後疫情時代之資安保衛戰
不隨風起舞、不變應萬變

陳勇君 Sunrise
精誠集團/智慧資安
博士
SunriseChen@uniXecure.com.tw
CISSP · ISO 27001/27701 LA

簡報綱要

資安事件的省思-【黑抓黑】時代，已經過時!

資安我軍編制 – 四大金剛

- 1. 情資驅動之資安主動防護趨勢 (外部資安評級情資系統)
- 2. 機器學習之網路異常分析機制 (資安我軍機器人)
- 3. 我軍白帽合縱代管趨勢 (MoC + 資安常年顧問)
- 4. 最後一道資安防線 (端點程式白名單機制 + 機動備份)

問題討論

資安事件的省思

1. 國內知名券商/被偽冒下單/資安事件

2. 國內/石化業者/勒索病毒/資安事件

帳號填充攻擊【Credential Stuffing】來勢洶洶

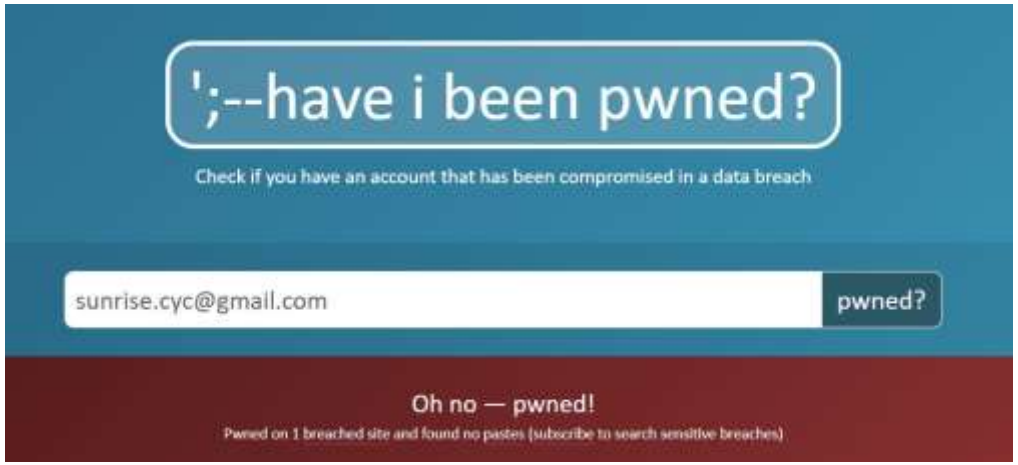
資料來源 (2019-0611)： https://www.ithome.com.tw/news/131199

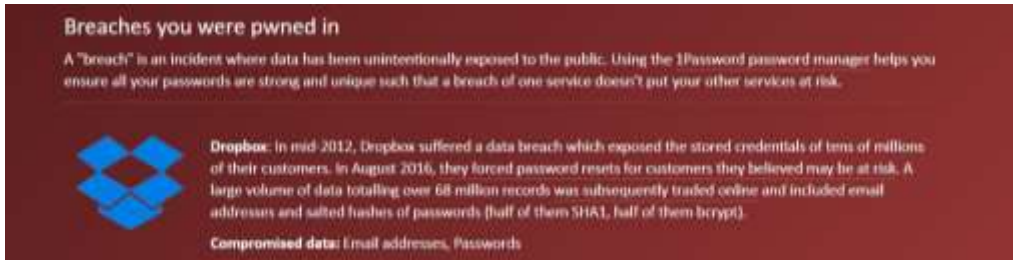
殭屍網路帳密撞庫攻擊 6 券商慘「被下單」

元大證券、凱基證券等在 110 年11月，遭到駭客以常見的「密碼撞庫攻擊」手法，冒名客戶下單買港股的資安事件，引爆各界關注。（圖 / CTWANT合成）

資料來源 (2019-0611)： https://fnc.ebc.net.tw/fncnews/headline/144157

我的最愛【帳密】是否已經被偷? 帳密無用論!





- Have I Been Pwned 網站，共收錄【615 個】被駭網站、逾【118 億】筆帳號
- 讓使用者輸入用來做為帳號的電子郵件信箱查詢。
- 建議：每個月，都應該定期檢查一下!

https://haveibeenpwned.com/

以駭制駭 – 步步危機

我們一同住在地球上

- 我們的【世界】緊密相連
- 我們的【系統】緊密相連

駭客眼中，我們的【身分】不堪一擊

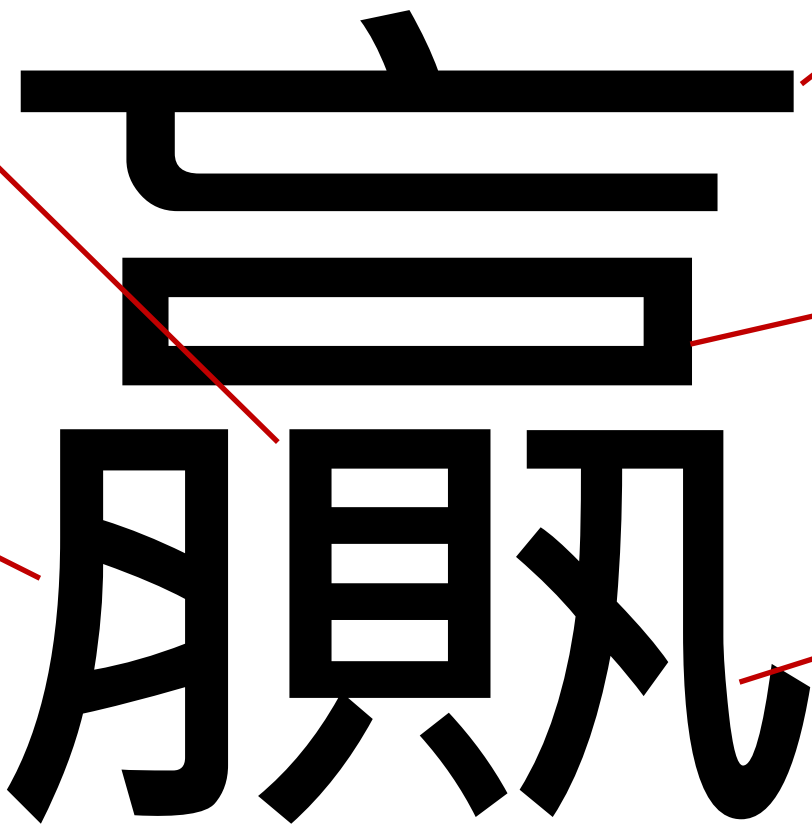
- 國家、家園、秘密、財產、安全 也是【不堪一擊】

因為，駭客可以攻擊

- 【任何人】：專挑【軟柿子】吃
- 【任何事情】：僅要連上網路
- 【任何地方】：無遠弗界，法力無邊

資料來源： Google 圖片，版權歸該搜尋網址與該公司團體所有.

為何駭客贏了，我們輸了！



貝：
駭客資源
衝動利誘
贏出價值

月：
陰魂不散
日積月累
贏得先機

亡：
沒有遠慮
必有近憂
贏得未來

口：
口碑相傳
我死你死
贏得感動

凡：
平凡小事
稀鬆平常
贏出信心

原來 APT/ 駭客 一直都【在】！一直都【贏】！

資安事件的省思

1. 國內知名券商/被偽冒下單/資安事件

2. 國內/石化業者/勒索病毒/資安事件

【國內石化業者】資安事件的省思

該買該建的資安措施都做了！為何還是失效？

- 導入 新世代防火牆、入侵偵測系統、SOC / SIEM、WAF、防毒軟體、APT 等防禦機制，卻仍【無法及早偵測發現 & 阻擋攻擊】？

因為駭客用【合法帳號/OS 內建程式】，所以都沒警示 ...

- 透過 MITRE 駭客戰術，【繞過/躲過】層層資安防護，
- 加上運用【OS 內建程式 (例如：Windows/PowerShell)】，【異常參數】下載惡意程式 (MimiKatz)
- MimKatz 直接竊取記憶體【暫存登入憑證】，不用側錄/猜測
- 立即變臉【特權帳號(AD 管理者)】，然後 ...

