LEO
國眾電腦

電子書

近日駭客勒索軟體攻擊事件

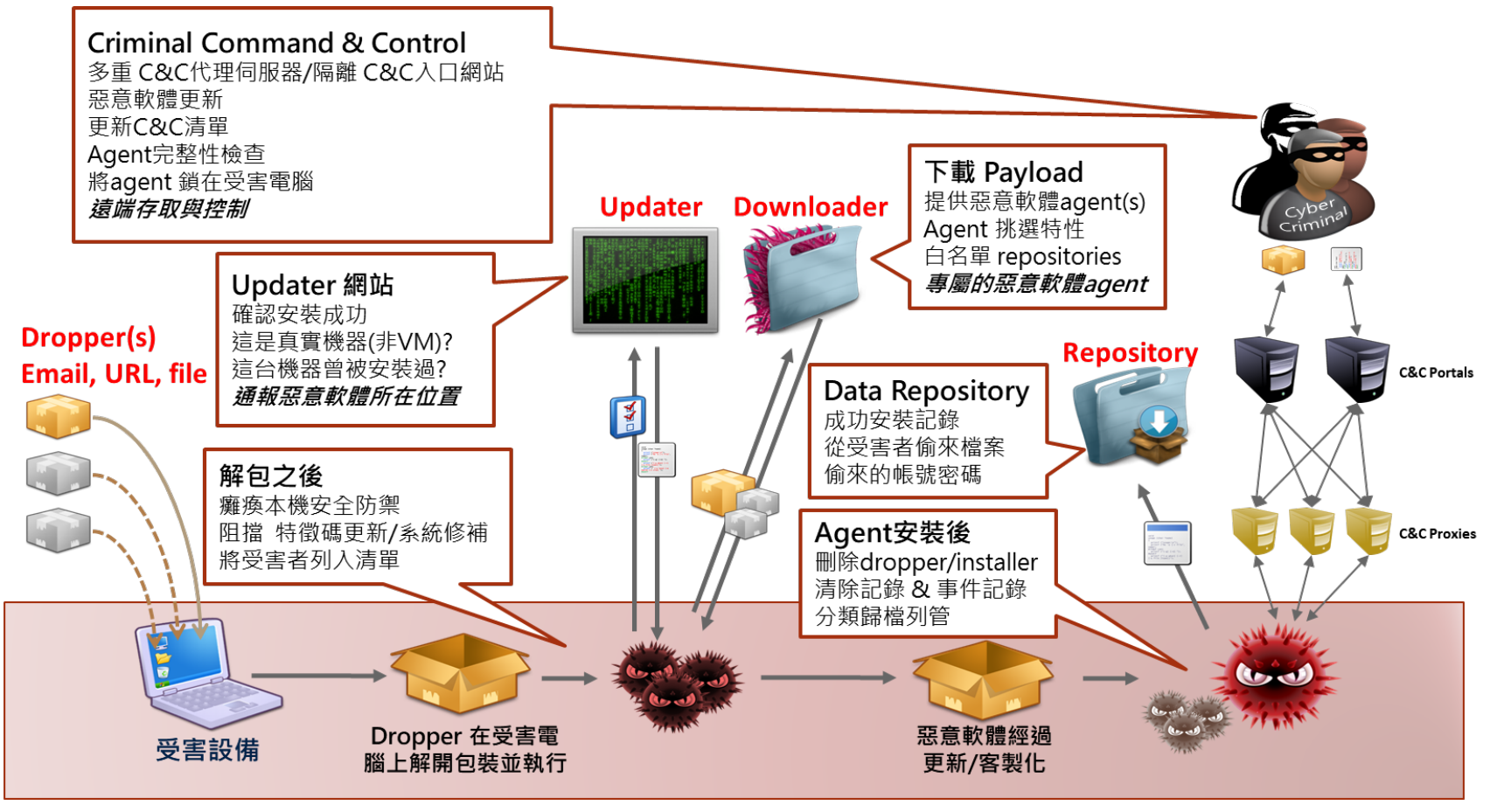
Cyberview
力悅資訊

新聞報導109年5月國內多家重要能源及科技公司接連遭勒索軟體攻擊，駭客入侵並將勒索軟體植入公司內部系統、個人電腦及伺服器等資訊設備，儲存的重要檔案均無法開啟，導致營運受到嚴重影響外，駭客亦要求交付贖金。

