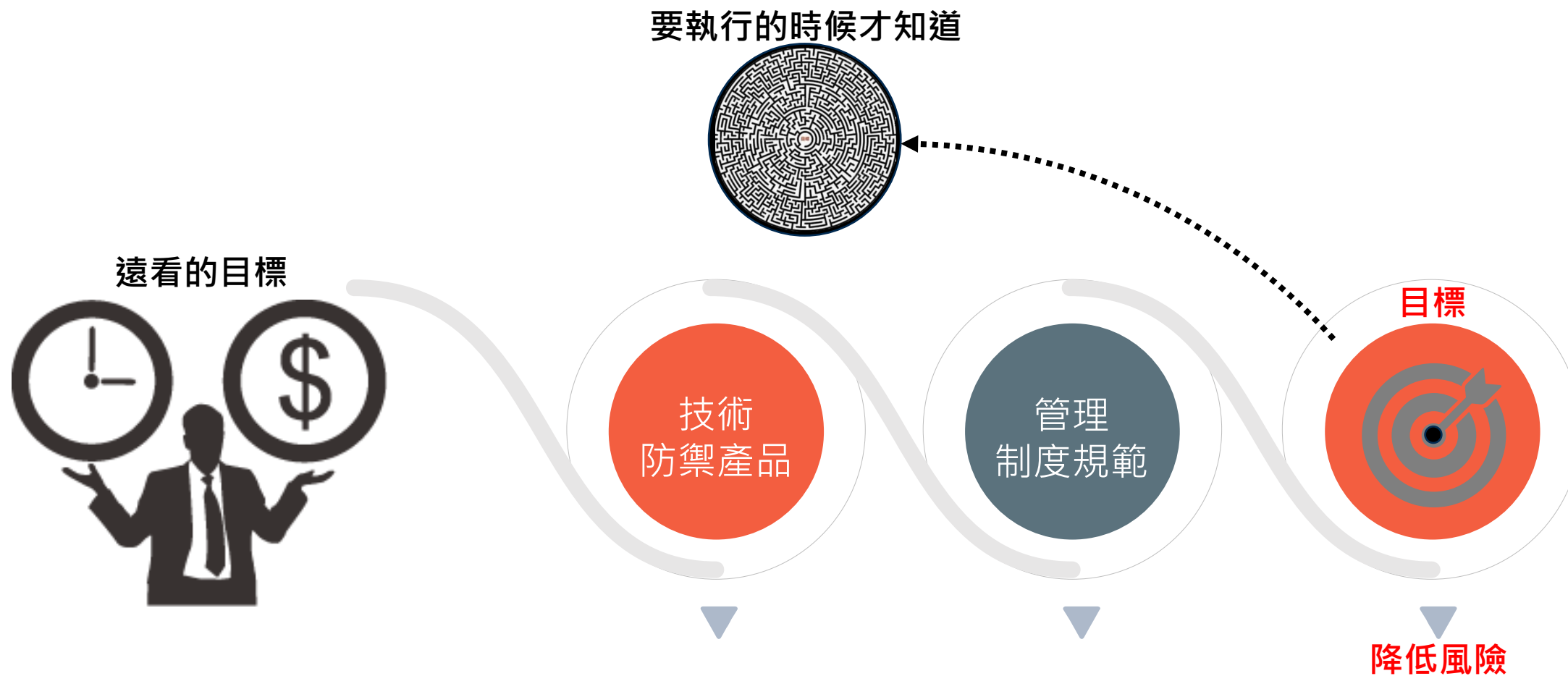


# 啟動資安左移新戰略 - 開闢事前新場戰 -

Speaker : Thomas Huang



# 做好資安的認知及困難

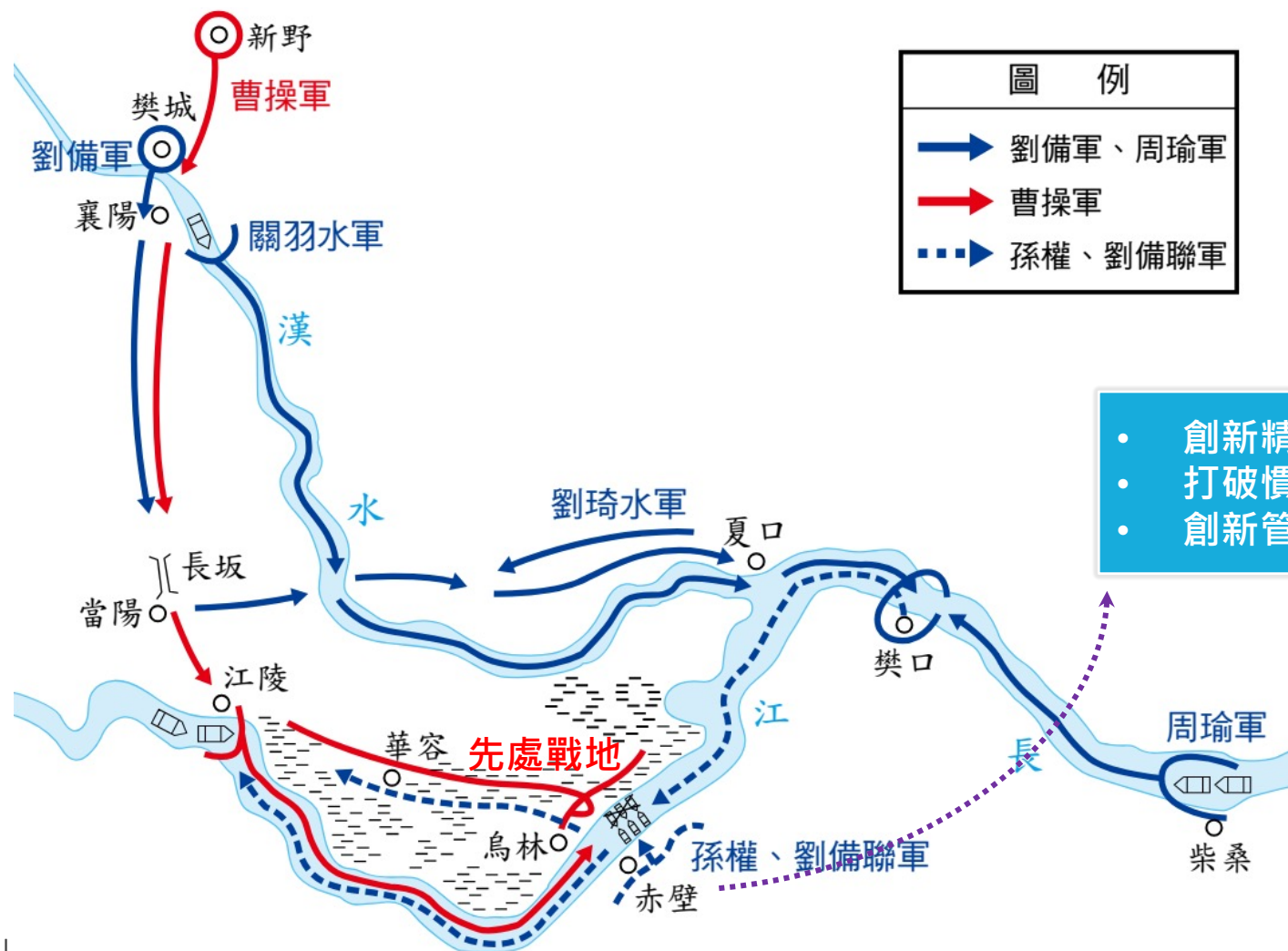


# 資安向左移才能降低風險(快速進兵、出奇制勝)

事前




事中

事後

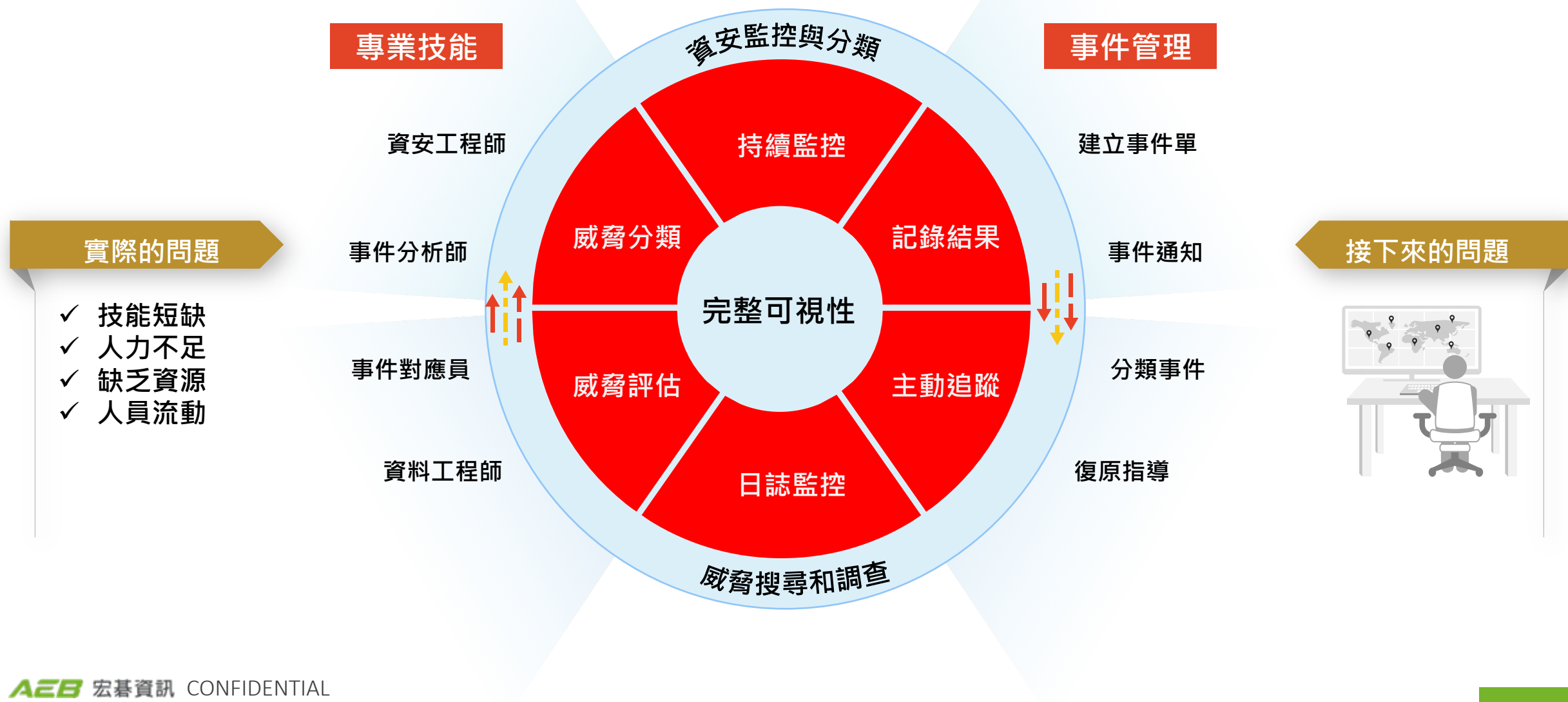


資料來源:張逸泉

# 需求定位

名詞	EDR	NDR	XDR	MDR	
範圍	端點和主機	網路和設備間流量	端點、主機、網路和設備間流量、應用程式	端點、主機、網路和設備間流量、應用程式	
