

# AI 資安現況與未來發展趨勢



Willy Lee  
Partner Business Development Manager  
0928-807-913  
willy.lee@cycraft.com



# 奧義智慧戰略事業群

## **Business Development**

---

**Denis Liang**

TW Business Development Director , Cross Industry

**Wendy Su**

Business Development Manager, Finance Sector

**Lori Luo**

Business Development Manager, Public Sector

**Shirley Wang**

Business Development Director, Public Sector

**Steven Kao**

Business Development Director, Hi-Tech Manufacturing Sector

**Harry Tsai**

Business Development Assistant Manager, Hi-Tech Manufacturing Sector

**Fion Lin**

Business Development Assistant Manager, CMR

## **Architecture Consultant**

---

**Perry Hsu**

Director, Architecture Consultant

**Vinci Tu**

Architecture Consultant

## **Partner Business Development**

---

**Willy Lee**

Partner Business Development Manager

**\* Customer Success**

---

**Technical Support**

**Project Management**



回想看看...

您資安團隊的績效是甚麼？

## KPI：漏洞修補數量

每年超過一萬個需修補的漏洞

根據 Flashpoint 報告，2023年揭露的漏洞超過 3.3 萬個，其中超過一半(52%) CVSS 得分為高至嚴重 (7.0-10.0)

## KPI：告警處理數量

每天超過五千個威脅警報

55%的資安人員表示每天超過 5千個警報，大型機構的人表示每天會接收超過 10 萬個警報。而且 99% 都是誤判！

如果每件事都是一樣優先，代表我們不知道哪個重要

# 運用CDM框架協助產品選擇

## Cyber Defense Matrix

	Identify 識別	Protect 保護	Detect 偵測	Respond 應變	Recover 復原
	<事前>		<事中>		<事後>
Devices 裝置					
Applications 應用程式	找出	保護	偵測	緊急	恢復
Networks 網路	出	護	測	急	復
Data 資料	弱	弱	破	應	還
Users 用戶	點	點	口	變	原
Degree of Dependency 相依性	Technology 科技			People 人員	
	Process 程序				

# 資安需求(情境)套用到各類別

Cyber Defense Matrix

	Identify 識別	Protect 保護	Detect 偵測	Respond 應變	Recover 復原
<b>Devices</b> 裝置	盤點硬體	電腦防毒	裝置異常	裝置隔離	備援主機
<b>Applications</b> 應用程式	盤點軟體	應用防火牆	軟體異常	軟體修補	備援容器
<b>Networks</b> 網路	盤點網段	網路防火牆	傳輸異常	網段隔離	異地備援
<b>Data</b> 資料	盤點資料	防資料外洩	資料異常	資料封存	資料備份
<b>Users</b> 用戶	盤點帳號	特權管理	權限異常	帳號凍結	AD備份
<b>Degree of Dependency</b> 相依性	Technology 科技				People 人員
	Process 程序				

