BROADCOM SOFTWARE

Threat Defence for Active Directory
-- 賽門鐵克AD威脅偵測解決方案

Jordan Giltrap

October 2021

本中文化由保安資訊提供
https://www.savetime.com.tw

賽門鐵克企業市場滲透率

1. 財富前500大企業有**195**家
2. 全球前2000大企業有**697**家
3. 全球前13大銀行全都是
4. 全球前10大電信公司有**8**家
5. 全球前10大汽車製商有**7**家
6. 全球超過**1.5**億個企業用戶

BROADCOM SOFTWARE

關於博通賽門鐵克

- 博通賽門鐵克長期獲美國總統任命，成為美國國家安全通訊諮詢委員會(NSTAC)一員，也是目前唯四的資安廠商之一。能提供總統建言，為通訊與資訊科技重要基礎建設的安全和保護盡一份力量。
- 博通賽門鐵克也是唯一參與國際網路工程研究團隊的資安廠商(IETF:Internet Engineering Task Force)，IETF是一個開放性的國際組織，其作用在於匯集網路設計師、網路操作員、網路廠商以及研究人員共同研發改進網路的工程架構與建立起一個平穩的網路環境。例如：TLS1.3、ECH(Encrypted Client Hello)、DNS 以及HTTP……等。
- 博通賽門鐵克是開放網路安全模式框架(Open Cybersecurity Schema Framework，OCSF）專案創始成員之一，OCSF專案包含一個開放規格，以用來建立各種安全產品及服務之安全遙測的標準化資料，以及各種可支援及加速採用OCSF模式的開源工具，以協助組織更快也更有效率地偵測、調查與阻止網路攻擊。

關於我們

服務電話:

0800-381-500
+886-4-23815000

網站:

www.savetime.com.tw

保安資訊

從協助顧客簡單使用賽門鐵克方案開始到滿足顧客需求更超越顧客期望的價值

- 保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。
- 自 1995 年起就全心全力專注在賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更熟悉用戶使用情境的優勢，能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。
- 許多顧客樂意與我們建立起長期友誼，把我們當成可信任的資安建議者、可提供良好諮商的資安策略夥伴以及總是第一個被想到的求助暨諮詢對象。

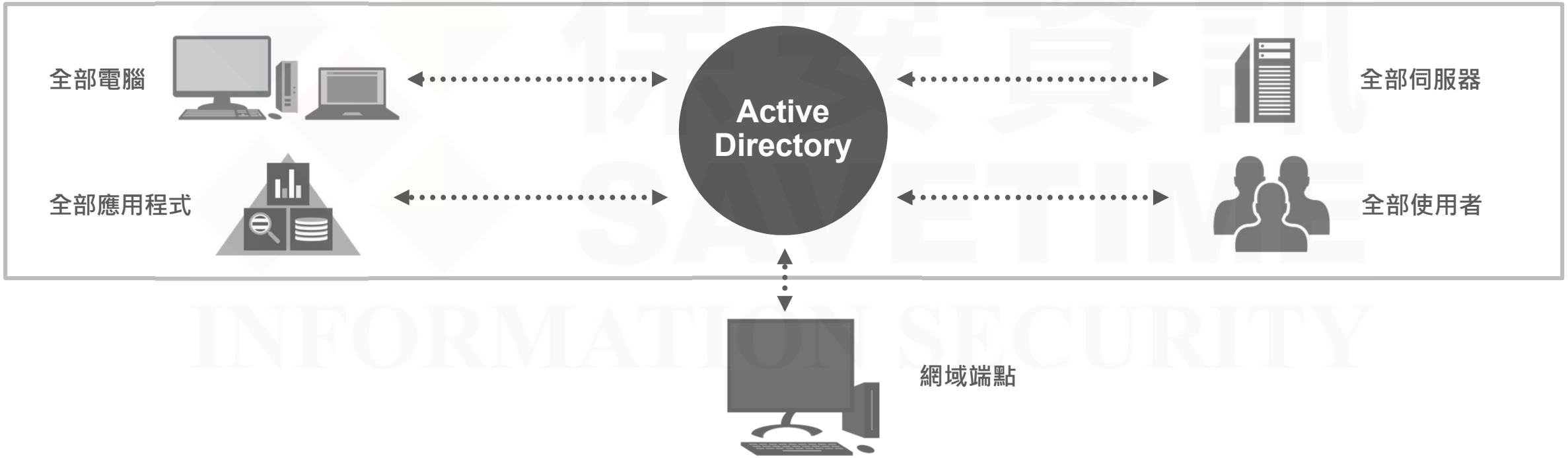
BROADCOM SOFTWARE

射人先射馬，擒賊先擒王
-- AD 威脅偵測的重要性

TDAD：Symantec
Threat Defence for Active Directory

Active Directory 幾乎是所有目標攻擊的重點

只要在被入侵的端點對AD網域進行相關查詢，攻擊者可以獲得有關公司的AD所有資訊並橫向移動



攻擊者只需要 7 分鐘就能入侵及並完全掌控網域控制器

BROADCOM SOFTWARE

Active Directory 是所有 APT 集團的首要攻擊目標

集團名稱	別名	憑證盜竊	列舉Active Directory組態	時間框架	發源地
APT 3	Boyusec, UPS	是	是	持續進行中	中國
APT 10	Stone Panda	是	是	持續進行中	中國
APT 28	Sofacy, Fancy Bear	是	是	持續進行中	俄羅斯
APT 29	Cozy Duke, Cozy Bear	是	是	持續進行中	俄羅斯
APT 32	OceanLotus	是	是	持續進行中	越南
APT 33	Charming Kitten	是	是	持續進行中	伊朗
APT 34	Twisted Kitten	是	是	持續進行中	伊朗
APT 35	Newscaster Team	是	是	持續進行中	伊朗
Turla	Snake, Uroburos	是	是	2017年最後現踪	俄羅斯
Shell_Crew	Deep Panda	是	是	2017年最後現踪	中國
Dark Seoul	Lazarus Group, Hidden Cobra	是	是	持續進行中	北韓

