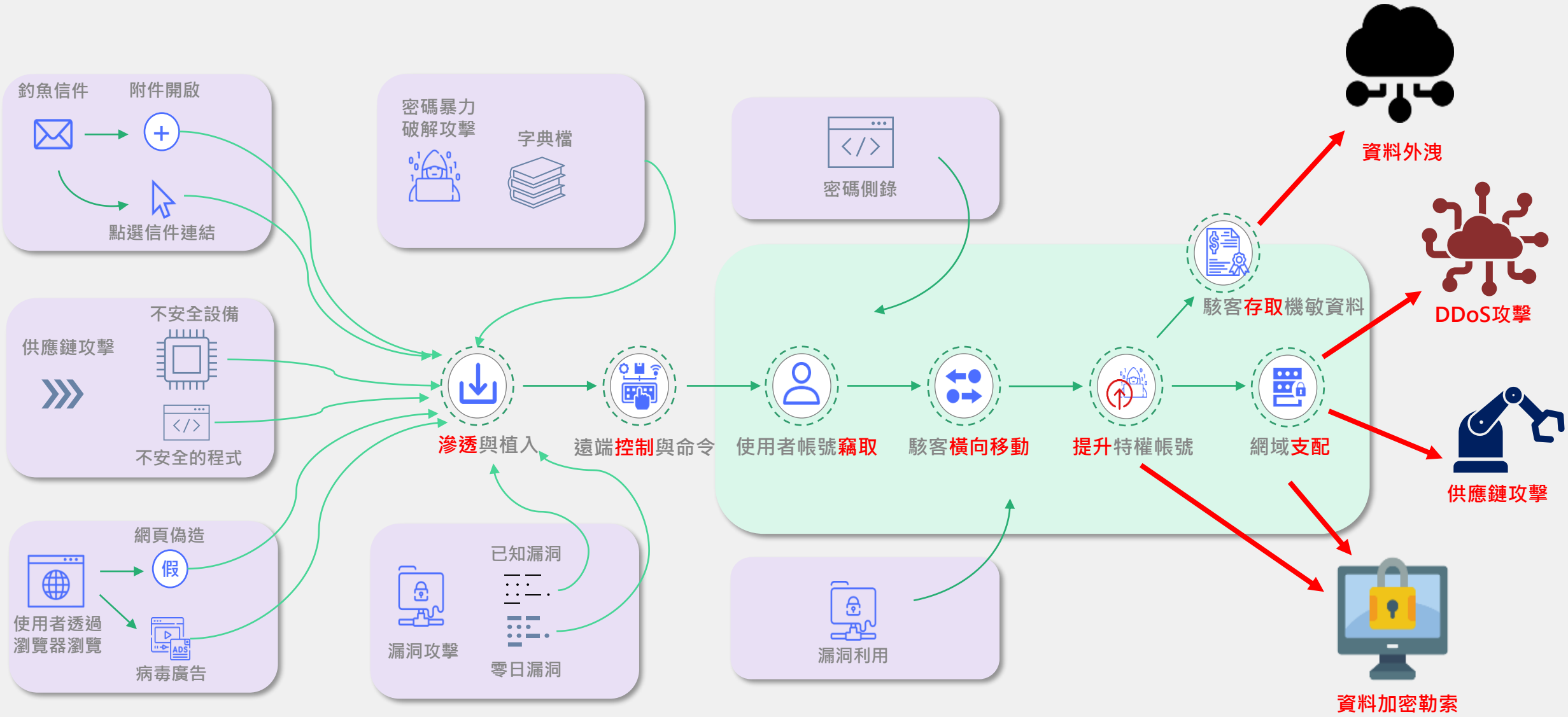
進階端點安全防護規劃 – FortiEDR
新世代端點防護與響應服務

Carlos Sheng

shengc@fortinet.com

防不勝防的駭客攻擊



面對駭客攻擊的思維與轉念

- 惡意程式的攻擊無時不在
- 若能及早發現就能預防治療
- 轉化被動防禦為主動保護
- IR鑑識成本高, 如何找到最有效的方法 (工具x服務, CP值高)

Endpoint Detection & Response

端點防護需要進階的強化偵測與事件回應
（EPP Endpoint Protection Platform ＋ EDR Endpoint Detection and Response）