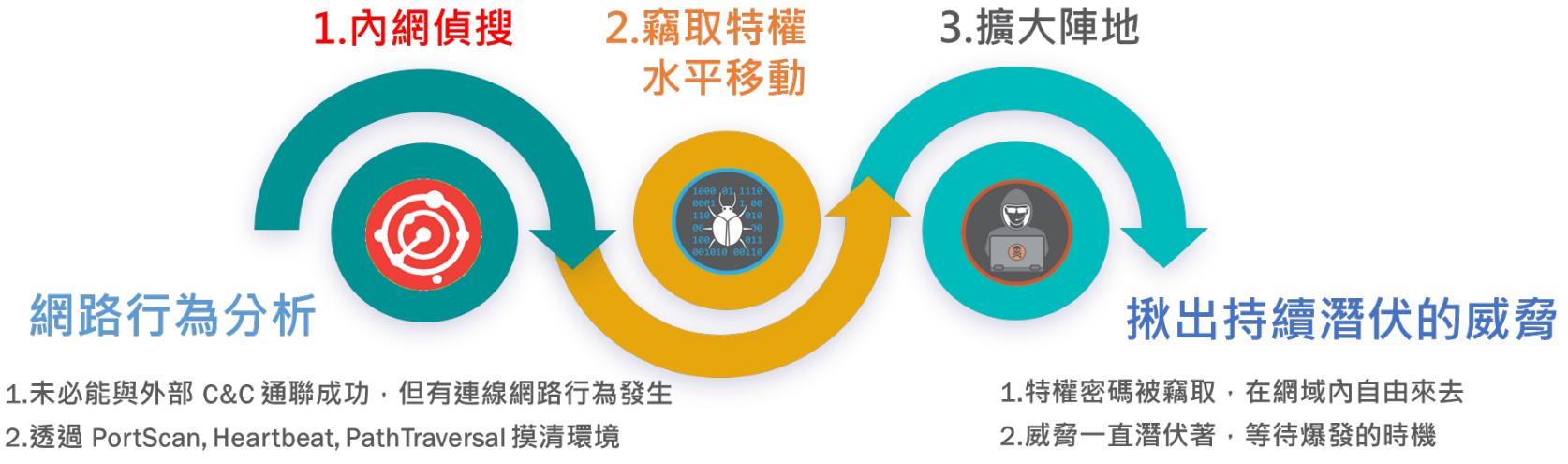
經過法務部調查局調查，駭客在數月前透過員工個人電腦、網頁及DB伺服器，入侵多家公司內部網路並開始刺探與潛伏，俟竊取特權帳號後侵入網域控制伺服器(AD)，並利用凌晨時段竄改群組原則(GPO)以派送具惡意行為的工作排程，當員工打開電腦會立即套用GPO並執行此工作排程，待核心上班時段，自動執行駭客預埋在內部伺服器中的勒索軟體下載至記憶體中執行，若檔案加密成功即會顯示勒索訊息及聯絡電子信箱。

