Symantec
網路安全戰士

讓網路威脅未攻先破 -- 賽門鐵克的 IPS 入侵預防技術

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

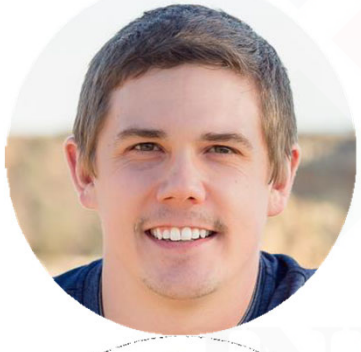
- 保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。
- 自 1995 年起就全心全力專注在賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更熟悉用戶使用情境的優勢，能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。
- 許多顧客樂意與我們建立起長期友誼，把我們當成可信任的資安建議者、可提供良好諮商的資安策略夥伴以及總是第一個被想到的求助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

BROADCOM SOFTWARE

線上研討會講師群介紹

Aryiro Toan，賽門鐵克端點安全產品線(SES)產品管理部負責人

- 2008 加入賽門鐵克
- 專注於所有網路安全相關的事務並樂於解決客戶的所有問題
- 所在地：加州、舊金山



Torrey Umland ，賽門鐵克端點安全產品線(SES)產品負責人，網路引擎

- 2011加入賽門鐵克
- 專注於防護軟體的高效能以及高品質的防護引擎
- 所在地：加州、洛杉磯

Parveen Vashishtha ，賽門鐵克端點安全產品線(SES)，安全回應總監

- 2006 加入賽門鐵克
- 專注於進階威脅的主動防護
- 所在地：印度、浦那

BROADCOM

議程

- 深入了解賽門鐵克入侵預防(IPS)
- 網路威脅分析
- 入侵預防的作用
- 建議

業界唯一涵蓋完整 MITRE ATT&CK 攻擊鏈框架的創新防護技術集

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)	預防惡意或人為破壞或獲得安全軟體正常運行	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

Innovation Across the Entire MITRE ATT&CK Chain

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	使用誘餌和誘餌(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合連秘密攻擊或APT，以提供目動入侵遏止、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

Symantec IPS 入侵預防

產品：

- Endpoint Protection (Windows)
- Endpoint Protection (Mac)
- Browser Intrusion Prevention

端點競爭對手：

- 沒有

主要功效

- 有效阻斷經由網路進行的漏洞利用以及惡意程式擴散

有助於解決以下的問題

- 幾乎能攔阻每一個經由網路散布的惡意攻擊
- 高空攔截 – 惡意檔案或行為在未入侵本機前就已被攔阻
- 主動偵測前所未見的威脅和漏洞利用
- 惡意程式的C&C連線足跡(背景連線通訊-phoning home) 一定會產生網路流量
- 由安全回應中心每日更新

運作原理

- 採用深層封包檢測技術檢查入埠/離埠的雙向網路封包。
- 確認並能拆解剖析L3+以上的網路通訊協協定。
- 使用特徵比對偵測已知及未知的威脅、漏洞利用、C&C網路流量。
- 新版更導入在WSS的核心技術:**WebPulse URL Reputation**，增強並加快惡意網址的防禦功能。

事實勝於雄辯

- Symantec IPS 每週攔截超過兩億次攻擊(200M+)
- Symantec 在網路攻擊及漏洞利用的威脅防禦能力領先業界

BROADCOM

入侵預防(IPS)的功效？繼續……

- **提升保護能力與可視性**
- **有利於避免威脅擴散以及威脅封包在內網流竄**
  - 在任何檔案下載前
  - 在指令或檔案被執行之前
- **回報網路資訊給端點偵測與回應(EDR)**
  - 網路連線與相對應的程序(Process)資訊
  - 檔案下載及傳輸
  - 曾經存取的網頁鏈接(URLs)
  - 網路統計資料
- **由管理主控台瀏覽防護週公告**
  - What did IPS do for you last week?

