索加密行為
- 評估資安團隊對勒索攻擊全流程的回應與復原能力
- 測試備份與還原流程的實用性與緊急應變效能

演練環境需求：

目標作業系統	Agent 需求	建議環境
Windows 10	需要（驗證端點行為）	windows/amd64

FIN7 | LockBit | Conti | Windows | DLP | Ransomware

總結

核心優勢

- **技術性與實用性**
  - 成功串接、結合數個分散平台 、API 與工具
  - 模組化方式管理，方便 未來擴充、新增功能
  - 針對情資精確命中，同時 上傳統整資料進平台，以提供後續利用

- **創新性與完整性**
  - 自動化整合所有內容，關聯化分析資訊，以提高效率
  - 針對專業與非專業 人士都有對應策略
  - 降低專業人力需求
  - 資訊安全對企業來 說不再是負擔

針對 BAS 的核心優勢

- 擴充性
  - 加速推薦劇本流程
  - 制式化的標準流程
  - 與服務對象的高度關聯性
  - 降低使用門檻
  - 打造專案優規，實現產品加值

謝謝大家喵