



CyCraft AI Copilot

XCockpit：賦能企業資安事件應變能力的關鍵 AI 副駕

Derick Chung



Agenda

1

公司簡介

2

資安從業人員現況

3

賦能事件調查關鍵 AI 副駕

4

實際應用案例

關於奧義智慧科技



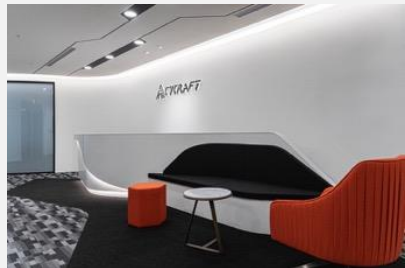
關於奧義智慧科技

> 人工智慧

奧義智慧是一家專注在 AI 自動化與資安韌性的新創企業。三位連續創業成功的創辦人在 2017 年所創辦，榮獲臺灣華威國際 (CID) 與新加坡淡馬錫 Pavilion Capital 基金的長期支持，團隊得以持續在人工智慧技術的研發保持領先，並受到 Gartner、IDC、與 Frost & Sullivan 等國際研調肯定。

> 客戶信賴

奧義智慧的使命是讓資安成為最有成就感的工作，領先將 AI 前瞻技術落實應用在資安實務工作，從端點偵測與回應、全球多元情資、網路流量過濾，到零信任架構，以及建構新一代 AI 資安戰情中心，協助穩健地實現高度資安韌性。奧義智慧很榮幸地獲得逾一百個政府機關、警政、國防單位，以及數十家金融機構、逾五十家高科技與關鍵領域龍頭企業的信賴，市佔率國內第一。



奧義智慧企業總部位於板橋亞東通訊園區，亞太區的營運中心設立在東京，並與日本日立集團緊密地合作國際拓展。

建置 7 x 24 AI SOC 全球資安脈動盡收眼底



2021.04

於美國設立子公司



2019.01

於日本設立子公司
CyCraft Japan



2017.07

奧義智慧科技
成立於臺灣



2019.11

於新加坡設立子公司
CyCraft Singapore

以臺灣自研技術，斬獲世界級肯定



Frost & Sullivan (2019)

《利用 CyCraft 的 CyCarrier AIR Platform 縮減數位鑑識所需之調查時長》(Reducing Digital Forensic Investigation Time with CyCraft's CyCarrier AIR Platform)

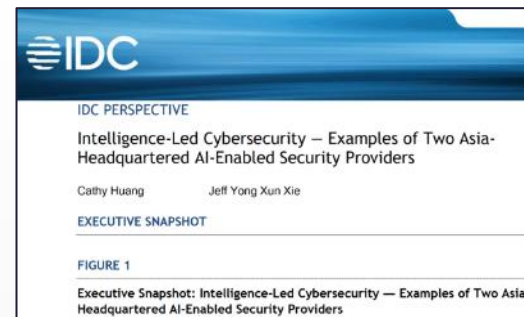
調查顯示奧義 AI 技術能降低 99% 的鑑識時間與 95% 的人力成本



Gartner (2021)

《大中華區 AI 新創公司指南》(Market Guide for AI Startups, Greater China)

資安公司唯一入選代表性企業案例



IDC Perspective (2021)

《智慧資安：以兩間總部位於亞洲的 AI 驅動資安公司為案例》(Intelligence-Led Cybersecurity — Examples of Two Asia-Headquartered AI-Enabled Security Providers)

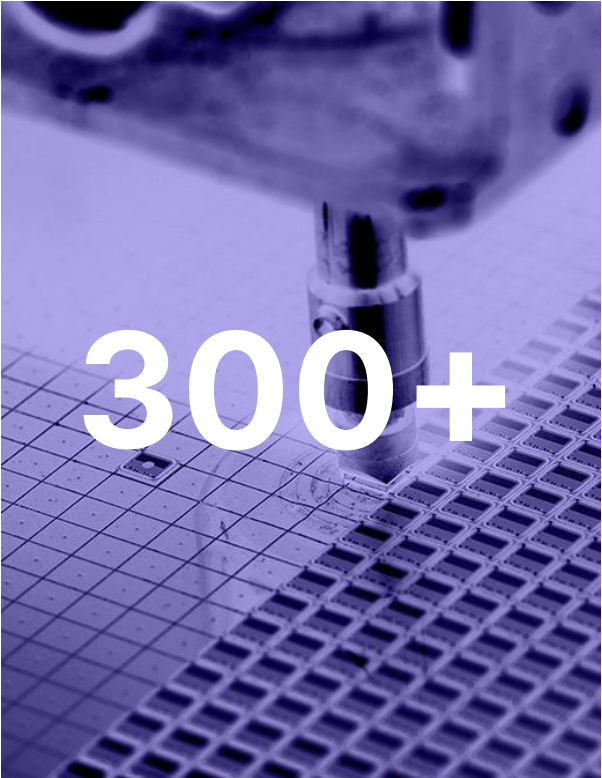
權威機構深入剖析奧義智慧技術優勢與市場實證



Gartner (2022)

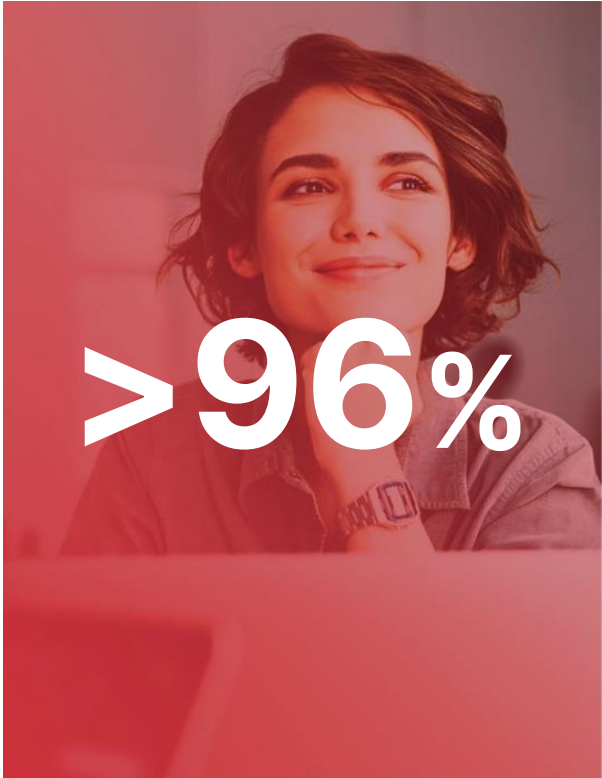
《新興科技：針對託管式偵測與回應的採用增長洞察報告》(Emerging Tech: Adoption Growth Insights for Managed Detection and Response)

頂尖研調機構認定比肩國際大廠的 MDR 服務商代表性範例



300+

各產業領域客戶
信賴採用



>96%

連續五年優異續約率



500,000+

即時監控端點



Gartner Peer
Insights



客戶評選五顆星的
MDR 解決方案

奧義國內用戶服務實績



政府公部門



金融業



高科技製造業



企業 (航空/電信)



軍警機關



教育單位



醫療單位

臺灣金融轉型兼顧 AI 與資安

奧義智慧榮獲首屆數位金融獎最佳金融科技新創公司



攜手SEMI 國際半導體產業協會
奧義智慧協防半導體供應鍊安全







Benson Wu • 1 度
 Craft FAST AI for a safer world!
 2 個月前 • 🌐

奧義智慧很榮幸地歡迎美國前太平洋陸戰隊指揮官、退役中將魯德 (Steven R. Rudder)、美台商會會長韓儒伯 (**Rupert Hammond-Chambers**) 以及美國國防產業代表們的蒞臨交流。兩小時的會議中，雙方熱烈討論 "Attention is all you need" 應用於資安紅藍攻防的實戰心得。現在是 AI 的大時代，奧義智慧新推出的 XCockpit 實現人機共駕，歡迎各位勞苦功高的資安從業人員朋友們，來下周的資安大會現場一睹為快！

美國 與 波蘭 參訪





CyCraft Technology
 1,117 人關注
 1 週前 • 🌐

Pioneering Taiwan-Poland Cybersecurity Collaboration

We are excited to announce that CyCraft has recently played a pivotal role in strengthening cybersecurity relations between Taiwan and Poland. Our advanced, AI-driven solutions were showcased to a visiting Polish delegation, emphasizing their capabilities to hasten threat detection and free up more time for strategic decision-making.