功能	<div>逐漸清晰，逐漸抽象</div> <div><div>360P720P1080P</div></div> <div>• 利用先進的技術和方法來偵測威脅，如 EDR、NDR 等</div> <div>• 提供 24/7 的即時監控和警示</div> <div>• 分析警示當中潛藏的危險徵兆</div> <div>• 提供專業的建議和指導，如隔離、復原、修復等</div>			• 利用先進的技術和方法來偵測威脅，如 EDR、NDR 等 <div>• 提供 24/7 的即時監控和警示</div> <div>• 分析警示當中潛藏的危險徵兆</div> <div>• 提供專業的建議和指導，如隔離、復原、修復等</div>	
優點	可端			• 檢測、 險。	可以為企業減輕資安人力的負擔，並提供及時、有效的處理，以避免損失擴大。
缺點	需並			整合，	需要與服務提供商建立信任和合作關係，並且可能需要支付較高的費用。
意圖	端點/接入區域保護免受滲透、監控和緩解、漏洞評估、警報和回應	網路流量的可視性/透明度、已知和未知威脅和橫向移動的偵測、警報和回應	多個安全（網路、端點、應用程式）的可視性/透明度，包括所有組件、整體監控和緩解、漏洞評估...等等事件的簡化和整合	多個安全（網路、端點、應用程式）的可視性/透明度，包括所有組件、整體監控和緩解、漏洞評估...等等事件的簡化和整合	
方法	惡意行為、攻擊指標、妥協指標、簽名、機器學習	攻擊指標、異常檢測、用戶行為、機器學習	機器學習、攻擊指標、異常檢測、用戶行為、惡意行為、妥協指標	機器學習、攻擊指標、異常檢測、用戶行為、惡意行為、妥協指標	