根據調查局專案人員掌握情資顯示，駭客預謀在近期將針對國內企業再度發動勒索軟體攻擊。

入侵與滲透過程示意圖



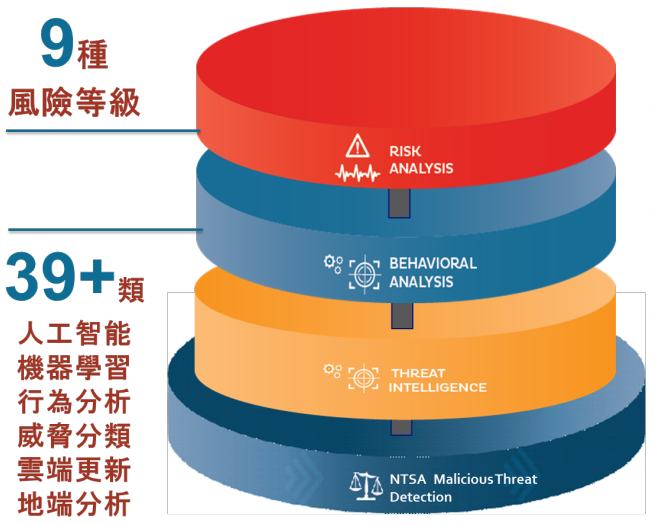
駭客攻擊手法分成五個步驟，首先是駭客入侵建立灘頭堡、偷組織內部的帳號密碼、用帳號密碼在內部水平擴散、持續從遠端遙控主機電腦存取資源、最後的目標是偷走機密資料。
水平感染會透過幾種行為進行擴散，例如：Port Scan, path traversal, heartbeat … 等手法，找到重要的標地主機，掃描所能使用的埠號與協定，於竊取到特權密碼後開始進行水平感染。通常這類的感染情事潛伏期都非常久，約莫 100 ~ 200 天，甚至更長。