Notably, Poland expressed particular concern over state-sponsored APTs like APT29, leading to in-depth discussions about our eva ……展開

[查看翻譯](#)

 讚
  回應
  轉發
  傳送

全球最高技術指標2023黑帽大會

< 語言生成技術應用於資安調查領域 >



The screenshot displays the Black Hat USA 2023 website. The header includes the Black Hat logo, the event dates (August 5-10, 2023), and the location (Mandalay Bay / Las Vegas + Virtual). A navigation bar lists various sections: ATTEND, TRAININGS, BRIEFINGS, ARSENAL, FEATURES, SCHEDULE, BUSINESS HALL, SPONSORS, and PROPOSALS. A sidebar on the left contains links for ALL SESSIONS and SPEAKERS. The main content area features a session titled 'IRonMAN: InterpRetable Incident Inspector Based ON Large-Scale Language Model and Association miNing' by Sian-Yao Huang, Cheng-Lin Yang, and Chung-Kuan Chen. The session is a 40-minute briefing on AI, ML, and Data Science. The abstract discusses the challenges of contextual incident investigation and the potential of large-scale language models (LLMs) for improving incident response.

black hat
USA 2023

REGISTER NOW

AUGUST 5-10, 2023
MANDALAY BAY / LAS VEGAS
+ VIRTUAL

ATTEND ▾ TRAININGS ▾ BRIEFINGS ▾ ARSENAL ▾ FEATURES ▾ SCHEDULE ▾ BUSINESS HALL ▾ SPONSORS ▾ PROPOSALS ▾

All times are Pacific Time (GMT/UTC -7h)

ALL SESSIONS

SPEAKERS

IRonMAN: InterpRetable Incident Inspector Based ON Large-Scale Language Model and Association miNing

Sian-Yao Huang | Data Scientist, CyCraft Technology
Cheng-Lin Yang | Senior Data Science Architect, CyCraft Technology
Chung-Kuan Chen | Security Research Director, CyCraft Technology

Format: 40-Minute Briefings
Track: AI, ML, & Data Science

Contextual incident investigation and incident similarity assessment are crucial components of modern IR and proactive threat hunting strategies. However, current automated systems often rely on pattern- and heuristic-based approaches due to their reliability and competitive performance. These approaches lack the ability to correlate events with contextual information and are susceptible to evasion through slight variations, resulting in false alerts. Recent advances in large-scale language models (LLMs) have shown promising results in language representation. By adopting LLM embedding strategies for security incidents, contextual relationships and similarities of events can be modeled, leading to a reduced false alert rate. However, LLM-based approaches often lack interpretability, which is essential for security analysts.

In this work, we propose the first explainable LLM-based incident inspector. We combine a large-scale language embedding model with a frequent association algorithm to extract significant tokens, providing strong interpretability for incident similarity in feature space representation. Moreover, the contextual comprehension capabilities of the LLM ensure robustness against input variations. We demonstrate the practicality of our method in real-world incidents by applying it to our global visibility platform (200M+ events per day). The significant tokens generated by our model clearly identify the reasons why incidents are believed to stem from the same APT groups. Additionally, compare the results generated by our method to feedback from security analysts and thus provide different analytical perspectives for incident analysis.

In conclusion, our method seamlessly merges traditional incident response strategies with advanced data science techniques, enriching the information available to security analysts. Moreover, our method can be applied to incident similarity, attribution and archiving. Our work, along with the comparative analysis, serves as a catalyst for the development of even more robust and interpretable methods for incident analysis.

AI 正在改變你我的工作與生活

資安託管不該是血汗專家，奧義協助客戶享受AI驅動帶來的資安韌性



We' re also the innovation, XCOCKPIT, an AI threat intelligence combines EDR, SIEM. Powered by the Large Language Model, virtual analyst, threat analysis, and threat reducing MTTR, minutes.

[查看翻譯](#)





資安從業人員現況



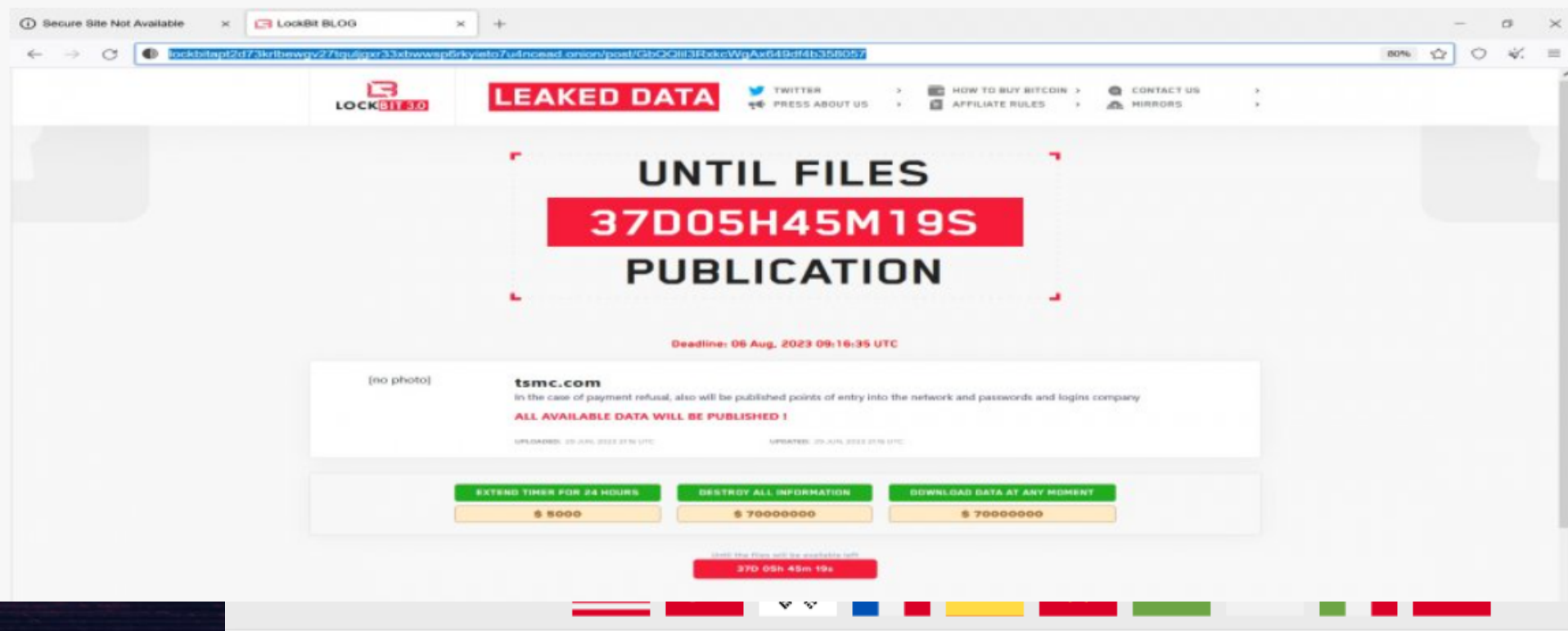
台積電供應商遭LockBit勒索7千萬美金，新版勒索即服務新增加價延長功能

LockBit是目前最活躍的勒索即服務（RaaS）供應商，此次是LockBit 3.0新版攻擊手法，新增受駭者可加價延長24小時的資料揭露時間

文/ 黃彥霖 | 2023-07-03 發表

讚 285

分享



Kubernetes Summit 2023
10/25 Wed - 10/26 Thu

盲鳥搶先開賣！

優惠價 NT\$ **1,990**/人

盲鳥優惠搶先卡位

8月21日 12:00 截止

Operations at Japan's Port of Nagoya resume, after probable LockBit ransomware attack

JULY 06, 2023



Ref:<https://industrialcyber.co/transport/operations-at-japans-port-of-nagoya-resume-after-probable-lockbit-ransomware-attack/>