IPS 如何運作？

IPS 如何運作？

- 辨識內容是準確保護和效能的關鍵
- 資料導引內容辨識
- 支援 200 多種協定和流量類型

BROADCOM

IPS 如何運作？

- 基於內容辨識的情境感知分析
- 掃描整個檔案或協定內容代價是非常高的
- 某些資訊必須暫存以供以後使用
- 解析時，掃描引擎會保留相關的部份並暫存解碼後的資訊

BROADCOM

IPS 如何運作？

- 掃描引擎根據識別的內容選擇最小指紋集作掃描
- 解析時的暫存資訊會在掃描時使用
- 高精度、快速的掃描引擎，誤報率最低

Symantec 入侵預防引擎

2021年最新的成就

- **瀏覽器入侵預防**
  - 在 SEP 14.3 RU2 以後新增 Chrome 擴充功能
    - 將 Symantec IPS 功能加入新式的瀏覽器
    - 為 HTTPS 通訊提供可視性和保護
    - 目前支援 Chrome，未來計畫支援更多瀏覽器
- **效能**
  - 2021 年重大改進 1G 與 10G 網路的輸送量
- **減少增量**
  - 明顯改善每日內容更新的頻寬消耗。
- **新的防勒索功能**
  - Parveen 將在下一節中詳細介紹這些功能

瀏覽器擴充功能的攔截頁面

BROADCOM

Symantec 入侵預防藍圖

- **瀏覽器入侵預防**
  - 將涵蓋到所有主要瀏覽器的擴充功能
    - Edge 擴充功能
    - Safari 擴充功能
    - Firefox 擴充功能
- **效能**
  - 持續量測和優化 10G 網路輸送量
  - 進一步優化在伺服器環境中運行的 IPS

瀏覽器擴充功能的擷截頁面

BROADCOM

賽門鐵克安全機制應變 -- IPS (入侵預防)

在端點啟用賽門鐵克入侵預防系統(IPS)的好處

2024/01/08

IPS 本週做了什麼工作

賽門鐵克的入侵預防系統(IPS)是業界一流的深層封包檢測技術引擎，可保護包括財富500強企業和消費者在內的數億個端點(桌機 / 筆電 / 伺服主機)。

過去的 7 天內，SEP 的網路層保護引擎 (IPS) 在 51 萬 1,900 台受保護端點上總共阻止了 5,430 萬次攻擊。這些攻擊中有 82% 在感染階段前就被有效阻止：

- 在9萬5,300台端點上，阻止了1,650萬次嘗試掃描Web伺服器的漏洞
- 在13萬9,300台端點上，阻止了1,260萬次嘗試利用的Windows作業系統漏洞的攻擊
- 在3萬9,300台Windows伺服主機上，阻止了1,080萬次攻擊
- 在5萬6,700台端點上，阻止了190萬次嘗試掃描伺服器漏洞
- 在1萬2,400台端點上，阻止了79萬8,400次嘗試掃描在CMS漏洞
- 在3萬8,600台端點上，阻止了120萬次嘗試利用的應用程式漏洞
- 在19萬6,000台端點上，阻止了410萬次試圖將用戶重定向到攻擊者控制的網站攻擊
- 在5,800台端點上，阻止了160萬次加密貨幣挖礦攻擊
- 在10萬300台端點上，阻止了810萬台次向惡意軟體C&C連線的嘗試
- 在682台端點上，阻止了27萬4,100次加密勒索嘗試

強烈建議用戶在桌機 / 筆電 / 伺服主機上啟用IPS(不要只把SEP/SES當一般的掃毒工具用，它有多個超強的主被動安全引擎，在安全配置正確下，駭客會知難而退)，以獲得最佳保護。點擊此處獲取有關啟用IPS的說明，或與保安資訊聯繫可獲得最快最有效的協助。

BROADCOM

賽門鐵克入侵預防系統(IPS)-當月份保護伺服器數據

2024/01/02

IPS 本月份貢獻了那些安全保護

賽門鐵克的入侵預防系統(IPS)是業界一流的深層封包檢測技術引擎，可保護包括財富500強企業和消費者在內的數億個端點(桌機 / 筆電 / 伺服主機)。

在過去30天內，SEP的網路層保護引擎(IPS)總共阻止了6萬400台受保護伺服器上的489萬次攻擊。這些攻擊中有92.8%在感染階段前就被有效阻止：

- 在4萬400台伺服器上，阻止了2,170萬次嘗試掃描Web伺服器的漏洞
- 在2萬8,800台伺服器上，阻止了910萬次嘗試利用的Windows作業系統漏洞的攻擊
- 在3萬2,700台伺服主機上，阻止了310萬次嘗試掃描伺服器漏洞
- 在1萬1,500台伺服主機上，阻止了110萬次嘗試掃描在CMS漏洞
- 在2萬1,600台伺服主機上，阻止了130萬次嘗試利用的應用程式漏洞
- 在3,300台伺服主機上，阻止了15萬100次試圖將用戶重定向到攻擊者控制的網站的攻擊
- 在1萬3,100台伺服主機上，阻止了160萬次加密貨幣挖礦攻擊
- 在1萬3,000台伺服主機上，阻止了210萬次向惡意軟體C&C連線的嘗試
- 在34台伺服主機上，阻止了2萬7,300次加密勒索嘗試