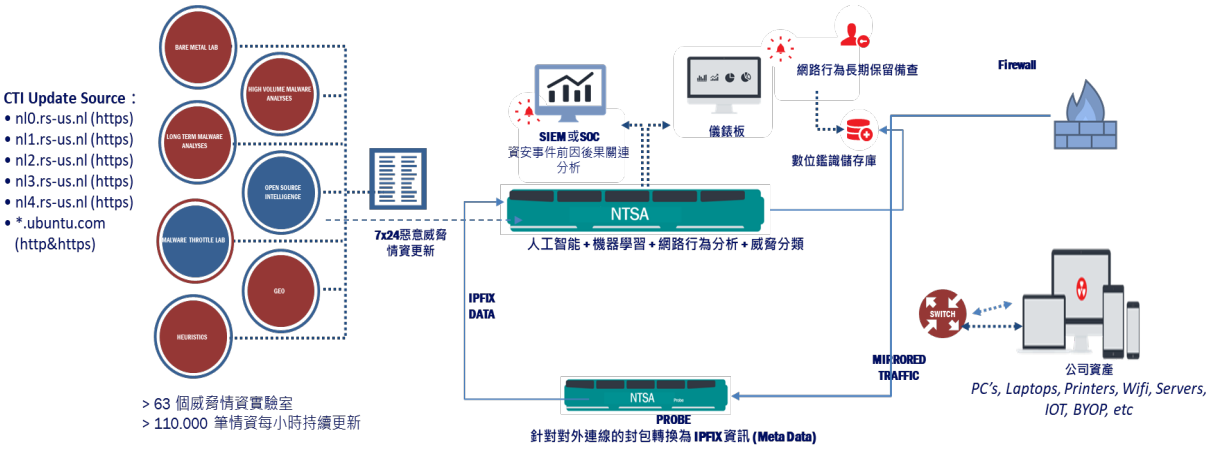


預防檢查及解決方案

1. 檢視網路防護機制，如對外網路服務是否存在漏洞或破口，觀察有無異常登入行為及異常網路流量，如異常的DNS Tunneling、異常對國內外VPS的連線等。

Bitdefender NTSA 早期預警雷達，可在短期之內找出異常連線等相關問題，發現問題來源提供作為阻斷惡意連線或者系統修復的依據參考

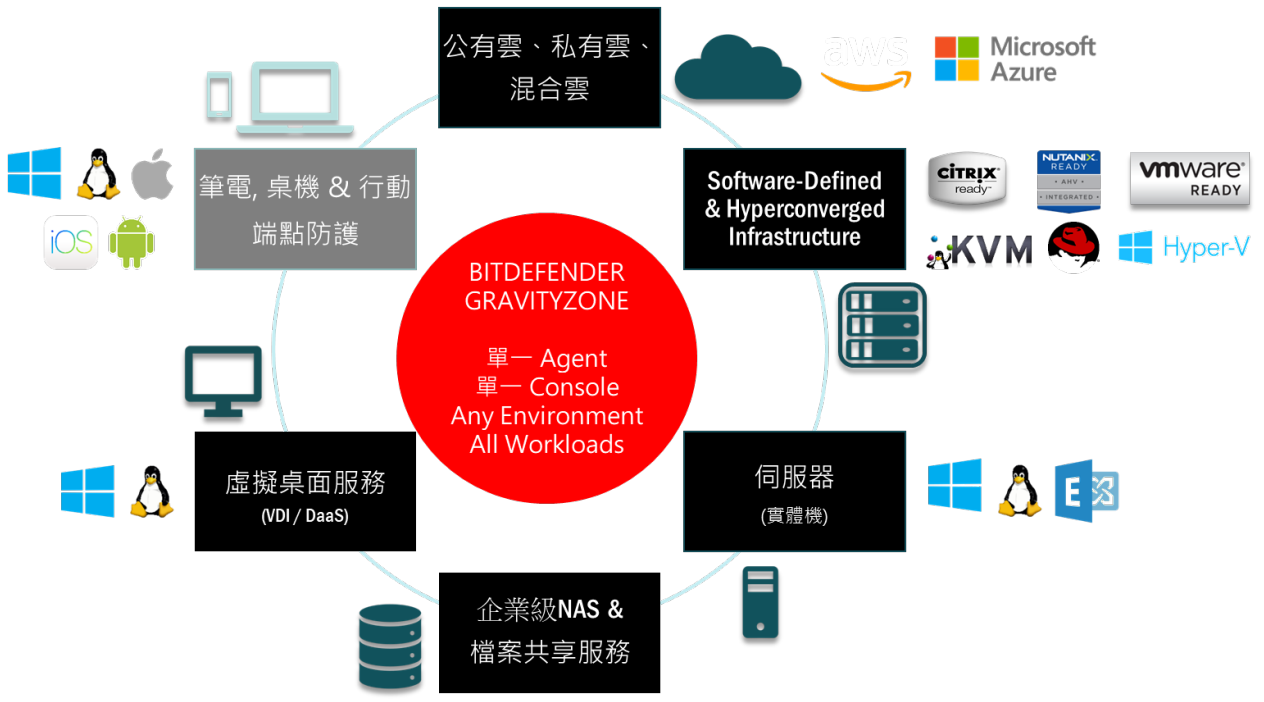




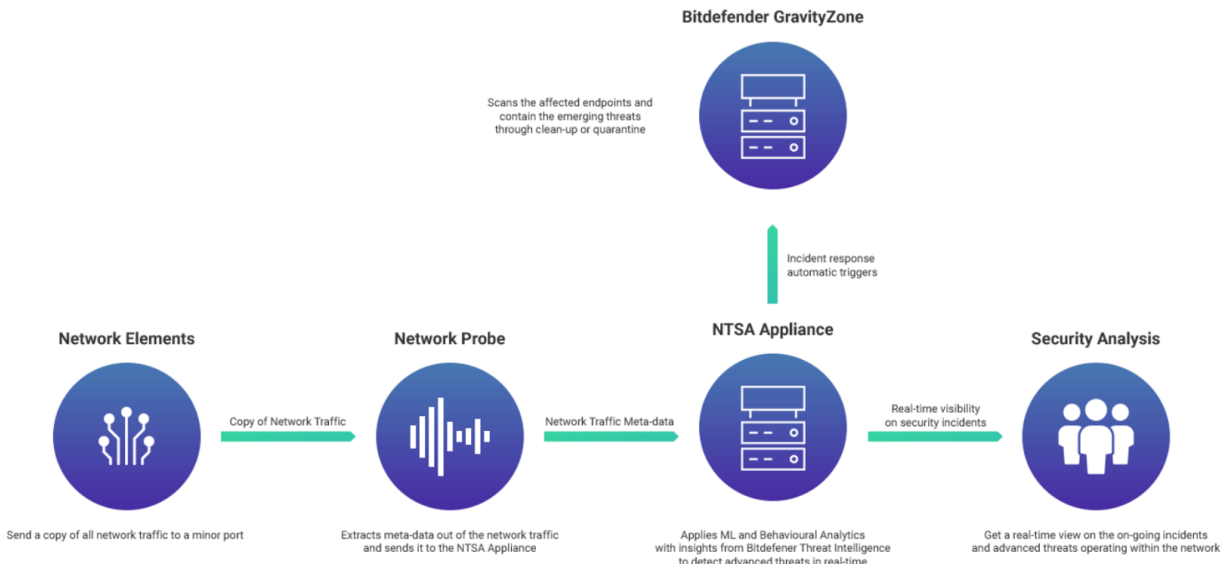
2. 注意具軟體派送功能之系統，如網域/目錄(AD)伺服器、防毒軟體、資產管理系統，尤其注意AD伺服器的群組原則遭異動、工作排程異常遭新增等。更新防毒軟體病毒碼，留意防毒軟體發出之告警，極可能是大範圍感染前之徵兆。