法規與產業趨勢均朝向反應時效性進行優化規範

企業資安事件頻傳 金管會規定金融業須於30分鐘內通報

2023-02-23 20:34 聯合報／記者戴瑞瑤／台北即時報導



金管會今首度召開金融機構資安長聯繫會議，由金管會副主委邱淑貞主持。圖／金管會提供

金管銀合字第 11102734661 號令

金管會：
資安事件在 30 分鐘內通報

金管會：30 分鐘通報

資安法：知悉事件 1 小時通報

上市櫃資安事件未即時發重訊最
重罰 500 萬

上市櫃公司被要求資安治理 將有大量資安需求釋出



上市上櫃公司資通安全管控指引的篇章與條文

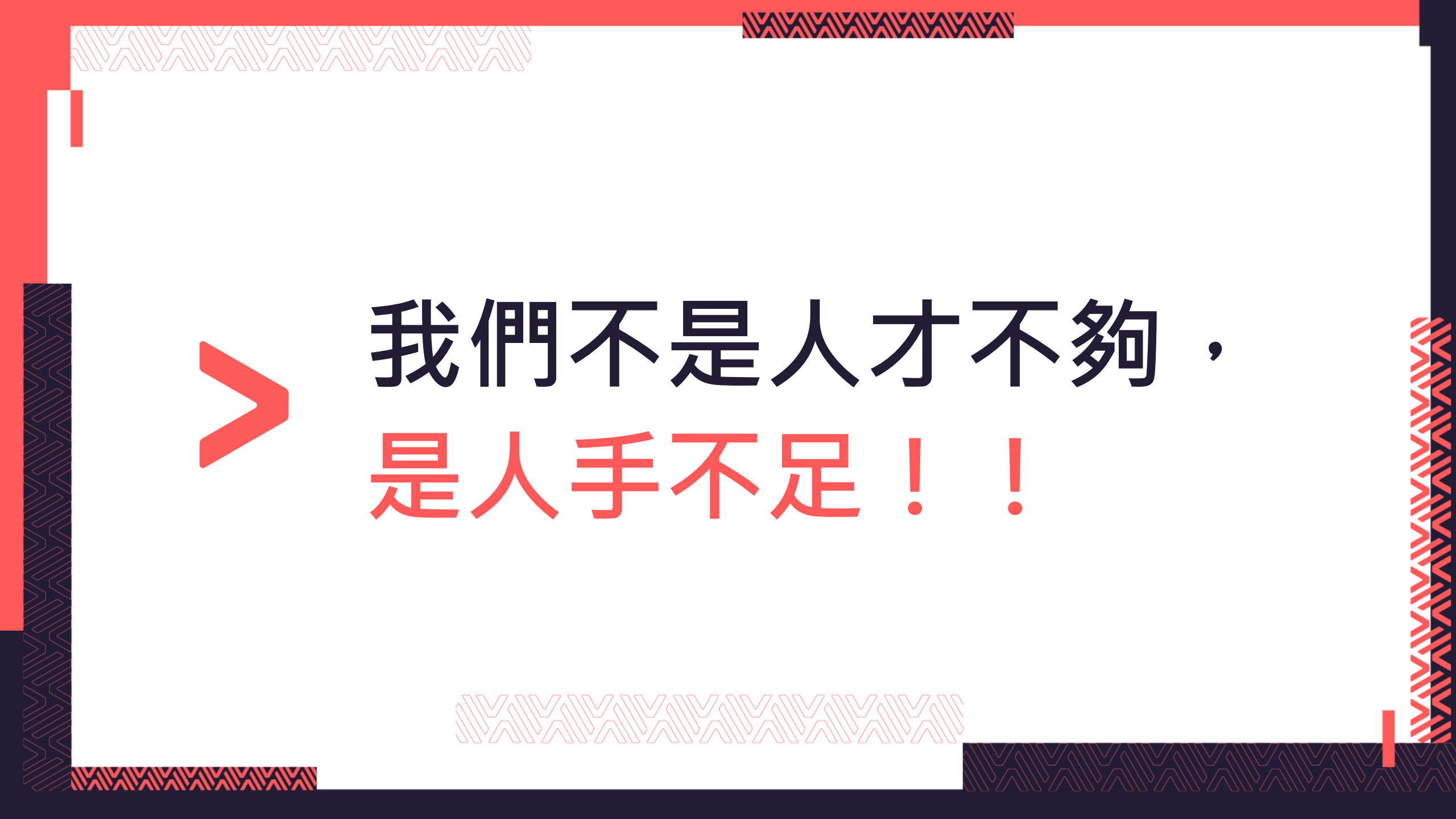
章節	章節名稱	條文數量
第一章	總則	2條
第二章	資通安全政策及推動組織	4條
第三章	核心業務及其重要性	4條
第四章	資通系統盤點及風險評估	2條
第五章	資通系統發展及維護安全	4條
第六章	資通安全防護及控制措施	12條
第七章	資通系統或資通服務委外辦理之管理措施	3條
第八章	資通安全事件通報應變及情資評估因應	3條
第九章	資通安全之持續精進及績效管理機制	2條
第十章	附則	1條

資料來源：臺灣證券交易所，2022年5月

推動上市櫃公司加入資通安全情資分享平臺

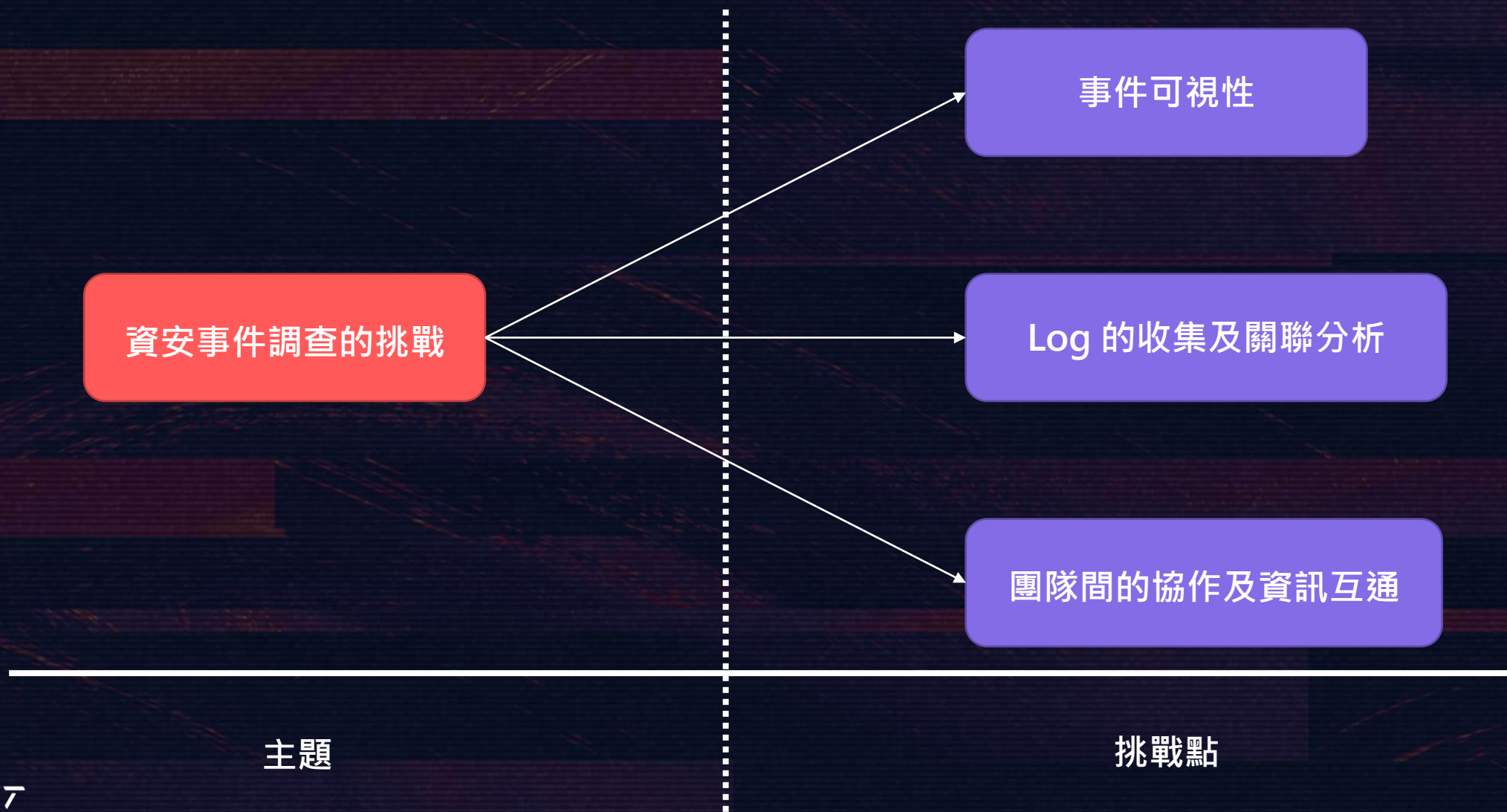
領域資安情資分享平臺	主管機關	可能參與的上市櫃產業
金融領域 (F-ISAC)	金管會	金融保險業
科技領域 (SP-ISAC)	科技部	電機機械、電器電纜、半導體業、電腦及週邊設備業、光電業、電子零組件業、電子通路業、資訊服務業、其他電子業
醫療領域 (H-ISAC)	衛福部	生技醫療業 (需為醫院)
能源領域 (E-ISAC)	經濟部	油電燃氣業
通訊領域 (C-ISAC)	NCC	通信網路業
交通領域 (T-ISAC)	交通部	航運業
TWCERT	NCC	未設參加限制，所有產業均得加入
第一級公司：2022上半年加入		
第二級公司：2022下半年到2023年底加入		
第三級公司：2024年底加入		