*https://attack.mitre.org/groups/G0022/

業界唯一涵蓋完整MITRE ATT&CK 攻擊鏈框架的創新防護技術集(SESC)

攻擊前		入侵				感染			侵擾				外滲		
攻擊前		初始訪問				執行	持久化	提升權限	躲過/破壞防禦	帳密盜用	發現	橫向移動	資料收集	命令和控制	資料滲漏
															
安全漏洞評估	**應用程式控管**	**維護連線安全**	**入侵預防**	**雲端信譽分析**	**進階機器學習**	**CP3 描述語言模擬器**	**漏洞利用防護**	**行為分析**	**竄改防護**	**欺敵技術**	**AD入侵防護**		**入侵預防**		
Threat Defense for AD會使用攻擊模擬技術持續探測網域的不當組態、漏洞及持續性，並由攻擊者觀點向Active Directory管理員呈現其網域狀態，以便立即緩和風險減少攻擊面	透過僅允許執行已知安全的 / 經授權的應用程式或限制存取登錄檔，將端點攻擊面減至最少，進而強化對進階攻擊的防禦	可識別惡意 Wi-Fi 連線，提供政策導向 VPN，以保護網路連線(中間人攻擊)及支援合規性	攔截利用已知漏洞的攻擊	利用賽門鐵克用戶及安全相關社群的集體智慧，來評比檔案或網頁的安全等級	藉由預先執行並偵測與分析程式碼的的惡意特徵，特別有利於發現新型態及不斷突變的威脅	藉由預先執行並偵測與分析描述語言相關的威脅，例如VB、Java、Powershell…等。	攔截零時差或未知型漏洞攻擊	記錄與分析端點行為來識別進階攻擊戰術與技術，偵測偽裝成合法使用者卻執行異常活動的攻擊者。包含Non PE以及執行DLL側載 (DLL Side-Loading)	預防惡意程式或人為破獲，停用或破獲安全軟體正常運行	使用誘騙和誘餌(如假檔案、假憑證、假網路共享、假快取項目及假端點)的主動式安全功能，欺騙攻擊者進入而讓自己曝光與其攻擊目標，能夠揭露並延誤攻擊者的行為	在端點結合AI、模糊和進階鑑識方法來因應各種秘密攻擊或APT，以提供自動入侵遏止、資安事端回應及網域安全評估等功能。這是唯一安全解決方案，能在攻擊者入侵端點後加以遏止，不會讓攻擊者存留在網域中。本解決方案可中斷偵查活動、防止憑證竊取、避免攻擊者利用Active Directory橫向移動至其他資產		攔截對外連線惡意命令和控制主機(C&C)，避免資料外洩及阻斷加密勒索攻擊活動中的密鑰遞交交握連線		

自適應(Adaptive)保護：深入洞見威脅態勢 | 自訂行為洞見 | 矯正

偵測與回應：系統運行記錄功能 | 行為鑑識 | 目標攻擊雲端分析 | 威脅獵手分析

全球情報網路(GIN) ：每天數十億次的查詢賦予完整的保護與偵測能力

整合式網路防禦 (Integrated Cyber Defense) 平台：
可與賽門鐵克及第三方資安與事件管理系統(SIEM)/威脅情報平台(TIP)/ 資安協調自動化與回應(SOAR)整合

BROADCOM SOFTWARE

業界唯一涵蓋完整MITRE ATT&CK 攻擊鏈框架的創新防護技術集(SESC)

攻擊前	入侵			感染			侵擾				外滲		
攻擊前	初始訪問			執行	持久化	提升權限	躲過/破壞防禦	帳密盜用	發現	橫向移動	資料收集	命令和控制	資料滲漏
安全漏洞評估 Threat Defense for AD會使用攻擊模擬技術持續探測網域的不當組態、漏洞及持續性，並由攻擊者觀點向Active Directory管理員呈現其網域狀態，以便立即緩和風險減少攻擊面	應用程式控管 透過僅允許執行已知安全的／經授權的應用程式或限制存取登錄檔，將端點攻擊面減至最少，進而強化對進階攻擊的防禦	維護連線安全 可識別惡意Wi-Fi連線，提供政策導向VPN，以保護網路連線(中間人攻擊)及支援合規性	入侵預防 攔截利用已知漏洞的攻擊	雲端信譽分析 利用賽門鐵克用戶及安全相關社群的集體智慧，來評比檔案或網頁的安全等級	進階機器學習 藉由預先執行並偵測與分析程式碼的的惡意特徵，特別有利於發現新型態及下斷突變的威脅	CP3 描述語言模擬器 藉由預先執行並偵測與分析描述語言相關的威脅，例如VB、Java、Powershell...等。	漏洞利用防護 攔截零時差或未知型漏洞攻擊	行為分析 記錄與分析端點行為來識別進階攻擊戰術與技術，偵測偽裝成合法使用者卻執行異常活動的攻擊者，包含Non PE以及執行DLL側載(DLL Side-Loading)	竄改防護 預防惡意程式或人為破壞，停用或破壞安全軟體正常運行	**欺敵技術** 使用誘騙和誘餌(如假檔案、假憑證、假網路共享、假快取項目及假端點)的主動式安全功能，欺騙攻擊者進入而讓自己曝光與其攻擊目標，能夠揭露並延誤攻擊者的行為	**AD入侵防護** 在端點結合AI、模糊和進階鑑識方法來因應各種秘密攻擊或APT，以提供自動入侵遏止、資安事端回應及網域安全評估等功能。這是唯一安全解決方案，能在攻擊者入侵端點後加以遏止，不會讓攻擊者存留在網域中。本解決方案可中斷偵查活動、防止憑證竊取、避免攻擊者利用Active Directory橫向移動至其他資產	入侵預防 攔截對外連線惡意命令和控制主機(C&C)，避免資料外洩及阻斷加密勒索攻擊活動中的密鑰遞交交握連線		