為何資安防護方案還是不足夠？還是失效？

不好管

- 資安設備越來越複雜，資安人員卻【很難接受足夠的訓練】

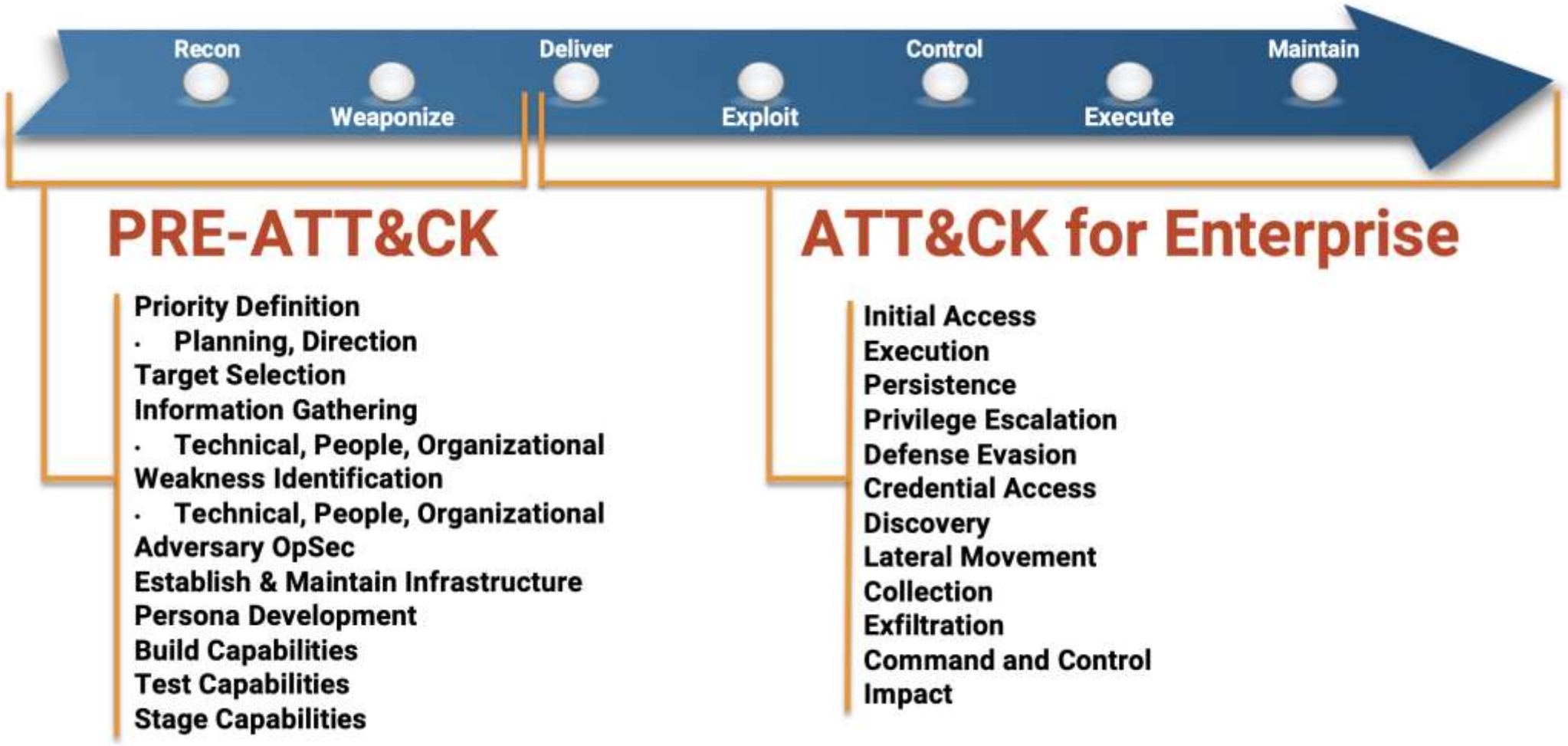
不能管

- 資安設備【警報量指數暴增】，處理警訊的效率跟不上

不夠快

- 當攻擊者穿透資安設備，客戶/廠商處理與反應的【時間太慢】

【訂計畫/設組織】之駭客攻擊策略



MITRE Att&ck (駭客攻擊策略)

資料來源： Google 搜尋/圖片結果，版權歸該搜尋網址與該公司團體所有.

【具戰略/備戰術】之駭客攻擊策略

MITRE Att&ck Matrix（駭客攻擊策略) for Enterprise

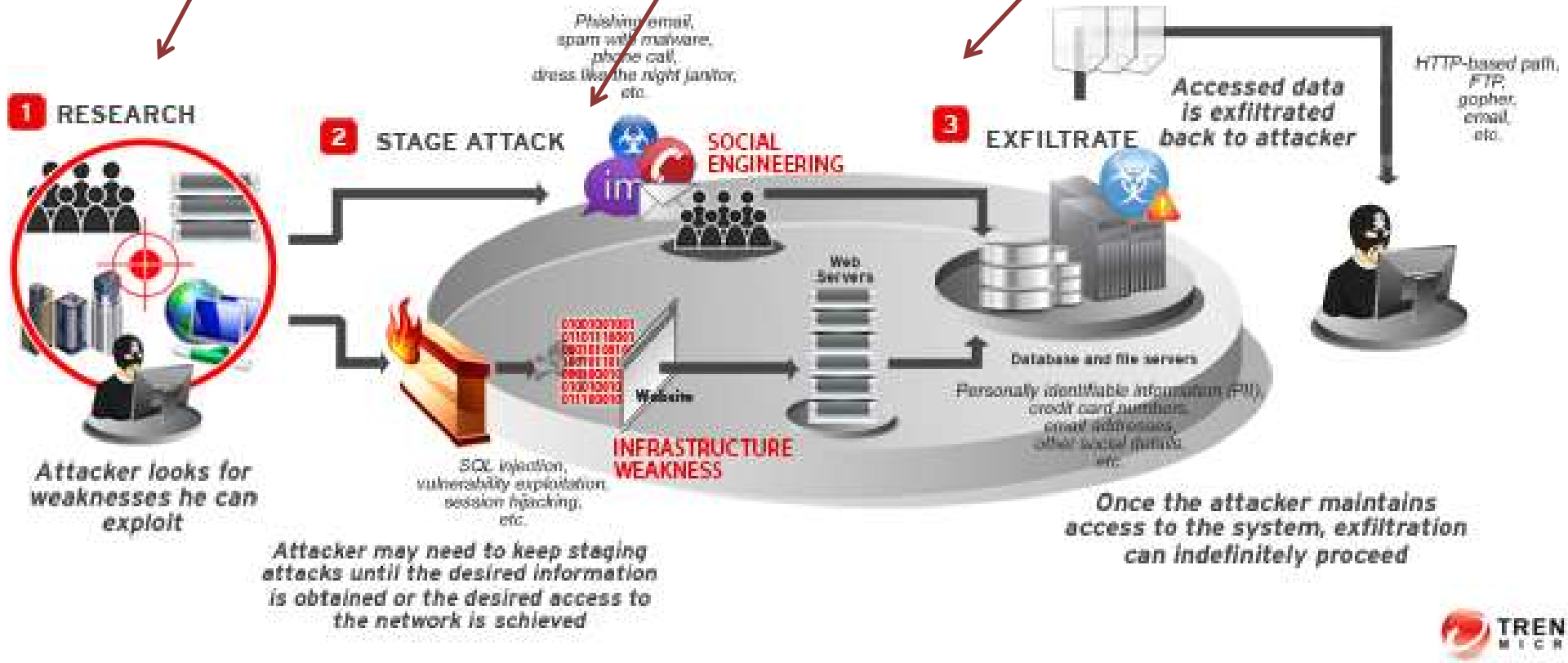
資料來源： Google 搜尋/圖片結果，版權歸該搜尋網址與該公司團體所有.

駭客攻擊程序：長期佈局、陰魂不散

情蒐與研究

網路攻擊
SE 攻擊

破壞/奪權/竊資



MALICIOUS DATA BREACH DIAGRAM

資料來源： https://blog.trendmicro.com.tw/?p=59745#more-59745

MoC = More Than SoC 的主動防禦

面對各種攻擊威脅，
應採取積極探索的方式，

從「被動反應 (SoC)」
改為「主動防禦 (MoC)」！

資料來源：https://www.ithome.com.tw/news/122072

藏鏡人（紅軍）vs 史艷文（我軍）

【情資】落差

- 後知後覺、不知不覺

【功力】落差

- 黑色產業鏈：龐大財力/深厚功力
- MITRE Attack

【速度】落差

- 情資爆炸、管理負擔、行政流程、溝通協調
- 觀看、分析、判斷、鑑識、處置、應變 都需要專業判斷與人力投資!

後疫情時代之資安防護思維

資安事件層出不窮，資安思維調適轉型

- 漏洞【不斷發現】、不斷【風險處理】
- 繼續【貓抓不到老鼠】，還是【守株待兔/不變抓萬變】

【黑抓黑】合縱連橫【白抓黑/白擋黑】資安我軍

- 企業機關【現有】資安團隊 +【友軍部隊】
  - 資安情資部隊 + 資安 AI 機器人 +
  - 資安代管部隊 + 資安常年顧問部隊 (含資安職能教育訓練學程)

【情資驅動、白抓黑、白擋黑】
雲端資安主動防禦新趨勢

資安需求趨勢

為何應該【白抓黑】&【白擋黑】? – 1/2

因為【黑抓黑】，代表【以黑追黑】，極有可能【追不到】...