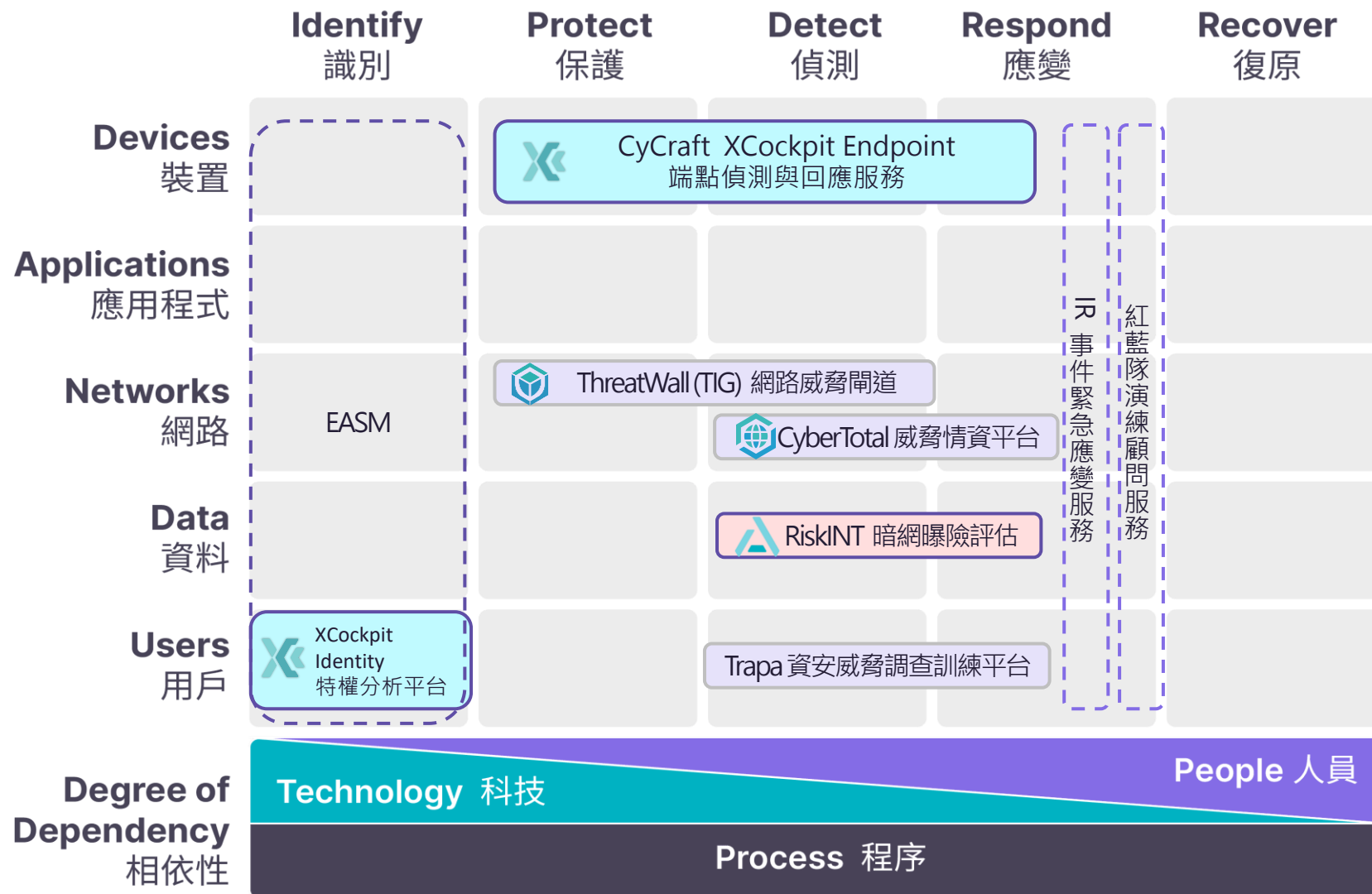
# 資安產品分類套用到各類別

## Cyber Defense Matrix

	Identify 識別	Protect 保護	Detect 偵測	Respond 應變	Recover 復原
<b>Devices</b> 裝置	Asset Mgt, Vuln Scanning, Vuln Mgt, Certificate Mgt	AV, Anti-Malware, EPP, FIM, HIPS, Vuln Mitigation, Allowlisting	Endpoint Detection, UEBA, XDR	EP Response, EP Forensics, SOAR	Restore
<b>Applications</b> 應用程式	SAST, DAST, SW Asset Mgt, Fuzzers, Bug Bounty	RASP, WAF, ASOC, ZT App Access, API Security	Source Code Compromise, Logic Bomb Discovery, App IDS, XDR		
<b>Networks</b> 網路	Netflow, Network Vuln Scanner	FW, IPS/IDS, Microseg, ESG, SWG, ZTNA	DDoS Detection, Net Traf Analysis, UEBA, XDR	DDoS Response, NW Forensics, SOAR	
<b>Data</b> 資料	Data Audit, Discovery, Classification	Encryption, Tokenization, DLP, DRM, DBAM, DB Access Proxy	Deep Web, Data Behavior Analytics, FBI, Brian Krebs, XDR	DRM, Breach Response	Backup
<b>Users</b> 用戶	Phishing Sim, Background Chk, MFA, Human Risk Mgt	Sec Awareness & Training, Adaptive People Protection	Insider Threat, User Behavior Analytics, XDR, Human Det & Resp		
<b>Degree of Dependency</b> 相依性	Technology 科技			People 人員	
	Process 程序				

# 奧義智慧產品對應 CDM 框架

## Cyber Defense Matrix



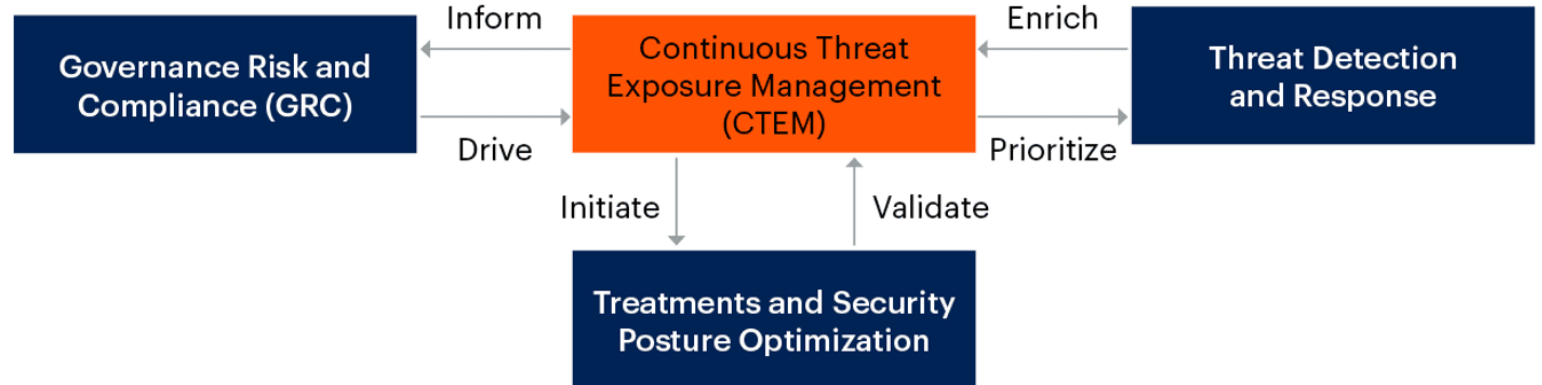
# CTEM 幫您重掌戰局

## Continuous Threat Exposure Management

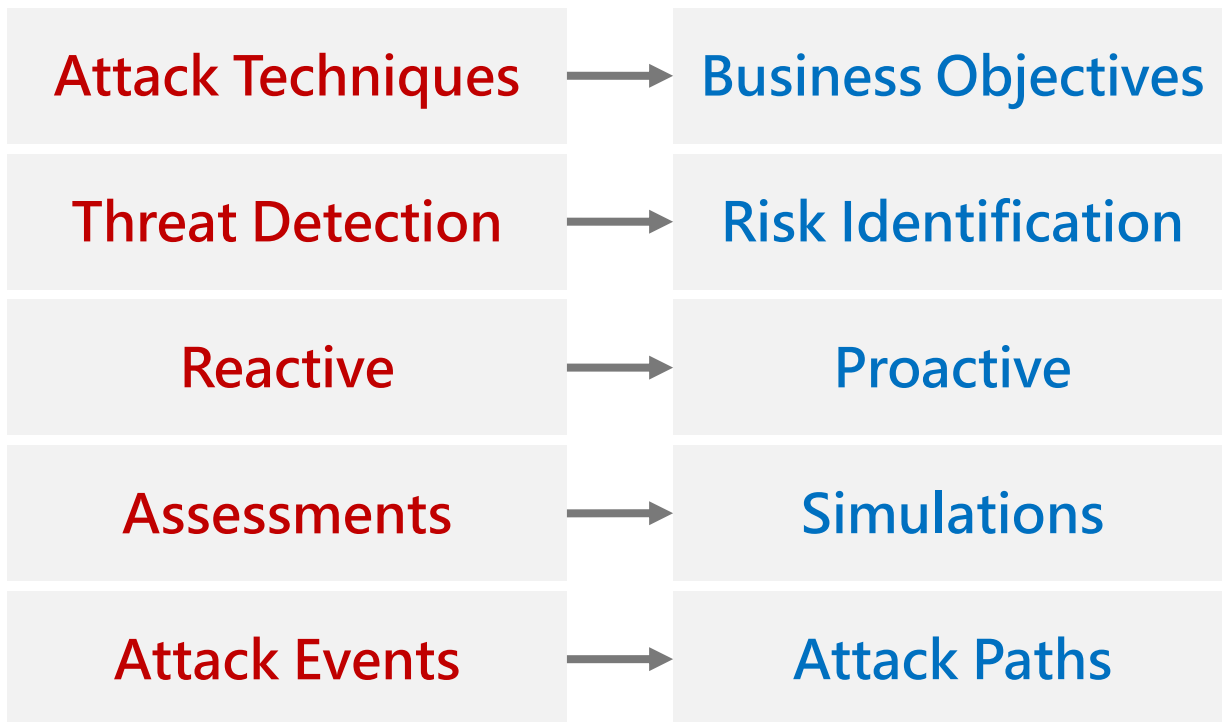
- > 2022年7月 Gartner 首次提出了持續威脅暴露管理概念(CTEM)，站在攻擊者的視角管理企業暴露風險面 Attack Surface。這是一種新的企業資安威脅管理方法，是識別、衡量關鍵資產風險並確定其優先順序的過程。
- > CTEM 有五個重要步驟的循環，Scoping (決定邊界)、Discovery (發掘資產)、Prioritization (盤點路徑)、Validation (評估驗證)、Mobilization (派工動員)