# MDR委外服務





# 我們提供MDR服務支援廠牌



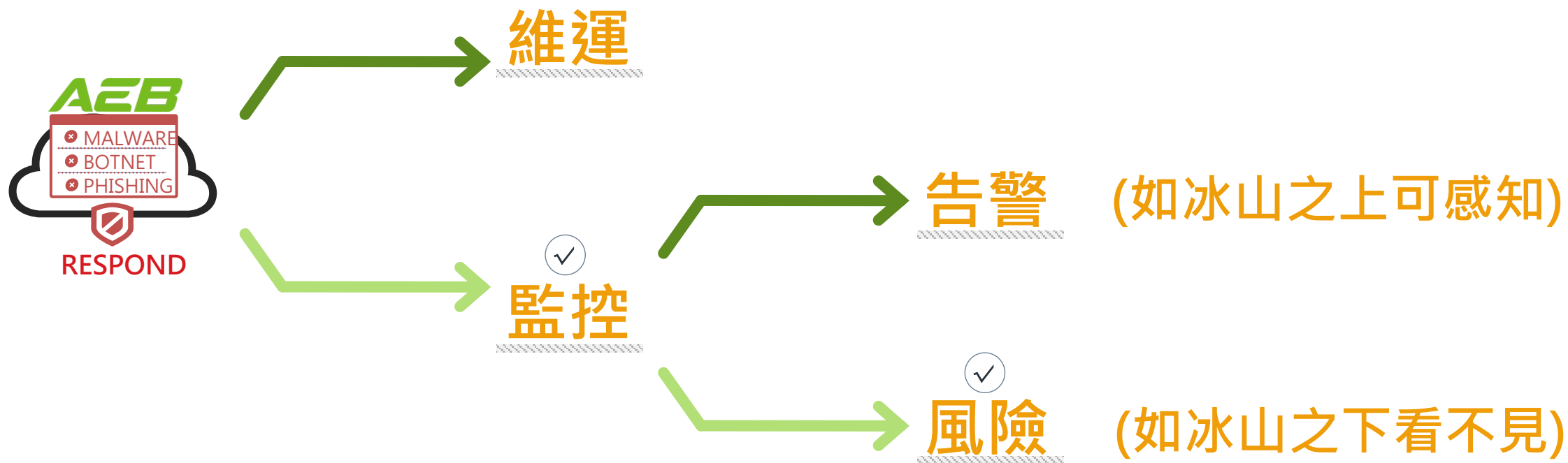
EP Guard端點守護者平台



AcerAeb Threat Response Center  
宏碁資訊台灣資安威脅監控團隊

# MDR服務的角度(理想跟現實差距大)

M=Managed的定義？



# 通報範例(言之有物)

事件編號	事件名稱		
60	'Evasion Technique - 361082167' generated by XDR Agent detected on host I227 involving user user		
開單時間	主機名稱	主機IP	風險等級
2024-02-08 17:05:43	I227		high
關聯主機			
無			
事件說明			
宏碁資訊MxDR團隊發現端點"I227"觸發'Evasion Technique - 361082167'事件。			
此行為是由於該主機企圖載入Alternate Data Stream之dll，故被XDR Agent判定為使用規避技術之可疑行為。			
此事件與事件單ID-9執行之程式相同，故判定為相似事件。			
風險說明			
使用Alternate Data Stream規避技術，可能可將惡意指令或惡意檔案掛載於正常檔案中，進而規避防毒軟體或其它防護機制。			
詳細內容請參考如下連結： <a href="https://cyrilwang.pixnet.net/blog/post/25654801">https://cyrilwang.pixnet.net/blog/post/25654801</a>			
