
CYCRAFT
奧義智慧科技
EVERYTHING
STARTS FROM
CYCRAFT

AI 驅動資安運維平台
(AI-Driven SOC)

透過多項奧義獨家的 CyCraft AI 人工智慧技術，自動化調查單位內端點情資資訊，快速整理駭客所在之數位場域活動狀態與根因分析，並視覺化呈現數位案情脈絡及端點關聯等，搭配即時解析技術彙整內、外部威脅情資，進而挖掘出更深入的潛在風險，找出傳統防禦設備無法偵測的資安威脅。

FAST

持續獵捕威脅、AI 動態鑑識分析，
即時告警縮短調查時間。

ACCURATE

MITRE ATT&CK 公開評測最低雜訊，
告警精準有效零誤報。

SIMPLE

高可讀性駕駛艙設計，
視覺化端點勢態、
案情脈絡盡收眼底。

THOROUGH

AI 根因分析徹底調查事件始末、
入侵動向，全面改善資安體質。

關於奧義智慧科技

奧義智慧 (CyCraft) 是世界領先的 AI 資安科技公司，企業總部設立於臺灣，並在日本、新加坡與美國設有海外子公司。奧義智慧以創新 AI 技術自動化資安防護，內建端點 EDR、情資 CTI、網路 TIG 並整合建構新一代 AI 資安戰情中心，獲得逾五十個政府機關、警政、國防單位，以及三成金融機構、數十家高科技與關鍵領域龍頭企業的信賴，市佔率國內第一。
從端點到網路、從調查到阻擋、從自建到託管，CyCraft AIR 涵蓋企業安全所需的一切面向，遵循 F/A/S/T 量化指標，提供客戶主動防禦，達到「威脅，視可而止」。

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

屢獲肯定 獲得信賴

MITRE | ATT&CK® Evaluations
美國 MITRE ATT&CK 公開評測
臺灣新創
唯 1 連續 3 年參加

Interop BEST OF SHOW AWARD 2020
日本最大 ICT 展會
資安解決方案
第 1 名

Momentum CYBER SCAPE
全球資安產業地圖
臺灣新創
唯 1 入選

奧義智慧為您提供

訂閱制服務

- 端點偵測與回應機制－EDR／MDR
  - 數位疫苗 (防勒索) 加強版 (*加購選項)
  - 主動威脅防禦 MPM 模組 (*加購選項)
  - ARTHAS 電腦資安鑑識與稽核系統 (*加購選項)
- 雲端安全 CWPP 解決方案
- 威脅情資調查分析平台 (CyberTotal)
- 網路威脅情資閘道 (ThreatWall)
- 企業曝險訂閱服務 (RiskINT)
- AD 攻擊路徑模擬評估服務

一次性服務

- 企業資安健檢服務－端點型
- 企業資安健檢服務－網路型
- 事件調查 (鑑識) 緊急應變服務－IR
- AD 攻擊路徑模擬評估服務
- 企業曝險調查服務

夥伴合作案

- AD Attack Path Assessment－AD 攻擊路徑模擬評估服務
- AI 數位航母：行動版事件調查與鑑識
- ARTHAS 電腦資安鑑識與稽核系統
- 電商用戶端點防毒防駭專案
- 反詐騙與偽冒網站監控服務
- 紅藍隊演練服務