資料來源：臺灣證券交易所，iThome整理，2022年5月



> 我們不是人才不夠，
是人手不足！！

資安事件應變的挑戰



XCockpit AI 副駕賦能企業資安事件應變能力



挑戰點

奧義 XCockpit 提供的協助

攻擊著陸時及時偵測，
增加威脅可視性



案情解說，提升人員對資安事件
處理的能量

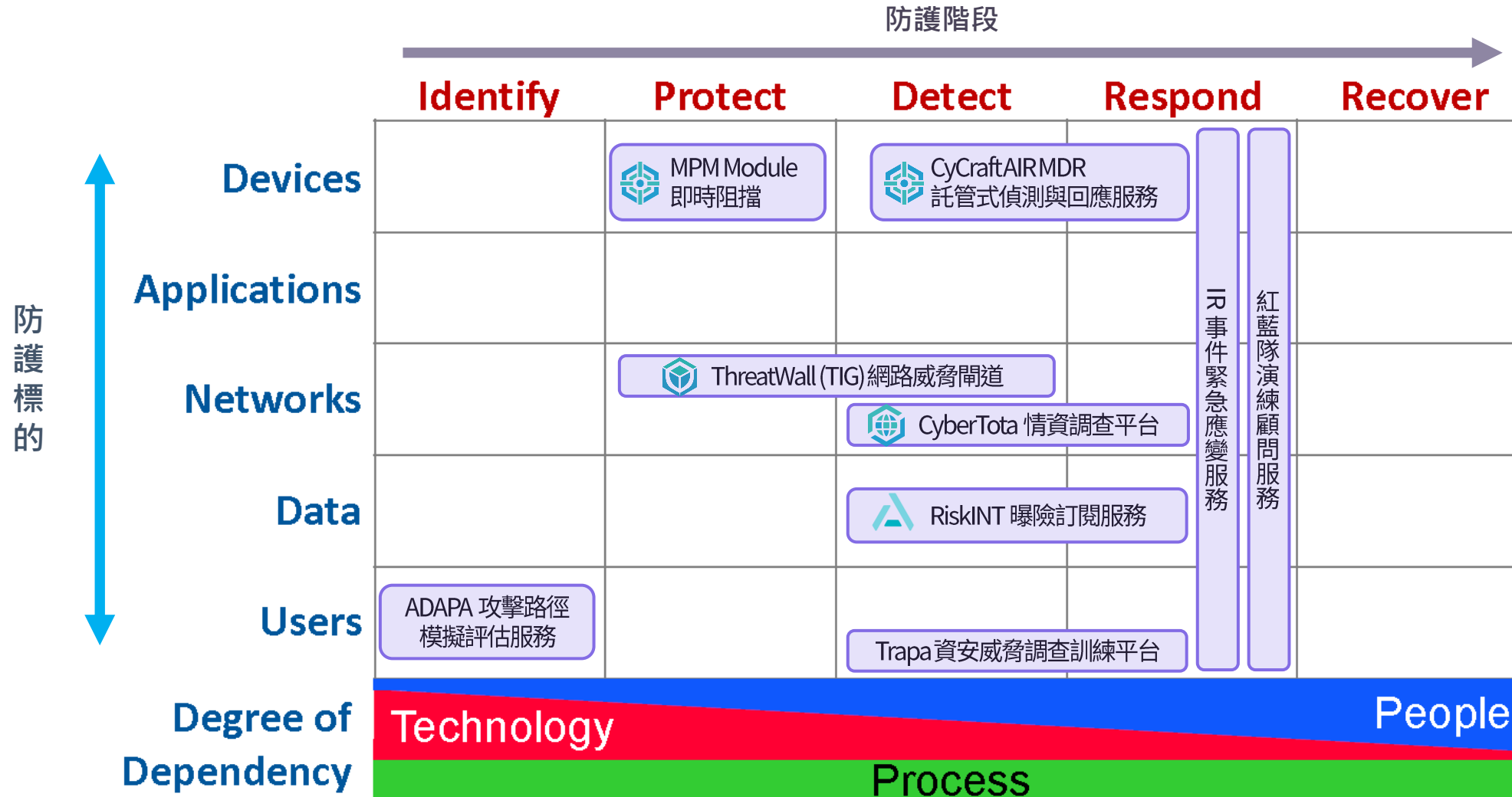
事件 log 自動比對關聯，
減輕人力的 log 拼湊時間



企業CDM框架應用實例

	事前		事中		事後
	辨識Identity	防禦Protect	偵測Detect	因應Respond	復原Recover
端點 Devices	防毒	AD身分認證 特權帳號管理	端點偵測及回應(EDR)		
應用程式 Applications	弱掃	網頁防串機制 網站應用程式防火牆(WAF)	釣魚網站及偽冒行動軟體偵測	資安情資關聯分析平台(SIEM)	異地備援機房
網路 Networks	威脅情資 惡意軟體防護	入侵防禦偵測 防火牆	分散式阻斷攻擊(DDos)防禦機制		
資料 Data	郵件防護/SandBox 內容淨化(CDR)	資料外洩防護(DLP) 資料加密機制	資料庫監控機制(DAM)		資料庫備份
人員 People	社交工程演練 資安教育訓練	導入安全資訊系統開發(SSDLC)	資安維運中心(SOC)	電腦事故應變小組(CIRT) 資安事故演練	備援演練
資安治理 Governance	資訊安全推動小組				
	資訊安全管理制度與內控制度				

奧義智慧資安服務應用於 CDM 框架



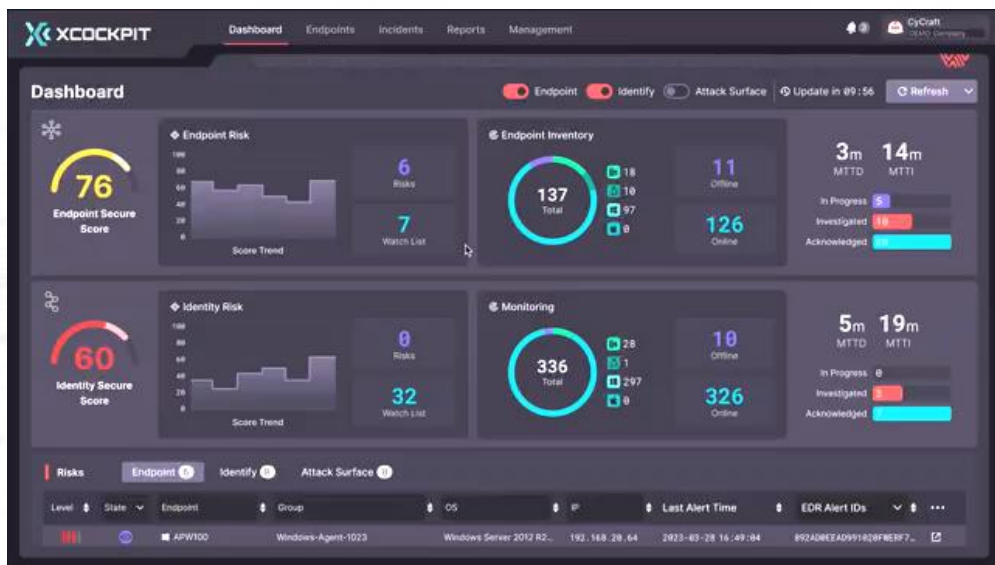
<https://owasp.org/www-project-cyber-defense-matrix/>

奧義智慧 AI 資安 全方位解決方案

類別	常態性服務 (年訂閱)	單次服務
端點 EDR/MDR	- AIR MDR 託管式偵測與回應 - XCockpit自動化資安威脅管理平台(MDR)	- 端點資安健診 - 政府合規 (GCB, VANS)、金融合規 (FCB)
網路 TIG	ThreatWall (TIG) 網路威脅閘道	網路流量資安健診
威脅調查 CTI	CyberTotal 情資調查平台	資安威脅案例研究 / 駭客族群追蹤研究
企業曝險 DarkWeb	- RiskINT 企業曝險監控訂閱 - XCockpit自動化資安威脅管理平台(EASM)*	RiskINT 企業曝險健診
AD安全	XCockpit自動化資安威脅管理平台(AD)*	ADAPA 攻擊路徑模擬評估
資安顧問		紅(藍)隊演練顧問
緊急事件 IR		IR 資安事件緊急應變
教育訓練	Trapa 資安威脅調查訓練平台	資安防禦框架 CDM 資安桌遊