- 既然是【追】，就表示我們是在後面【追】駭客，就表示可能【追不上】!
- 如果真要【追上】，不但【產品】要追得上，連【資安同仁的資安專業】也要追得上 ...
  - 貓當然有機會可以抓到老鼠，但是在資安領域中，我們 資安同仁&委外廠商是否具備【貓抓老鼠】的能力？

為何應該【白抓黑】&【白擋黑】? – 2/2

或許我們追不上駭客，但是我們卻比駭客【更加清楚知道】我們的環境！

- (1) 透過【外部資安評級情資服務】，至少【知己知彼】同步跟駭客的資安情資。
- (2) 駭客攻擊，一定會在【網路】與【Server/PC】上面留下執行過的軌跡紀錄!
  - 透過如同行車紀錄器一般，使用【網路紀錄器】& 【電腦紀錄器】來清楚了解
  - (A) 知道單位內的【正常(白名單)的網路行為】
  - (B) 也可清楚知道【Server/PC】執行那些【正常(白名單)的應用程式】!
- (3) 然後藉由資安專家代管代分析(MoC) & 資安常年顧問，進行事前及早發現、事中立即警示、事後應變鑑識！
- (4) 最後一道防線，不讓【惡意程式(勒索軟體)】執行 & 【機動備份】!

1. 情資驅動資安主動防護趨勢

外部資安評級【情資】服務

黑色產業鏈(駭客紅軍) – 財力雄厚/武力強大

資料來源： Google 搜尋/圖片結果，版權歸該搜尋網址與該公司團體所有.

2022/07 比特幣【最新行情】財力越來越強

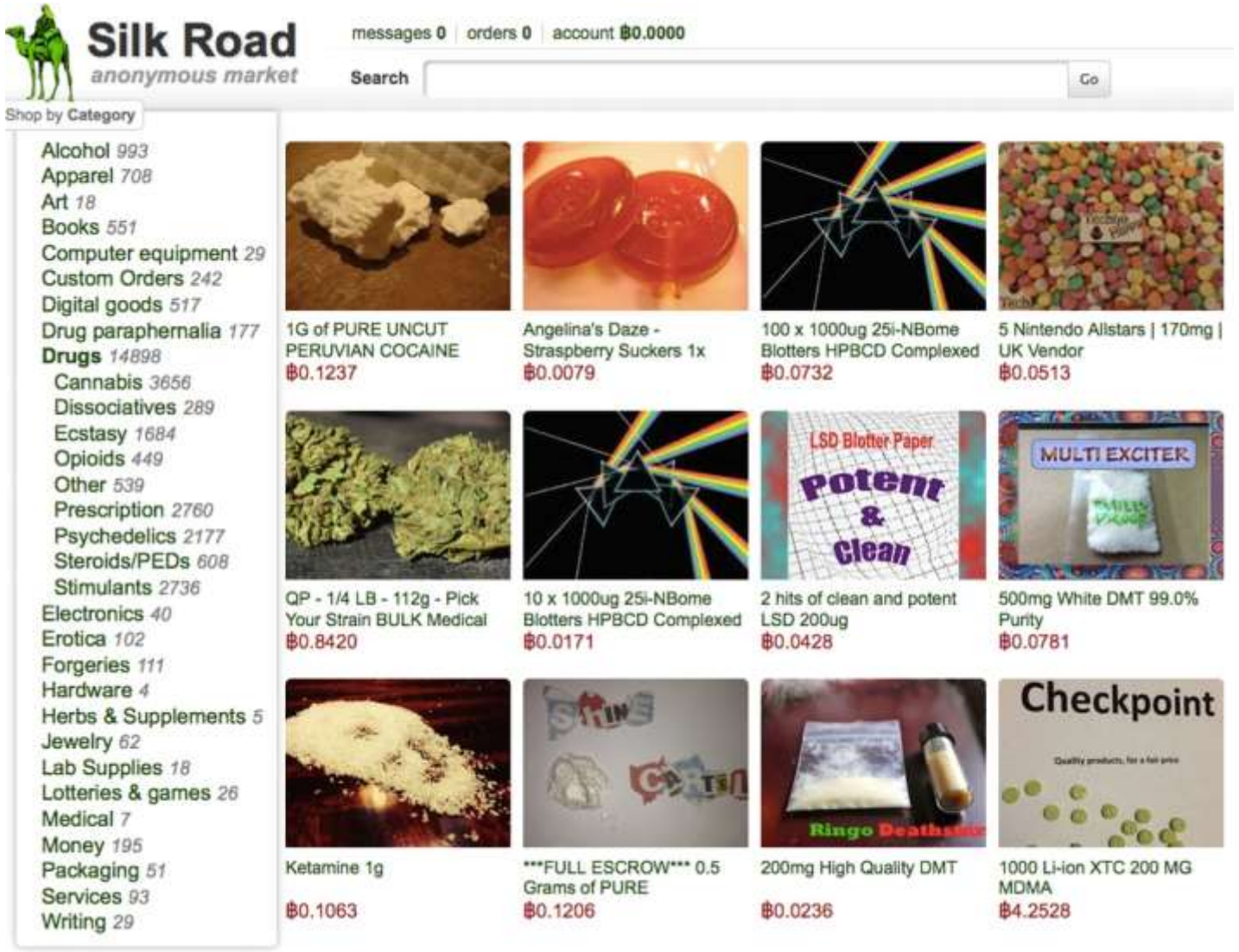
↑	20,143.02	最高價 (24h)
↓	19,055.31	最低價 (24h)
$	13.30 億	成交量 (USD)

GandCrab 勒索病毒宣布收山 – 賺了 20E 美元後

- GrandCrab 首次出現在 2018/01 月份，特色是快速改版，並且黑色產業鏈策略聯盟，每位組織內的駭客至少賺了 150 萬美元，準備快活退休去囉。
- 那些被 GandCrab 加密的受害者，駭客也呼籲儘速付款，否則 20天後解密金鑰就會被刪除，資料也永遠救不回來了。 <<2019/06/03>>

資料來源： https://www.ithome.com.tw/news/131042

【破獲】轟動全世界的暗網線上販毒網站



資料來源： Google 搜尋/圖片/影片結果，版權歸該搜尋網址與該公司團體所有.

暗網【實體綁架】案例

我的經歷非常可怕。每一秒、每一分，每一小時，我都擔心會沒命。

1.1 外部資安評級服務

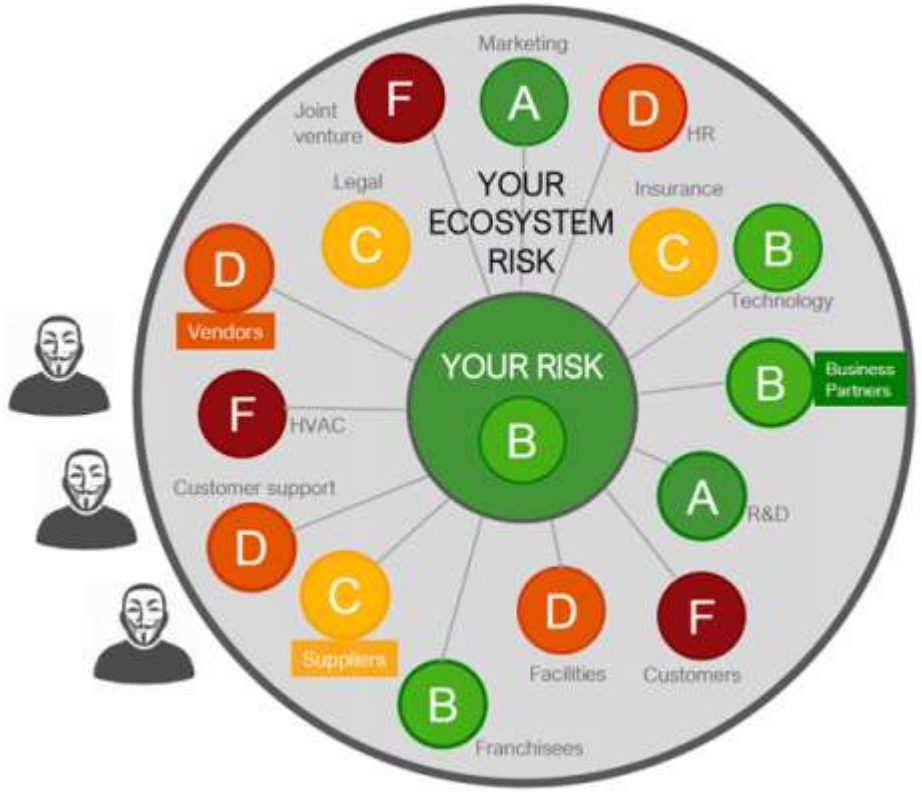
企業單位自己

關係企業

供應鏈/委外資服廠商

...

機關 63% 的資安事故-源自【生態系】資安漏洞



- 資訊安全【不再是】自己資訊處做好即可，所有系所、社團、委外資服廠商、供應鏈、合作廠商，已經構成一個【資安共同生態系】！
- 任何一個生態系的成員的資安水平都會【相互關聯與衝擊影響】！
- 駭客往往從【生態系較弱成員】下手攻擊，然後可以快速與便利地成功【擴散/蔓延/感染/牽累】到【整個生態系】！
- 所以【整體生態系風險管理】儼然成為資安防護趨勢

資料來源： Google 搜尋/圖片/影片結果，版權歸該搜尋網址與該公司團體所有.