奧義智慧 Medium

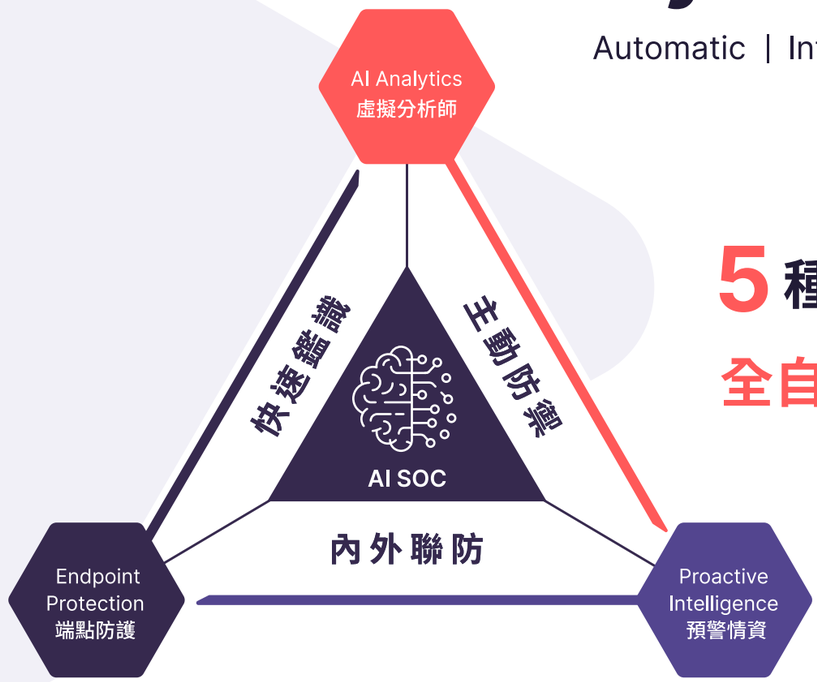
奧義智慧
Facebook 粉絲專頁

奧義智慧官方網站

engage@cycarrier.com | +886-2-7739-0077

CyCraft AIR

Automatic | Intelligent | Resilient



5 種關鍵報告
全自動快速結案

EDR MDR TIG CTI Expert

端點威脅獵捕告警

採用屢獲國際評測肯定的 CyCraft AI 引擎，結合 Protect Module 與 EDR 的防護機制，即時阻擋勒索軟體，即時解析、即時通報，快速反制最先進的駭客攻擊。

資安威脅鑑識分析報告

AI 自動關聯分析全場域的端點狀態，全球獨創自動繪製入侵根因時序圖，並產製具體駭客手法 (通過美國 MITRE ATT&CK® 駭侵框架評測)