自適應(Adaptive)保護：深入洞見威脅態勢｜自訂行為洞見｜矯正

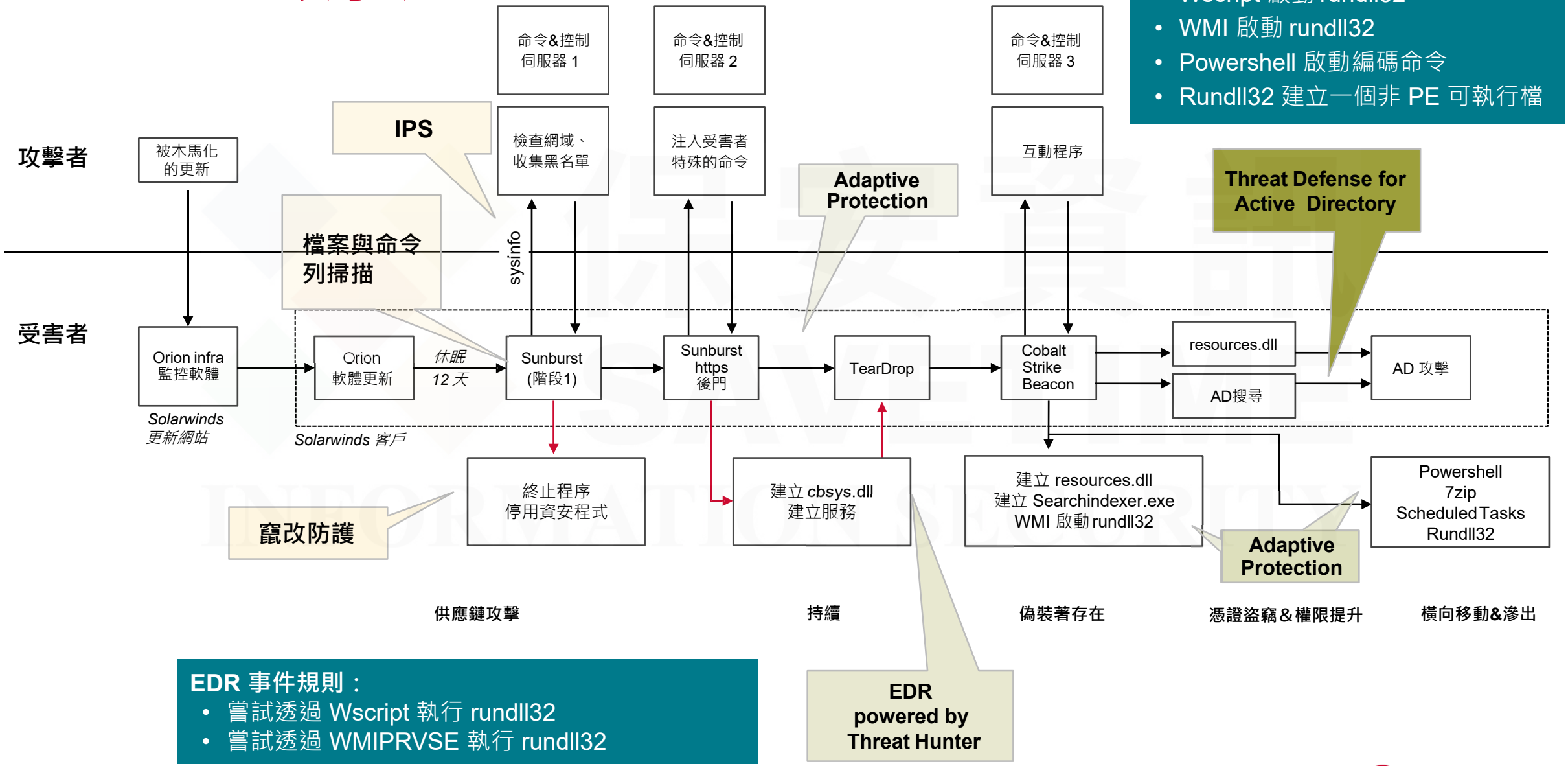
偵測與回應：系統運行記錄功能｜行為鑑識｜目標攻擊雲端分析｜威脅獵手分析

全球情報網路(GIN)：每天數十億次的查詢賦予完整的保護與偵測能力

整合式網路防禦 (Integrated Cyber Defense) 平台：
可與賽門鐵克及第三方資安與事件管理系統(SIEM)/威脅情報平台(TIP)/ 資安協調自動化與回應(SOAR)整合

BROADCOM SOFTWARE

Sunburst 攻擊鏈



TDAD Mitre Att@ck 適用範圍 – 憑證存取

技術	子技術	防護
來自儲存的密碼	Windows 憑證管理員等	TDAD Dark Corners
作業系統憑證傾印	LSASS 記憶體、SAM、NTDS 等	TDAD 偽裝帳號
竊取或偽造 Kerberos Tickets	Golden Ticket, Silver Ticket, Kerberoasting 等	TDAD Dark Corners & 偽裝帳號
不安全的憑證	檔案、註冊表、私密金鑰中的憑證等	TDAD 會掃描 sysvol xml 檔案以查找洩漏的特權憑證