【白抓黑】&【白擋黑】的四大資安我軍機制 (1/4)

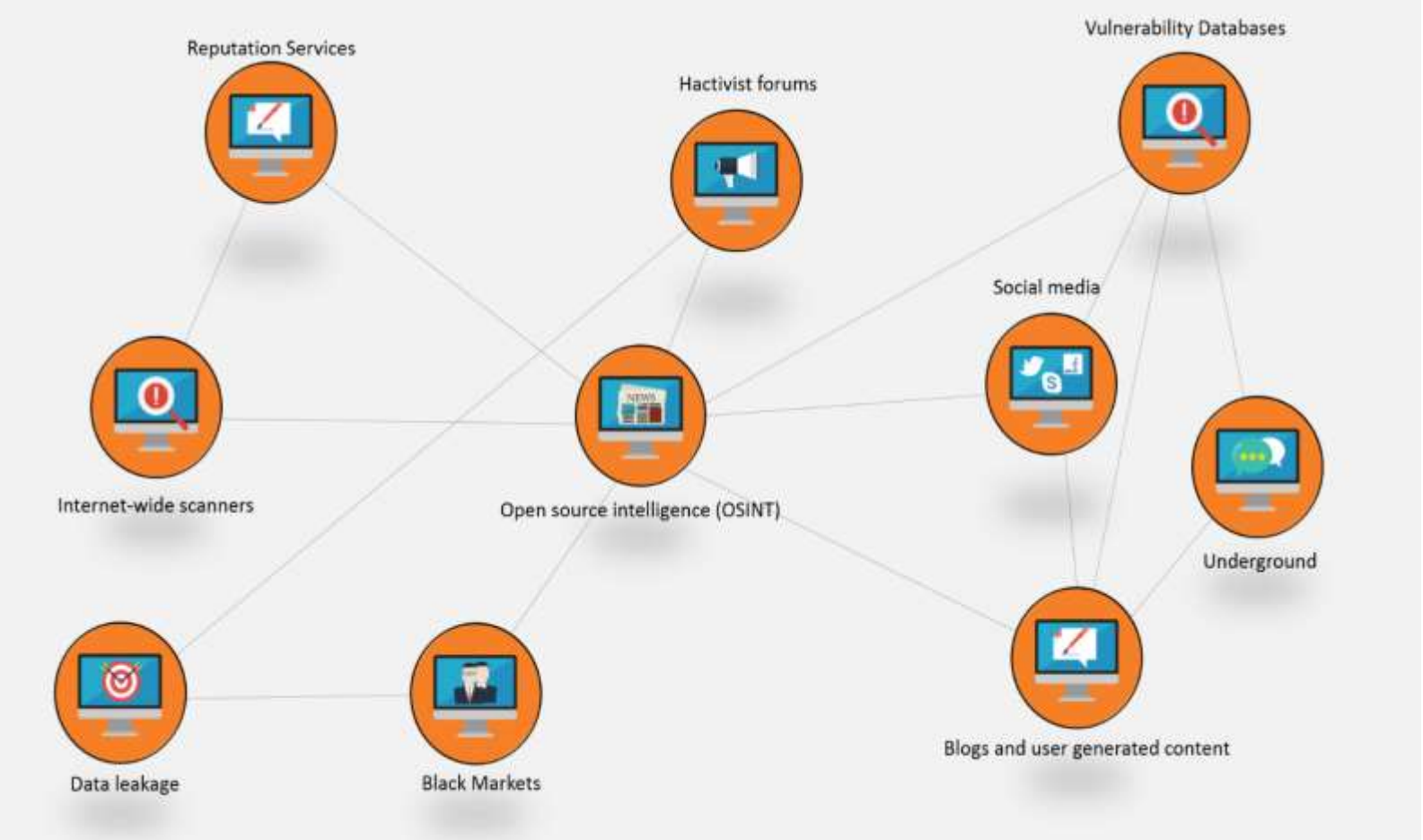
1. 網駭情資通報機制：外部資安評級情資服務

- 最可怕的風險：
  - 【駭客知道，我們卻不知道】的資安弱點或者問題
  - 如同我們不知道【武漢肺炎】的帶原者在哪裡？
- 外部資安評級情資服務
  - 【7 x 24】全天候，全世界大數據分析，【知己知彼】的資安評級
  - 單位對外，委外廠商、供應鏈 等 所有數位服務足跡之【20 個】資安構面涵蓋
  - 資安風險立即警示：
    - 資安評級分數【降低】、重大弱點/問題【被駭客發現】、暗網【機敏外洩】、...
  - 完整/清楚的【弱點/問題】的說明與【改善處理建議】

何謂【外部資安評級情資服務】？

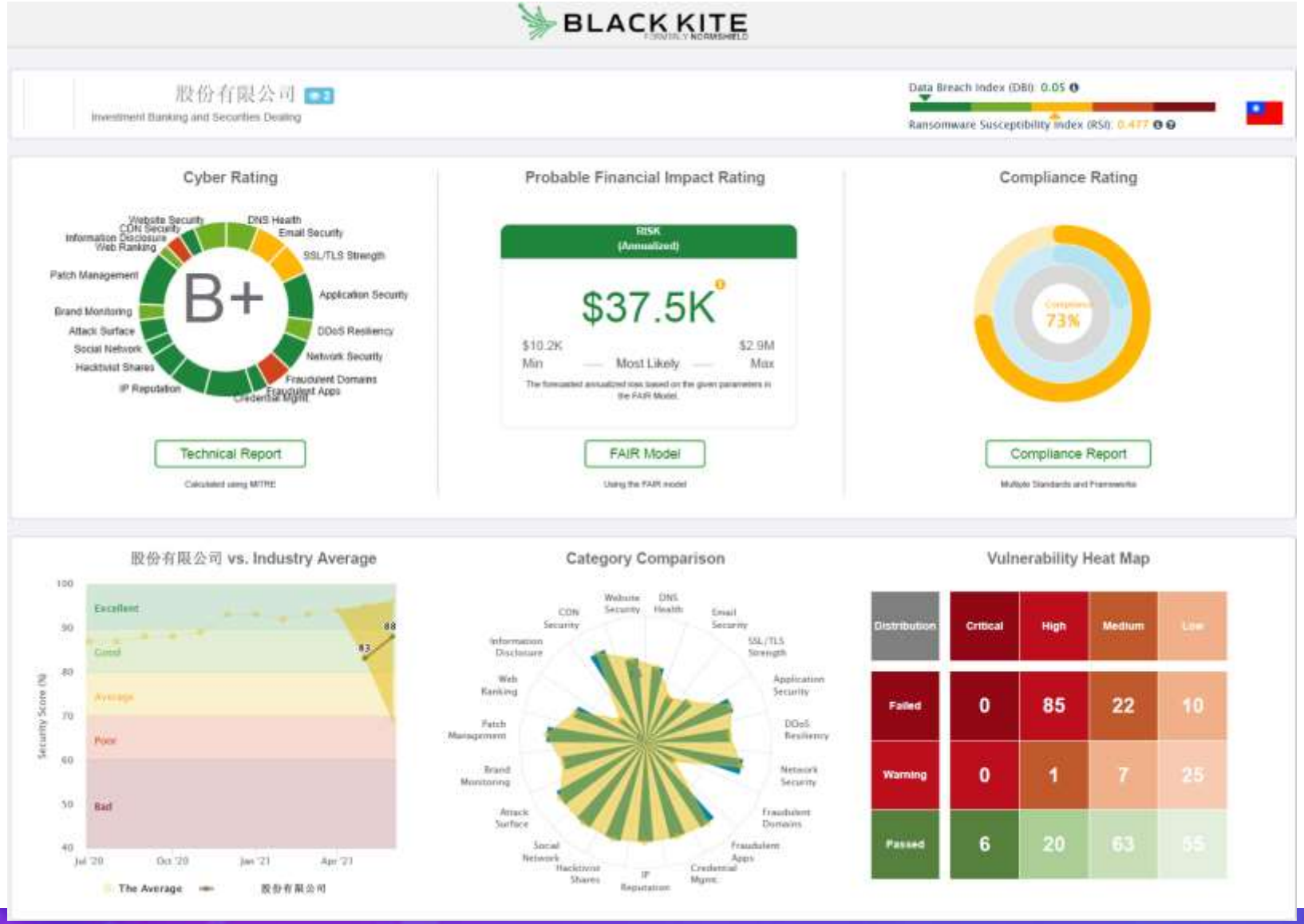
- (a)【沒有】侵入式弱掃
- 也【沒有】進行滲透測試
- 而是完整收集網際網路上面(包含暗網，駭客論壇，地下弱掃網站、情蒐網站、OSINT、CeBKys、Shodan、Zoomeye)的大數據分析。

- (b) 以【外部與駭客】角度
- 檢視企業機關的【全球數位足跡(Digital Footprint)】
- 運用【4 個】資安構面，【20 個】資安領域類別來分析 貴企業機關 的資安等級
- 也包含貴企業機關在【同業水平】的資安評價比較



