



預視威脅 掌握全局

企業資安困境 需要改變戰局的 AI 新科技

不斷演進的 合規需求

近年來資安相關法規愈發受到重視，如同《資通安全管理法》等合規需求不斷演進，使資源有限的企業組織面臨日益沉重的合規壓力

效率不彰的 管理策略

隨著企業組織高速成長、業務需求不斷變化，公司內部資產與服務也越來越複雜，在缺乏可視性的情況下，內部管理也變得越管越難

因駭而生的 營運損失

面對來勢洶洶的駭客攻擊，一旦受害不僅可能導致營運中斷與資料外洩，還會影響公司形象，使客戶信任度下降、損害企業重大利益



自動化威脅曝險管理平台「XCockpit」，整合「外部資產曝險管理」、「身分攻擊面管理」、「端點安全態勢管理」三大防禦構面，提供一站式的全方位自動化資安防護，並內建 AI 資安語言模型「CyCraftGPT」，自動化分析及解說案情。

EASM

外部資產曝險管理

IASM

身分攻擊面管理

ENDPOINT

端點安全態勢管理



XASM 多模態曝險管理方案

eXtended Attack Surface Management

EASM

IASM

ENDPOINT

The screenshot shows the XCOCKPIT platform interface. At the top, there's a navigation bar with tabs for Dashboard, Endpoints, IASM, EASM (which is currently selected), and Reports. Below the navigation is a domain selector for 'abc-tech.com'. The main area features a network graph where a central node labeled 'abc-tech.com' is connected to numerous other nodes of various colors (red, orange, blue, green) representing different assets or endpoints. A red callout bubble labeled 'STEP 1' points to a modal window titled 'Event Details'.

Event Details

10 Compromised Endpoint (DESKTOP-JASON)
⌚ 2025-01-31 08:31
The credential in compromised endpoint (jason_kao) can be used to access www.abc-tech.com

Assets

- https://www.abc-tech.com/supplier/login.aspx
- https://e-learning.abc-tech.com/menu/login.aspx
- http://upload.abc-tech.com/

Owner

Jason_kao

The following accounts have also been found on this endpoint.

- https://www.abc-tech.com/supplier/login.aspx
- 172.16.10.100
- william@abc-tech.com
- jason_kao@mail.abc.com

Endpoint

DESKTOP-JASON (181.233.110.50)

Informations

- Location: TW
- OS: Windows 10 Enterprise x64
- Time Zone: 台北 (UTC+08:00)
- OS: Windows 10 專業版 (10.0.19045) x64
- Malware: C:\Users\user\AppData\Local\Temp\215122\Comparing.pif



1 外部資產曝險管理

XCockpit EASM 監測到駭客論壇、暗網市場上，
員工的帳號資訊已遭外洩，且外洩來源為員工端點



3 端點安全態勢管理

XCockpit Endpoint 自動執行全場域端點鑑識，精準識別惡意程式與攻擊管道，並以 CyCraftGPT 分析攻擊根因

INVESTIGATED 2025-0202-Malware

Event Severity All ▾ Search Events Reset

總覽：
在 2025 年 2 月 2 日，電腦 DESKTOP-JASON (作業系統為 Windows Serve 2008 R2 Standard 所屬群組為 PHC Servers) 發生以下高風險事件。根據 EDR 警報 ID 14346123，於 2025 年 2 月 2 日 11:55 和 11:57，來自 IP 位 192.168.61.55 (帳號：jason_kao) 及 PB00058 被偵測到可疑登入行為，隨後，在 2024 年 12 月 4 日 11:56:08 至 11:56:31 之間，偵測到兩個高風險事件：首先是 C:\Windows\NetworkDistribution\fbicomv-2.dll 被辨識為惡意軟體 Mimikatz，其後在 11:56:31 被偵測到 C:\windows\NetworkDistribution\lzlib.dll，該檔案已被隔離。這些事件顯示出潛在的網路攻擊和系統安全風險。

8 Logon KALI → DESKTOP-JASON 2025-02-02 11:55:46

Details

- Network • 172.16.10.100
- Information • Remote Desktop Access (RDP)
- Inbound connection from 172.16.10.100