01 即時阻斷

強化端點安全能力

透過NGAV機器學習強化端點安全防護能力以對抗未知、新型態惡意程式與攻擊手法。

02 自動隔離

保持營運不中斷

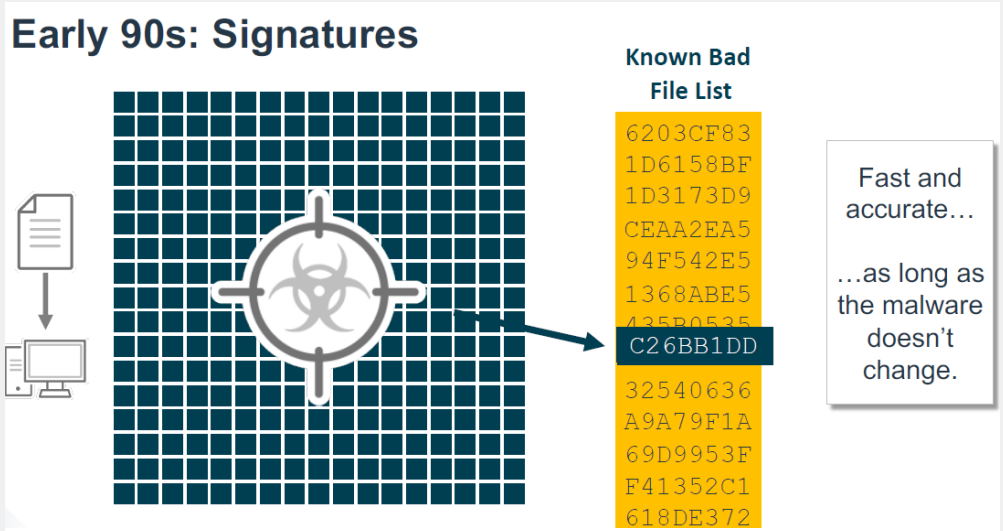
通過端點系統即時監控、快速回應與恢復以降低突破性感染攻擊事件帶來的衝擊。

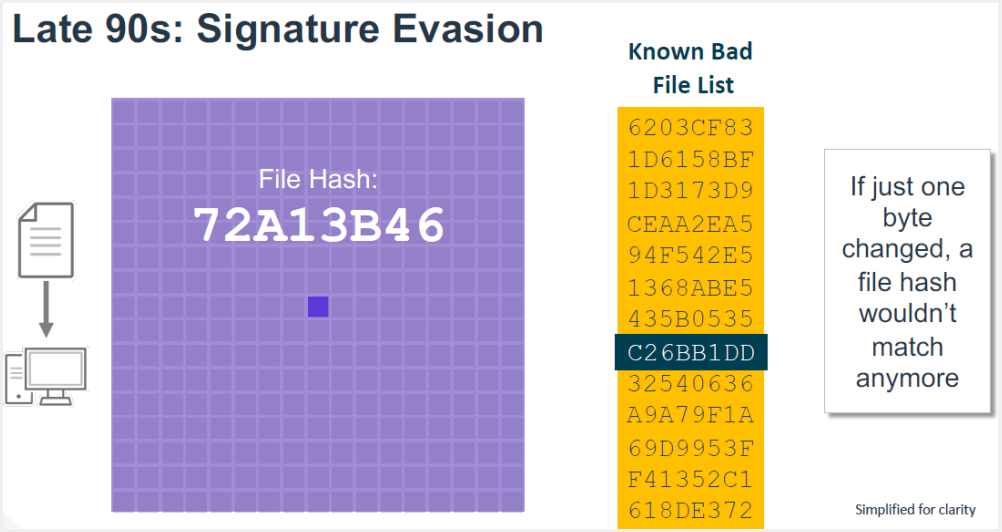
03 安全聯防

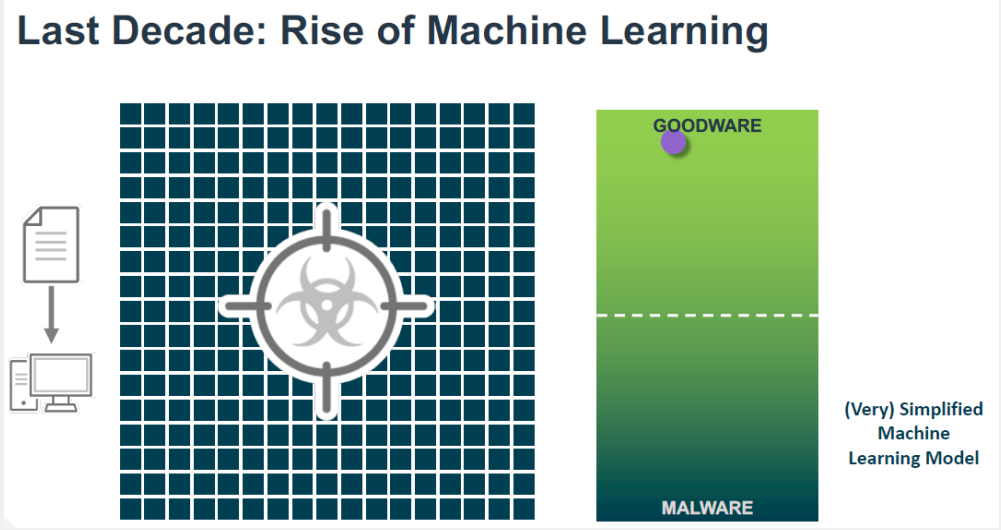
簡化安全維運

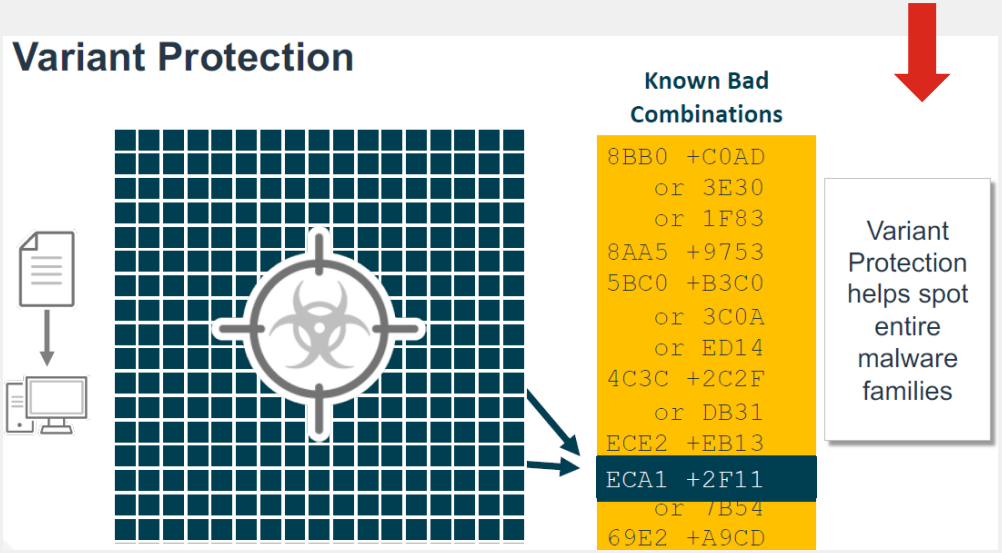
經由專業資安服務和安全設備自動化整合後，應對資安事件的調查與處理。

對於未知的威脅，機器學習助力精準防護！

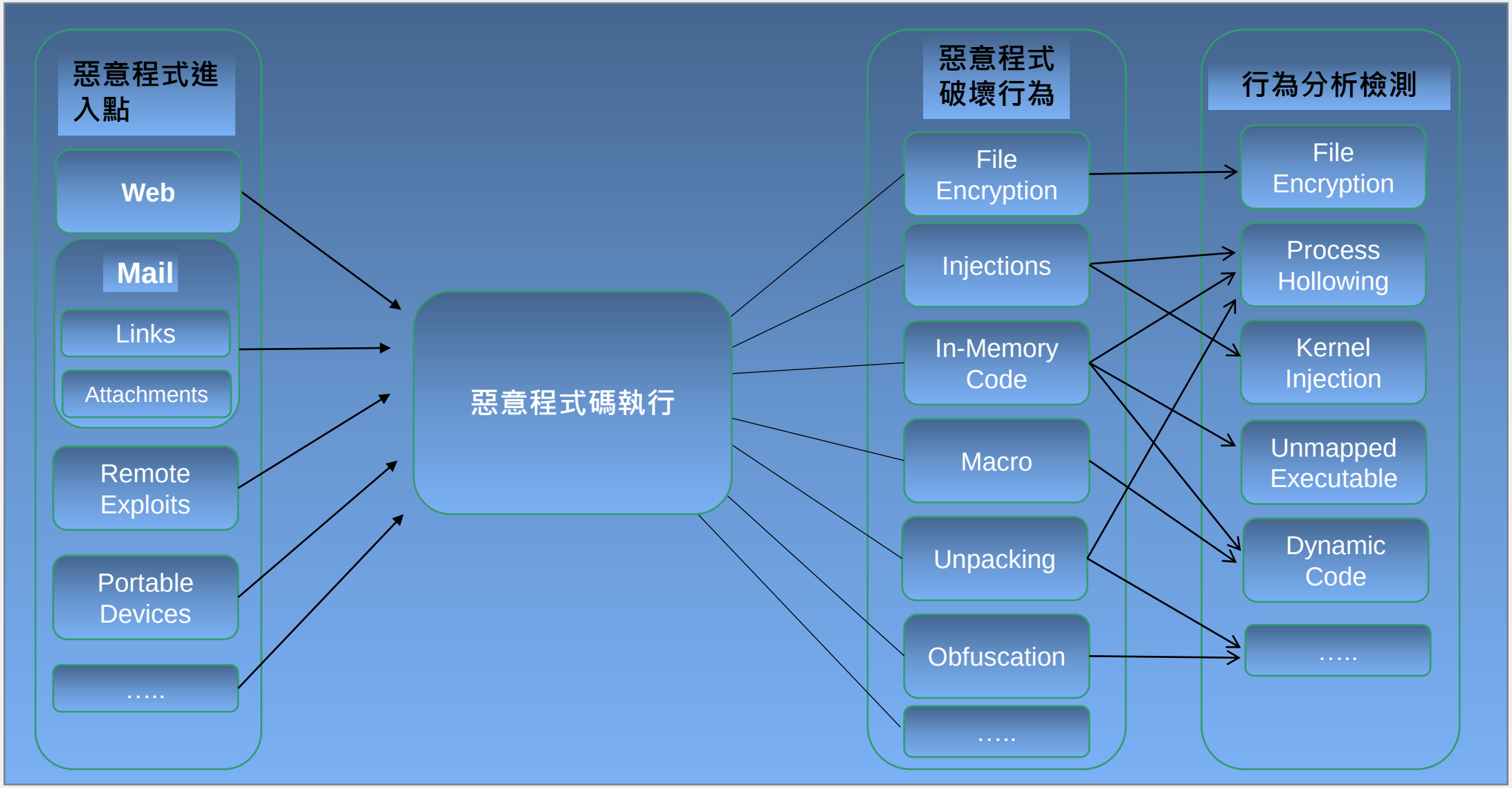








協防突破性感染 – 端點破壞行為偵測與阻斷 避免擴散



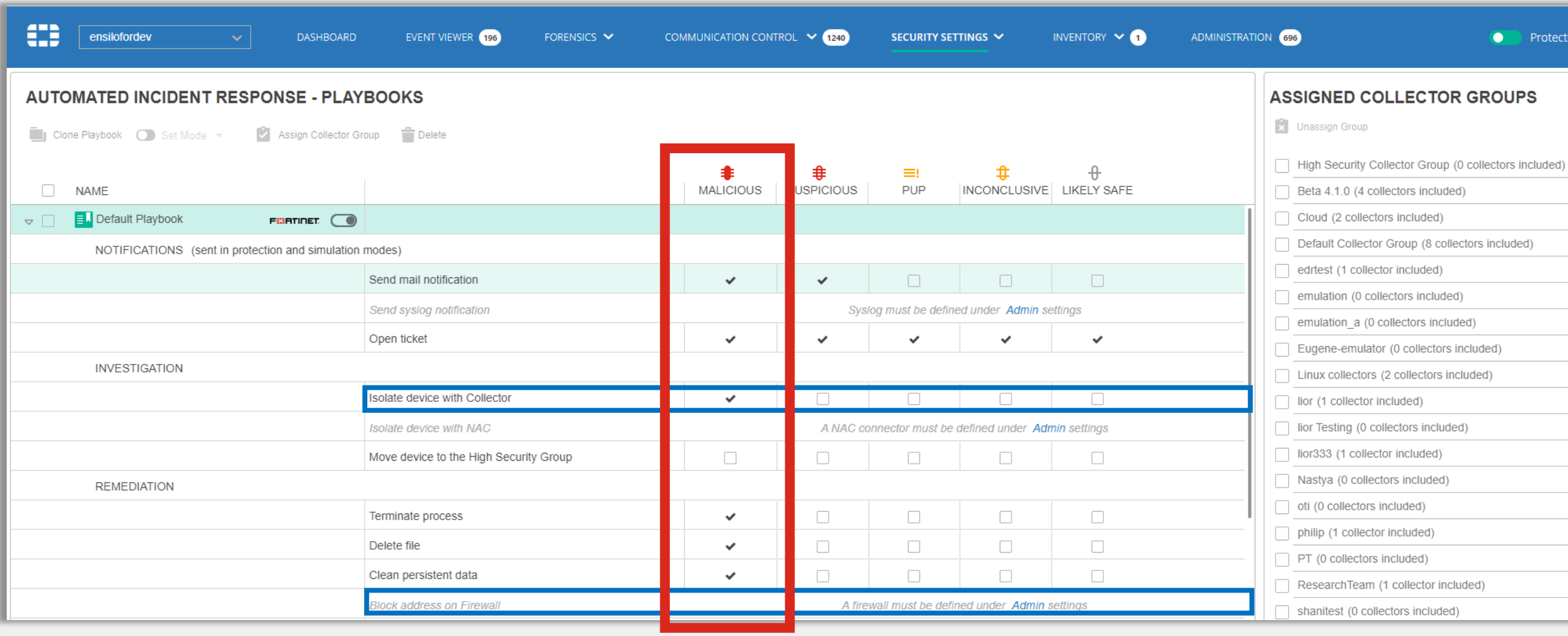