端點偵測及應變服務周報

統整全單位資安監控 (作業系統分布、掃描狀態、威脅勢態、帳號活動分析與軟體列表)，自動勾稽未納管端點及不明裝置列表。

威脅情資快篩報告

AI 即時解析來自全球逾 133 個國家的最新情資，包含品質與數量皆領先於業界的駭侵情報與攻擊樣態等，提供威脅情報獵捕、預警分析及關聯情資分析。

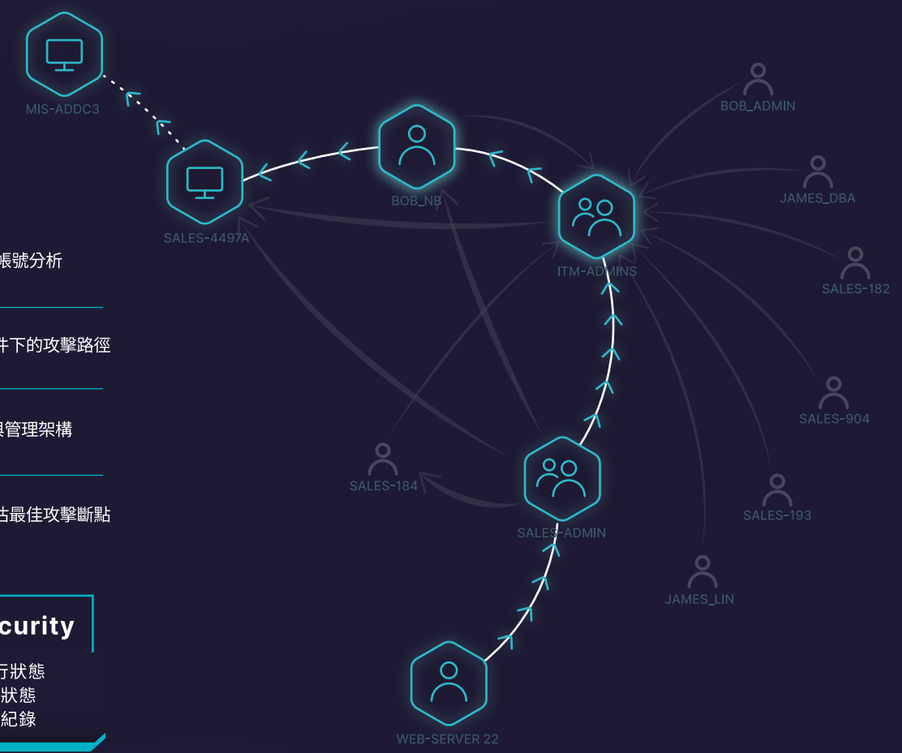
專家顧問處置建議

5×8 資安專家在線提供諮詢。
7×24 AI SOC 全天候主動防禦。

從量化到量測 洞悉入侵途徑

AD ATTACK PATH ASSESSMENT

AD 攻擊路徑模擬評估服務



創新科技 整合 EDR 端點與 AD 帳號分析

智慧預測 AI 模擬並預測不同條件下的攻擊路徑

洞悉全貌 可視化 AD 帳號關係與管理架構

防禦評估 AI 量化威脅邊界與評估最佳攻擊斷點

Endpoint Security

程式與服務的執行狀態
作業系統的安全狀態
帳號活動的歷史紀錄

AD Account Security

帳號與物件權限關係
隱匿的特權帳號分析
AD 安全性設定評估

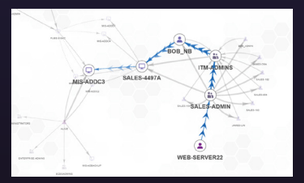
Attack Simulation

攻擊入侵點預測

攻擊路徑機率計算

Path Generation

MITRE ATT&CK 知識庫分析
特權帳號的攻擊影響評估



CYCRAFT MDR

超前部署　建構堅韌防線

我國自研技術

履獲國際大獎肯定的臺灣自研 AI 資安技術，在地資安團隊提供最優質貼近客戶的服務，主動式防禦組織資安無虞

部署彈性簡易

奧義 MDR 解決方案提供自建或雲端建置方案，超低系統資源使用，支援 Windows、Linux、macOS 跨系統平台，輕量彈性免去繁瑣負擔

主動安全防護

結合機器學習提供快速、精確的主動式威脅獵捕，自動化根因分析找出駭客入侵途徑、挖掘場域潛在風險

成功導入案例

已獲如中央部會、警政國防、金融機構、半導體企業，以及關鍵基礎建設、航空、電信、電商等關鍵領域機關採用與信賴，全面強化資安防禦及韌性

VANS 資安弱點通報機制模組

(* 加購選項)

掌握場域風險情勢，進行資產與弱點管理，並落實資通安全管理法之資產盤點與風險評估應辦事項

* 註：此項目為加購模組，須購買或具有 CyCraft MDR、Xensor 端點系統、奧義智慧資安健檢等產品或服務才可選購；詳情請洽奧義智慧業務同仁詢問。

THREATWALL

威脅情資閘道

奧義智慧情資驅動 **TIG (Threat Intelligence Gateway)** 網路安全解決方案 **ThreatWall** 採用獨家 **AI** 主動式惡意網域偵測引擎，整合 **CyberTotal** 全球威脅情資平台，利用品質及數量皆領先於業界的最新威脅情資，即時 **AI** 解析惡意行為、即時動態更新最新阻擋規則，有效防範新型態網路威脅與零時差攻擊，並以具脈絡的威脅資訊，豐富化系統收集的入侵指標。

內建 DNS 防禦

支援 Domain 類型黑名單，相容 DNS Response Policy Zone (RPZ) 防禦，防止惡意 DNS 查詢，並節省企業額外建置 RPZ 設備之成本