搜索

技術	子技術	防護
帳號搜索	本機帳號、網域帳號等	TDAD 偽裝帳號

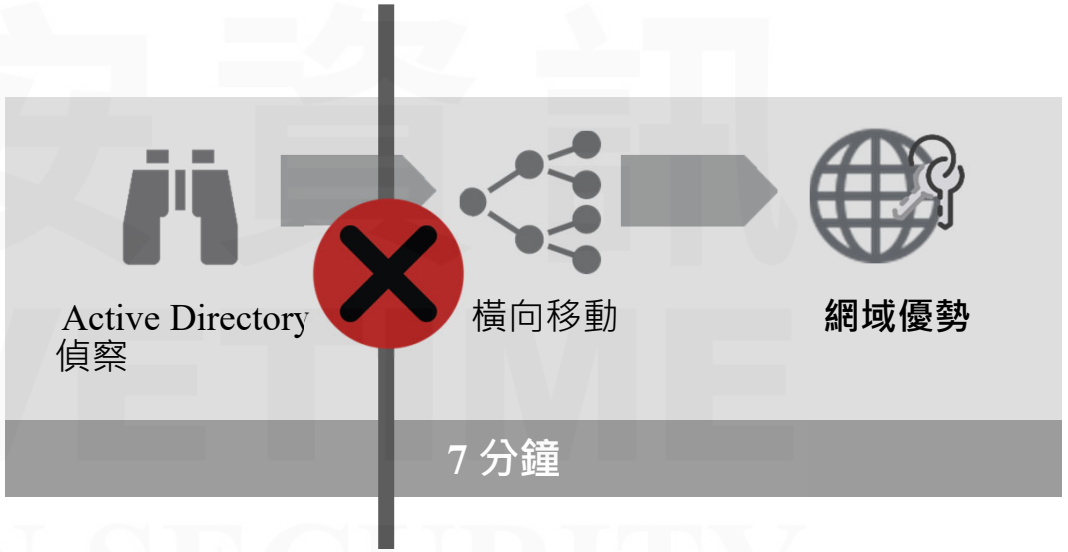
橫向移動

技術	子技術	防護
使用備用身份驗證材料	Pass the Hash Pass the Ticket 等	TDAD 偽裝帳號

BROADCOM SOFTWARE

內建 Active Directory 資源外洩預防功能

- **連接到 AD 網域的每個端點都會自動混淆 AD 查詢結果/偵察嘗試**
  - 混淆是由 AI 發動的
  - 內建在 SES 代理程式中
  - 無執行程序，不消耗資源
  - 無變動 Active Directory
- 在突破點**阻止第一個橫向移動**權限嘗試
- **防止漏洞**，防止攻擊者有能力竊取網域管理員帳密



BROADCOM SOFTWARE

Threat Defense for Active Directory 如何運作

攻擊模擬

設置錯誤&後門


特權帳號


安全性設定


網域控制器


Kerberos


GPO

+

網域混淆

AD 物件


端點


伺服器


應用程式


使用者

+

鑑識與緩解

攻擊鍊 & 留存軌跡


橫向移動


憑證竊取


偵察


被感染的端點

=

自動阻止AD違規

優點

- 防止攻擊擴散
- 減少平均控制時間
- 減少攻擊面向

BROADCOM SOFTWARE

持續 AD 評估

攻擊模擬 & 報告

使用者帳號評估	Kerberos漏洞評估	服務帳號評估	橫向評估	委派評估	LDAP評估	網路搜索評估	持續性檢測
發現潛在危險的管理帳號	發現網域控制器允許修改特權憑證屬性	發現暴露於Kerberos破解易受攻擊服務帳戶	使用本機管理員帳戶發現橫向移動路徑	發現危險的電腦帳戶委派	允許匿名或未加密綁定的網域控制器	主機啟用網路搜索	• 隱藏SID • Golden Ticket • 無特權管理員所有者ACL • DSRM登錄 • 萬能鑰匙 • 網域複寫後門 • 惡意的安全軟體提供商