針對駭客攻擊行為阻擋

- 駭客執行攻擊行為，均被端點防禦阻擋，駭客使用數套黑客工具及執行一個加密程式。

SVR-ERPDB (10 events)			Malicious		20-Sep-2021, 03:39:29		
5961961	SVR-ERPDB	rel_enc.exe	Suspicious	3 destinations	20-Sep-2021, 03:39:29	20-Sep-2021, 03:49:50	⊘
5961528	SVR-ERPDB	GetPassword_x64.exe	PUP	Sensitive Inform...	20-Sep-2021, 03:20:55	20-Sep-2021, 03:21:20	⊘
5961511	SVR-ERPDB	NetworkPasswordDump...	Likely Safe	Sensitive Inform...	20-Sep-2021, 03:20:37	20-Sep-2021, 03:20:37	⊘
5961412	SVR-ERPDB	SniffPass.exe	Malicious	File Execution At...	20-Sep-2021, 03:16:09	20-Sep-2021, 03:16:09	⊘
5960173	SVR-ERPDB	mimikatz.exe	Malicious	File Execution At...	20-Sep-2021, 02:33:00	20-Sep-2021, 02:33:00	⊘
5957245	SVR-ERPDB	iepv.exe	Inconclusive	File Read Attempt	20-Sep-2021, 00:24:42	20-Sep-2021, 03:15:07	⊘
5957301	SVR-ERPDB	WirelessKeyView64.exe	PUP	Sensitive Inform...	20-Sep-2021, 00:24:42	20-Sep-2021, 00:57:15	⊘
5957254	SVR-ERPDB	netpass64.exe	PUP	Sensitive Inform...	20-Sep-2021, 00:24:42	20-Sep-2021, 00:57:14	⊘
5957233	SVR-ERPDB	mimikatz.exe	Malicious	Sensitive Inform...	20-Sep-2021, 00:24:40	20-Sep-2021, 02:33:00	⊘
5957220	SVR-ERPDB						

rel_enc.exe	加密程式的執行檔。
GetPassword x64.exe	登入密碼查看工具，直接讀取內存中的密碼。
Network Password Dump 64.exe	可恢復儲存在 Windows 中的網絡密碼。
SniffPass.exe	監聽本機及區域網路所傳送的密碼。
iepv.exe	破解IE帳號、密碼，可顯示 Internet Explorer Web 瀏覽器儲存的密碼。
WirelessKeyView64.exe	無線網路密碼查看工具。
netpass64.exe	密碼抓取。
Mimikatz	密碼抓取及提權，登錄系統用戶名的密碼。