XCockpit AI 賦能 事件調查關鍵副駕





> 全方位資安威脅監控

Comprehensive Threat Monitoring

EDR 端點威脅監控 + AD 特權帳號監控 + ASM 企業曝險監控

> 風險鑑別與營運指標量測

Risk Identification And Team Performance Metrics

整體風險等級評估，與資安團隊營運效率指標 MTTD / MTI

> 新世代 AI 虛擬分析師

AI-powered Virtual Analyst

整合 AI 自動分析、歸納與解說案情，降低人力成本，提高工作效率

> 全新視覺化資安介面

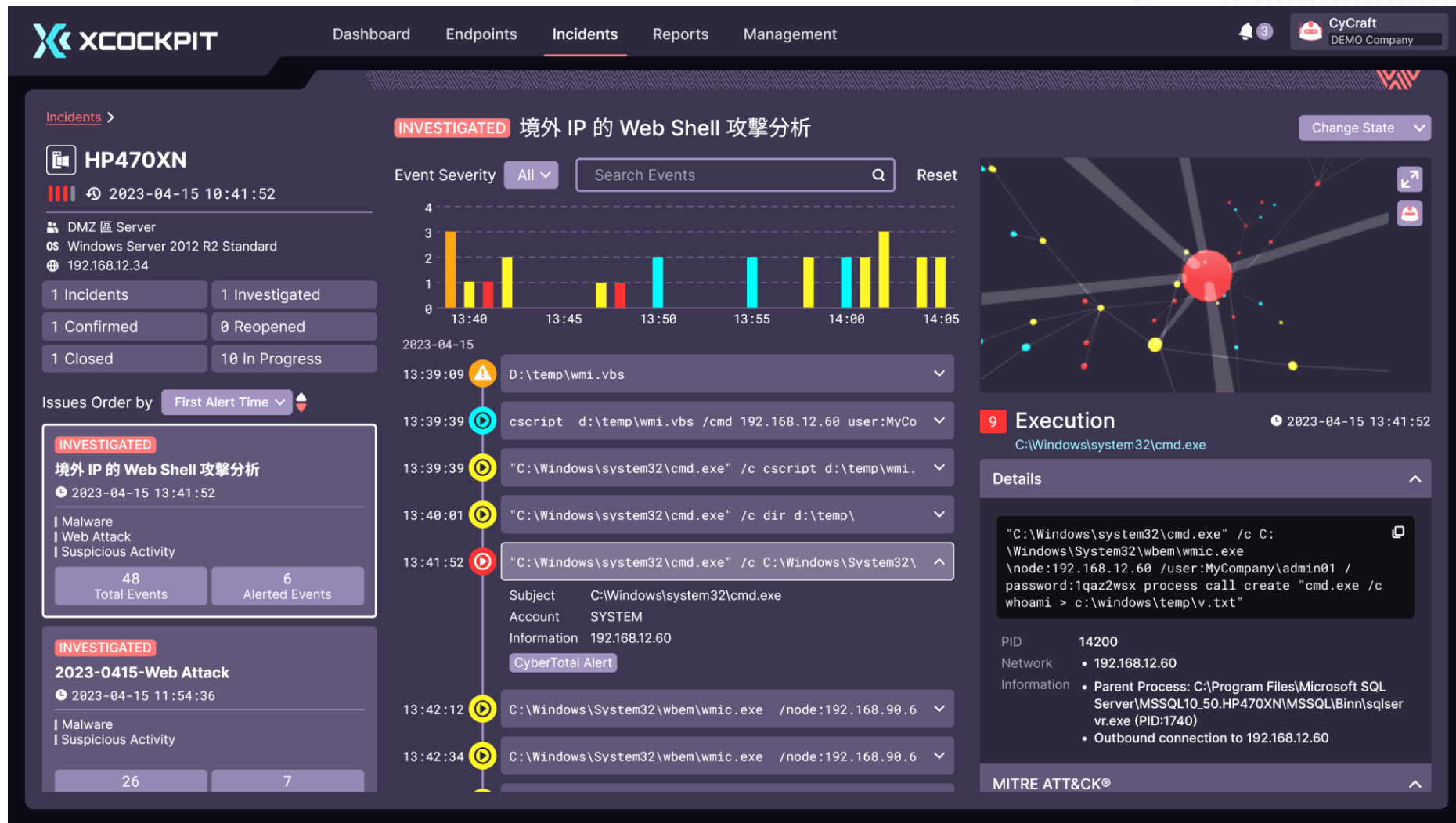
New Visualized Cybersecurity Dashboard

快速與簡潔介面，並提供各種資安營運報告、案情關聯分析報告

視覺化案情分析

Root Cause Analysis

- AI 助手自動處理從端點告警，關聯相關資訊、呈現攻擊案情、與根因分析 Root Cause，輔助分析師快速了解案情。



自動化案件管理

Automated Case Management

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

The screenshot displays the XCOCKPIT security dashboard, specifically the 'Incidents' section. The interface is dark-themed with a top navigation bar containing 'Dashboard', 'Endpoints', 'Incidents' (active), 'Reports', and 'Management'. On the right, there's a user profile for 'CyCraft DEMO Company' and a notification bell icon.

The main content area is titled 'Incidents' and shows '10 Search Results'. On the left, there's a sidebar with filters: 'Pinned Only' (toggle), 'Endpoint' (input), 'First Alert Start Time' (calendar), 'First Alert End Time' (calendar), 'Issue Name' (input), 'Alert ID' (input), 'States' (checkboxes for In Progress, Investigated, Reopened, Confirmed, Closed), and 'Attack Types' (checkbox for Ransomware).

The incident list is sorted by 'First Alert Time'. Each incident card displays the following information:

- Endpoint (e.g., HP470XN, HP1790I, DELL2311TN, PCC232, X201IT, MKT321T, OFFICE5022T)
- Status (e.g., INVESTIGATED, CONFIRMED, CLOSED)
- Title (e.g., 2023-0415-Web Attack, 2023-0415-Attacker Activity, 2023-0409-Malware, 2023-0404-Malware, 2023-0403-Malware, 2023-0402-Attacker Activity, 2023-0416-Malware)
- Timestamp (e.g., 2023-04-15 13:41:52, 2023-04-15 11:54:36, 2023-04-15 09:14:30, 2023-04-14 23:58:36, 2023-04-09 16:49:04, 2023-04-04 10:38:02, 2022-04-03 14:33:59, 2022-04-03 11:08:09, 2023-04-02 15:54:21, 2023-04-02 13:42:44)
- Tags (e.g., Malware, Web Attack, Suspicious Activity, Suspicious Process)
- Summary (e.g., 境外 IP 的 Web Shell 攻擊分析)
- Counts (Total Events, Alerted Events)

The bottom right corner of the dashboard features the CYCRAFT logo.

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。

The screenshot displays the XCOCKPIT Incident Viewer interface. The top navigation bar includes Dashboard, Endpoints, Incidents, Reports, and Management. The left sidebar shows a list of incidents, with the selected incident titled "HP470XN Server". The main content area is divided into two panels: "Incident Briefing" (highlighted with a yellow border) and "Execution".

Incident Briefing:

事件摘要：
在 DMZ 區的 HP470XN Server 上，AI 發現了高風險駭客活動。在 2023 年 4 月 15 日 13:41 至 14:16 之間，共發生 6 個事件。這些事件中的攻擊手法有 Web Shell 攻擊與系統憑證竊取，MITRE ATT&CK ID 包括 T1505.003、T1003.003。攻擊者使用了 CMD.EXE 和 SHTASKS 命令行進行攻擊活動，以提升其權限和建立後門。此外，攻擊者還竊取帳密資料庫 NTDS 檔案。應盡快處理這些攻擊，以避免更嚴重影響。

建議措施：
該主機上的帳號可能已被竊取，請確保其他電腦上沒有這些帳號的可疑活動。檢查是否有出現新的可疑檔案，HASH 是否與原始檔案匹配。檢查系統 NTDS 檔案是否受到保護，並注意可能後續發生的滲透攻擊 (Lateral Movement)。

Execution:

Details:

```
"C:\Windows\system32\cmd.exe" /c C:\Windows\System32\wbem\wmic.exe /node:192.168.12.60 /user:MyCompany\admin01 /password:1qaz2wsx process call create "cmd.exe /c whoami > c:\windows\temp\v.txt"
```

Information:

- PID: 14200
- Network: 192.168.12.60
- Information: Parent Process: C:\Program Files\Microsoft SQL Server\MSSQL10_50.HP470XN\MSSQL\Binn\sqlservr.exe (PID:1740)
- Outbound connection to 192.168.12.60

MITRE ATT&CK®

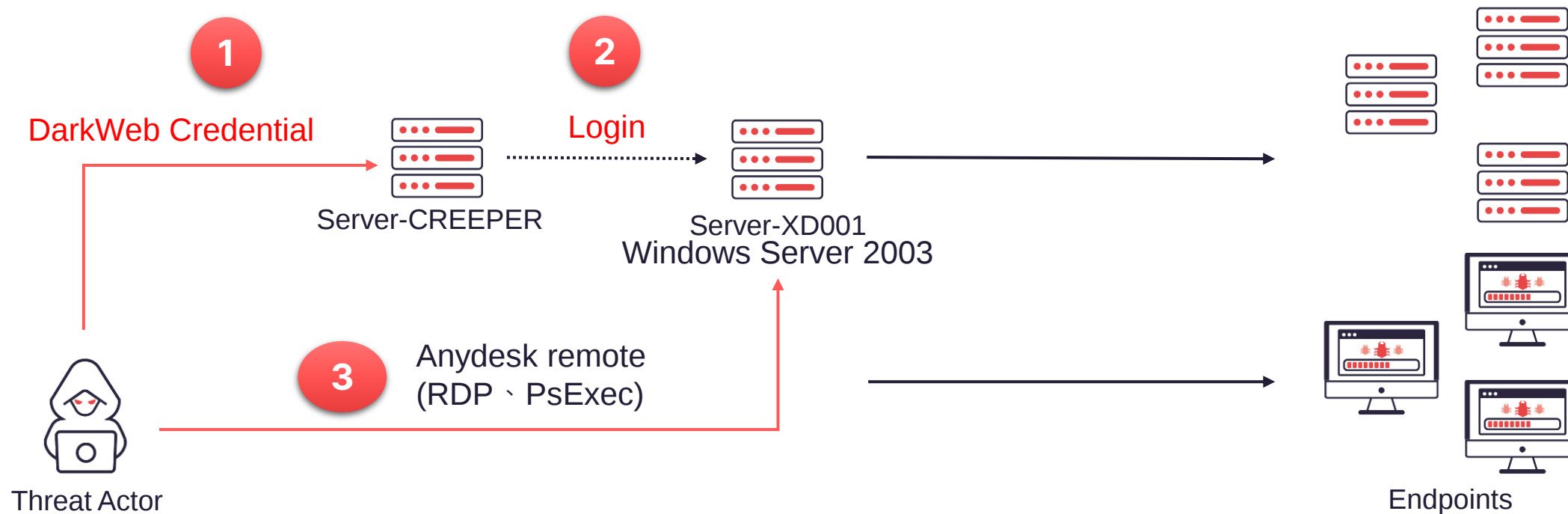
- T1027.000 Command-Line Interface
- T1053.005 Scheduled Task/Job: Scheduled Task
- T1505.003 Server Software Component: Web Shell

The interface also includes a "Close" button at the bottom right of the Execution panel.