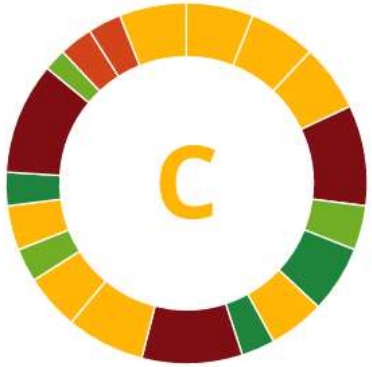
【外部資安評級情資服務】方法論

外部資安評級情資服務範例報告【上半部】



外部資安評級情資服務範例報告【下半部】

BlackKite 資安外部評級計分【三大】指標



資安【技術問題】指標

- 運用 MITRE 公認公開之資安評分標準
- 提供企業機關資安主管快速【資安評級(字母表示法)】
- 讓資安技術主管可以【往下詳探】每個資安領域的安全議題。

MITRE

資安【財損預估】指標

- FAIR 是目前唯一公開公正的【資安衝擊財損量化模式】的國際標準。
- 因此，BK 使用 FAIR Model 來計算【當單一資安事故發生時，對特定企業機關可能的財物損失衝擊影響】。

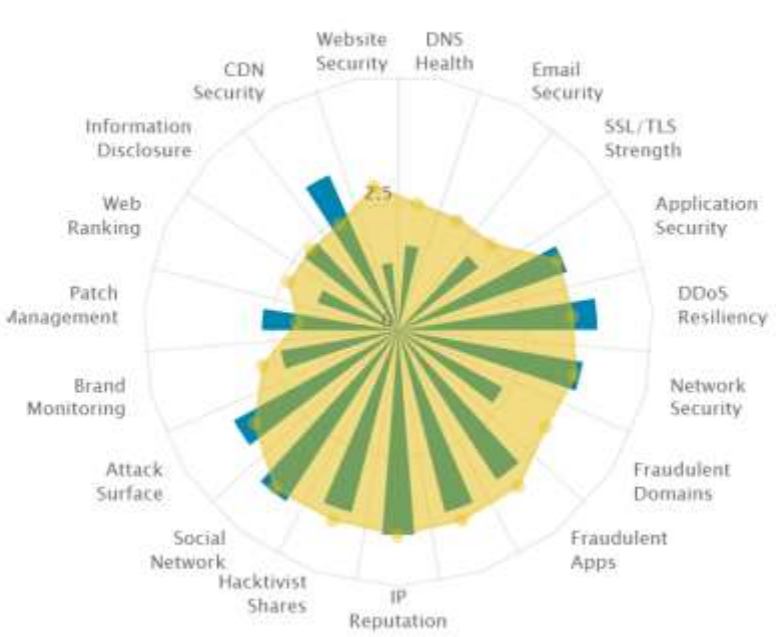
FAIR INSTITUTE

資安【合規】指標

- 根據【網駭空間發現】，關聯分析相對資安標準與法規之控制項目，判別該控制項目可能的符合程度。
- 包含：ISO 27001、PCI-DSS、GDPR、HIPAA、NIST 800-53 等等。

SFG SHARED ASSESSMENTS

資安評級趨勢變化/同業比較/領域優劣/熱點發現



資安變化/同業比較

【紫色曲線】代表【自己機關】
【黃色區域】代表【同級機關】

每個資安【領域】優劣分析

【藍色條棒】代表【自己機關】
【黃色區域】代表【同級機關】

資安問題【熱點】快搜

主要觀察重點：Failed 的
Critial & High

【20 個】資安領域類別 &【500+】檢查控制項目

【20 個】資安領域類別 &【500+】檢查控制項目

皆可『Drill-Down』到詳細說明

2. 機器學習之網路異常分析機制

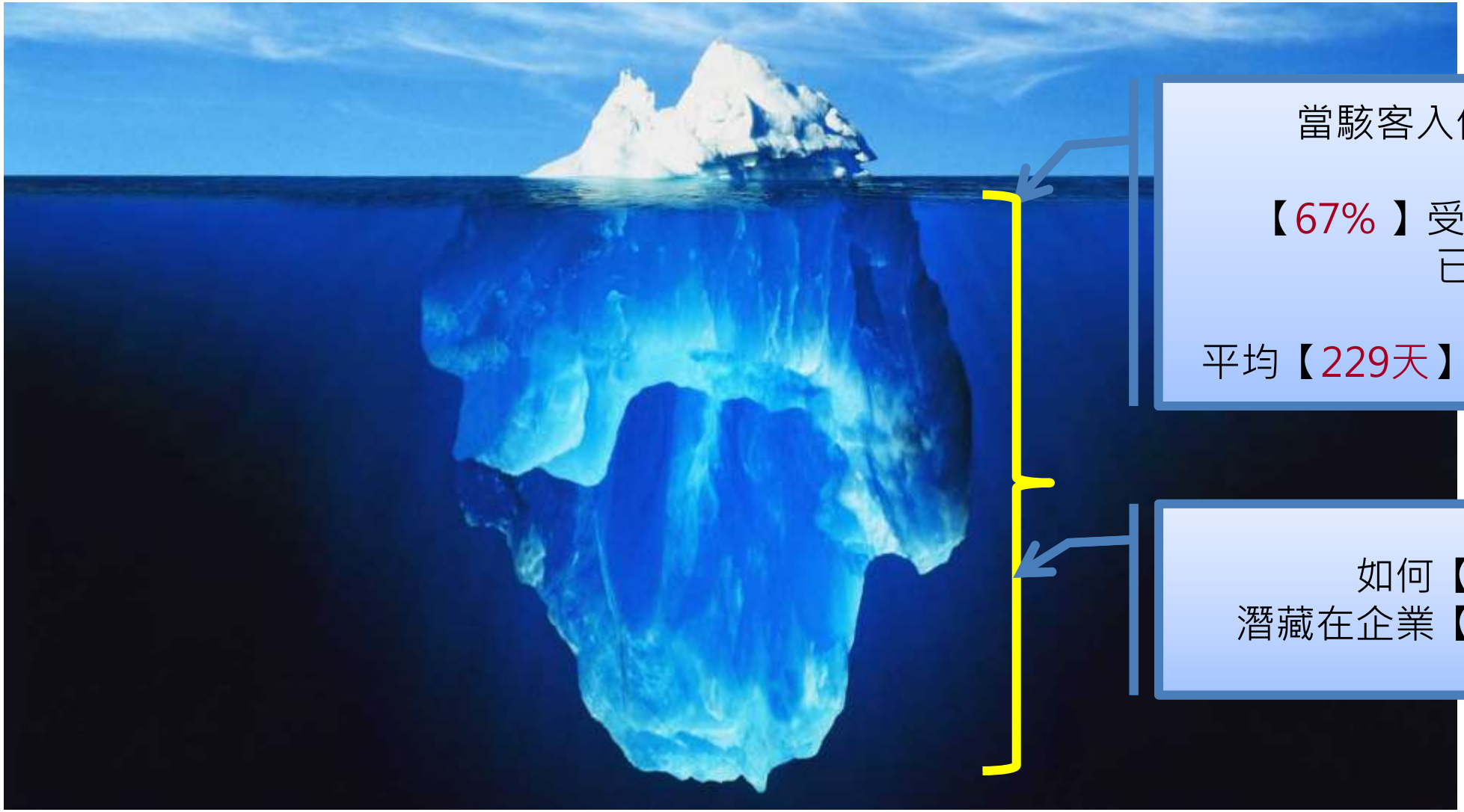
網路行為白名單【機器學習】
當駭客用 AI 自動化攻擊我們
僅有機器人【才有機會打贏】機器人

資料來源： Google 搜尋/圖片/影片結果，版權歸該搜尋網址與該公司團體所有.

機器人戰爭時代已經來臨 vs 資安我軍

資料來源： Google 搜尋/圖片結果，版權歸該搜尋網址與該公司團體所有.

沒看到 -【不表示】真安全



當駭客入侵到企業內部時

【67% 】受駭的企業沒有察覺
已被入侵

平均【229天】受駭的企業才會發現

如何【提早洞察】
潛藏在企業【暗處潛行】的威脅

資料來源： Google 搜尋/圖片結果，版權歸該搜尋網址與該公司團體所有.

魔鬼終結者：黑暗宿命 - 末日再臨

一般人打不贏機器人

一般企業打不贏駭客

資料來源： Google 搜尋/圖片結果，版權歸該搜尋網址與該公司團體所有.

同仁【真正/了解】企業網路是否【不尋常】行為?