強烈建議用戶在桌機 / 筆電 / 伺服主機上啟用IPS(不要只把SEP/SES當一般的掃毒工具用，它有多個超強的主被動安全引擎，在安全配置正確下，駭客會知難而退)，以獲得最佳保護。點擊此處獲取有關啟用IPS的說明，伺服主機上啟動IPS如有效能優化的需求可與保安資訊聯繫可獲得最快最有效的協助。

BROADCOM

賽門鐵克入侵防禦引擎 -- 傑出的特點

- **通訊協定和檔案類型感知**
  - 能感知約270種通訊協定和檔案類型或事件
- **應用程式感知 - 檔案和執行緒中繼資料**
  - IPS 引擎可以存取負責生成網路流量的檔案或執行緒中繼資料
    - 檔案的名稱和路徑
    - 檔案的數位內容狀態
    - 檔案的主要、次要版本
    - 檔案大小
- **檔案信譽**
- **執行緒歷程訊息**
- **網域的信譽**
- **感染惡意軟體時的威脅修復功能**

BROADCOM

保護內容的類型

- **IPS 引擎支持 3 種類型的動作**
  - 阻止
  - 稽核
  - 自行定義
- **封鎖內容**
  - 當引擎遇到惡意流量時重置連線(中斷)
- **審核內容**
  - 不阻擋任何東西
  - 有助於終端使用者提高對網路中潛在有害流量／活動的認知
- **可自行定義的 IPS 規則**
  - 客戶能夠建立自己的 IPS 封包過濾規則
  - 自定義的 IPS 規則優先權高於內建的賽門鐵克IPS規則
- **注意：視管理需求，管理員可以從 SEPM 控制台更改 IPS 的行為，例如**
  - 允　許 → (變更為)阻止
  - 不記錄 → (變更為)記錄

感染前即有涵蓋的防護

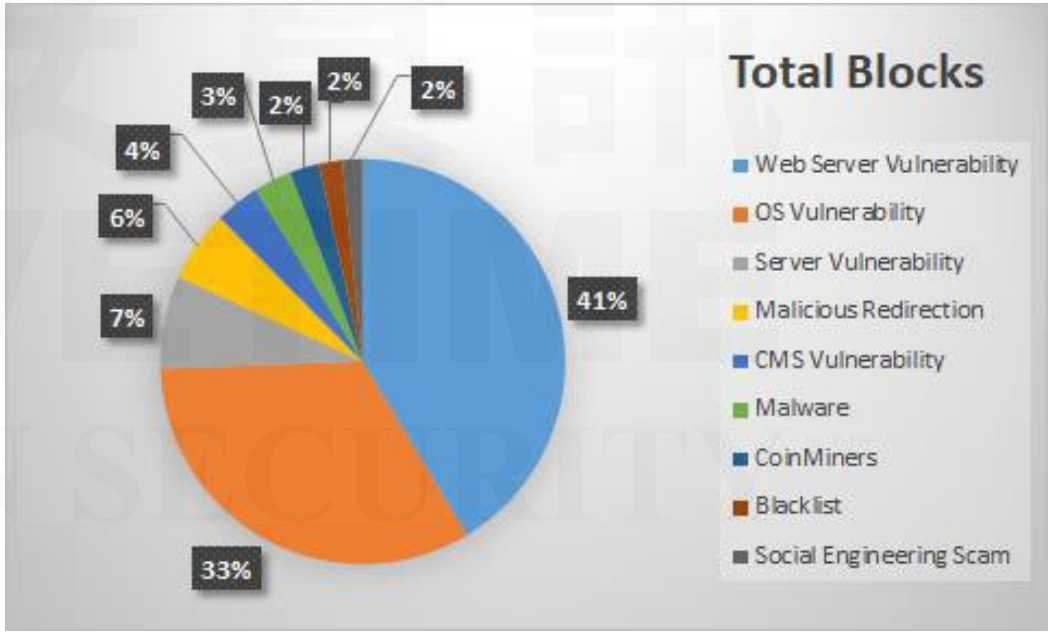
- **IPS 引擎在感染前的防護階段功力不凡**
  - **漏洞**
    - 伺服主機層級
      - Microsoft Exchange Server CVE-2021-26855, Oracle Weblogic Server RCE CVE-2020-14882, Laravel Framework CVE-2017-16894, Adobe Flex BlazeDS RCE CVE-2017-3066
    - 用戶端作業系統層級
      - Microsoft SMB MS17-010 Disclosure Attempt, Microsoft Windows Remote Desktop Services RCE CVE-2019-0708, MSRPC Server Service RPC CVE-2008-4250, Microsoft Windows SMB Remote Code Execution CVE-2017-0143, Microsoft Server Message Block RCE CVE-2020- 0796
    - 應用程式層級
      - Microsoft MSHTML RCE CVE-2021-40444 , Telerik UI Arbitrary File Upload CVE-2017-11317, Malicious RTF File CVE-2017-0199, Microsoft Office CVE-2018-0802
  - **利用網路傳播的威脅**
    - 漏洞利用工具組
    - 加密劫持
    - 表單劫持
    - 惡意重導向的網頁
    - 社交工程詐騙