主動防禦超前部署

採用獨家 AI 主動式惡意網域偵測引擎，結合 CyberTotal 情資資料庫並以 AI 自動化分析，即時動態更新阻擋規則，杜絕零時差攻擊

部署架構高度彈性

依企業需求可雲端部署或 On-Premise 部署，支援 Inline 及 Mirror 模式彈性架構，可部署於企業防禦最前線，減輕後端資安設備負擔

產出威脅阻擋報表

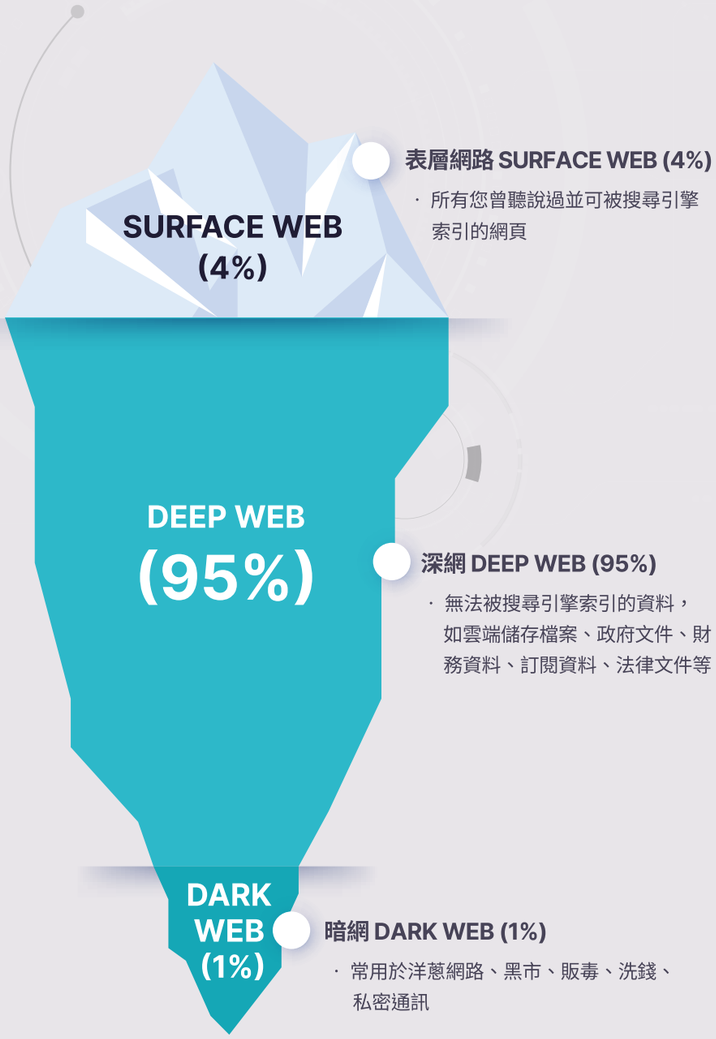
產出之報表可對應不同威脅類型，包含釣魚網站 (Phishing)、挖礦網站 (Cryptomining)、惡意網站 (Malware)、殭屍網路 (Botnet)、勒索軟體 (Ransomware) 等

RISKINT

企業曝險訂閱服務

進階網路威脅甚囂塵上，大量外流的機敏資訊在暗網中流竄，造成難以估量的損害。RiskINT 協助企業用更全面的視角洞悉預警情資，詳細監控並盤查企業外流的機敏資訊、存取憑證與遭偽冒的網域等，並配合 CyberTotal 全球威脅情資平台，使企業搶佔先機、增強主動式防禦能力，獲得有效應對潛在威脅的必要時間。

知己知彼，百戰百勝；做好萬全的準備，才能擁有真正可靠的防禦對策。



表層網路 SURFACE WEB (4%)

- 所有您曾聽說過並可被搜尋引擎索引的網頁

深網 DEEP WEB (95%)

- 無法被搜尋引擎索引的資料，如雲端儲存檔案、政府文件、財務資料、訂閱資料、法律文件等

暗網 DARK WEB (1%)

- 常用於洋蔥網路、黑市、販毒、洗錢、私密通訊

機敏資料曝險 (Data Leakage Risk)

監控企業的文件、圖檔、原始碼等機敏檔案是否外洩至暗網，以利企業掌握消息後進一步追溯洩露源頭

主機存取曝險 (Server Hacking Risk)

監控是否有企業內外網主機的非法存取憑證於暗網流傳，避免主機曝露成為駭客第一線攻擊目標

員工個資曝險 (Employee Phishing Risk)

監控暗網中是否存在有企業的員工個資、企業信箱、密碼原則等內容，減少員工遭到社交工程攻擊並成為資安破口的風險

網站釣魚曝險 (Website Phishing Risk)

監控是否有針對企業官網域名稱 (Domain) 進行惡意偽冒，並用以散布釣魚連結、木馬病毒、不實內容的類似域名