每家公司的網路架構/網路行為【都不相同】

- 而且還在每天【變化、調整、遽增】、甚至【加密】

當資安事件還是發生，就表示資安設備失效

- 但是【一定】有網路行為發生，才能導致【奪權、破壞、竄改、竊資、斷服務】

有心人士運用【合法帳號管道】，進行不尋常網路行為連線時

- 通常資安設備【不會發現、不會警示】

我軍需要有 A.I. 機器部隊 – 讓網路異常無所遁形

我軍需要

- 越來越熟悉、越來越智慧

機器人

- 自我學習、自我成長、不會請假、不會生病
- 不用升遷、不會離職、沒有脾氣、沒有情緒

每天經驗專業都能持續傳承

- 看得懂、記得住、比得出、擋的掉

$$P(\theta_k|\mathbf{D},\mathcal{M}_k) = \frac{P(\mathbf{D}|\theta_k,\mathcal{M}_k)\,P(\theta_k\,|\,\mathcal{M}_k)}{P(\mathbf{D}\,|\,\mathcal{M}_k)}$$

$$P(\mathbf{D}\,|\,\mathcal{M}_k) = \int P(\mathbf{D}\,|\,\theta_k,\mathcal{M}_k)P(\theta_k\,|\,\mathcal{M}_k)\,d\theta_k.$$

企業網路免疫系統 (EIS)

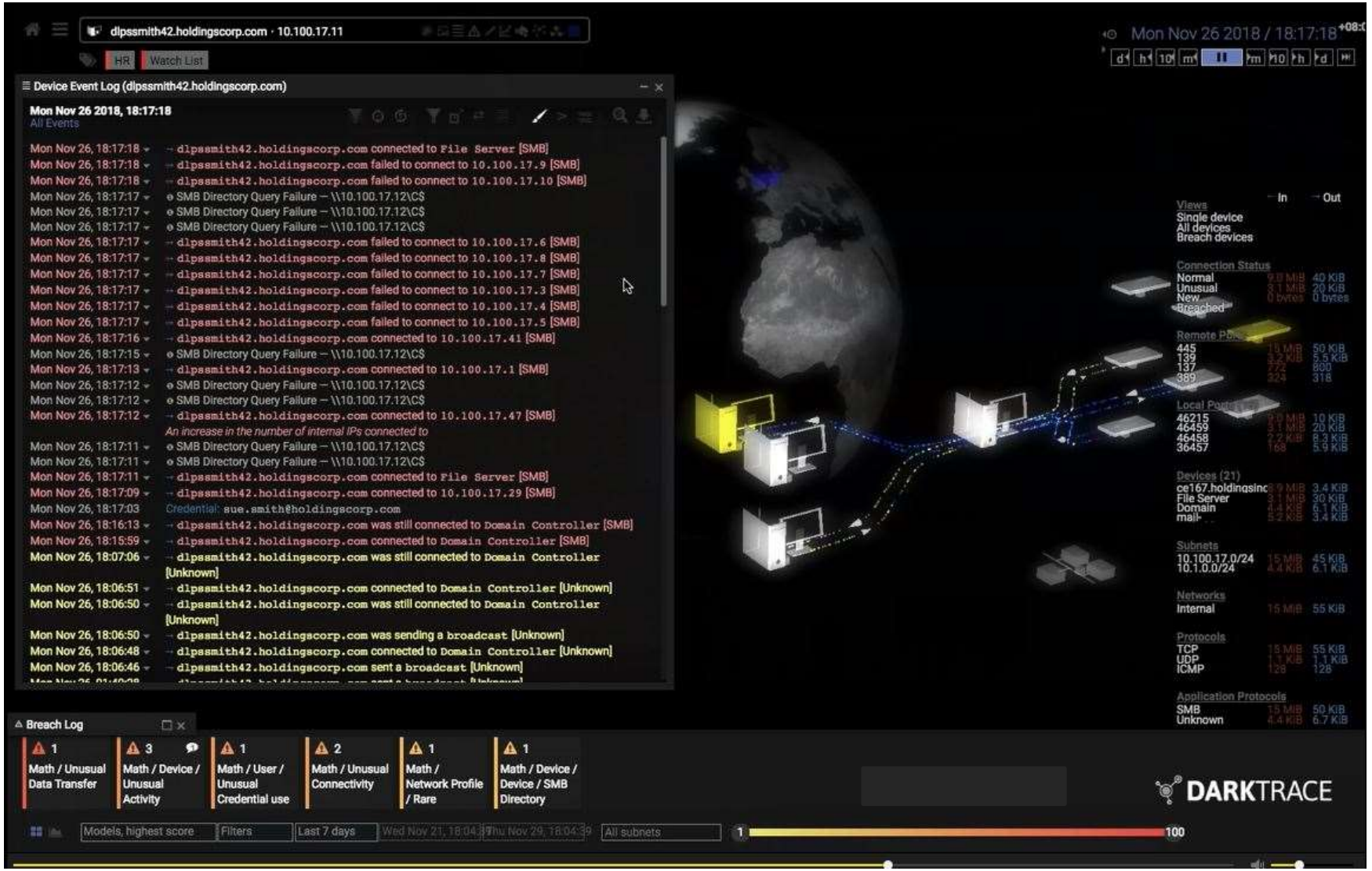
資料來源： Google 搜尋/圖片結果，版權歸該搜尋網址與該公司團體所有.

【白抓黑】&【白擋黑】的四大資安我軍機制 (2/4)

2. 1 網路異常分析機制 : 網路行為白名單

- 7 x 24 即時自我【機器學習】
  - 400+ 參數構面 / 貝式演算法+
  - 100%【威脅可視化】介面
- 偵測所有已知及未見的【網路異常】行為
  - 連線對象、協定、時間、流量...
- 自動化【回應及防阻】機制
  - TCP/Reset
- 每天經驗專業，都能持續傳承
  - 看得懂、記得住、比得出、擋的掉

各式網路威脅完全【可視化】



資料來源： https://www.youtube.com/watch?v=O_OYOw1vpPA&feature=emb_logo

3. 我軍白帽合縱代管趨勢

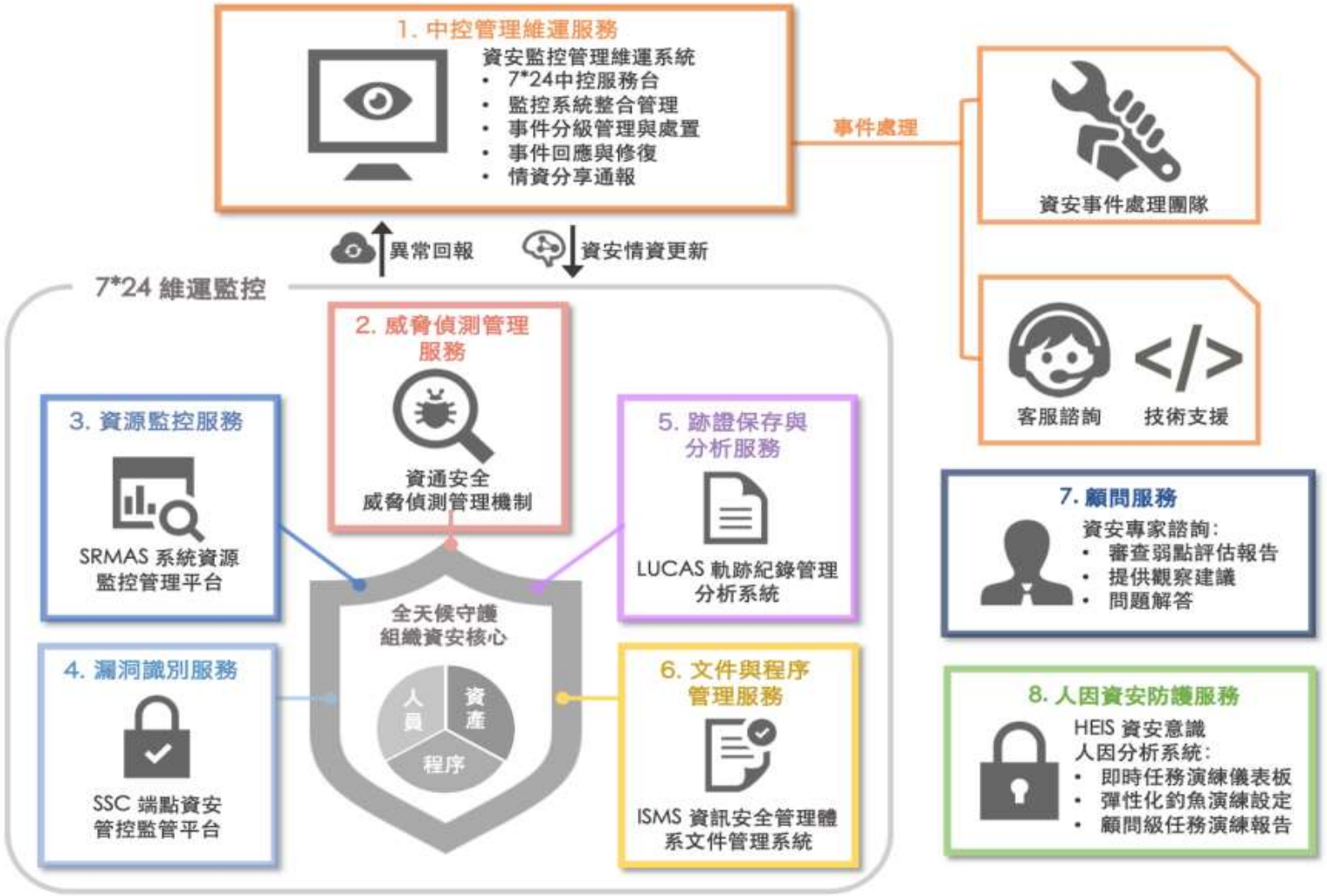
【MoC (EDR/MDR) + 資安常年顧問】

VS

資料來源： Google 搜尋/圖片結果，版權歸該搜尋網址與該公司團體所有.