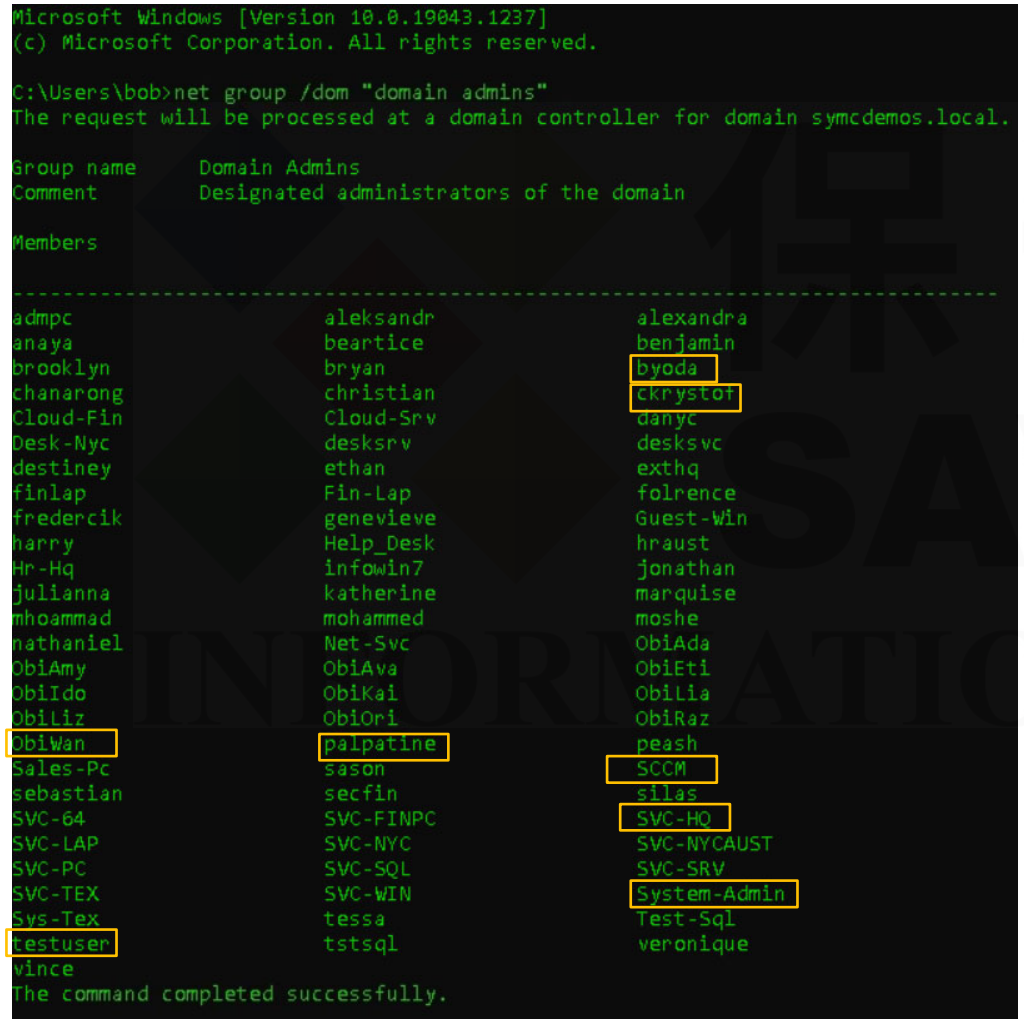
BROADCOM SOFTWARE

網域混淆機制如何運作

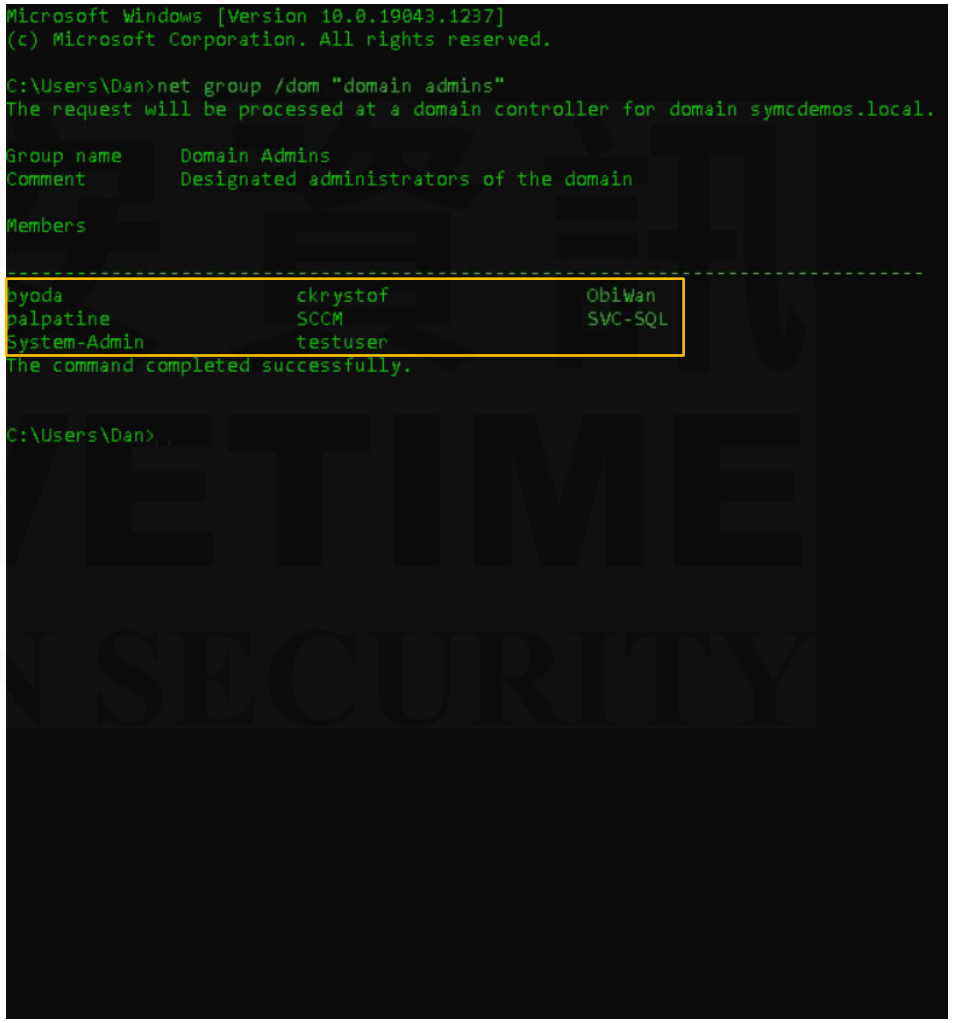
BROADCOM SOFTWARE

混淆範例

有 TDAD 的防護



無 TDAD 的防護



BROADCOM SOFTWARE

自動化鑑識分析與緩解

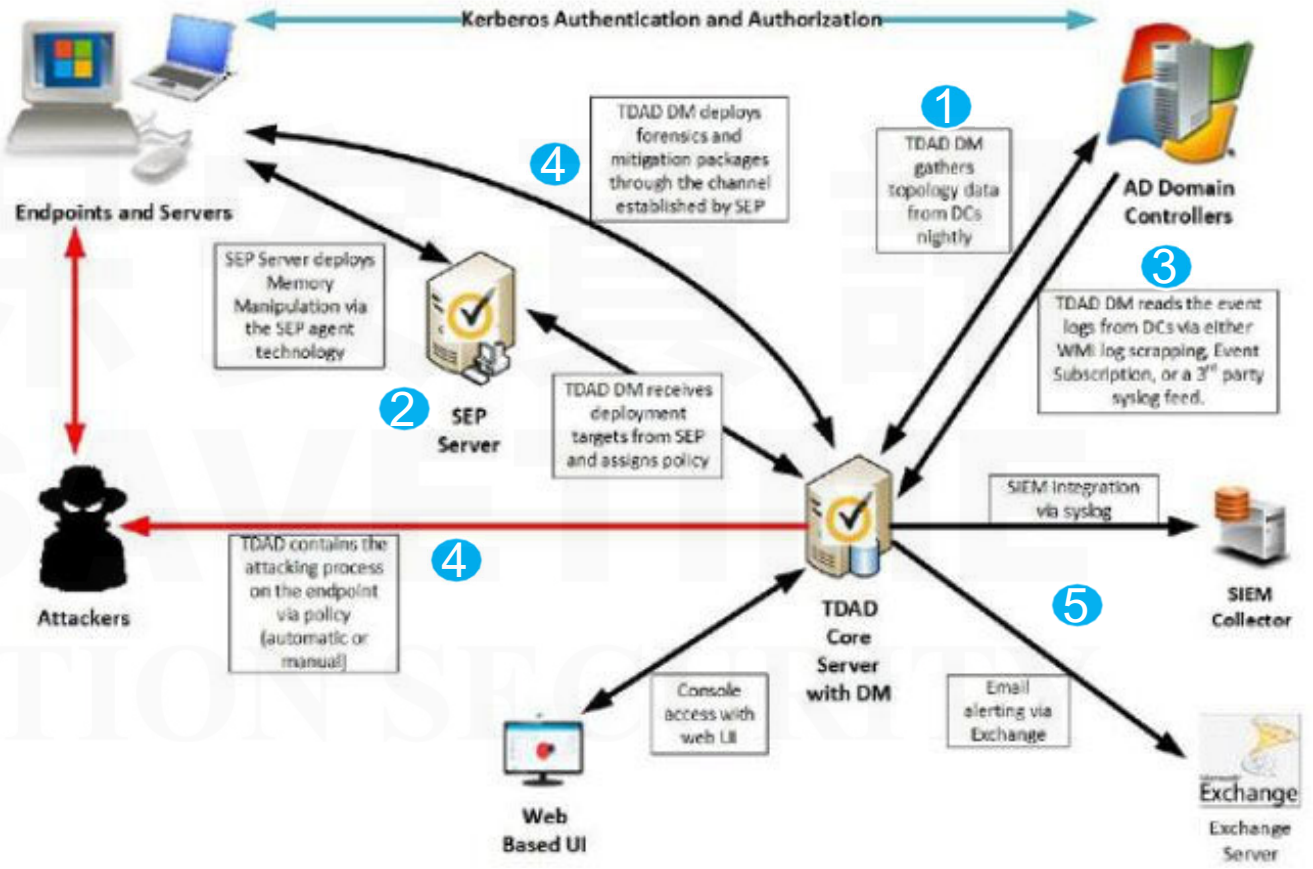
- 檢測到的威脅觸發給主控台警示，並依需求掃描端點的記憶體以鑑識和程序軌跡
- Rapid Forenics Reporting 提供了攻擊端點時的快照和攻擊鏈的詳細訊息
