BEST PRACTICE - 高科技製造業

# 化被動為主動
# 高科技製造客戶成功阻絕再訪攻擊

**代表客戶:**

台灣知名液晶背光模組製造商，專注於創新顯示系統整合方案，並積極布局 AI、AR/MR 與 AIoT，開發生成式 AI、邊緣 AI 與智慧應用，致力成為智慧顯示與人工智慧解決方案的領導品牌。

**挑戰與痛點: 客戶身分識別管理系統遭駭客滲透並提權，面臨進階威脅攻擊**

1. AD / Entra ID 架構複雜，導致權限控管漏洞與帳號遭盜用
2. 入侵前僅部署傳統端點保護，缺乏抵禦身分識別攻擊的防禦韌性
3. 入侵後無法有效阻斷駭客再次滲透，防禦長期處於被動狀態

## 奧義智慧服務實績:

**XCockpit 平台 + 奧義 IR 應變團隊**

1. 導入 XCockpit Endpoint，全天候 7*24 持續監控 5,500 台端點與伺服器，透過 AI 技術即時偵測並阻斷駭客再次利用 AD 提權發動攻擊。
2. 奧義 IR 應變團隊迅速進駐，協助釐清事件根因、揭露系統漏洞，將被動防禦轉化為主動修補行動。
3. 結合 XCockpit IASM 模組，深入分析 AD 權限配置風險，阻斷駭客提權攻擊路徑，並持續監控權限變動與安全態勢。

## 成果與效益:

1. 應變期間透過 XCockpit IASM 與 AI 攻擊路徑分析功能，成功識別超過 300 條 AD 提權攻擊路徑，並完成權限配置矯正，徹底阻絕駭客再訪風險。
2. 事件後全面導入 XCockpit 平台，整合外部情資、身分識別與端點安全三大模組，簡化操作介面，顯著提升資安團隊效能並強化整體防護。

## XCockpit 威脅曝險管理平台

XCOCKPIT
CyCraft AI Copilot

### XCockpit Platform

整合端點安全、外部曝險與身分攻擊面管理的資安平台，能自動識別資產曝險與預視攻擊路徑，協助企業迅速應對威脅，確保營運不中斷。

*示意圖內容僅為產品展示，所有數據及資料均與客戶無關。

> "奧義的 XCockpit 平台及 IR 團隊，協助我們在事件當下迅速控管風險、穩定營運；事件後所提供的資安強化建議，也成為我們優化治理與提升整體防禦成熟度的重要依據。"
>
> — 高科技製造業資安長

CYCRAFT
www.cycraft.com
+886-2-7739-0077 | contact-tw@cycraft.com

關於奧義