BitDefender GravityZone全方位跨平台防毒系統

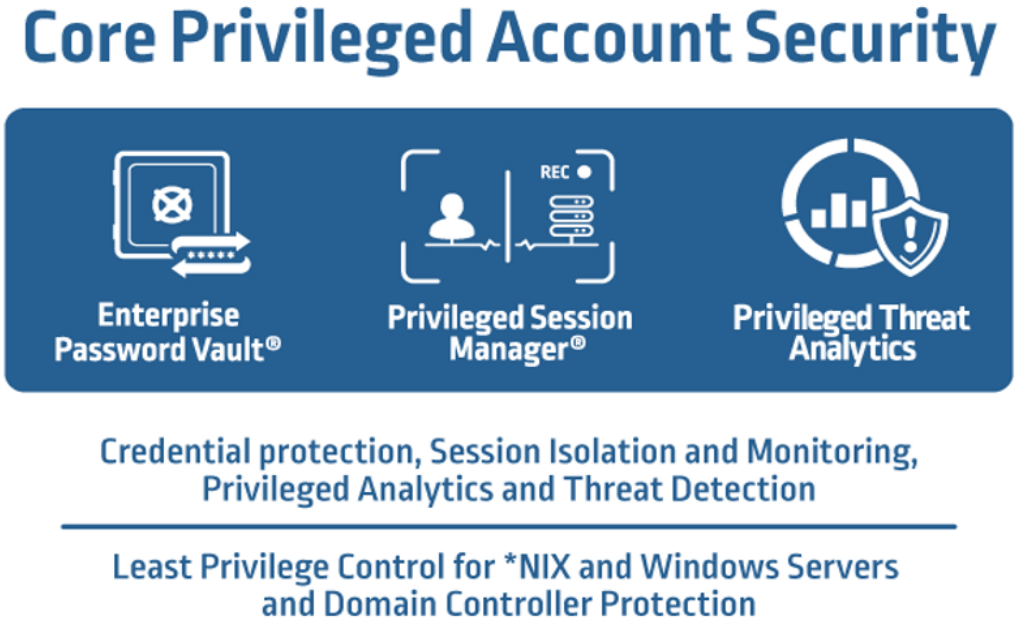
- 完整虛擬環境支援，通過Mware、Citrix、Nutanix認證。
- 增強虛擬環境效能，增加30%虛擬機密度，17%應用程式反應速度。
- 單一Agent即可提供防毒、沙箱、Patch Management、應用程式控管、硬碟加密、EDR等..多項功能，大幅節省成本與端點效能。
- 單一主機可管理Win、Linux、Mac、Android、IOS、VMware、Citrix、Nutanix、Exchange、AWS、Azure、Hyper-V、ICAP檔案伺服器所有環境。
- Central Scan端點只需安裝輕量agent，掃描功能集中至security server，同一檔案在所有端點只需掃描一次。