- 自動緩解透過消除其執行能力來阻止執行

偵測類型
用戶資訊收集
電腦資訊收集
憑證竊取
外部暴力猜解
不受信任的LDAP綁定

BROADCOM SOFTWARE

與 SEP 整合的架構

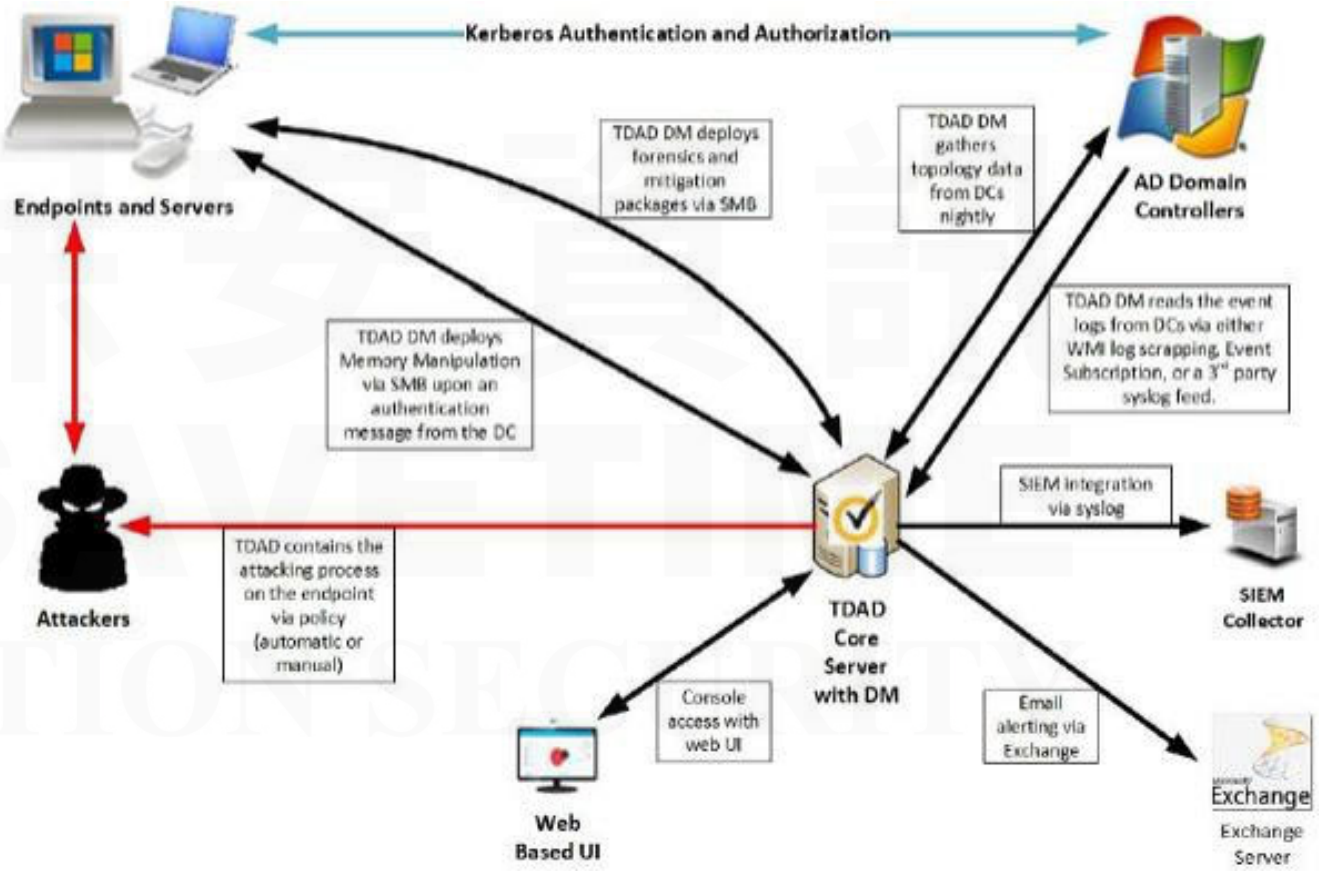
- 簡化部署 -- 由核心伺服器、部署管理員（DM）和 SEPM 組成
- 每個 AD 網域需要一個 DM
- 多個 DM 可以存在於單個核心伺服器上。例如：具有 3 個子網域的根網域
- 核心伺服器支援 Windows Server 2016 & 2019
- Windows 7 及以後的版本
- 不支援混合設定（SEPM 註冊到 ICDm）