萬一不幸感染後的防護保障機制

- **防護可涵蓋被入侵後阻止惡意軟體流量或下載**
  - 阻止惡意軟體向惡意主機回報
  - 阻止惡意軟體橫向擴散
- **勒索軟體產生的流量也會被再次檢測和阻止**
  - 網路加密流量
  - 勒索軟體向惡意主機回報
- **豐富多元的各種網路偵測規則可用於檢測勒索軟體感染前的常用工具**
- **各種紅隊工具的阻止和稽核檢測**
- **Webshell 活動的常見內容**

根據數字顯示

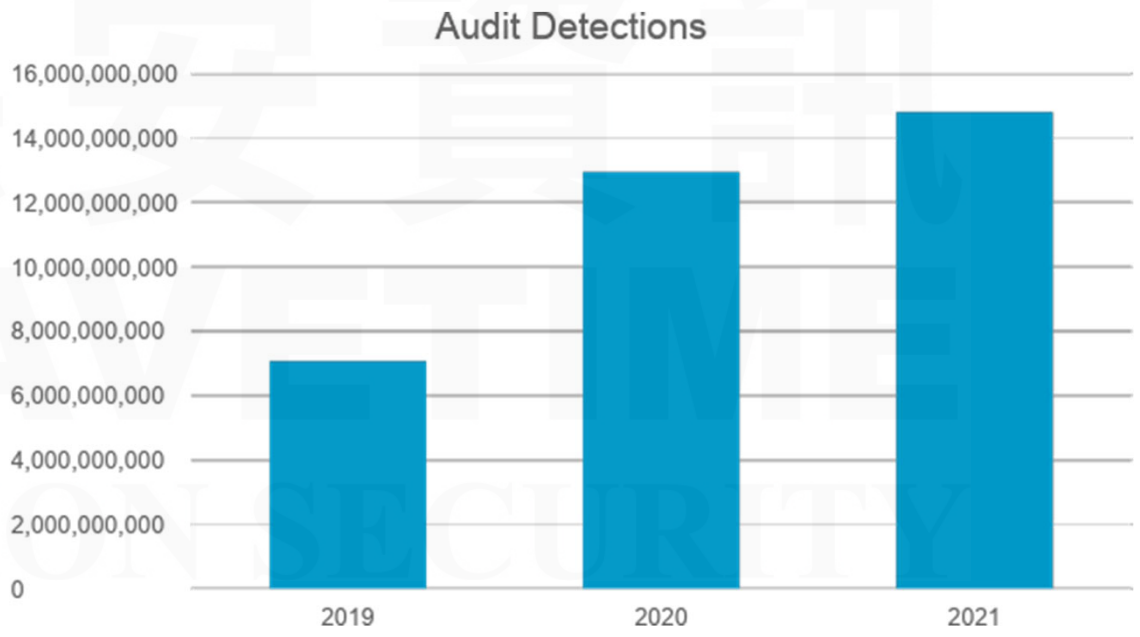
- **賽門鐵克2021 年的 IPS 阻擋保護的統計資料 <截至2021年 9月底>**
  - 成功阻擋 1,220 萬台非重複機器的 77 億次攻擊
  - 其中 94% 的攻擊在尚未被感染階段即被阻擋
  - 統計指標：共 55.5 萬台機器，每天有 2,800 萬個威脅
  - 對非重複的 46 萬台伺服器有超過 10 億次攻擊
  - 統計指標：對 1700 萬台非重複機器的稽核內容檢測到 148 億次攻擊