調查結果			
經確認為使用者"suser"執行位於外接式儲存裝置上的程式"G:\agent.exe"，並載入usbtools.dll，而被判定為使用Alternate Data Stream規避技術而觸發通報。			
程式的數位簽署者為Hengyida Information Technology CO.,LTD.，為位於中國成都的四川恒易达信息技术有限公司；該簽章曾頻繁的簽署其他帶有PUA的程式，可藉此規避部分防護軟體的阻擋。			
立即處理建議			
建議確認該位於外接裝置上的程式是否為單位內部所允許的應用程式，並請該使用者勿於公務電腦上執行或開啟非公務相關的檔案或程式。			
後續改善建議			
用者名稱為本機帳號，較難追查操作者為誰。 如電腦有共用的必要，建議採取適當的防護手段，如封鎖USB或是限制該共用帳號的執行權限。			
發現惡意程式或連線之惡意中繼站			
未發現惡意程式或連線至惡意中繼站行為。			

1 探索問題

2 掌握問題特徵

3 探索關聯性

4 確認因果關係

5 尋找可能的對策

6 執行最佳對策



# 總結

左移的觀念  
(預防)

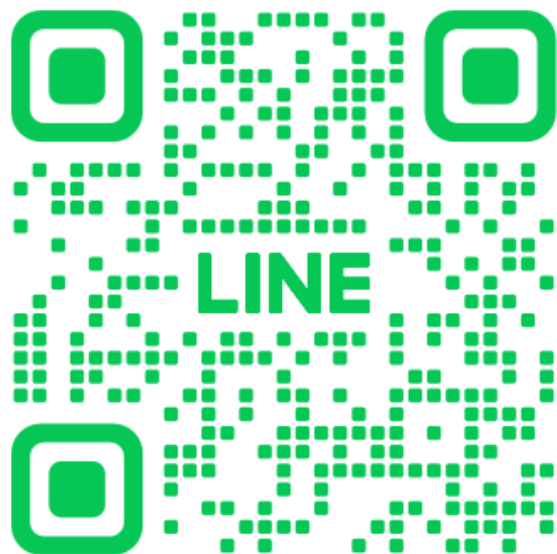
完整可視性  
(XDR平台)

服務的認知  
(MDR服務)

MDR服務  
記得找AEB

**AEB**

現場抽獎



2024資安大會-AEB 議程問卷：啟動  
資安左移新戰略





*The Best  
is Yet to Come !*