XCOCKPIT

CyCraft AI Copilot

預視威脅 掌握全局

CYCRAFT
奧義智慧科技

企業資安困境 需要改變戰局的 AI 新科技

01 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

02 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

03 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

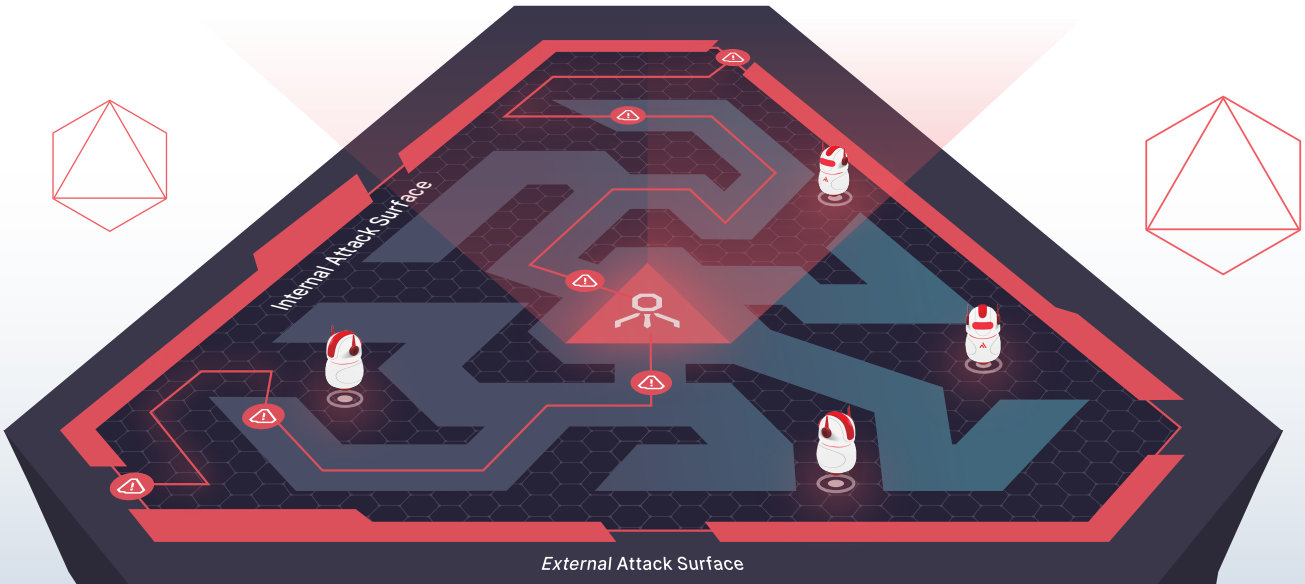
XCOCKPIT
CyCraft AI Copilot

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

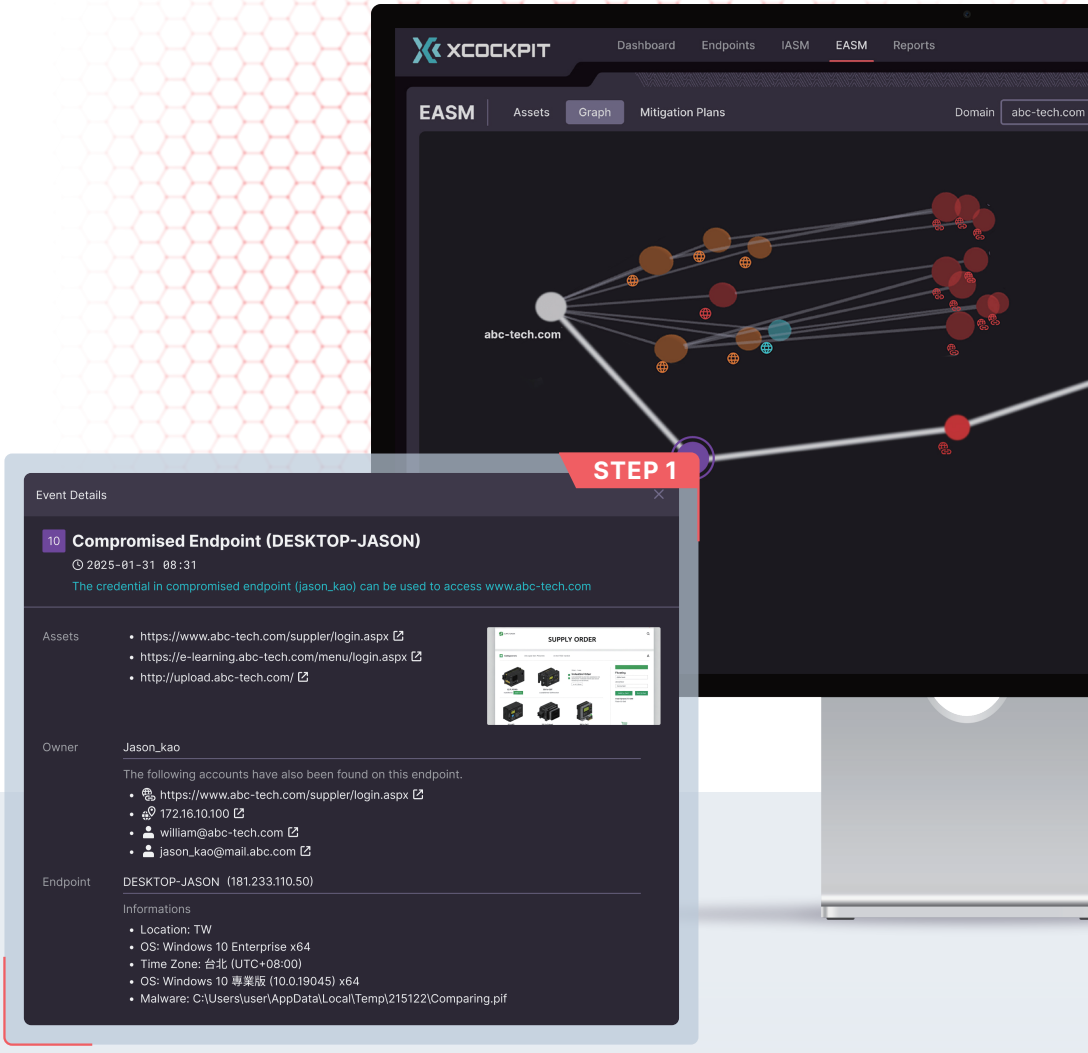


XCockpit 自動化威脅曝險管理平台

XASM 多模態曝險管理方案

eXtended Attack Surface Management

EASM IASM ENDPOINT

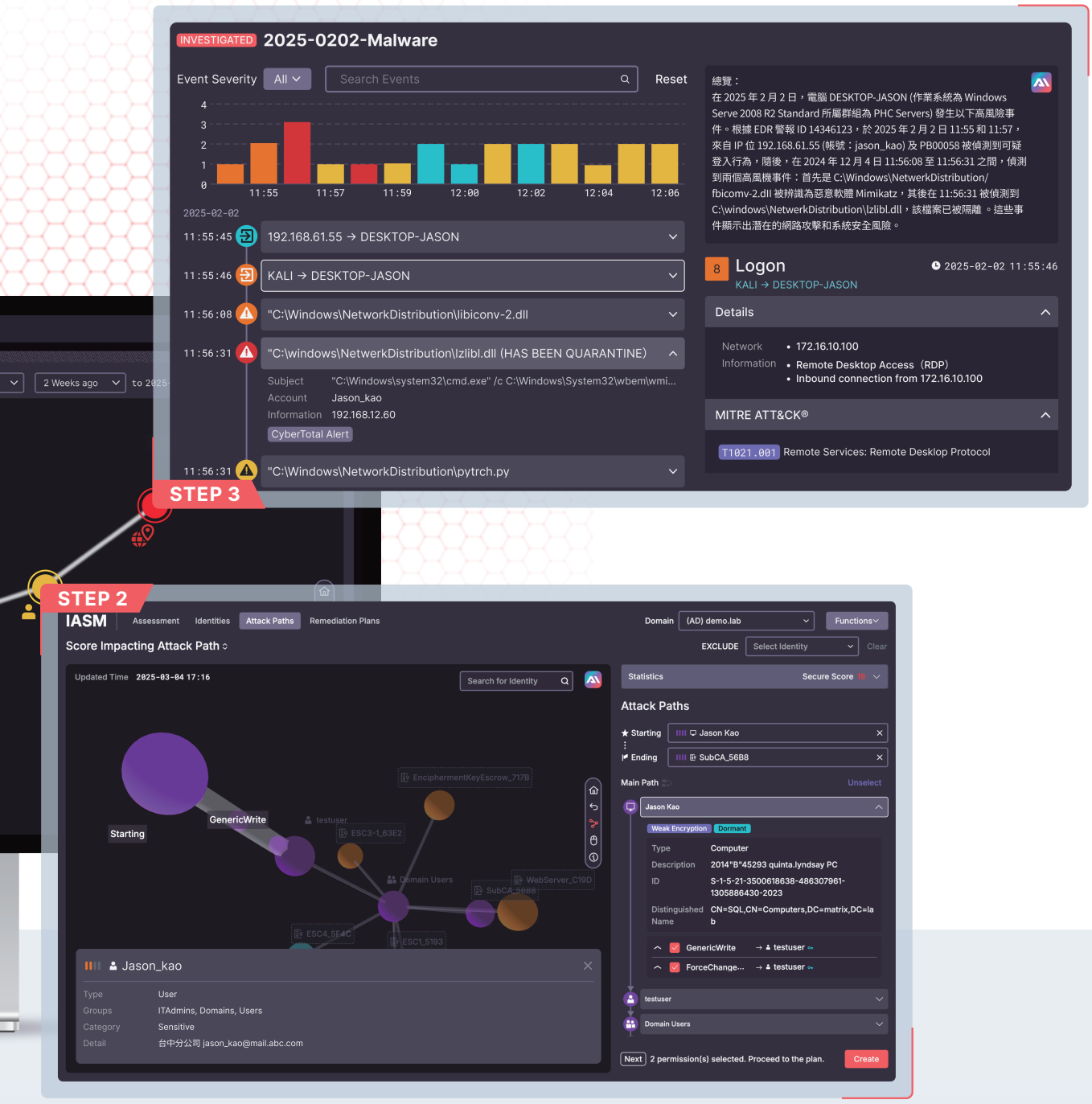