實際應用案例



Lockbit 入侵攻擊

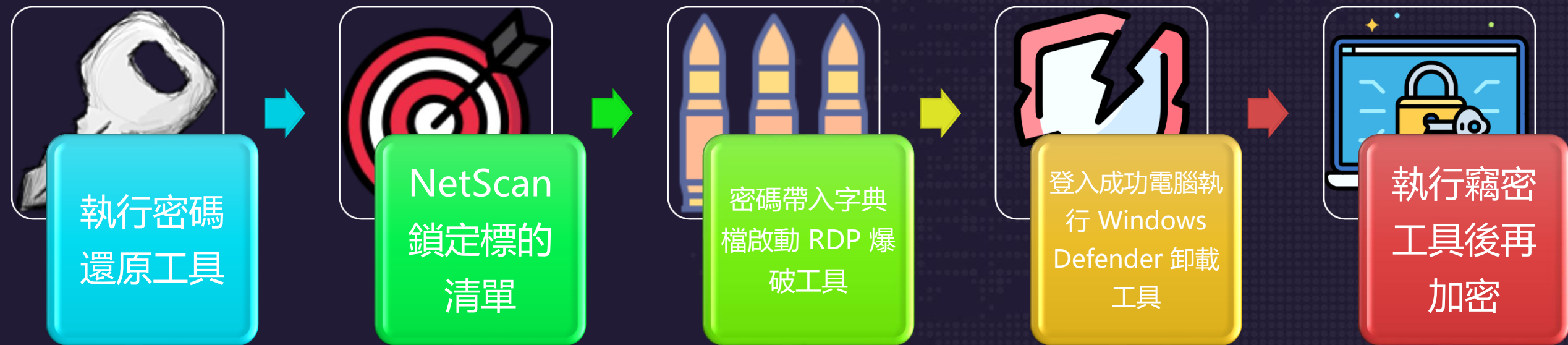


勒索軟體擴散混合技

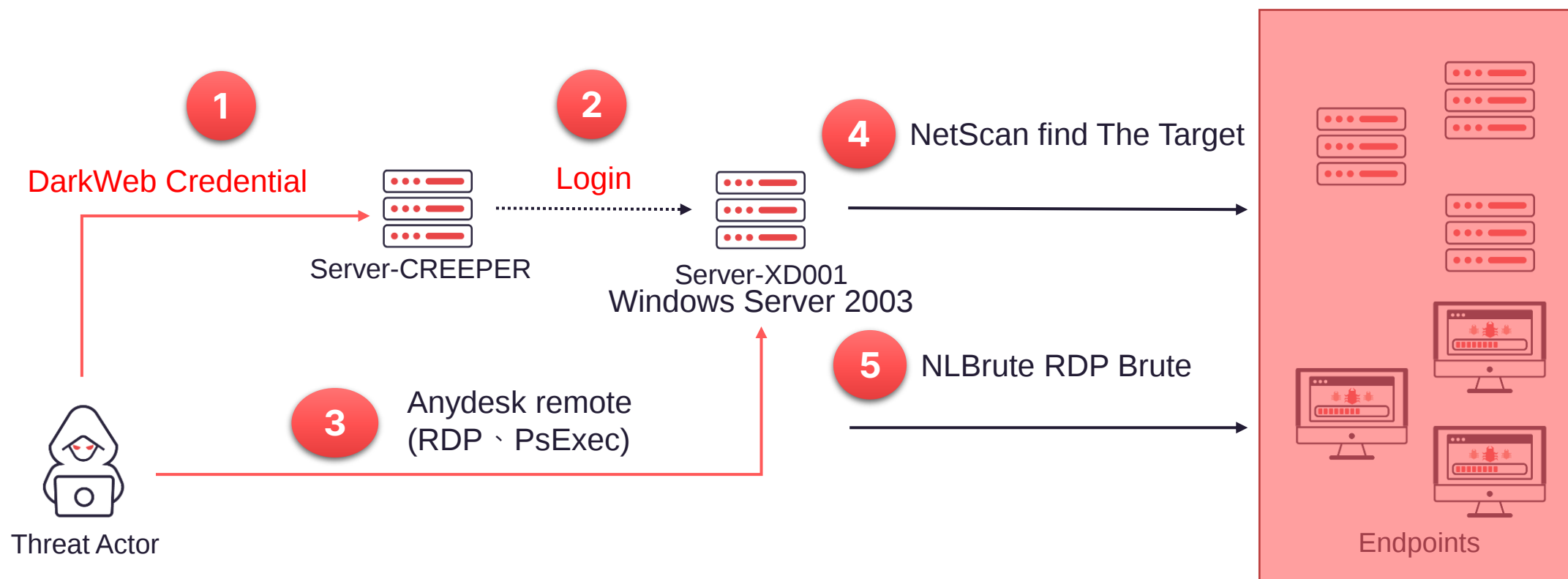
> 密碼竊取工具

- > Mimikatz 微軟 OS 層密碼竊取工具
- > BULLETPASSVIEW64.EXE 應用程式密碼竊取工具
- > MSPASS.EXE MSN 密碼竊取工具
- > DIALUPASS.EXE 網路連接程式密碼竊取工具
- > NETPASS.EXE 微軟服務密碼竊取工具
- > CHROMEPASS.EXE Chrome 瀏覽器密碼竊取工具
- > IEPV.EXE IE 瀏覽器密碼竊取工具
- > OPERAPASSVIEW.EXE opera 瀏覽器密碼竊取工具

勒索軟體擴散步驟



Lockbit 入侵攻擊手法



Incidents >

CREEPER

2023-05-17 16:33:12

CYCORP

OS Windows Server 2019 Datacenter 1809

192.168.41.14

6 Incidents

3 Investigated

0 Confirmed

0 Reopened

2 Closed

0 In Progress

Incidents Order by First Alert Time

INVESTIGATED

2023-0504-Malware

2023-05-04 12:06:20 (14m)

Malware
Attacker Activity
Suspicious Activity27
Total Events3
Alerted Events

CLOSED

2023-0504-Malware

2023-05-04 10:12:12

Suspicious Process
Malware
Attacker Activity
Suspicious Activity1
Total Events7
Alerted Events

MERGED

2023-0503-Suspicious Process

2023-05-03 15:57:07 (2m)

Suspicious Process
Malware
Attacker Activity
Suspicious Activity

INVESTIGATED 2023-0504-Malware

Change State

Event Severity

All

Search Events



Reset



2023-05-04

12:06:20

C:\WINDOWS\System32\rundll32.exe

Subject C:\Windows\SysWOW64\rundll32.exe

Account CREEPER

Information 192.168.41.19

COBALTSTRIKE.1

METASPLOIT.SH1

12:06:20

\127.0.0.1\ADMIN\$\3a008d3.exe

12:06:20

\127.0.0.1\ADMIN\$\3a008d3.exe

12:07:31

net user poweranger 1qaz!@WSX /ADD

12:07:31

C:\WINDOWS\system32\cmd.exe /_ poweranger 1qaz!@WSX /ADD

12:07:31

C:\WINDOWS\system32\net1 user poweranger 1qaz!@WSX /ADD

12:07:42

schtasks /Create /SC MINUTE /_ \Administrator\updater.d11"

12:15:49

C:\Windows\System32\WindowsP_YAKwAkAesAKQApAHwASQBFAFGA

12:16:15

"C:\WINDOWS\system32\cmd.exe" /c echo dump start

12:16:21

"C:\WINDOWS\system32\reg.exe" save HKLM\SAM sam.hiv

12:16:21

"C:\WINDOWS\System32\Windows_0A1ABzAGEAbQAUAGgAaQB2AA==



9 Execution

C:\Windows\SysWOW64\rundll32.exe

2023-05-04 12:06:20

Details

C:\WINDOWS\System32\rundll32.exe

PID 1732

Network 192.168.41.19

Malware COBALTSTRIKE.1

Information

- Parent Process:
 - \Device\Mup\127.0.0.1\ADMIN\$\3a008d3.exe (PID:972)
 - C:\WINDOWS\System32\rundll32.exe
- Analysis: NETWORK FUNCTIONS
- Directory: C:\USERS\ADMINISTRATOR
- Suspicious Code - 00043B0000
- Suspicious Code - 0003FB0000
- Analysis: REFLECTIVE CODE LOADING
- Analysis: THREAD FUNCTIONS
- Outbound connection to 192.168.41.19
- Suspicious Code - 0001260000
- Analysis: APT MALWARE

MITRE ATT&CK®

S0154 Cobalt Strike

Incidents >

INVESTIGATED 2023-0504-Malware

Change State



CREEPER

2023-05-17 16:33:12

CYCORP

Windows Server 2019 Datacenter 1809

192.168.41.14

6 Incidents

3 Investigated

0 Confirmed

0 Reopened

2 Closed

0 In Progress

Incidents Order by First Alert Time

INVESTIGATED

2023-0504-Malware

2023-05-04 12:06:20 (14m)

Malware
Attacker Activity
Suspicious Activity27
Total Events3
Alerted Events

CLOSED

2023-0504-Malware

2023-05-04 18:12:12

Suspicious Process
Malware
Attacker Activity
Suspicious Activity1
Total Events7
Alerted Events

MERGED

2023-0503-Suspicious Process

2023-05-03 15:57:07 (2m)

Suspicious Process
Malware
Attacker Activity
Suspicious Activity

Event Severity

All

Search Events



Reset



2023-05-04

12:06:20 C:\WINDOWS\System32\rundll32.exe

Subject C:\Windows\SysWOW64\rundll32.exe
Account CREEPER
Information 192.168.41.19