### Continuous Threat Exposure Management



# CTEM - 升級新資安思維



計畫視野，超越了圍繞駭客攻擊手法的傳統思維，進而對齊企業的商業營運為主

思維升級，從威脅偵測，改成風險識別為導向

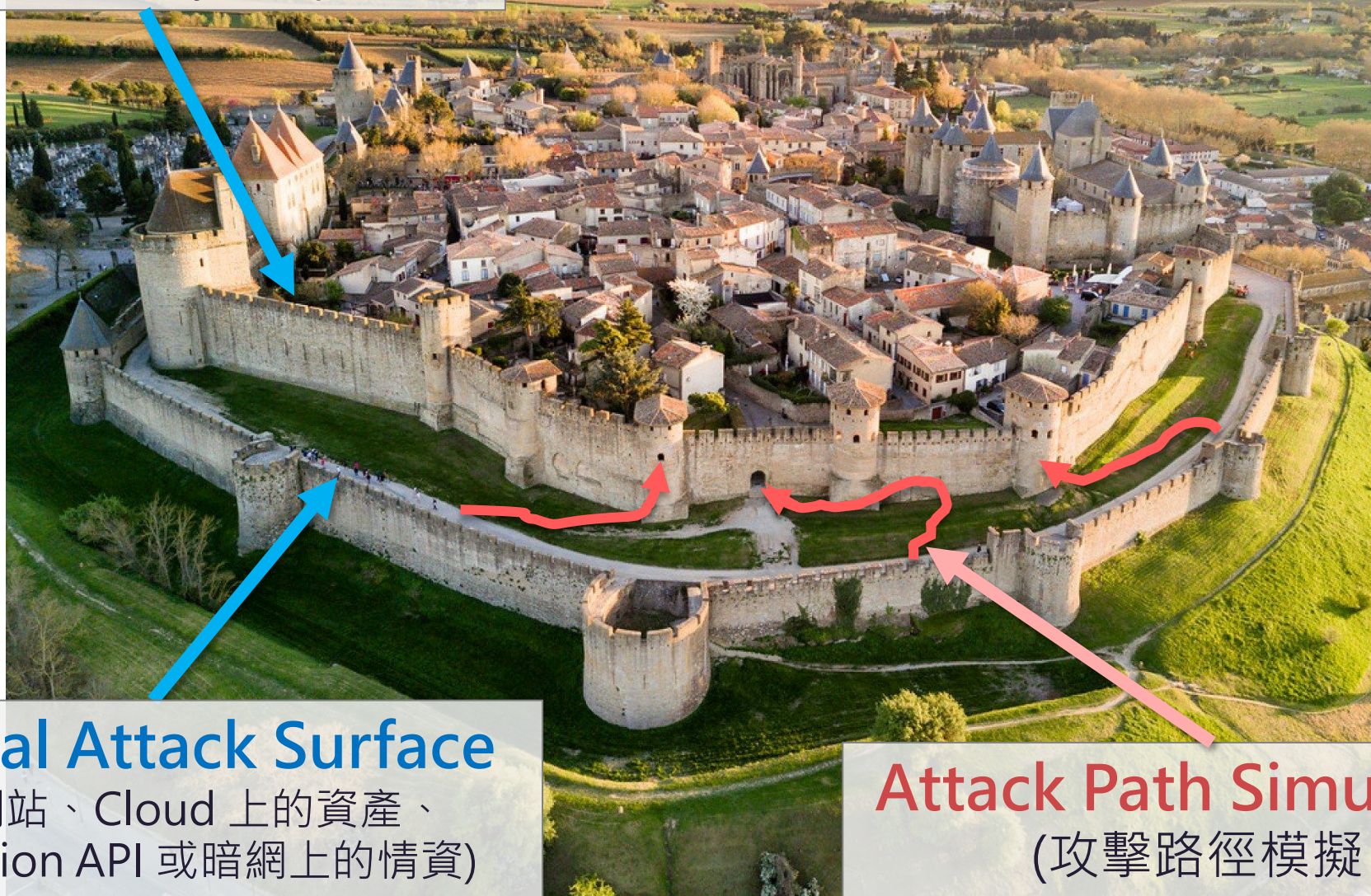
從被動等待威脅，改成主動找出 Attack Surface

從資產盤點，改成攻擊模擬來驗證 Attack Path

處理單位，從攻擊事件改成“攻擊路徑”為核心

CTEM 並不關注攻擊事件(Event)本身，而是關注攻擊路徑(Attack Path)。思考攻擊可能在哪儿發生及可能採用的攻擊戰術，以及可能採取的攻擊戰術和實施手段(Attack Surface)。

## Internal Attack Surface (AD, Azure Identity, Endpoints)



## 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)



講了這麼多，  
AI 是該啟動了！

# 奧義智慧是臺灣唯一一家 入選 Gartner 及 IDC 報告的 AI 資安公司



## 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)

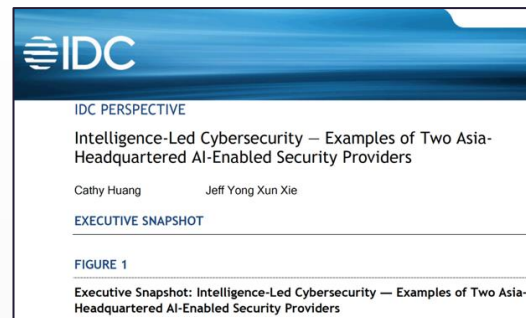
調查顯示奧義 AI 技術能降低 99% 的鑑識時間與 95% 的人力成本



## Gartner (2021, 2022)

《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, 2023)

《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

# CyCraft AI

於國際各大技術會議  
發表資安與AI研究超過 30 場

獨特數據來源，豐富的大陸駭客  
攻擊活動數據，完整的威脅情資

自主的技術：頂尖 AI 科技與資安團隊

運用 AI 大型語言模型 LLM  
於資安事件調查分析



black hat  
USA 2023

REGISTER NOW  
AUGUST 8-10, 2023  
PROFESSIONAL CONFERENCE

Available throughGala Incident Inspector Based On LargeScale Language Model and Association Mining

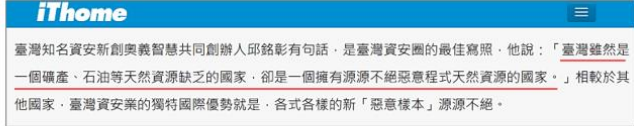
CYCRAFT  
臺灣駭客科技

針對臺灣高科技產業的  
OPERATION SKELETON KEY

獨家的養份：把駭客攻擊當作天然肥料

超過 50 萬台  
端點部屬

每天 2.8 億  
筆的資料



iThome

臺灣知名資安新創奧義智慧共同創辦人邱銘彰有句話，是臺灣資安圈的最佳寫照，他說：「臺灣雖然是一個礦產、石油等天然資源缺乏的國家，卻是一個擁有源源不絕惡意程式天然資源的國家。」相較於其他國家，臺灣資安業的獨特國際優勢就是，各式各樣的新「惡意樣本」源源不絕。

# 自主的技術：頂尖 AI 科技與資安團隊



運用 AI 大型語言模型 LLM  
於資安事件調查分析

**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  
Date: Thursday, August 10 | 10:20am - 11:00am (Jasmine AE, Level 3)  
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 analysis.