1 外部資產曝險管理

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



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

* 根據真實案例改寫，所有資訊皆已去識別化

XCOCKPIT

CyCraft AI Copilot

EASM IASM ENDPOINT

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

帳號外洩端點溯源

監測外洩的帳號情資，並溯源外洩的來源端點、盤點受影響的服務等，協助企業快速應處

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

《資安法》技術面分析

可一鍵產生企業曝險總覽報告，幫助企業檢核《資通安全管理法》技術面之合規項目

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*

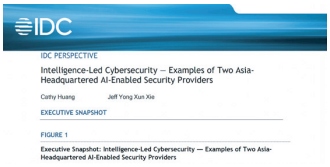
> XCockpit 平台提供了我們設備鑑別評估、外部曝險評估、高權限風險評估等決策資訊，不僅有利於動態管控存取安全，也是金融產業在適用零信任框架上的一大助力。
>
> —— *全球人壽 資安長*

> 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 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

MITRE ENGENUITY | ATT&CK Evaluations

美國 MITRE ATT&CK 公開評測 APT29

第 1 名

Interop BEST OF SHOW AWARD 2020 Grand Prize

日本最大 ICT 展會 資安解決方案

第 1 名

Momentum CYBER CYBER SCAPE

全球資安產業地圖 臺灣新創

唯 1 入選

Startup Island

臺灣新創領導品牌 《NEXT BIG》

唯 1 資安新創

CYCRAFT

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@cycraft.com
886-2-7739-0077

Facebook　技術部落格　官方網站