BROADCOM SOFTWARE

獨立架構

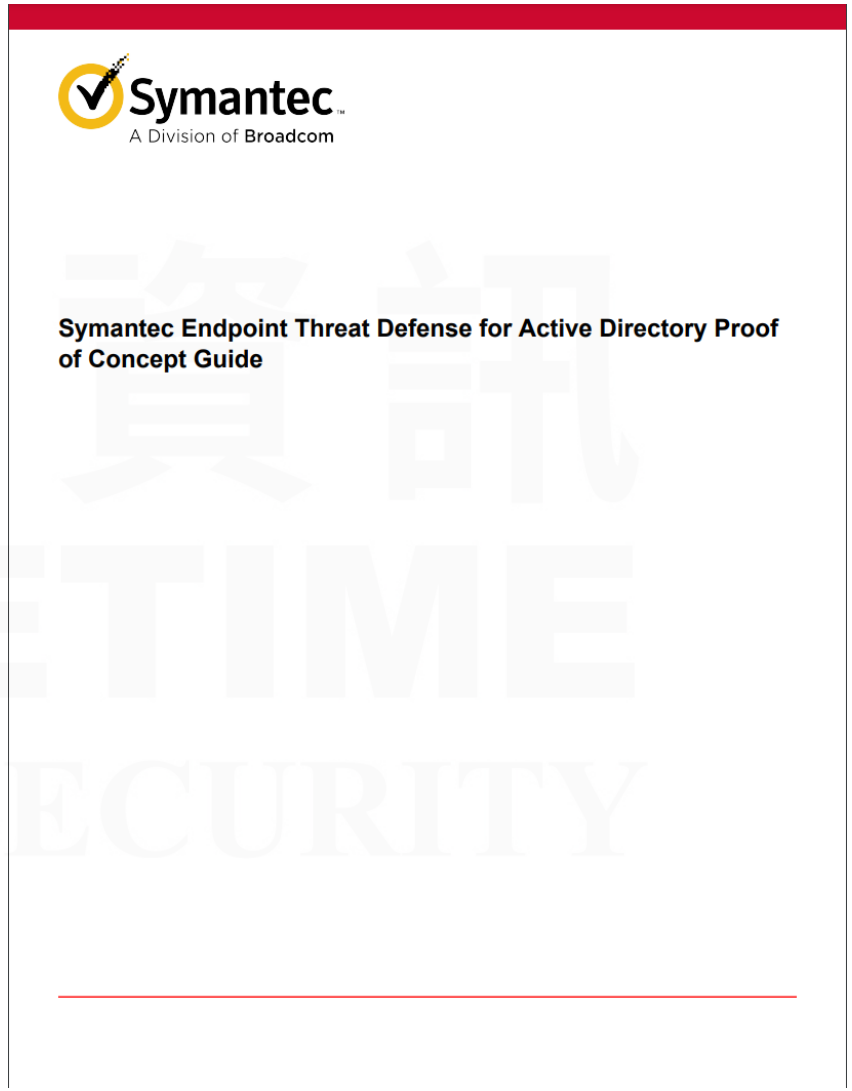
- 適用於執行混合 SESC 部署的客戶
- 未與 SEP 整合
- 在每個端點開機時從 DC 進行身份驗證時使用SMB協定部署政策



BROADCOM SOFTWARE

概念驗證 (POC)

- 可以在 **support.broadcom.com** 找到的 **TDAD POC** 指南
- 在客戶測試環境中部署（獨立模式）
- **確認預需配置 - AD 配置和網路埠**
  - 多網域 = 多個 DM = 所有 DC 都要有需要的通訊埠
  - TDAD 的下一個版本將不需要攝入 AD 網域控制器日誌 ~Q1 2022