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.

CYRCRAFT  
奧義智慧科技

針對臺灣高科技產業的  
OPERATION SKELETON KEY

天下雜誌

訂閱天下

天下新聞新聞 · 那斯達克跌光今年漲幅，就因他威爾沒給承諾？

產業 > 製造

中國駭客「凱美拉行動」：台7家半導體公司受害，連設計圖都被看光光

一個客戶的意外發現，讓資安公司奧義智慧查出：至少有7家台灣半導體相關公司被中國駭客攻擊，部份案例潛伏時間甚至超過1年，連晶片設計圖、技術藍圖等文件都淪陷。難怪台積電供不應求，資安過不了評鑑，就不能供貨。

# 獨家的養份：把駭客攻擊當作天然肥料

超過 50 萬台  
端點部屬

每天 2.8 億  
筆的資料



iThome



臺灣知名資安新創奧義智慧共同創辦人邱銘彰有句話，是臺灣資安圈的最佳寫照，他說：「臺灣雖然是一個礦產、石油等天然資源缺乏的國家，卻是一個擁有源源不絕惡意程式天然資源的國家。」相較於其他國家，臺灣資安業的獨特國際優勢就是，各式各樣的新「惡意樣本」源源不絕。



# 生成式 AI 的資安應用場景

## 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，強化人員資安敏感度。

## 事前備戰

管理攻擊面  
預視攻擊路徑

### RedTeam 攻擊模擬機器人

AI 自動模擬攻擊路徑 Attack Path，能夠持續地驗證攻擊路徑的有效性，縮短與 Attack Surface 之間的誤差。

## 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，生成鑑識報告，提供攻擊案情分析給資安團隊決策與應變。



# 生成式 AI 的資安應用場景

## 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，強化人員資安敏感度。



## 事前備戰

管理攻擊面  
預視攻擊路徑

### RedTeam 攻擊模擬機器人

AI 自動模擬攻擊路徑 Attack Path，能夠持續地驗證攻擊路徑的有效性，縮短與 Attack Surface 之間的誤差。



## 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，生成鑑識報告，提供攻擊案情分析給資安團隊決策與應變。





# News 資安新聞機器人：AI 情報員 Crafty

Line ID: @Crafty

他不是聊天機器人！不能連續問答，有新聞的問題才有可能回應



奧義智慧 - AI 情報員 Crafty

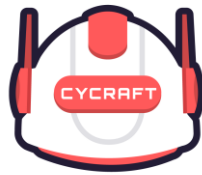
我是奧義智慧 Craft AI 情報員 Crafty，專注於提供客戶中文資安新聞。我目前僅參考最近三個月內台灣的五個主要新聞網站，包括四個主要台灣中文網站和一個英文媒體（IThome、TechNews、BusinessNext、InfoSecurity、Theregister）。使用時請注意以下事項：

- 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 的觀點與立場。以其他方式使用本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。有關這些主題的任何內容僅供參考，不能取代合格專業人員的建議。

上午 4:31



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

沒有 MITRE 被攻擊的新聞細節



# 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!

# 老闆很急，在線等!!

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，電腦就有可能被植入惡意程式



上午 3:53



我們發現了與上市公司重大訊息相關的新聞出現，彙整如下：

# 群光公司發生網路資安事件，未造成重大損害

# 摘要：

群光公佈網路資安事件

群光 ( 2385 ) 在2024年4月21日發生網路資安事件，該公司的資安單位已啟動相關防禦機制與復原作業，並檢視證交所資安事件重訊規定，未有公司核心資通系統、官方網站遭駭客攻擊或入侵，致無法營運或正常提供服務，亦未有個資、機密文件檔案資料外洩之情事，因此未造成公司重大損害或影響。

根據評估，對公司營運無重大影響，且不適用保險理賠金額。群光將持續提升網路與資訊基礎架構之安全管控，以確保資訊安全。

# 相關報導：

群光公司表示他們的資安單位在發現駭客攻擊時立即啟動防禦機制，並未影響核心資通訊系統或網站運作，也沒有個資外洩。該公司確認事件為勒索軟體攻擊，但對營運並無重大影響。製造業面臨勒索軟體等資安風險，需重視安全管控。群光公司強調他們已經採取措施應對此次網路資安事件，並保證公司的核心系統和網站運作不受影響，並且沒有任何個資外洩的情況發生。這次事件被確認為勒索軟體攻擊，提醒製造業面臨著各種資安風險，必須加強安全管控措施以確保公司資訊安全。

[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.ithome.com.tw/news/162448>