3.1 MOC = More Thank SOC

MOC 至少包含【八大服務】



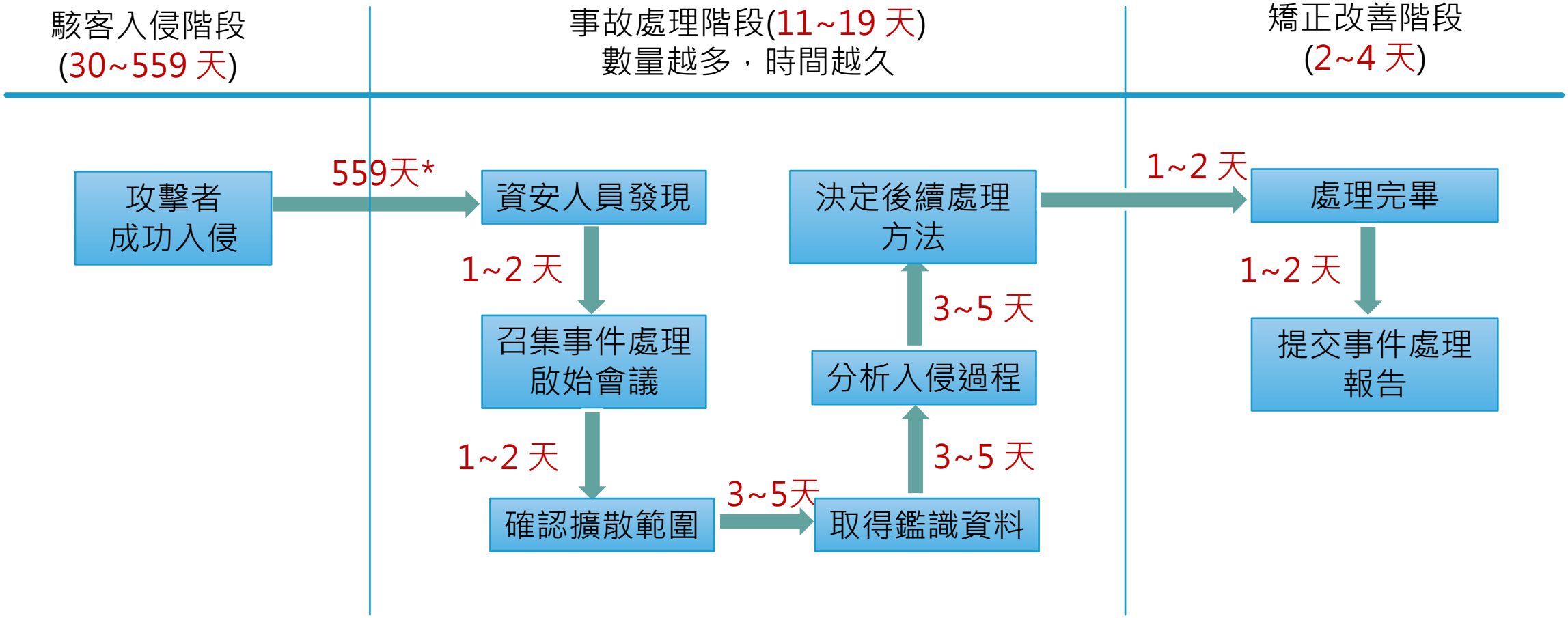
MoC = SOC + NOC + LM (Event+Network) + UEBA + GCB + VANS + AV + EDR + MDR + PS + SE

【白抓黑】&【白擋黑】的四大資安我軍機制 (3/4)

3. 1 MoC (電腦紀錄鑑識機制 : EDR + MDR)

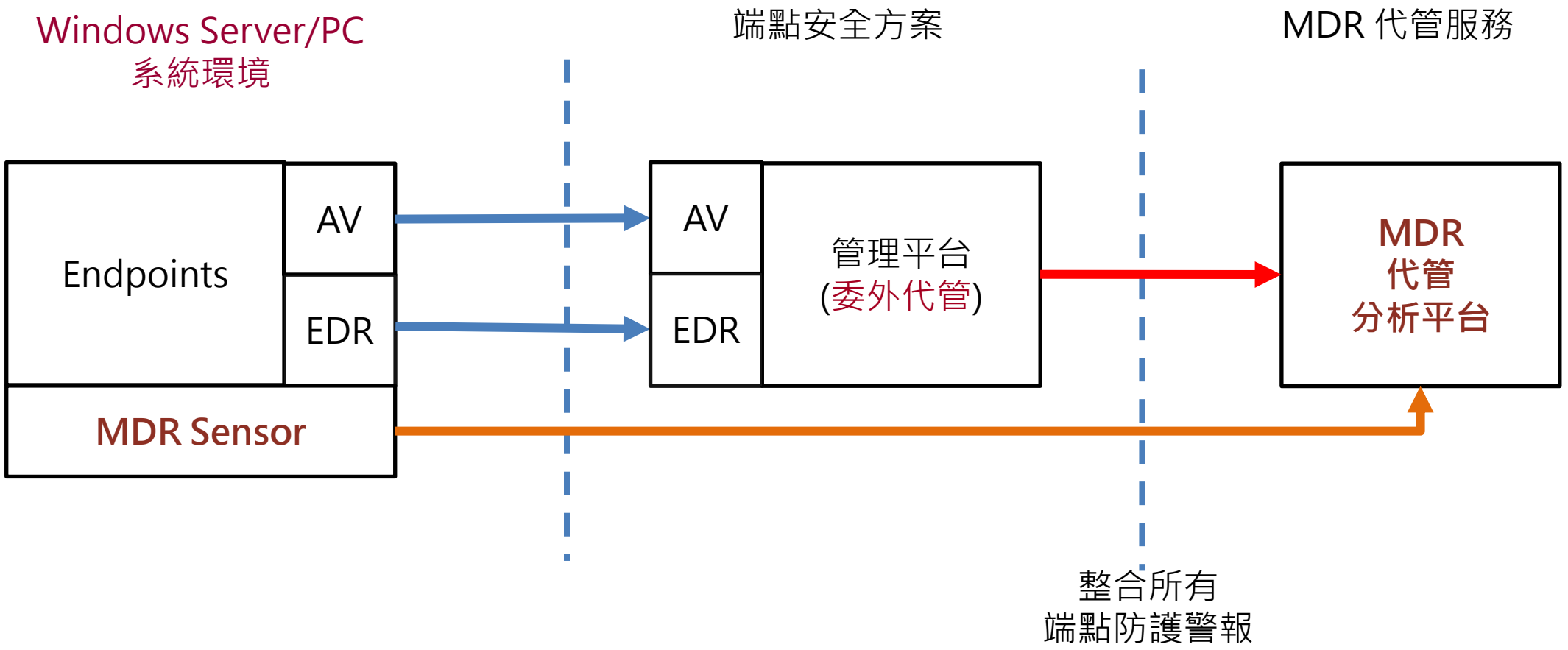
- 駭客【走過/做過】，必有紀錄
  - 所有駭客或惡意程式，如果要執行或者進行破壞，一定會在【Server/PC】落地執行，即使自我隱藏，都會【產生執行紀錄】
- 【即時紀錄匯出】，確保留下證據
  - 但是駭客或惡意程式，多數將會進行【毀屍滅跡】甚或【自我刪除】
  - 所以每台【Server/PC】須要規劃或者啟動【電腦紀錄器】，一有紀錄，立即匯出【電腦稽核紀錄】
- MoC 資安專家【代管】，智慧快速應對
  - (1) 事前徵兆，最速發現：電腦紀錄器，專家代分析！
  - (2) 事中警示，立即應變：徵兆全都錄，替威脅獵捕！
  - (3) 事後鑑識，矯正預防：I.R. 速應變，事故沒煩惱！

傳統 SOC/資安事故處理程序：曠日費時(數十天)