MITRE ATT&CK®

T1021.001 Remote Services: Remote Desktop Protocol

STEP 3



STEP 2

IASM

Assessment Identities Attack Paths Remediation Plans

Score Impacting Attack Path c

Updated Time 2025-03-04 17:16

Search for Identity

Domain (AD) demo.lab Functions

EXCLUDE Select Identity Clear

Statistics Secure Score 10

Attack Paths

- Starting Jason Kao
- Ending SubCA_56B8

Main Path Jason Kao

Type Computer

Description 2014-B*45293 quinta.lyndsay PC

ID S-1-5-21-3500618638-486307961-1305886430-2023

Distinguished Name CN=SQL,CN=Computers,DC=matrix,DC=lab

Next 2 permission(s) selected. Proceed to the plan. Create

Starting GenericWrite

Jason_kao

Type User

Groups ITAdmins, Domains, Users

Category Sensitive

Detail 台中分公司 jason_kao@mail.abc.com

2 身分攻擊面管理

XCockpit IASM 分析 AD 帳號安全性，並進行攻擊路徑溯源，發現特定供應商系統存在外洩風險



► EASM 外部資產曝險管理



企業曝險態勢分析

自動識別組織的數位資產，如域名、IP 地址，
並 7*24 自動監測 15 種類型的曝險情資



GitHub 曝險情資

可自訂關鍵字，針對 GitHub 程式庫等環境獵捕外洩情資，持續監測供應鏈與第三方的安全

► IASM 身分攻擊面管理



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

監測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



稽核帳號安全

時時監測帳號安全設定，包含密碼設定原則、帳號鎖定原則、異常權限設定等

* 主要針對地端的 Active Directory (AD)、雲端的 Entra ID (原 Azure Active Directory) 與 Azure 進行偵測

* 根據需求可提供一次性或訂閱制的服務方案，詳細資訊請洽業務團隊

► ENDPOINT 端點安全態勢管理



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，自動開單與管理案件，提升團隊的工作效率



視覺化根因分析

以生成式 AI 自動產生鑑識報告、歸納事件關聯，並提供視覺化的根因分析，協助團隊了解案情



AI 即時偵測鑑識

7*24 主動式威脅獵捕，可即時偵測攻擊與異常端點行為，並在 3 分鐘內建單，15 分鐘內調查完案情

* 支援 Windows、Linux、macOS 系統

* 提供全 API 整合 SOC/SIEM 工單系統，詳細資訊請洽業務團隊

* 視需求可單獨採購 EASM、IASM、Endpoint 平台，或是報告解讀等專業服務，詳細資訊請洽業務團隊

實績案例 客戶信賴



客戶案例

“
XCockpit 平台的設計邏輯清晰，讓沒有資安背景的主管或同仁都能理解呈現的資訊，滿足跨部門協作需求、降低一來一往的溝通成本。

—— 經濟部資訊處 處長

“
XCockpit 平台提供了我們設備鑑別評估、外部曝險評估、高權限風險評估等決策資訊，不僅有利於動態管控制存取安全，也是金融產業在適用零信任框架上的一大助力。

—— 全球人壽 資安長

“
奧義的 AI 應用讓我們即時掌握資安異常，迅速排除隱患，並減輕資訊人員負擔，使團隊專注於創新應用開發。

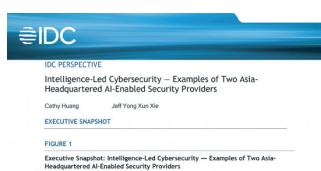
—— 萊爾富資訊總處 資訊長



Gartner

《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

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

權威機構深入剖析奧義技術優勢與市場實證



Frost & Sullivan

《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 技術能大幅提升鑑識效率



美國 MITRE ATT&CK
公開評測 APT29

第 1 名



日本最大 ICT 展會
資安解決方案

第 1 名



全球資安產業地圖
臺灣新創

唯 1 選



臺灣新創領導品牌
《NEXT BIG》

唯 1 資安新創



奧義智慧科技 (CyCraft Technology) 是一間專注於 AI 自動化技術的資安科技公司。於 2017 年創立，企業總部位於臺灣，於日本、新加坡皆設有子公司，為全球地區的政府機關、警政國防、銀行和高科技製造產業提供專業資安服務。

contact-tw@cyraft.com
886-2-7739-0077



Facebook



技術部落格



官方網站