BROADCOM

Audit Detection Value for Ransomware Protection

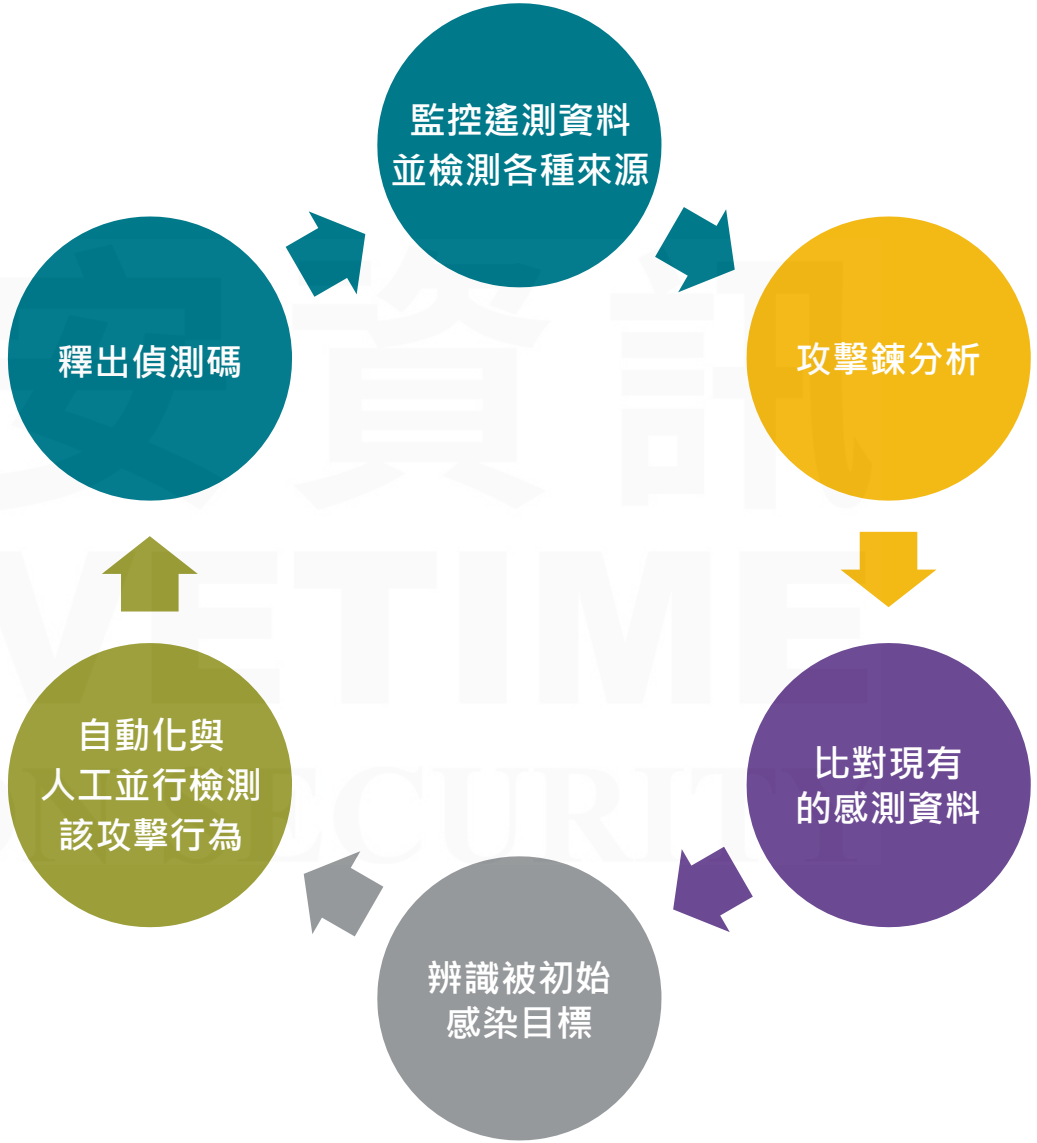
- 檢測到入侵者使用的工具統計有
  - Cobaltstrike
  - Psexec / Paexec
  - ADfind
  - Radmin, Teamviewer, Anydesk, Atera, Screenconnect
  - Powershell
  - Certutil
  - Rubeus
  - SystemBC
  - Weirdloop
  - XenArmour
  - Rclone
  - Softperfect Network Scanner



BROADCOM

威脅來源與獵捕

- **賽門鐵克反應團隊監控多個來源並據以搜尋新的威脅**
  - 應用內部多樣化的引擎／技術來遙測真實網路世界
  - 還有各種威脅態勢監測系統



BROADCOM

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®
connecting everything®