COBALTSTRIKE.1 METASPLOIT.SH1

12:06:20 \\127.0.0.1\ADMIN\$\3a008d3.exe

12:06:20 \\127.0.0.1\ADMIN\$\3a008d3.exe

12:07:31 net user poweranger 1qaz@WSX /ADD

12:07:31 C:\WINDOWS\system32\cmd.exe /_ poweranger 1qaz@WSX /ADD

12:07:31 C:\WINDOWS\system32\net1 user poweranger 1qaz@WSX /ADD

12:07:42 schtasks /Create /SC MINUTE /_ \Administrator\updater.dll

12:15:49 C:\Windows\System32\WindowsP_YAKwAkAEsAKQApAhWASQBFAFGa

12:16:15 "C:\WINDOWS\system32\cmd.exe" /c echo dump start

12:16:21 "C:\WINDOWS\system32\reg.exe" save HKLM\SAM sam.hiv

12:16:21 "C:\WINDOWS\System32\Windows... 0A1ABzAGEAbQAuAGgAaQB2AA==

總覽:

在 2023 年5月4日 12:06:20 至 12:16:21 期間，位於 "CYCORP" 群組中，名為 CREEPER 的主機上發生了以下高風險事件。在 12:06:20，關於攻擊技術的記錄包括使用 "CobaltStrike" 這種後滲透和橫向移動工具以及 "Metasploit" 這種惡意軟件執行檔 (Technique ID: T1003.000, OS Credential Dumping; T1550.000, Use Alternate Authentication Material; S0154, CobaltStrike, a post-exploitation and lateral movement tool; T1055.000, Process Injection. Malware: COBALTSTRIKE, METASPLOIT)。在 12:16:21，攻擊者使用指令 "powershell.exe" 和 "reg.exe" 來嘗試從快取憑據和安全帳戶管理器中獲取憑據 (Technique ID: T1003.005, OS Credential Dumping: Cached Domain Credentials; T1027.000, Obfuscated Files or Information; T1003.002, OS Credential Dumping: Security Account Manager)。

9 Execution

2023-05-04 12:06:20

C:\Windows\SysWOW64\rundll32.exe

Details

C:\WINDOWS\System32\rundll32.exe

PID 1732

Network 192.168.41.19

Malware COBALTSTRIKE.1

Information

- Parent Process: \Device\Mup\127.0.0.1\ADMIN\$\3a008d3.exe (PID:972)
- C:\WINDOWS\System32\rundll32.exe
- Analysis: NETWORK FUNCTIONS
- Directory: C:\USERS\ADMINISTRATOR
- Suspicious Code - 00043B0000
- Suspicious Code - 0003FB0000
- Analysis: REFLECTIVE CODE LOADING
- Analysis: THREAD FUNCTIONS
- Outbound connection to 192.168.41.19
- Suspicious Code - 0001260000
- Analysis: APT MALWARE

MITRE ATT&CK®

S0154 Cobalt Strike

Incidents >

CREEPER

2023-05-17 16:33:12

CYCORP

05 Windows Server 2019 Datacenter 1809

192.168.41.14

6 Incidents

3 Investigated

0 Confirmed

0 Reopened

2 Closed

0 In Progress

Incidents Order by

First Alert Time

INVESTIGATED

2023-0504-Malware

2023-05-04 12:06:28 (14m)

Malware

Attacker Activity

Suspicious Activity

27

Total Events

3

Alerted Events

CLOSED

2023-0504-Malware

2023-05-04 10:12:12

Suspicious Process

Suspicious Activity

Malware

Attacker Activity

1

Total Events

7

Alerted Events

MERGED

2023-0503-Suspicious Process

2023-05-03 15:57:07 (2m)

Suspicious Process

Suspicious Activity

Malware

Attacker Activity

INVESTIGATED 2023-0504-Malware

Change State

Event Severity

All

Search Events

Q

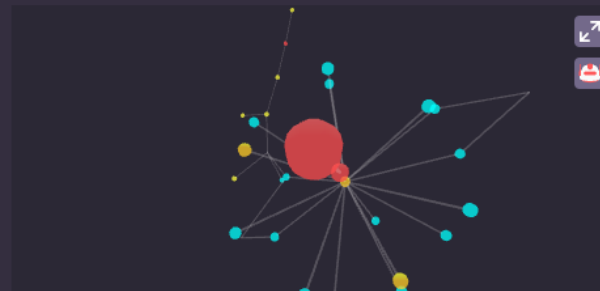
Reset



COBALTSTRIKE.1 METASPLOIT.SH1

- 12:06:20 \127.0.0.1\ADMIN\$\3a008d3.exe
- 12:06:20 \127.0.0.1\ADMIN\$\3a008d3.exe
- 12:07:31 net user poweranger 1qaz!@WSX /ADD
- 12:07:31 C:\WINDOWS\system32\cmd.exe /_ poweranger 1qaz!@WSX /ADD
- 12:07:31 C:\WINDOWS\system32\net1 user poweranger 1qaz!@WSX /ADD
- 12:07:42 schtasks /Create /SC MINUTE /_ \Administrator\updater.dll
- 12:15:49 C:\Windows\System32\WindowsP_YAKwAkAeSAKQApAHwASQBFAFgA
- 12:16:15 "C:\WINDOWS\system32\cmd.exe" /c echo dump start
- 12:16:21 "C:\WINDOWS\system32\reg.exe" save HKLM\SAM sam.hiv
- 12:16:21 "C:\WINDOWS\System32\Windows_0AIBzAGEAbQAuAGgAaQB2AA==
- 12:16:27 "C:\WINDOWS\system32\cmd.exe" /c echo T1145-1 start

Subject C:\Windows\System32\reg.exe
Account ADMINISTRATOR



9 Execution

2023-05-04 12:16:21

C:\Windows\System32\reg.exe

Details

"C:\WINDOWS\system32\reg.exe" save HKLM\SAM sam.hiv

PID 4832

SID S-1-5-21-3188494444-2937684683-888728269-500

Information • Parent Process:
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe (PID:900)

MITRE ATT&CK®

- T1003.002 OS Credential Dumping: Security Account Manager
- T1003.005 OS Credential Dumping: Cached Domain Credentials
- T1059.001 Command and Scripting Interpreter: PowerShell

Incidents >



CREEPER

2023-05-17 16:33:12

CYCORP

OS Windows Server 2019 Datacenter 1809

192.168.41.14

6 Incidents

3 Investigated

0 Confirmed

0 Reopened

2 Closed

0 In Progress

Incidents Order by

First Alert Time

INVESTIGATED

2023-0504-Malware

2023-05-04 12:06:20 (14m)

Malware

Attacker Activity

Suspicious Activity

27

Total Events

3

Alerted Events

CLOSED

2023-0504-Malware

2023-05-04 10:12:12

Suspicious Process

Suspicious Activity

Malware

Attacker Activity

1

Total Events

7

Alerted Events

MERGED

2023-0503-Suspicious Process

2023-05-03 15:57:07 (2m)

Suspicious Process

Suspicious Activity

Malware

Attacker Activity

INVESTIGATED 2023-0504-Malware

Change State

Event Severity

All

Search Events



Reset



COBALTSTRIKE.1 METASPLOIT.SH1

- 12:06:20 \127.0.0.1\ADMIN\$\3a008d3.exe
- 12:06:20 \127.0.0.1\ADMIN\$\3a008d3.exe
- 12:07:31 net user poweranger 1qaz!@WSX /ADD
- 12:07:31 C:\WINDOWS\system32\cmd.exe /_ poweranger 1qaz!@WSX /ADD
- 12:07:31 C:\WINDOWS\system32\net1 user poweranger 1qaz!@WSX /ADD
- 12:07:42 schtasks /Create /SC MINUTE /_ \Administrator\updater.dll
- 12:15:49 C:\Windows\System32\WindowsP_YAKwAkAEsAKQApAHwASQBFAFGA
- 12:16:15 "C:\WINDOWS\system32\cmd.exe" /c echo dump start
- 12:16:21 "C:\WINDOWS\system32\reg.exe" save HKLM\SAM sam.hiv
- 12:16:21 "C:\WINDOWS\System32\Windows_0AIBzAGEAbQAUAGgAaQB2AA==
- 12:16:27 "C:\WINDOWS\system32\cmd.exe" /c echo T1145-1 start

Subject C:\Windows\System32\reg.exe
Account ADMINISTRATOR

總覽:

在 2023 年 5 月 4 日 12:06:20 至 12:16:21 期間，位於 "CYCORP" 群組中，名為 CREEPER 的主機上發生了以下高風險事件。在 12:06:20，關於攻擊技術的記錄包括使用 "CobaltStrike" 這種後滲透和橫向移動工具以及 "Metasploit" 這種惡意軟件執行檔 (Technique ID: T1003.000, OS Credential Dumping; T1550.000, Use Alternate Authentication Material; S0154, CobaltStrike, a post-exploitation and lateral movement tool; T1055.000, Process Injection. Malware: COBALTSTRIKE, METASPLOIT)。在 12:16:21，攻擊者使用指令 "powershell.exe" 和 "reg.exe" 來嘗試從快取憑據和安全帳戶管理器中獲取憑據 (Technique ID: T1003.005, OS Credential Dumping: Cached Domain Credentials; T1027.000, Obfuscated Files or Information; T1003.002, OS Credential Dumping: Security Account Manager)。