關鍵詞：群光公司, 資安單位, 勒索軟體

【資安日報】4月22日，資安研究機構MITRE證實遭遇Ivanti零時差漏洞攻擊

利用Ivanti一月份揭露的零時差漏洞攻擊行動再度出現！資安研究機構MITRE證實遭遇漏洞攻擊，並直到最近才確認遇害



## 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 / MTTR

## 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

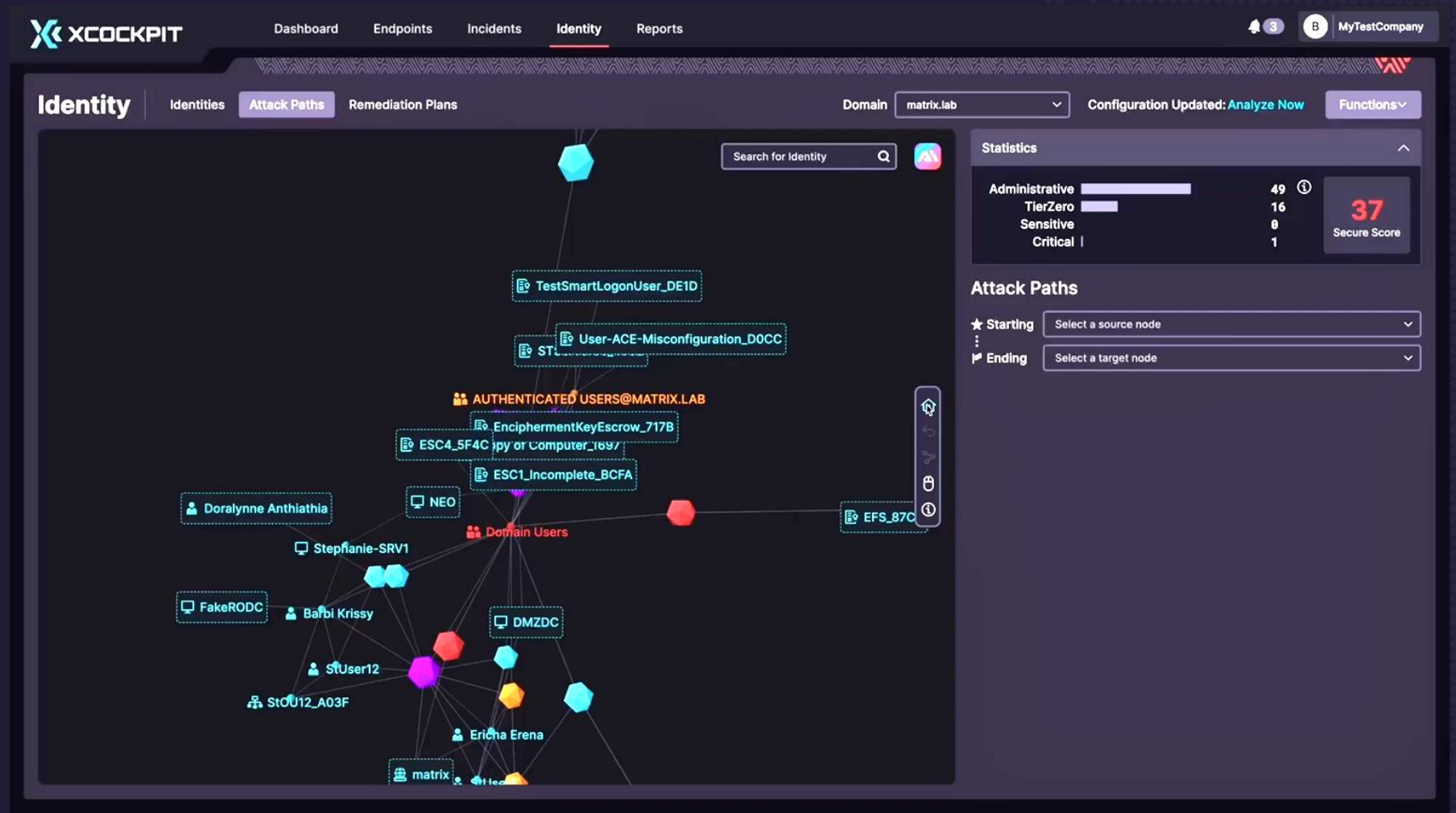
## 全新視覺化資安介面

Visualized Cybersecurity Dashboard  
快速與簡潔介面，並提供各種資安營運  
報告、案情即時瀏覽，與關聯分析報告

# 事前備戰：RedTeam 攻擊模擬機器人

## 帳號衝擊 模擬分析

CyCraft AI 的權限帳號分析，洞悉公司帳號曝險全貌，模擬攻擊路徑 Attack Path，協助企業管理潛在特權帳號。



# 這跟傳統特權帳號盤點，有甚麼不同？



- > 以前只對已知的特權帳號稽核，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，分析出隱匿在公司內的複雜帳號結構。

# XCockpit AD 安全分析

## 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

# 事中應戰：BlueTeam 事件應變機器人

11 Search Results

Order by First Alert Time

## Incidents

Pinned Only

Endpoint

First Alert Start Time

First Alert End Time

Incident Name

Alert ID

State

- In Progress 0
- Investigated 4
- Confirmed 3
- Closed 4
- Merged 2
- Reopened 0

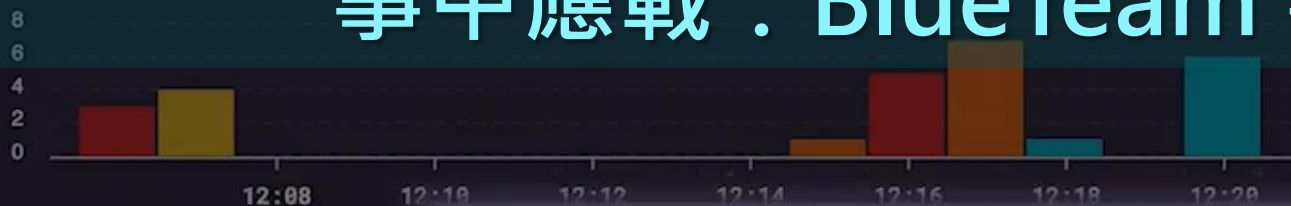
Attack Type

<p><b>CODERED</b></p> <p><b>CONFIRMED</b></p> <p>2023-0504-Attacker Activity 2023-05-04 12:08:46 (19m)</p> <p>Attacker Activity Suspicious Activity</p> <p>206 Total Events   2 Alerted Events</p>	<p><b>CREEPER</b></p> <p><b>INVESTIGATED</b></p> <p>2023-0504-Malware (ja) 2023-05-04 12:06:20 (14m)</p> <p>Malware Attacker Activity Suspicious Activity</p> <p>27 Total Events   3 Alerted Events</p>	<p><b>CREEPER</b></p> <p><b>INVESTIGATED</b></p> <p>2023-0504-Malware (en) 2023-05-04 12:06:20 (14m)</p> <p>Malware Attacker Activity Suspicious Activity</p> <p>27 Total Events   3 Alerted Events</p>	<p><b>CREEPER</b></p> <p><b>INVESTIGATED</b></p> <p>2023-0504-Malware 2023-05-04 12:06:20 (14m)</p> <p>Malware Attacker Activity Suspicious Activity</p> <p>27 Total Events   3 Alerted Events</p>	<p><b>NIMDA</b></p> <p><b>CONFIRMED</b></p> <p>2023-0504-Suspicious Process 2023-05-04 12:03:54 (2m)</p> <p>Suspicious Process   Suspicious Activity Malware Attacker Activity</p> <p>146 Total Events   6 Alerted Events</p>
<p><b>CREEPER</b></p> <p><b>CLOSED</b></p> <p>2023-0504-Malware 2023-05-04 10:12:12</p> <p>Suspicious Process   Suspicious Activity Malware Attacker Activity</p> <p>1 Total Events   7 Alerted Events</p>	<p><b>CODERED</b></p> <p><b>INVESTIGATED</b></p> <p>2023-0503-Malware 2023-05-03 17:23:41 (44m)</p> <p>Malware Attacker Activity Suspicious Activity</p> <p>355 Total Events   4 Alerted Events</p>	<p><b>NIMDA</b></p> <p><b>CLOSED</b></p> <p>2023-0503-Suspicious Activity 2023-05-03 17:22:41 (9m)</p> <p>Suspicious Activity</p> <p>12 Total Events   2 Alerted Events</p>	<p><b>CODERED</b></p> <p><b>CLOSED</b></p> <p>2023-0503-Malware 2023-05-03 15:59:30 (15m)</p> <p>Malware Attacker Activity Suspicious Activity</p> <p>81 Total Events   9 Alerted Events</p>	<p><b>NIMDA</b></p> <p><b>CONFIRMED</b></p> <p>2023-0503-Suspicious Process 2023-05-03 15:54:40 (2m)</p> <p>Suspicious Process   Suspicious Activity Malware Attacker Activity</p> <p>160 Total Events   5 Alerted Events</p>
<p><b>CREEPER</b></p> <p><b>CLOSED</b></p> <p>ABDD\n 2023-05-03 15:46:15 (12m)</p> <p>Suspicious Process   Suspicious Activity Malware</p> <p>5 Total Events</p>				