資安事件自動處理與響應 —> 彈性多樣化的處理方式



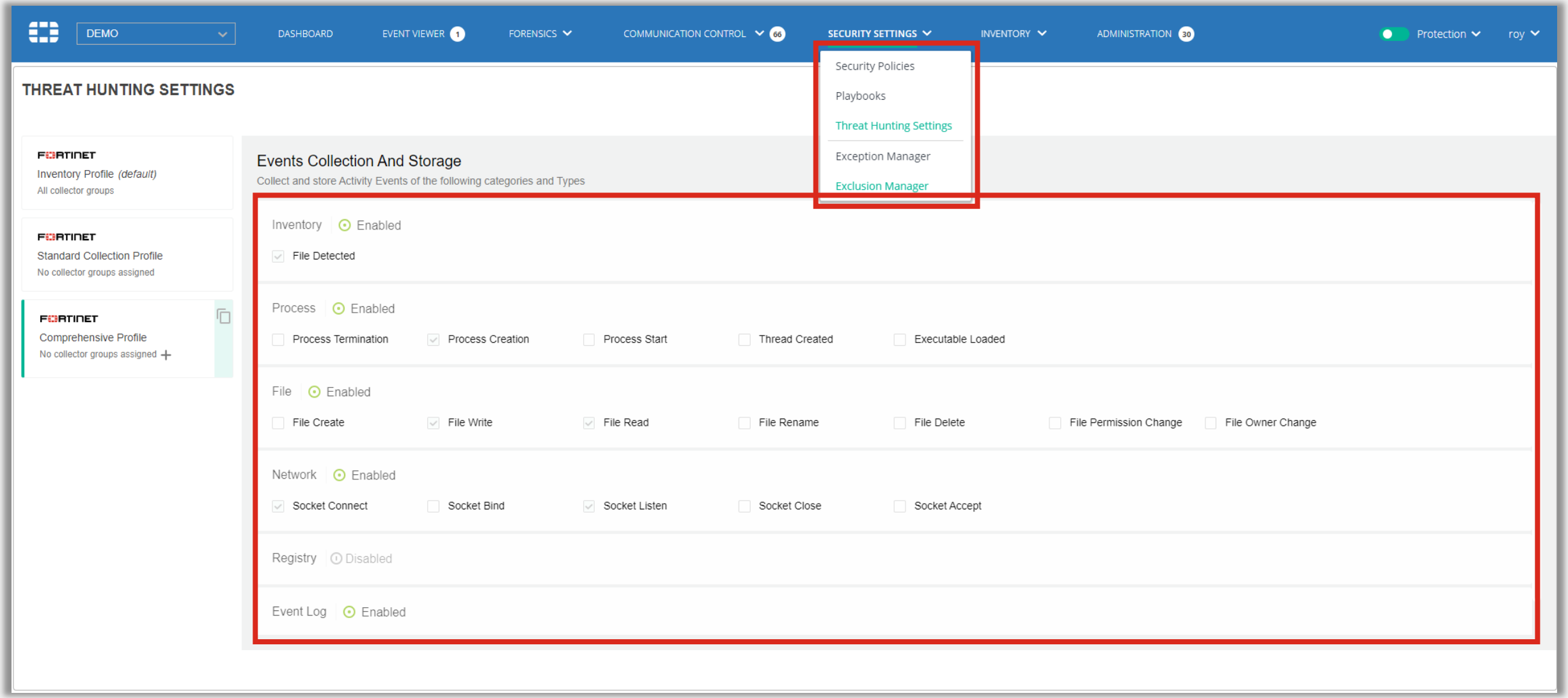
安全聯防提升整體防禦能力

設定要進行自動聯防的Playbook

資安事件觸發聯防動作