9 Execution

2023-05-04 12:16:21

C:\Windows\System32\reg.exe

Details

"C:\WINDOWS\system32\reg.exe" save HKLM\SAM sam.hiv

PID 4832

SID S-1-5-21-3188494444-2937684683-888728269-500

Information

Parent Process:

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe (PID:900)

MITRE ATT&CK®

- T1003.002 OS Credential Dumping: Security Account Manager
- T1003.005 OS Credential Dumping: Cached Domain Credentials
- T1059.001 Command and Scripting Interpreter: PowerShell

X

XCockpit

Dashboard

Endpoints

Incidents

Reports

8

BetaMe

AI-SOC-DEMO

Incidents >

CREEPER

2023-05-17

CYCORP

OS Windows Server 2019

192.168.41.14

6 Incidents

0 Confirmed

2 Closed

Incidents Order by

INVESTIGATED

2023-0504-Malware

2023-05-04 12:06

Malware

Attacker Activity

Suspicious Activity

27

Total Events

CLOSED

2023-0504-Malware

2023-05-04 18:12

Suspicious Process

Malware

Attacker Activity

1

Total Events

MERGED

2023-0503-Suspicious

2023-05-03 15:57:07 (2m)

Suspicious Process

Suspicious Activity

Malware

Attacker Activity

2023-0504-Malware - Incident Viewer

Event Graph

Incident Briefing

Note

Switch to 2D Graph

總覽：

在 2023 年5月4日 12:06:20 至 12:16:21 期間，位於 "CYCORP" 群組中，名為 CREEPER 的主機上發生了以下高風險事件。在 12:06:20，關於攻擊技術的記錄包括使用 "CobaltStrike" 這種後滲透和橫向移動工具以及 "Metasploit" 這種惡意軟件執行檔（Technique ID: T1003.000, OS Credential Dumping; T1550.000, Use Alternate Authentication Material; S0154, CobaltStrike, a post-exploitation and lateral movement tool; T1055.000, Process Injection. Malware: COBALTSTRIKE, METASPLOIT）。在 12:16:21，攻擊者使用指令 "powershell.exe" 和 "reg.exe" 來嘗試從快取域憑據和安全帳戶管理器中獲取憑據（Technique ID: T1003.005, OS Credential Dumping: Cached Domain Credentials; T1027.000, Obfuscated Files or Information; T1003.002, OS Credential Dumping: Security Account Manager）。

建議：

根據這些攻擊技術和攻擊者的行為，建議採取以下措施：

1.加強端點安全措施。更新所有的操作系統和應用程式，禁用不必要的服務。

2.建立日誌，使得能夠追蹤所有重要登錄活動，並監測任何檔案的下載和執行，以及所有的網絡流量。

3.立即進行調查，並隔離受到影響的端點。在進行調查和清除受影響的機器之前，不要在您的網絡中更改密碼。

4.從快取中清除所有的帳戶憑據，並在您的網絡中更新所有的密碼，以及強化你的身份驗證機制。

The above analysis summary is automatically generated by a virtual analyst AI model and is for reference only. The generated content may be incomplete or incorrect. For a complete analysis of the case, please

9 Execution

2023-05-04 12:16:21

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Details

"C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe" -noP -sta -w 1 -enc UgB1AGcALgB1AHgAZQAgAHMAYQB2AGUAIABIAEsATABNAFwAUwBBAE0AIABzAGEAbQAuAGgAaQB2AA==

PID900

SIDS-1-5-21-3188494444-2937684683-888728269-500

Information

Parent Process:C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe (PID:4332)

MITRE ATT&CK®

T1003.002

OS Credential Dumping: Security Account Manager

T1003.005

OS Credential Dumping: Cached Domain Credentials

T1027.000

Obfuscated Files or Information

T1059.001

Command and Scripting Interpreter: PowerShell

Change State

用不必要的服務。

檔案的下載和執行，

除受影響的機器之

的密碼，以及強化你

ed by a virtual

ed content may be

case, please

2023-05-04 12:16:21

powershell.exe

0\powershell.

ABNAFwAUwBBAE0

38728269-500

verShell\v1.0\powersh

unt Manager

in Credentials

Close

12:17:59

"C:\WINDOWS\system32\cmd.exe" /c echo T1098-1 finished

12:18:04

"C:\WINDOWS\system32\cmd.exe" /c echo T1084-1 start

CYCRRAFT

MPM 模組即時隔離 Lockbit 勒索軟體

The screenshot displays the XCOCKPIT security dashboard. The top navigation bar includes 'Dashboard', 'Endpoints', 'Incidents' (active), 'Reports', and 'Management'. A user profile 'jason.lin@cyca... AI-SOC-DEMO' is in the top right. The left sidebar shows 'Incidents >' with a 'RANSOM' icon, a date filter '2023-07-11', and a list of incidents: 'LockME', 'OS Windows 10 Pro', and '10.50.34.132'. Below this are filters for '2 Incidents', '0 Confirmed', and '0 Closed'. The main area is titled 'Event Details' and shows a 'Threat Activity' event (ID 9) from '2023-07-11 13:41:54'. The event details include: 'C:\Users\xuser\Desktop\Lockbit3.exe (HAS BEEN QUARANTINED)', 'PID 800', 'Account XUSER', 'Malware TROJAN.RANSOM.BLACKMATTER.H', and 'Hash 03B14473EEF5B7E38D9A5041C1AF0A76'. The 'Information' section lists: 'Triggered Process: C:\Windows\explorer.exe (PID:800)', 'This file has been successfully quarantined!', 'File Size: 162 KB', and 'Source: Malware Protection'. A 'Close' button is visible. The bottom status bar shows '13:41:54' and a warning icon. The bottom right corner features the CYCRAFT logo.

XCOCKPIT Dashboard Endpoints Incidents Reports Management 3647 jason.lin@cyca... AI-SOC-DEMO

Incidents > **RANSOM** 2023-07-11

LockME
OS Windows 10 Pro
10.50.34.132

2 Incidents
0 Confirmed
0 Closed

Incidents Order by

INVESTIGATED

2023-0711-Ran
2023-07-11

1 Ransomware
1 Malware

6 Total Events 4 Alerted Events

Event Details

9 Threat Activity 2023-07-11 13:41:54

C:\Users\xuser\Desktop\Lockbit3.exe (HAS BEEN QUARANTINED)

PID 800
Account XUSER
Malware TROJAN.RANSOM.BLACKMATTER.H
Hash 03B14473EEF5B7E38D9A5041C1AF0A76

Information

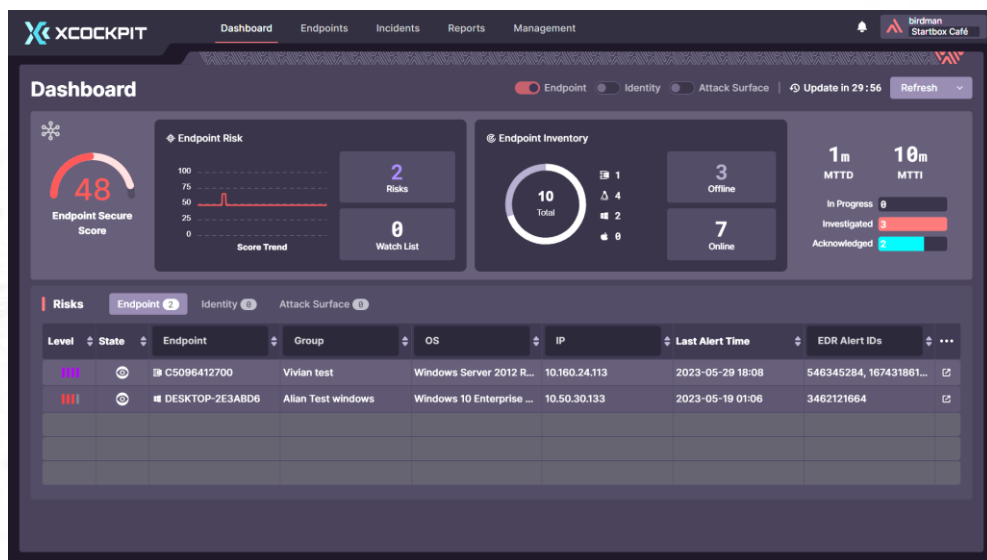
- Triggered Process: C:\Windows\explorer.exe (PID:800)
- This file has been successfully quarantined!
- File Size: 162 KB
- Source: Malware Protection

Close

13:41:54 C:\Users\xuser\Desktop\Lockbit3.exe (HAS BEEN QUARANTINED)

Information

- Triggered Process: C:\Windows\explorer.exe (PID:800)



攻擊威脅偵測
(EDR+AD)

即時 (1秒)

告警建單時間
(MTTD)

平均 3 分鐘

案情調查時間
(MTTI)

平均 15 分鐘

> Enhance Analyst Productivity

優化分析師效率，提高其工作效能和產出能力

> Expand Team Capability

擴大團隊能力，提高團隊整體效能和生產力

> Streamline Workflow Processes

精簡工作流程，提高分析師的工作效率

Fast / Accurate / Simple / Thorough



快速 F

Fast / Accurate / Simple / Thorough



A 精確

簡潔 S
Brand



Fast / Accurate / Simple / Thorough

T 全貌
Value



Fast / Accurate / Simple / Thorough