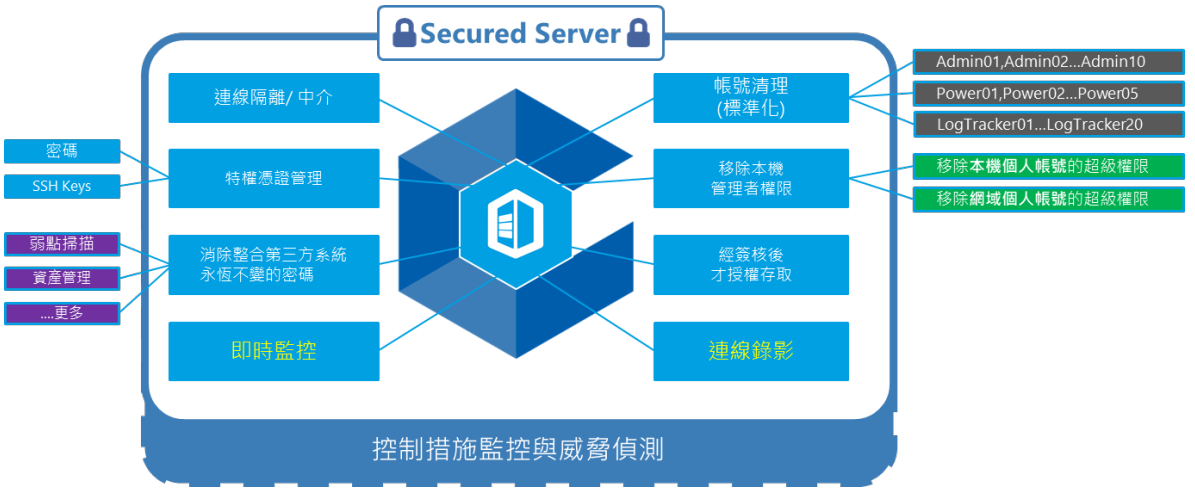


Gravityzone整合NTSA

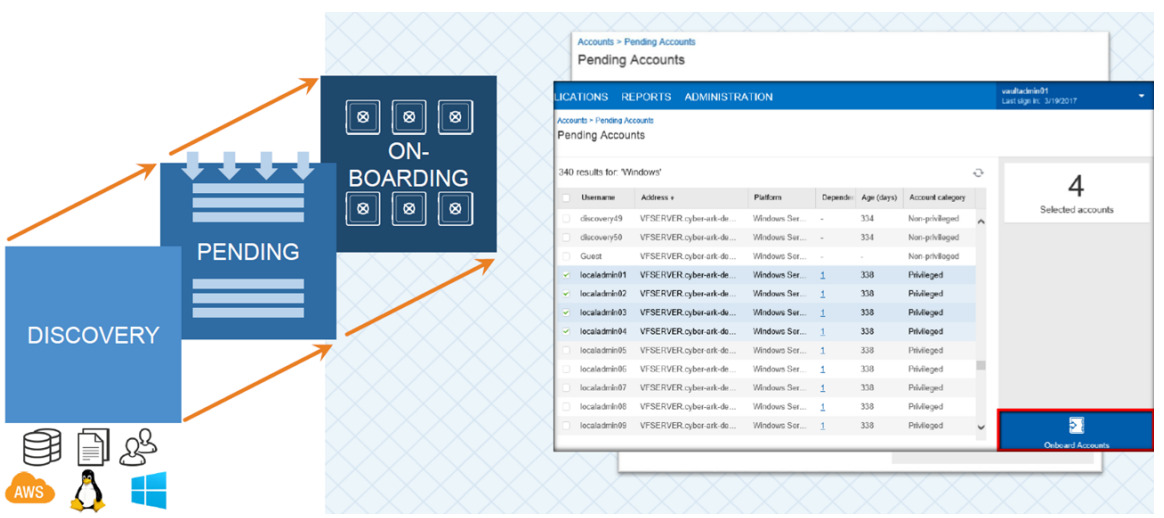


3. 加強監控網域中特權帳號，應限定帳號使用範圍與登入主機。
   CyberArk CorePAS解決方案

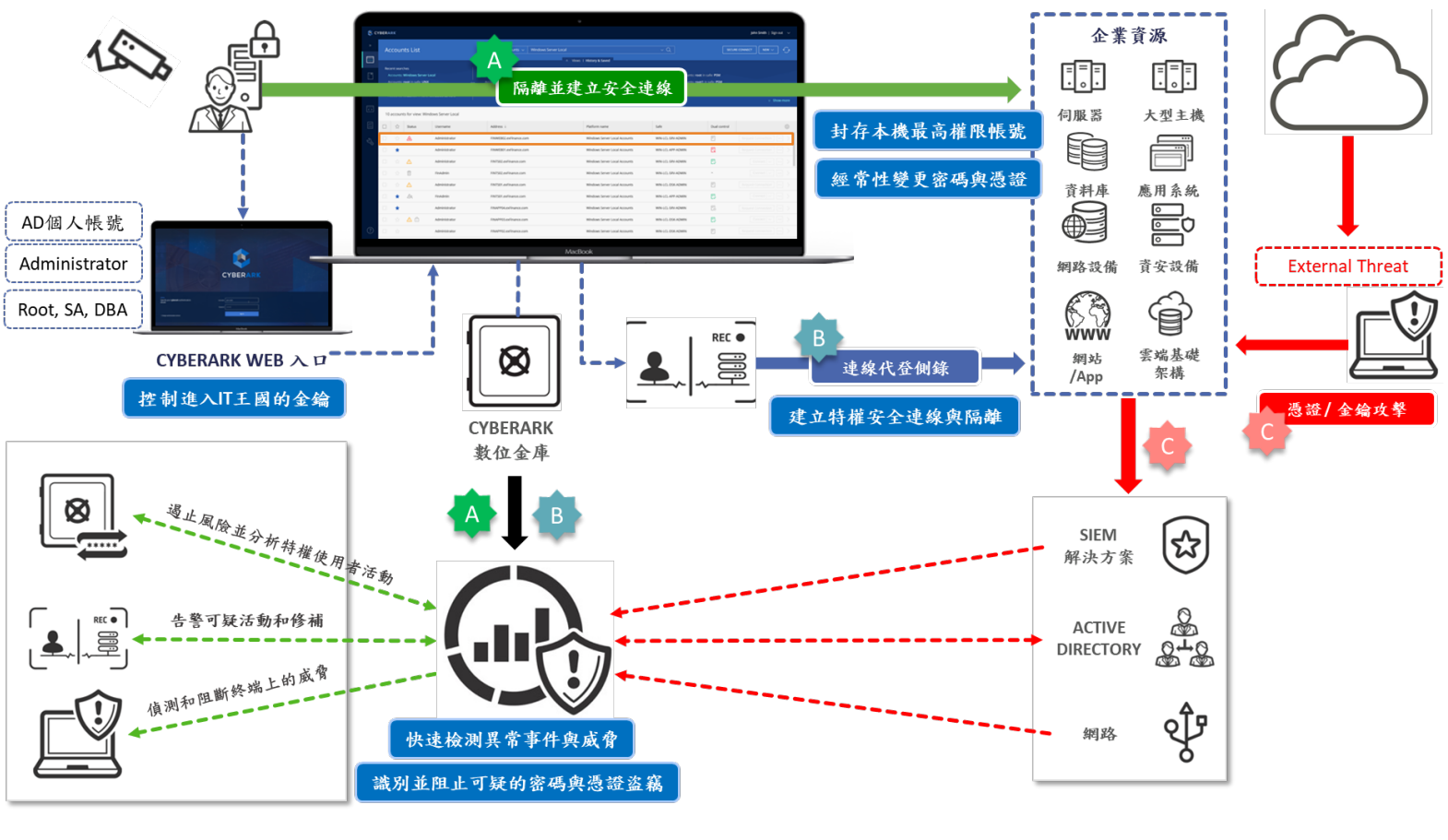




改善與提升Account Discovery 自動搜尋與收納特權密碼 (Accounts Discovery)



Privileged Threat Analytics



效益與價值

1. 防止惡意程式入侵與危害，由「端點管控、防護」開始。
2. 保護系統管理員特權帳號，避免惡意人士竊取資料或破壞系統。
3. 對應惡意威脅的各階段攻擊，做到進階防護、偵測、反應與風險分析。
4. 早期感染偵測縮短風險空窗期，避免產生重大損失。
5. 建立存取憑據及帳密的保護與管理符合資安法規標準(國內資通安全管理法要求)。
6. 追蹤和記錄使用特權連線期間的每個使用者活動。
7. 特權帳號完整的稽核與資安防禦與管理需求。

聯絡人：何俊宏
國眾整合資訊服務聯絡電話：02-2799-6789 分機2633
國眾整合資訊服務電子郵件：louisho@leosys.com

LEO 國眾電腦

Cyberview 力悅資訊