### 自動化案件管理

AI處理告警與調查：自動開單分析 (Alert Triage) 並收攏案情、自動管理案件狀態

# 事中應戰：BlueTeam 事件應變機器人



- 12:16:15 "C:\WINDOWS\sys...
- 12:16:21 "C:\WINDOWS\sys...
- 12:16:21 "C:\WINDOWS\Syst...
- 12:16:27 "C:\WINDOWS\sys...
- 12:16:27 "C:\WINDOWS\sys...
- 12:17:01 C:\Windows\Syste...
- 12:17:02 "C:\WINDOWS\sys...
- 12:17:07 "C:\WINDOWS\system32\cmd.exe" /c echo T1145-1 finished

## Details

```
"C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe" -noP - sta -w 1 -enc UgB1AGcALgB1AHgAZQAgAHMAYQB2AGUAIABIAEsATABNAFwAUwBBAE0AIABzAGEAbQA uAGgAaQB2AA==
```

此指令是在 Windows PowerShell 中執行的，可能會對電腦的安全性產生負面的影響。在這個命令中，Base64 編碼文本是 "UgB1AGcALgB1AHgAZQAgAHMAYQB2AGUAIABIAEsATABNAFwAUwBBAE0AIABzAGEAbQAuAGgAaQB2AA=="，解碼後變成 "C:\WINDOWS\system32\reg.exe" save HKLM\SAM sam.hiv"，它的作用是将系統註冊表的 SAM database 保存到一個檔案中。指令中含有的攻擊技術包括: T1003.005、T1003.002 OS Credential Dumping、T1027.000 混淆文件或資訊，顯示此指令的用意是想要在不經被授權的情況下取得使用者的憑證以及登入資訊，這是一個常見於橫向滲透攻擊的指令。

2023-05-04 12:16:21  
powershell.exe  
powershell.exe" -noP -  
AEsATABNAFwAUwBBAE0AIABzAGEAbQA  
可能會對電腦的安全性產生負面的影響。在這  
IAABIAEsATABNAFwAUwBBAE0AIABzAGE  
NDOWS\system32\reg.exe" save  
表的 SAM database 保存到一個檔案中。指  
002 OS Credential Dumping、T1027.000  
經被授權的情況下取得使用者的憑證以及登

## AI 自動化鑑識

AI 根據 APT 威脅模型，可識別各種混淆與攻擊手法，拆解攻擊內容

12:17:59 "C:\WINDOWS\system32\cmd.exe" /c echo T1098-1 finished

PID 900  
SID S-1-5-21-3188494444-2937684683-888728269-500  
Information • Parent Process:  
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe (PID:4332)

