



由被動轉為主動

面對各種攻擊威脅，採取積極探索的方式！

CyberWin MDR 藉由**專家數位鑑識技巧**，自動化且智慧化，打造出唯一**100%** 辨識出惡意程式，針對資安事件處理**數位鑑識**之解決方案。

CyberWin MDR	V.S.	傳統資安防禦架構
【單一】 團隊/即可處理	人力協調	需 【多家】 廠商時間可配合狀況下
【事中】 即時分析與處理	處理時效	等到 【事後】 才處理
【主動式】 資安威脅獵捕分析	分析模式	【被動式】 等待資安警示/資安事故
高度 【自動化】 分析 & 鑑識專家 服務	自動化程度	需 【大量人力】 介入蒐證、處理、應變
【本土】 全域聯防及情資即時更新	情資整合	各組織自行費心處理 Or 購買國外情資
可鎖定/鑑別 【未知】 的攻擊手法	處理範圍	主要偵測 【已知】 的攻擊方式
I.R. 吃到飽，客戶僅需確認處理結果	管理負擔	每次事件，需 【全程參與】 並負擔 【繁雜應變】 工作

MDR 管理平台畫面 – 代管單位警報列表

當駭客入侵系統的幾分鐘內，CyberWin MDR 便開始啟動偵查與鑑識，將資安衝擊損失，降低到最小。

事件編號	事件名稱	主體名稱	發生時間	警報時間	最後發件時間	事件狀態
cyberwin-202010140001	Powercat 駭客工具連線安全	DESKTOP-1427584	2020-09-13 12:38	2020-09-16 05:41:01	2020-09-16 05:42:04	已開單
cyberwin-202010140002	新增未知未知駭客	DESKTOP-1427584	2020-09-14 11:05	2020-09-16 05:41:01		已開單
cyberwin-202010140003	駭客工具進入網路管理程式	DESKTOP-1427584	2020-09-13 12:38	2020-09-16 05:41:01		已開單

MDR 管理平台畫面 – 代管單位警報資訊

經分析團隊確認為惡意程式，以信件發出通知，使用者登入分析平台點選惡意程式即可刪除。

警報資訊	
cyberwin-202010140002	
已開單	
事件狀態	
詳細資訊	
事件識別碼	B57323UBRfa4OCJ6dEs
事件名稱	利用schtasks.exe新增排程工作
事件編號	
發生時間	2020-10-14 16:35:37
鑑識時間	

惡意程式路徑	hash	狀態	最後更新時間
C:\Users\stanley\AppData\Roaming\RegSvc.exe	b716f7611af99dfe7eb188defe75bdbe	未處理	2020-10-14 16:48:27
C:\Users\stanley\AppData\Local\Temp\ImpC871.tmp.bat	null	未處理	2020-10-14 16:51:03
C:\Users\stanley\AppData\Local\Microsoft\CLR_v4_0_32\UsageLogs\AsyncClient.bin.exe.log	null	未處理	2020-10-14 16:51:03
C:\Users\stanley\Desktop\AsyncClient.bin\AsyncClient.bin.exe	b716f7611af99dfe7eb188defe75bdbe	未處理	2020-10-14 16:54:21

創穩資云 資安專家代管服務可以協助：

- (1) 事前徵兆，最速發現：電腦紀錄器，專家代分析！
- (2) 事中警示，立即應變：徵兆全都錄，替威脅獵捕！
- (3) 事後鑑識，矯正預防：I.R. 吃到飽，事故沒煩惱！