BROADCOM SOFTWARE

產品更新

SEP 14.3 RU3 – 9/17

- 加強對就地取材工具的防護。
- 使用用戶升級政策控制用戶自動升級的靈活性。該政策支援位置感知，以便您可以針對子群組做升級。
- 使用機器學習和雲端分析改進對 Linux 威脅的防護。
- Symantec Endpoint Protection Manager支援 Windows 伺服器 2022。
- Windows 用戶端支援 Windows 伺服器 2022 和 Windows 10 嵌入式，並在 Windows 11 和 Windows 11 嵌入式預發佈版本上進行測試。
- Windows 用戶端改進，包括：用於混合管理的新Troubleshooting頁面和 Debug 日誌改進。
- Linux 代理改進包括：更多命令列工具（sav）選項；使用本機儲存庫的安裝包離線安裝 Linux 代理的能力；還有更多。
- 2021 年 10 月推出 Mac 用戶端改進。

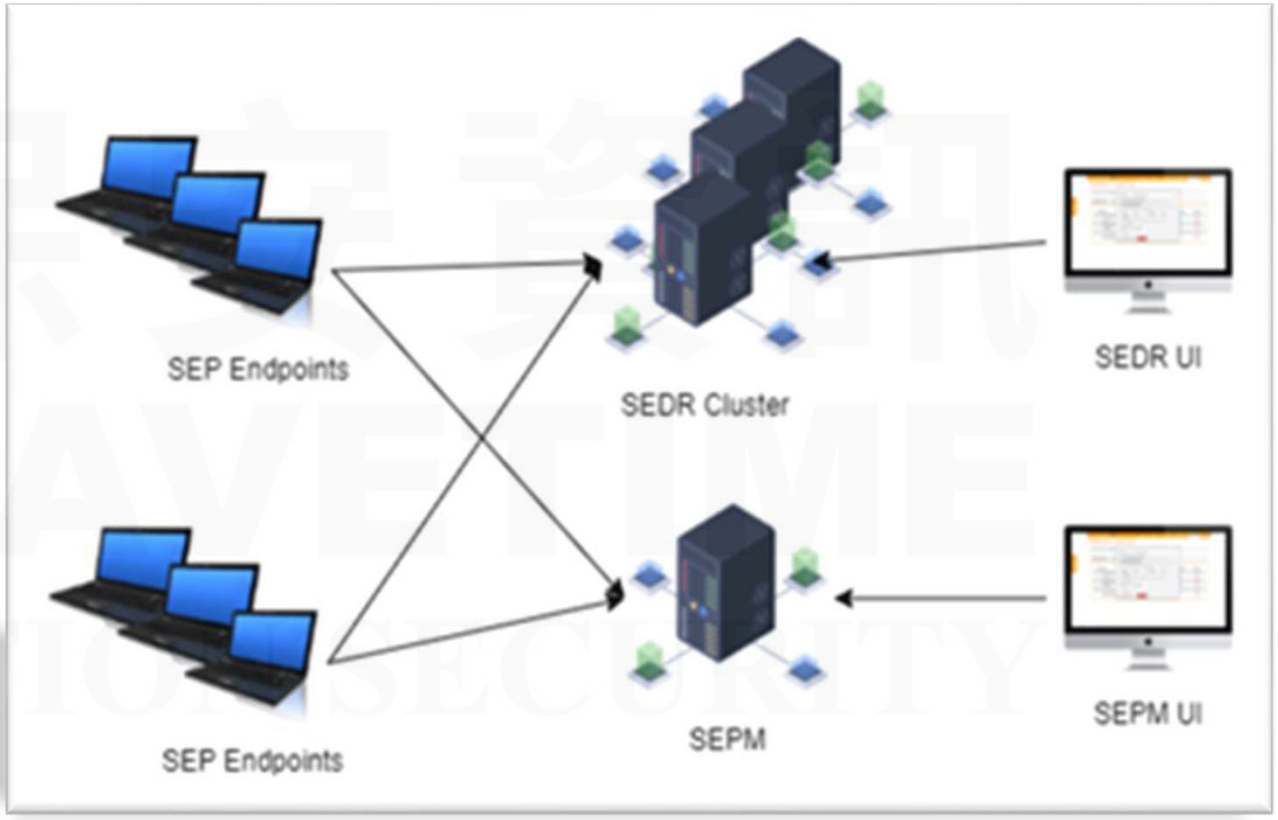
BROADCOM SOFTWARE

EDR 5.0 – Q1 2022

- **地端管理硬體叢集**
  - 效能和可擴充性
  - 高可用性故障轉移
  - 10倍於單一台硬體能力
- **介面與 ICDm 上的 SESC 等同**
  - 程序歷程檢視
  - 增強事件圖形檢視
  - 時間線記錄檢視
- **代理程式與平台支援**

Linux 作業系統上的 SEP 14.3 RU4 額外功能
  - 允許 & 拒絕 PE 與 non-PE 檔案
  - 網路隔離
  - EAR 歷程 & EOC 搜尋
  - 取得檔案 & 嬌正檔案

Mac 作業系統上的SEP 14.3 RU4額外功能
  - 取得檔案
  - 網路隔離
  - 取得檔案



BROADCOM SOFTWARE

TDAD Demo

感謝您

賽門鐵克解決方案專家--保安資訊
https://www.savetime.com.tw

保安資訊 SAVETIME INFORMATION SECURITY

相關參考資訊下載(PDF)--保安資訊整理提供

- 賽門鐵克全球情資(GIN)資訊圖表
- 賽門鐵克端點安全解決方案全覽
- 賽門鐵克郵件安全解決方案全覽
- 賽門鐵克網頁/雲端安全解決方案全覽
- 賽門鐵克端點安全在2020 MITER Engenuity ATT&CK®評比中大放異彩

BROADCOM®

BROADCOM®
SOFTWARE