MITRE ATT&CK®



# 生成式 AI 的資安應用場景

## 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，強化人員資安敏感度。

## 事前備戰

管理攻擊面  
預視攻擊路徑

### RedTeam 攻擊模擬機器人

AI 自動模擬攻擊路徑 Attack Path，能夠持續地驗證攻擊路徑的有效性，縮短與 Attack Surface 之間的誤差。

## 事中應戰

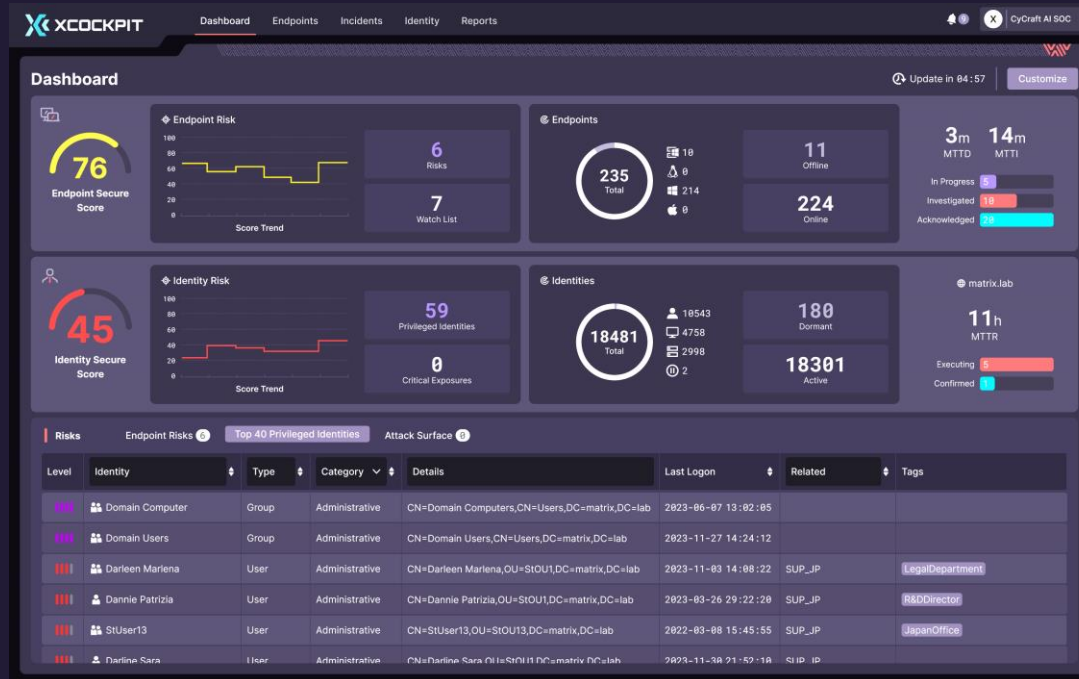
即時偵測威脅  
案情分析解說

### BlueTeam 事件應變機器人

AI 自動全天候偵測攻擊，精準告警，生成鑑識報告，提供攻擊案情分析給資安團隊決策與應變。

# XCOCKPIT

CyCraft AI Copilot



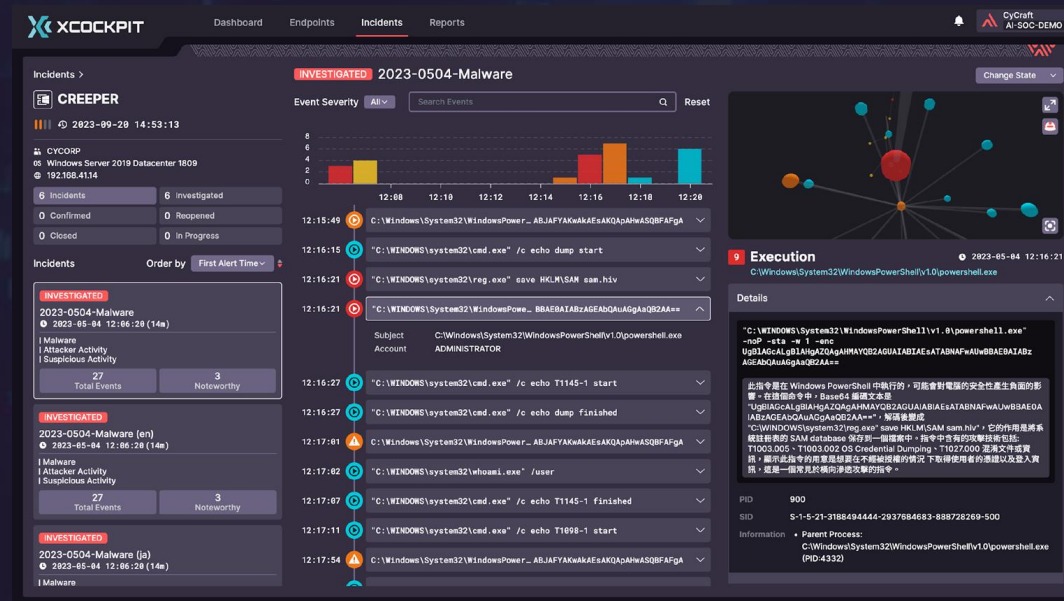
## 自動化威脅曝險管理平台

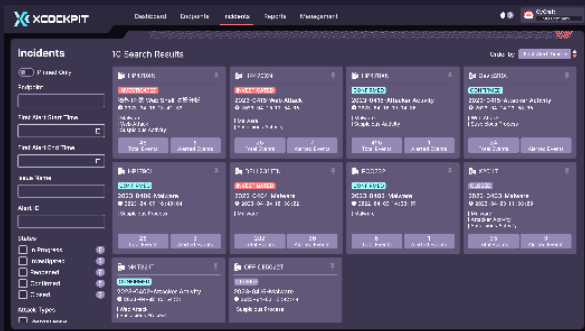
XCockpit 是一套全新的自動化威脅曝險管理平台，依循 Continuous Threat Exposure Management (CTEM) 框架打造。由獨家 Cyber + AI 技術針對端點安全、特權帳號衝擊分析、外部攻擊面等三大核心面向組成，提供視覺化的態勢管理介面，時時的攻擊面監測，與 AI 攻擊路徑模擬系統，協助企業量化風險指標，有效強化資安韌性。

# 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。

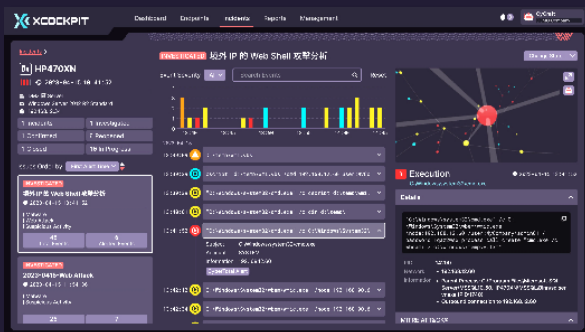




# 自動化案件管理

## Automated Case Management

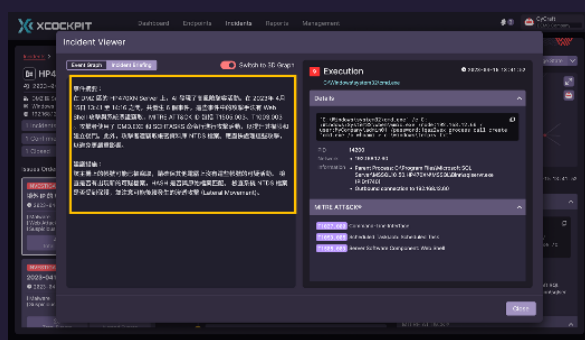
> AI 處理告警與事件，自動開單進行 Alert Triage，並歸納與關聯資訊，自動管理案件狀態，減少資安團隊工作量。



# 視覺化案情分析

## Root Cause Analysis

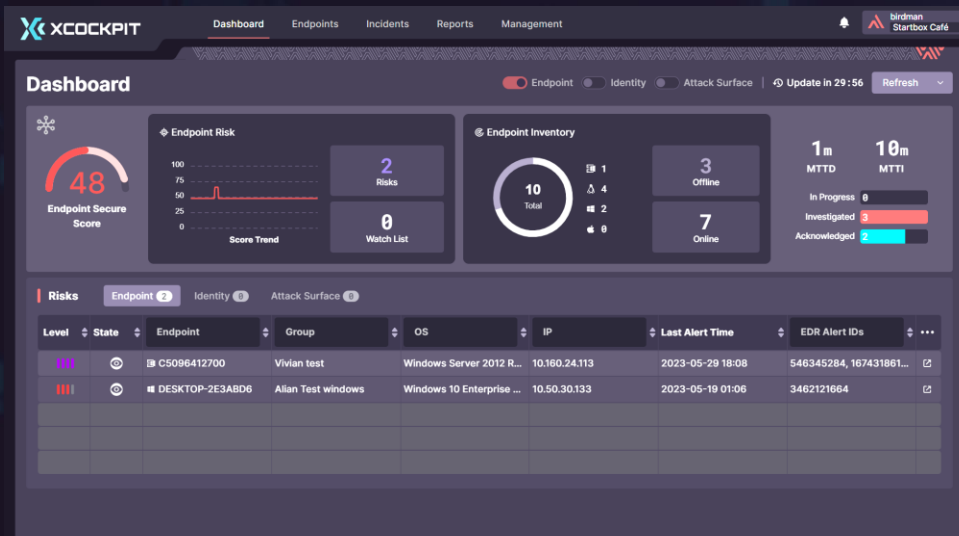
> AI 自動處理從端點告警，關聯相關事件、MITRE ATT&CK 攻擊手法識別、視覺化攻擊案情、與根因分析 Root Cause，輔助分析師快速了解案情。