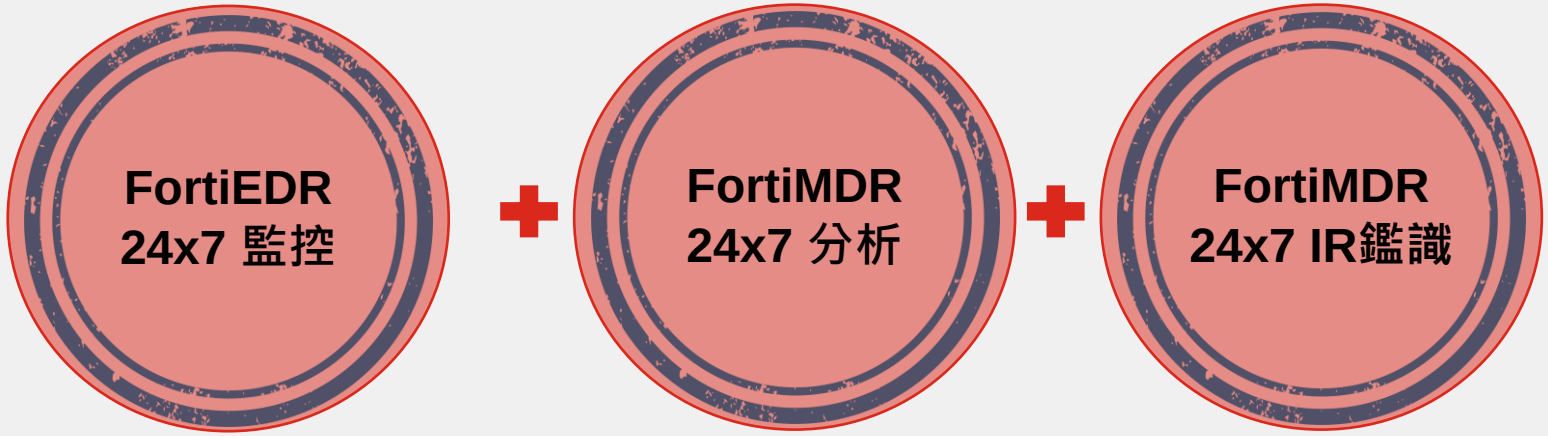
在防火牆上加入惡意IP黑名單進行阻擋

主動式威脅捕獵 –
深度端點軌跡記錄與追蹤以提供即時資安鑑識能力

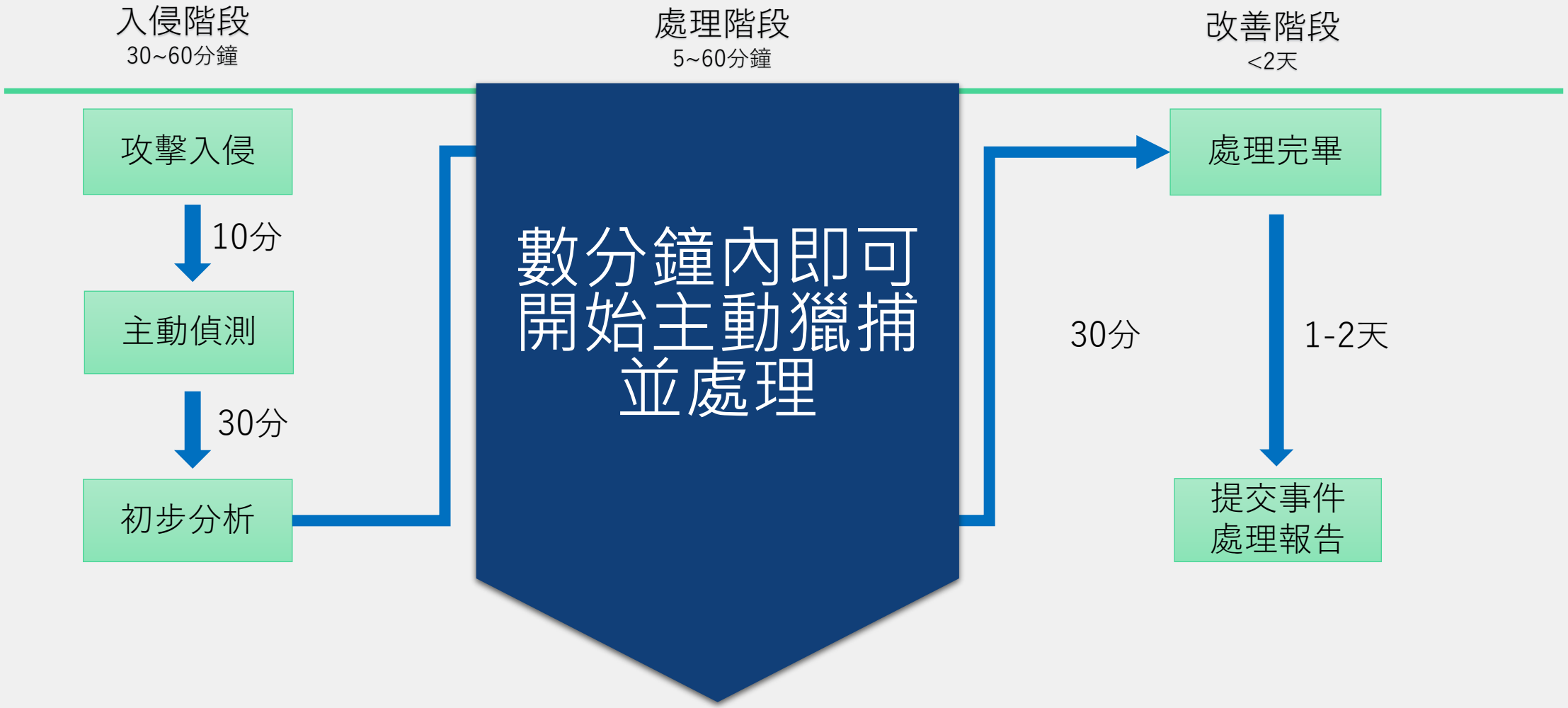


為何需要 MDR 服務…?