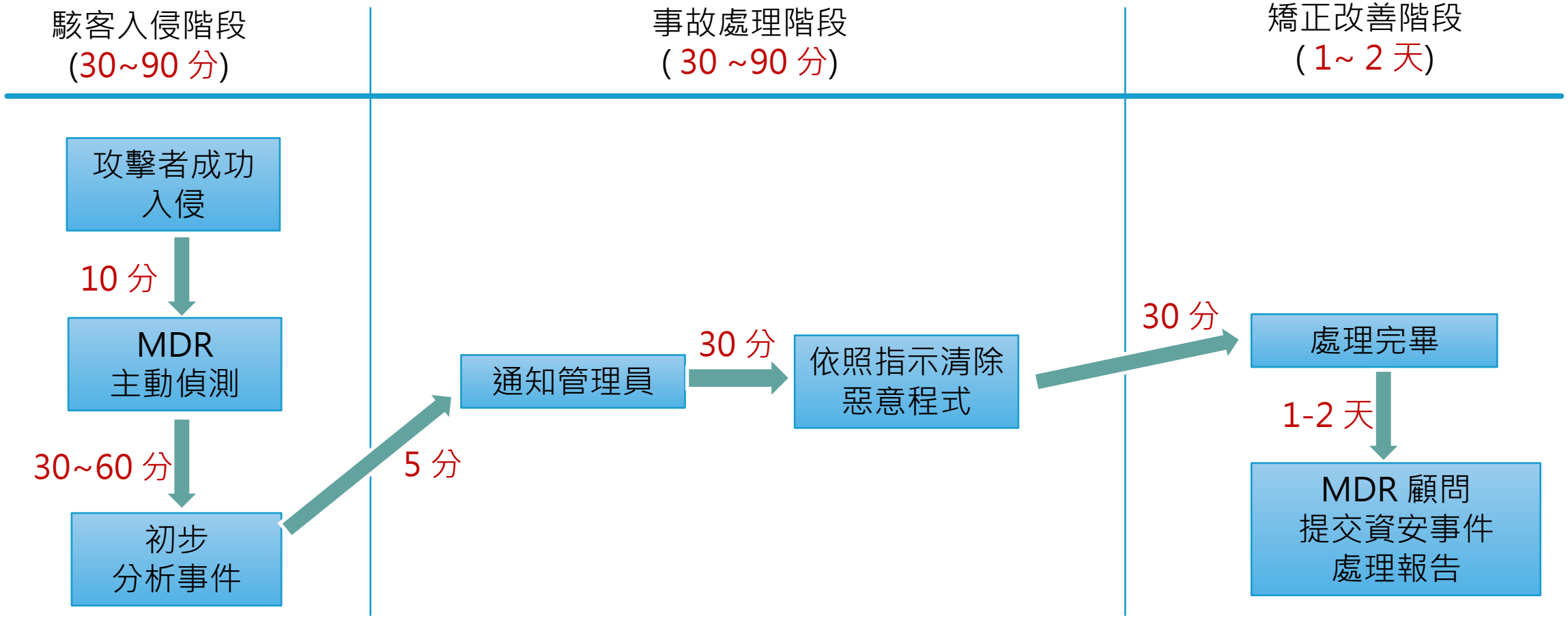


* 資料來源：https://www.chinatimes.com/realtimenews/20171008001001-260412?chdtv

MoC (MDR) 端點偵防應變處理服務架構圖



MoC (MDR) 服務成效 – 即時發現、迅速應變(時)



3.2 資安常年顧問

常年資安顧問，協助資安治理、監理 以及應變！

客戶現況

- 上市櫃公司之整體資安規劃，端視【廠商推廣、資安事件、媒體宣傳 以及 法規需求】

客戶痛點

1. 關於資安議題，容易頭痛醫頭、腳痛醫腳
2. 資安管理【顧問偏重管理】，資安產品服務【廠商偏重技術】，未能完善整合角度規劃建議!
3. 當外部同業發生資安事件，欠缺資安顧問提供該事件之分析評估與預防建議，借鏡效尤！
4. 如果不幸自身發生資安事件，往往僅能既有資安廠商【臨時成軍】來應變？緩不濟急！

圖片來源 ： https://www.himss.org/resources/three-ways-improve-your-security-incident-response-plan

常年資安顧問，協助資安治理、監理 以及應變！

解決方案

1. 內外部資安事件的評估應變與改善建議。
2. 資安議題(弱點/發現)的說明/改善建議。
3. 弱點誤判諮詢、修補討論諮詢與指導。
4. 如無法修補調整之補償措施建議 等。
5. 外部資安評級情資報告服務諮詢.
6. 資安相關法規合法性諮詢服務。
7. 年度資安規劃諮詢服務。
8. 資安監理規劃建議服務。

方案效益

1. 因為常年長期合作，資安顧問較能體察自身組織文化特性，隨時量身客製資安規劃策略
2. 彈性配合上市櫃公司產業特性【臨時機動性】資安需求，隨時進行資安顧問諮詢服務與處理
3. 即時借鏡國內外上市櫃同業資安事件，藉由資安顧問事件分析進行自我檢視與超前佈署!
4. 如果發生資安事件，可以【即時獲得】專業評估應變與處理諮詢協助

常年資安顧問團隊

圖片來源 ： https://blog.apnic.net/2021/05/26/what-can-you-expect-from-your-incident-response-team/

4. 端點合法程式機制 + 機動備份機制

最後一道防線

4.1 端點：(Server/PC) 程式白名單

4.2 機動備份機制

資料來源： Google 搜尋/圖片結果，版權歸該搜尋網址與該公司團體所有.

【白抓黑】&【白擋黑】的四大資安我軍機制 (4/4)

4.1 端點合法程式機制 : 端點(Server/PC) 程式白名單

- 資安【沒有】100% 安全
  - 我們擔心的不是被入侵成功，而是擔心【入侵成功後的衝擊影響】破壞、竊取、斷服務
- 【最後一道防線】，端點白名單程式機制!
- 駭客或者惡意程式一定要【執行】，才能進行【破壞、竊取、斷服務】等行為
- 至少我們可以導入【最後一道防線】，讓惡意程式【無法執行】
- 自動學習 & 簡易維運【Server/PC】程式白名單
  - 信任來源/目錄/廠商、程式簽章/DB、灰名單沙箱檢測、黑名單程式比對
  - 如有臨時業務職掌需求，可以隨時【提權簽核/側錄稽核】!

4.2 機動備份

- 關鍵主機 & 機敏電腦 (高階主管、營業關鍵設備)

後疫情時代之資安防護思維

不隨風起舞、不變應萬變

後疫情時代之資安防護思維

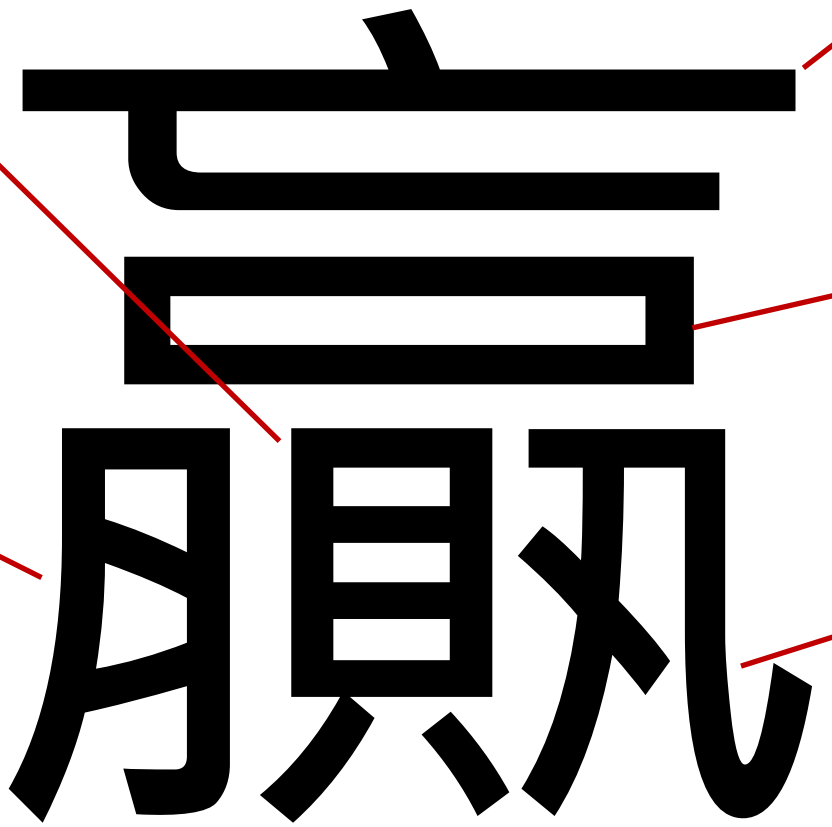
資安事件層出不窮，資安思維調適轉型

- 漏洞【不斷發現】、不斷【風險處理】
- 繼續【貓抓不到老鼠】，還是【守株待兔/不變抓萬變】

【黑抓黑】合縱連橫【白抓黑/白擋黑】資安我軍

- 企業機關【現有】資安團隊 +【友軍部隊】
  - 資安情資部隊 + 資安 AI 機器人 +
  - 資安代管部隊 + 資安常年顧問部隊 (含資安職能教育訓練學程)

共組資安我軍、一起贏得勝利！



貝：
運用情資
善用外資
贏出價值

月：
養成習慣
日積月累
贏得先機

亡：
危機意識
安全第一
贏得未來

口：
情資分享
口碑相傳
贏得主動

凡：
平凡投入
白抓檔黑
贏出信心

資安我軍一直都【在】！讓我們一起【贏】！

問題 & 討論