# 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

# 新資安團隊：人類與 AI 混合編隊

客戶實績：日本大型上市集團，超過 25 家子公司，包含多個國家，超過 10 萬台電腦

團隊總產能提升 **20** 倍

以前人力限制只能調查約 5% 的資安事件。  
現在 AI 可協助團隊完成 100% 告警處理

MTTR 提升 **336** 倍

以前需要至少 3.5 個工作天分析寫報告。  
現在 15 分鐘 CyCraft AI 生成 **中文鑑識報告**

值班人員效率提升 **42** 倍

以前每個告警平均需要 2.1 個小時判斷。  
現在 3 分鐘從告警到完成開單

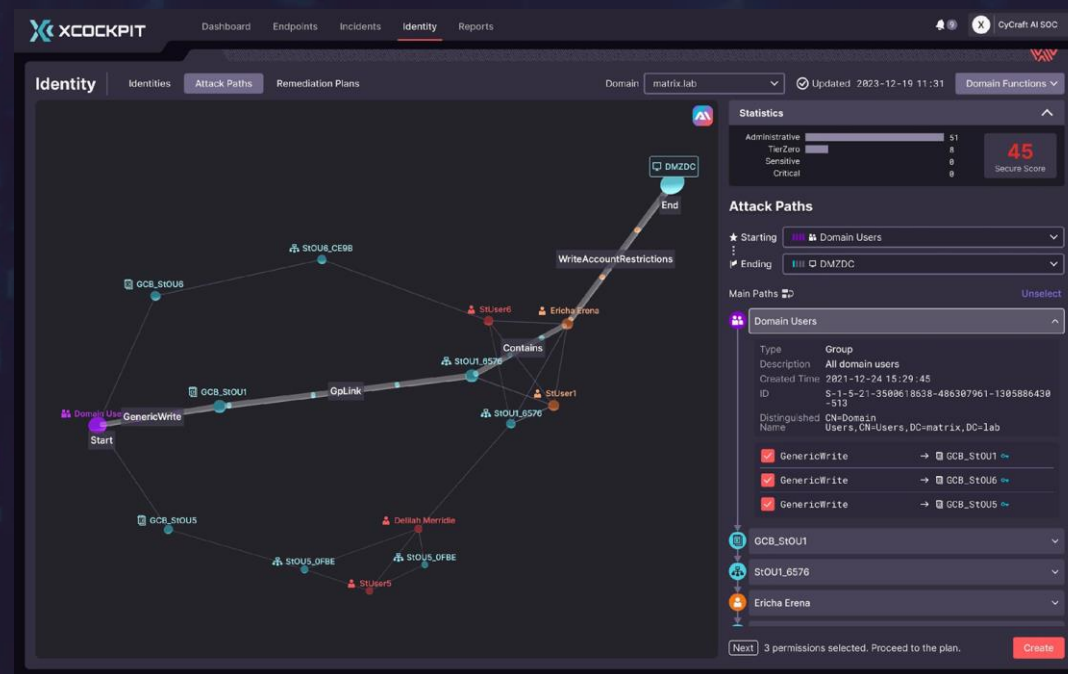
威脅可視性提升 **34** 倍

以前只能看到約 180 個 AD 特權帳號活動。  
現在 AI 模擬攻擊路徑，可找出約 6200 個潛在特權帳號活動

# 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。



# XCockpit

## 外部資產曝險管理 (EASM)

- 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。

The screenshot displays the XCockpit EASM interface. The top navigation bar includes 'Dashboard', 'Endpoints', 'Incidents', 'Identity', 'EASM', and 'Reports'. The main content area is titled 'EASM' and shows a list of assets for the domain 'apple-tech.com'. The table below lists various assets with their risk levels, types, information, last seen dates, and status.

Risk	Asset	Type	Information	Last Seen	Status	Tags
High	2017survey.apple-tech.com	FQDN	https://2017survey.apple-tech.com/survey...	2023-08-30 02:14	Unreachable	LEAKED INTRANET
High	elearning.apple-tech.com	FQDN	https://elearning.apple-tech.com/citcms/unl...	2023-08-30 02:14	Unreachable	LEAKED INTRANET
High	epmd.apple-tech.com	FQDN	https://epmd.apple-tech.com/	2023-08-30 02:14	Unreachable	LEAKED INTRANET
High	eportal.apple-tech.com	FQDN	https://eportal.apple-tech.com/ri/portal	2023-08-30 02:14	Unreachable	LEAKED INTRANET
High	128.233.68.195	IP	hostname: NA_windows 10 Enterprise x64	2023-08-30 02:14	Unreachable	COMPROMISED
High	fex.apple-tech.com	FQDN	https://fex.apple-tech.com/LoginWebUser...	2023-08-30 02:14	Unreachable	LEAKED INTRANET
High	healthy.apple-tech.com	FQDN	https://healthy.apple-tech.com/nws	2023-08-30 02:14	Unreachable	LEAKED INTRANET
High	sso3.apple-tech.com	FQDN	https://sso3.apple-tech.com/	2023-08-30 02:14	Unreachable	LEAKED INTRANET

Below the asset list, there is a section for 'elearning.apple-tech.com - Events'. This section shows a table of events with columns for Severity, Event Time, Identity, Edge Type, and Category.

Severity	Event Time	Identity	Edge Type	Category
10	2023-08-30 2:14	Surface	Compromised Endpoint	Device
10	2023-08-30 2:14	apple-tech02797	Compromised Credentials	User

\* 預計2024年第四季提供服務



CyCraft AI Copilot

## 量化企業風險

## 透視組織營運

**Attack Techniques Recognition**  
攻擊手法偵測識別

**Attack Path Simulation**  
攻擊路徑模擬預測

**Attack Surface Discovery**  
攻擊面風險評估

即時監控端點威脅  
自動化鑑識分析

即時監測特權帳號  
自動分析 AD/Azure

掃描盤點企業對外所有  
服務與裝置的風險

蒐集企業外洩情資  
彙整產業資安新聞

- 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

- 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

- 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

- 資安長專屬，資安情資新聞推播 Line Bot。
- 可客製化 Bot，增加客戶體驗，提高服務黏著度

# 經銷商獎勵計畫

## 成交獎勵 (至2024.09.30)

### 成交獎勵

於活動期間下單奧義智慧全品項單筆單年度訂單金額達NT\$100萬元(未稅)以上，即可獲得NT\$12,000元獎勵金

### 加碼菁英獎勵

1. 於活動期間成交達標三筆訂單且個別訂單年度金額達NT\$100萬元以上者，即可獲得NT\$15,000元獎勵金
2. 於活動期間成交最大筆金額訂單者，可再獲得NT\$15,000元獎勵金

活動說明：

1. 訂單計算金額皆為未稅。
2. 續約專案不列入計算。
3. 奧義智慧保有修改內容及審核資格之權利。

## 認證獎勵 (2024.07-2024.12)

### 認證獎勵

於活動期間完成奧義規劃之認證課程並取得證照，即得到NT\$8,000元獎勵金

活動說明：

奧義智慧保有修改內容及審核資格之權利。

CyCraft Expert / 奧義專家養成				
Product Fields	XCockpit Master			
	Endpoint (EDR & MDR)		Identity	EASM
T1 Foundation	Xensor EDR Foundation Est. June	XCockpit Endpoint Foundation Est. June	XCockpit Identity Foundation Est. May	XCockpit EASM Foundation
T2 Specialty	Xensor Skill Master Est. Sep	XCockpit Incident Master Est. Sep	XCockpit Identity Master Est. June	

奧義 AI 資安年會

CRAFT CON  
TAIWAN

CYCRAFT  
奧義智慧科技

# 台灣首場資安為主題的 AI 技術研討會

2024.07.12 (五) 08:30 - 17:00

格萊天漾大飯店 艋舺廳  
(台灣台北市萬華區艋舺大道101號14樓)



#Deep Learning



#FIRST CTI Summit



#BSIDE Tokyo



#Active Directory



#CYBERSEC



#CMD Embedding



#FIRST CTI Summit



#Black Hat USA



#TROOPERS

 **XCOCKPIT**  
CyCraft AI Copilot