- 要分析：EDR產品的保存端點的各種活動資料，需要有人分析才有效益
- 要專業：當EDR發出可疑行為分析警報時，可以有專業技術團隊協助
- 要即時：可以即時透過遠端方式處理威脅，無須等到事後處理
- 要完整：可以提供專業的事件分析報告，完整分析資安事件發生的過程
- 要可控：由專業資安技術團隊提供深入分析，可以減少企業在資安的支出

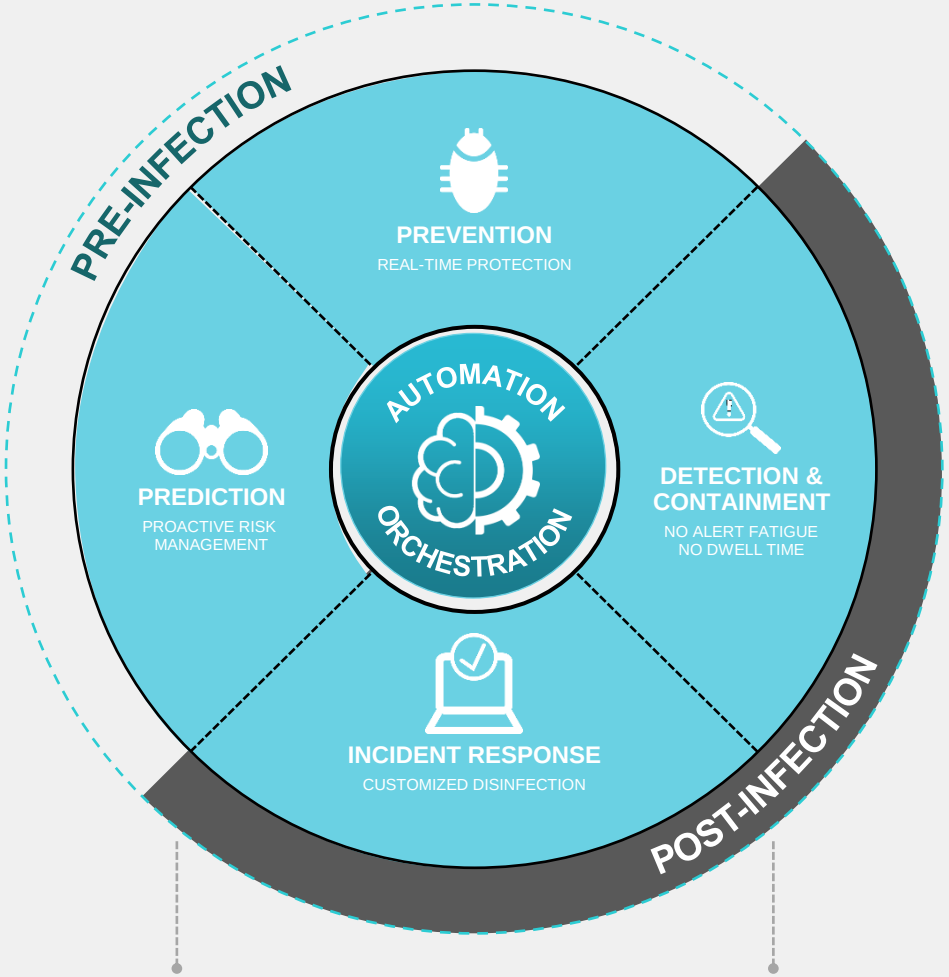


FortiMDR 處理流程



考慮採用進階端點防護的幾個參考建議

- ✓ 是否具備針對未知攻擊手法（如零日攻擊）的檢測與防護能力，經過第三方驗證？
- ✓ 防護時效性（是7x24不間斷的即時防護VS傳統排程式掃瞄）？
- ✓ 端點使用者體驗（作業系統支援度與效能影響）與部署方式的選擇（雲端或落地）？
- ✓ 與現有資安防護體系的整合？
- ✓ 鑑識能力（能記錄那些端點行為軌跡）與專業服務（MDR：本地還是國外遠端服務）？



AV Comparatives. Business Security Tests. March / June 2020 and Aug/Nov 2020.


FORTINET